AVG Internet Security 2012

Manual del usuario

Revisión del documento 2012.20 (3/29/2012)

Contenido

1. Introducción

Este manual del usuario proporciona documentación exhaustiva para **AVG Internet Security 2012**.

AVG Internet Security 2012 proporciona varios niveles de protección para todo lo que realiza en línea, lo que supone que no tiene que preocuparse por el robo de identidad, los virus o la visita a sitios dañinos. La Tecnología de nube protectora de AVG y la Red de protección de la comunidad de AVG están incluidas, lo que significa que recopilamos la información sobre amenazas más actual y la compartimos con nuestra comunidad para garantizar que sus miembros reciben la mejor protección:

- Realice compras y operaciones bancarias en línea de forma segura con Firewall, Anti-Spam e Identity Protection de AVG
- Manténgase seguro en las redes sociales con la función Protección de redes sociales de AVG
- Navegue y realice búsquedas con seguridad con la protección en tiempo real de LinkScanner

2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG Internet Security 2012 tiene como propósito proteger las estaciones de trabajo con los siguientes sistemas operativos:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 y x64, todas las ediciones)
- Windows 7 (x 86 y x64, todas las ediciones)

(y posiblemente Service Packs superiores para determinados sistemas operativos)

***Nota**: el componente Identity Protection no es compatible con Windows XP x64. En este sistema operativo, puede instalar AVG Internet Security 2012, pero sólo sin el componente IDP.*

2.2. Requisitos mínimos y recomendados de hardware

Requisitos mínimos de hardware para **AVG Internet Security 2012**:

- Equipo Intel Pentium de 1,5 GHz
- 512 MB de memoria RAM
- 1000 MB de espacio libre en el disco duro (para la instalación)

Requisitos recomendados de hardware para **AVG Internet Security 2012**:

- Equipo Intel Pentium de 1,8 GHz
- 512 MB de memoria RAM
- 1550 MB de espacio libre en el disco duro (para la instalación)

3. Proceso de instalación de AVG

¿Dónde consigo el archivo de instalación?

Para instalar **AVG Internet Security 2012** en su equipo debe obtener el archivo de instalación más reciente. Para asegurarse de que instala la versión actualizada de **AVG Internet Security 2012**, se recomienda descargar el archivo de instalación del sitio Web de AVG (http://www.avg.com/). La sección ***Centro de soporte / Descarga*** proporciona una descripción general estructurada de los archivos de instalación para cada edición de AVG.

Si no está seguro de qué archivos debe descargar e instalar, es recomendable que utilice el servicio ***Seleccione el producto*** en la parte inferior de la página Web. Después de responder a tres preguntas sencillas, este servicio definirá los archivos exactos que necesita. Presione el botón ***Continuar*** para obtener acceso a una lista completa de archivos de descarga que se ajustan a sus necesidades personales.

¿Cómo es el proceso de instalación?

Una vez que ha descargado y guardado el archivo de instalación en el disco duro, puede iniciar el proceso de instalación. La instalación es una secuencia de cuadros de diálogo sencillos y fáciles de entender. Cada cuadro de diálogo describe brevemente qué se debe hacer en cada paso del proceso de instalación. A continuación le ofrecemos una explicación detallada de cada ventana de diálogo:

3.1. Bienvenido: Selección de idioma

El proceso de instalación se inicia con el cuadro de diálogo ***Bienvenido al instalador de AVG***:

En este cuadro de diálogo puede seleccionar el idioma que se utilizará para el proceso de instalación. En la esquina derecha del cuadro de diálogo, haga clic en el cuadro combinado para

desplegar el menú de idioma. Seleccione el idioma que desee y el proceso de instalación seguirá en el idioma elegido.

Atención: en este momento sólo selecciona el idioma del proceso de instalación. La aplicación AVG Internet Security 2012 se instalará en el idioma seleccionado, y en inglés, que siempre se instala automáticamente. No obstante, es posible instalar más idiomas y trabajar con AVG Internet Security 2012 en cualquiera de ellos. Se le solicitará que confirme su selección completa de idiomas alternativos en uno de los siguientes cuadros de diálogo de configuración denominados Opciones personalizadas.

3.2. Bienvenido: Contrato de licencia

En el próximo paso, el cuadro de diálogo ***Bienvenido al instalador de AVG*** proporciona el texto completo del contrato de licencia de AVG:

Lea atentamente el texto completo. Para confirmar que lo leyó, lo entendió y acepta el contrato, presione el botón ***Aceptar***. Si no está conforme con el contrato de licencia, presione el botón ***No acepto*** y el proceso de instalación se terminará de inmediato.

Política de privacidad de AVG

Además del contrato de licencia, este cuadro de diálogo de configuración también le ofrece la opción de obtener más información sobre la política de privacidad de AVG. En la esquina inferior izquierda del cuadro de diálogo puede ver el vínculo ***Política de privacidad de AVG***. Haga clic en él para obtener acceso al sitio Web de AVG (http://www.avg.com/), donde encontrará los principios de la política de privacidad de AVG Technologies en su totalidad.

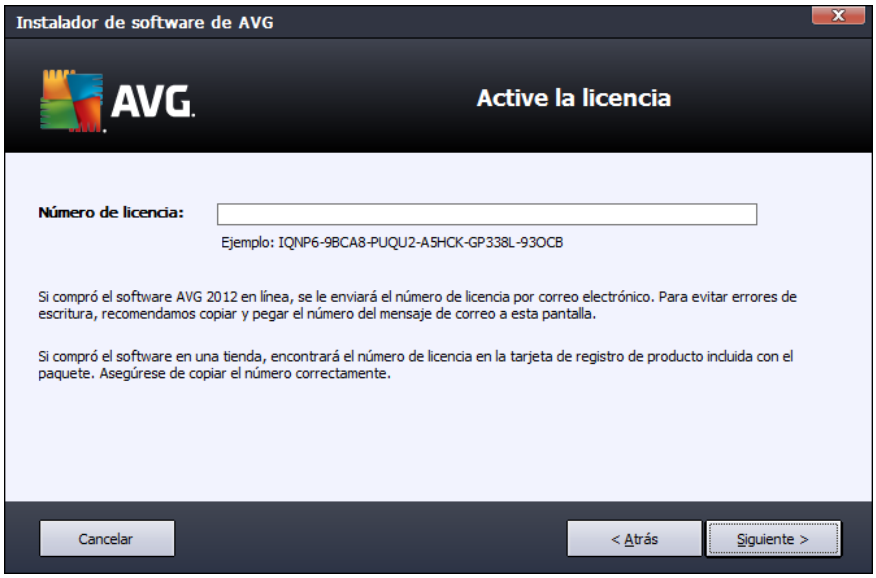
Botones de control

En el primer cuadro de diálogo de configuración, sólo hay dos botones de control disponibles:

- ***Versión impresa***: haga clic para imprimir el texto completo del contrato de licencia de AVG.
- ***No aceptar***: haga clic para rechazar el contrato de licencia. El proceso de configuración se cancelará inmediatamente. **AVG Internet Security 2012** no se instalará.
- ***Atrás***: haga clic para volver al cuadro de diálogo de configuración anterior.
- ***Aceptar***: haga clic para confirmar que ha leído, comprendido y aceptado el contrato de licencia. La instalación continuará y avanzará un paso, al cuadro de diálogo de configuración siguiente.

3.3. Activar la licencia

En el cuadro de diálogo ***Activar la licencia*** se le invita a introducir su número de licencia en el campo de texto incluido:



Dónde encontrar el número de licencia

El número de venta se puede encontrar en el paquete del CD en la caja de **AVG Internet Security 2012**. El número de licencia se encuentra en el correo electrónico de confirmación que recibió después de la compra en línea de **AVG Internet Security 2012**. Debe escribir el número exactamente como se muestra. Si está disponible el número de licencia en formato digital (*en el correo electrónico*), se recomienda utilizar el método de copiar y pegar para insertarlo.

Cómo utilizar el método de copiar y pegar

Si utiliza el método de ***copiar y pegar*** para especificar su número de licencia de **AVG Internet Security 2012** en el programa, se asegurará de que el número se introduce correctamente. Por favor siga estos pasos:

- Abra el correo electrónico que contiene su número de licencia.
- Haga clic con el botón primario del mouse al principio del número de licencia, manténgalo presionado, arrastre el mouse hasta el final del número y, entonces, suelte el botón. El número deberá quedar resaltado.
- Presione la tecla ***Ctrl*** y, mientras la mantiene presionada, presione la tecla ***C***. De este modo se copia el número.
- Haga clic en la posición en la que desee pegar el número copiado.
- Presione la tecla ***Ctrl*** y, mientras la mantiene presionada, presione la tecla ***V***. De este modo se pega el número en la ubicación seleccionada.

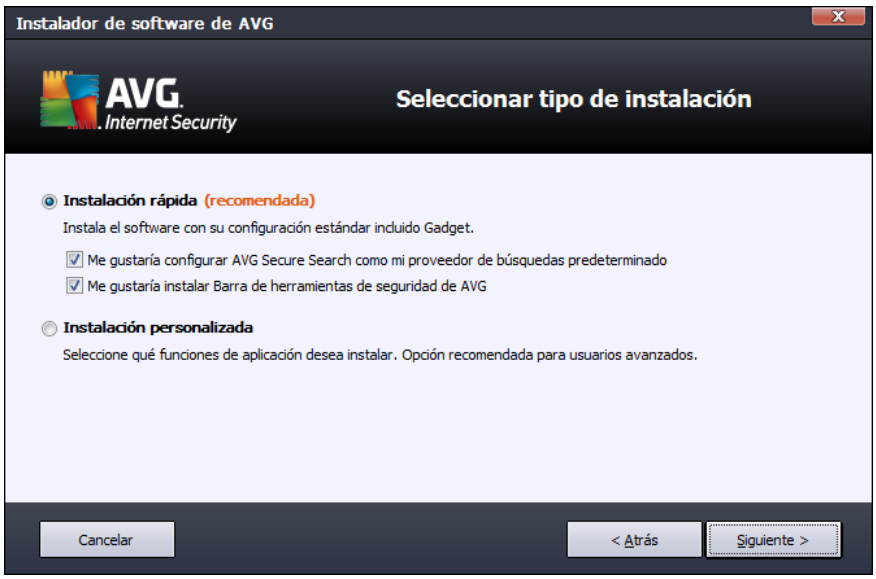
Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- ***Cancelar***: haga clic para salir del proceso de configuración inmediatamente; **AVG Internet Security 2012** no se instalará.
- ***Atrás***: haga clic para volver al cuadro de diálogo de configuración anterior.
- ***Siguiente***: haga clic para seguir con la instalación y avanzar un paso.

3.4. Seleccionar el tipo de instalación

El cuadro de diálogo ***Seleccionar el tipo de instalación*** ofrece la posibilidad de elegir entre dos opciones de instalación: instalación ***rápida*** e instalación ***personalizada***:



Instalación rápida

Para la mayoría de los usuarios, se recomienda mantener la ***instalación rápida*** estándar, que instala **AVG Internet Security 2012** en modo totalmente automático con la configuración predefinida por el proveedor del programa, inclusive el gadget de AVG. 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 Internet Security 2012**.

En esta opción, las dos casillas de verificación aparecen confirmadas, y se recomienda mantener ambas opciones marcadas:

- ***Me gustaría configurar AVG Secure Search como mi proveedor de búsquedas predeterminado***: mantener marcada para confirmar que desea utilizar el motor de búsqueda AVG Secure Search, que colabora estrechamente con el componente LinkScanner para su máxima seguridad en línea.
- ***Me gustaría instalar AVG Security Toolbar***: mantener marcada para instalar AVG Security Toolbar, que le ofrece seguridad máxima mientras navega por Internet.

Presione el botón ***Siguiente*** para continuar con el siguiente cuadro de diálogo, Instalar AVG Security Toolbar.

Instalación personalizada

La opción ***Instalación personalizada*** sólo debe ser utilizada por usuarios con experiencia que tengan un motivo importante para instalar **AVG Internet Security 2012** con una configuración distinta de la estándar (por ejemplo, para ajustarse a necesidades específicas del sistema).

Si elige esta opción, una sección nueva llamada ***Carpeta de destino*** aparece en el cuadro de diálogo. Ahora especifique la ubicación donde **AVG Internet Security 2012** debe instalarse. De forma predeterminada, **AVG Internet Security 2012** se instalará en la carpeta de archivos de programa ubicada en el disco C:, como se estableció en el campo de texto del cuadro de diálogo. Si desea cambiar esta ubicación, utilice el botón ***Examinar*** para ver la estructura de la unidad y seleccione la carpeta correspondiente. Para volver al destino predeterminado predefinido por el proveedor del software, utilice el botón ***Predeterminado***.

Luego, presione el botón ***Siguiente*** para pasar al cuadro de diálogo Opciones personalizadas.

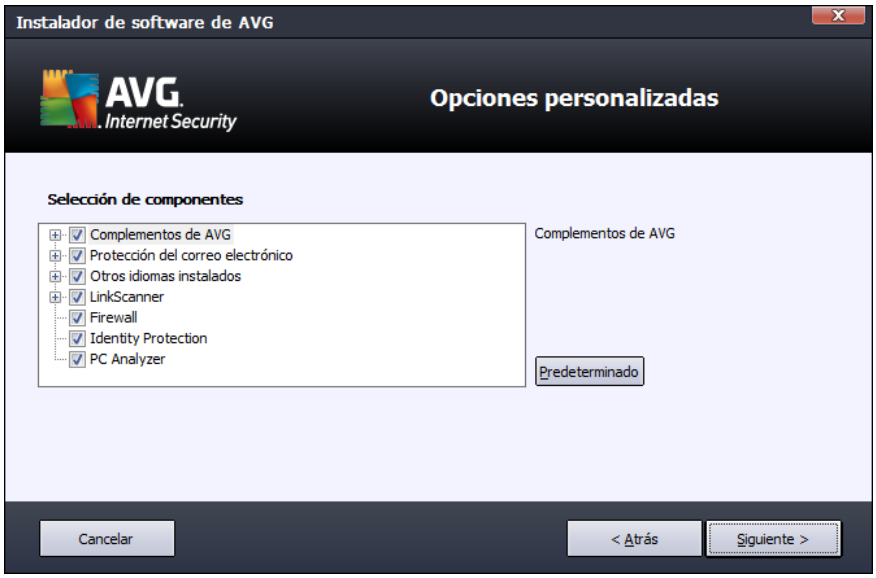
Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- ***Cancelar***: haga clic para salir del proceso de configuración inmediatamente; **AVG Internet Security 2012** no se instalará.
- ***Atrás***: haga clic para volver al cuadro de diálogo de configuración anterior.
- ***Siguiente***: haga clic para seguir con la instalación y avanzar un paso.

3.5. Opciones personalizadas

El cuadro de diálogo ***Opciones personalizadas*** le permite configurar parámetros detallados de la instalación:



La sección ***Selección de componentes*** proporciona una descripción general de todos los componentes de **AVG Internet Security 2012** que se pueden instalar. Si la configuración predeterminada no se adapta a sus necesidades, puede quitar o agregar componentes específicos.

Sin embargo, sólo puede seleccionar de entre los componentes incluidos en la edición del AVG que compró.

Resalte cualquier elemento de la lista ***Selección de componentes*** y aparecerá una breve descripción del componente correspondiente en la parte derecha de esta sección. Para obtener información detallada sobre las funciones de cada componente, consulte el capítulo Descripción general de los componentes de esta documentación. Para volver a la configuración predeterminada predefinida por el proveedor del software, utilice el botón ***Predeterminado***.

Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- ***Cancelar***: haga clic para salir del proceso de configuración inmediatamente; **AVG Internet Security 2012** no se instalará.
- ***Atrás***: haga clic para volver al cuadro de diálogo de configuración anterior.
- ***Siguiente***: haga clic para seguir con la instalación y avanzar un paso.

3.6. Instalar AVG Security Toolbar

En el cuadro de diálogo ***Instalar AVG Security Toolbar***, decida si desea instalar AVG Security Toolbar. Si no cambia la configuración predeterminada, este componente se instalará automáticamente en su navegador de Internet (*los navegadores compatibles actualmente son Microsoft Internet Explorer 6.0 o superior y Mozilla Firefox 3.0 y superior*) para proporcionarle una protección exhaustiva en línea mientras navega por Internet.

Además, tiene la opción de decidir si desea elegir *AVG Secure Search (powered by Google)* como su proveedor de búsquedas predeterminado. De ser así, mantenga marcada la casilla de verificación correspondiente.

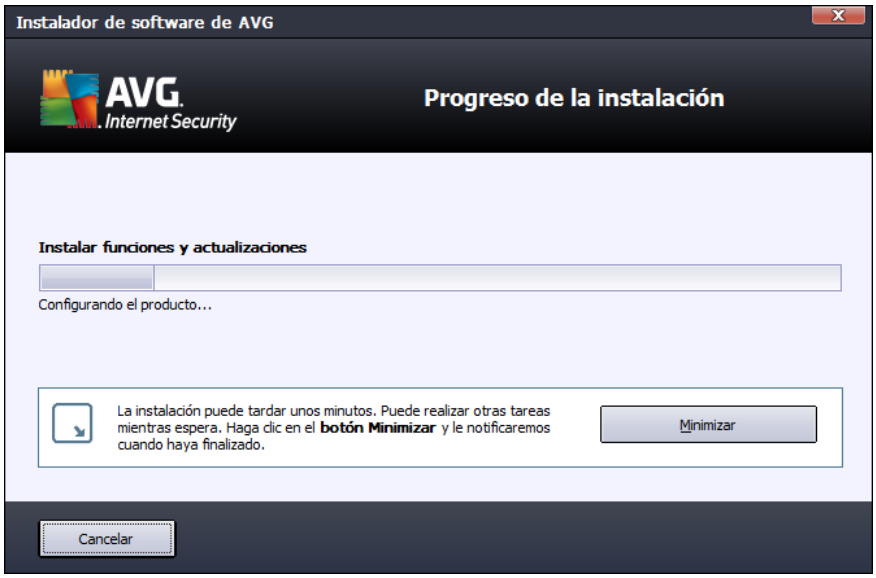
Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- ***Cancelar***: haga clic para salir del proceso de configuración inmediatamente; **AVG Internet Security 2012** no se instalará.
- ***Atrás***: haga clic para volver al cuadro de diálogo de configuración anterior.
- ***Siguiente***: haga clic para seguir con la instalación y avanzar un paso.

3.7. Progreso de la instalación

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



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

Botones de control

En este cuadro de diálogo, sólo hay un botón de control disponible: ***Cancelar***. Este botón sólo se debe utilizar si desea detener el proceso de instalación en ejecución. Tenga en cuenta que, en tal caso, **AVG Internet Security 2012** no se instalará.

3.8. La instalación se ha realizado correctamente

El cuadro de diálogo ***La instalación se realizó correctamente*** confirma que **AVG Internet Security 2012** se ha instalado y configurado por completo:

Programa de mejora de productos

Aquí puede decidir si desea participar en el Programa de mejora de productos (*para obtener información detallada, consulte el capítulo Configuración avanzada de AVG / Programa de mejora de productos*) que recopila información anónima sobre las amenazas detectadas con el fin de aumentar el nivel general de seguridad de Internet. Si está de acuerdo, deje marcada la opción ***Acepto participar en la seguridad en la red de AVG 2012 y programa de mejora de productos...*** *(está confirmada de forma predeterminada)*.

Reinicio del equipo

Para finalizar el proceso de instalación, debe reiniciar el equipo: seleccione si desea ***Reiniciar ahora*** o posponer esta acción: ***Reiniciar más tarde***.

4. Después de la instalación

4.1. Registro del producto

Después de haber finalizado la instalación de **AVG Internet Security 2012**, registre su producto en línea en el sitio Web de AVG (http://www.avg.com/). 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.

La forma más fácil de registrarse es directamente desde la interfaz del usuario de **AVG Internet Security 2012**. En el menú principal, seleccione el elemento Ayuda/Inscribirse ahora. Será redirigido a la página ***Registro*** del sitio Web de AVG (http://www.avg.com/). Siga las instrucciones que se proporcionan en la página.

4.2. Acceso a la interfaz del usuario

Se puede obtener acceso al cuadro de diálogo principal de AVG de varios modos:

- haga doble clic en el icono de la bandeja del sistema AVG
- haga doble clic en el icono AVG del escritorio
- desde el menú ***Inicio / Todos los programas / AVG 2012***

4.3. Análisis de todo el equipo

Existe el riesgo potencial de que un virus informático se transmitiera a su equipo antes de la instalación de **AVG Internet Security 2012**. Por esta razón debe ejecutar un Análisis de todo el equipo para estar seguro de que no hay infecciones en su equipo. El primer análisis puede tardar un tiempo *(alrededor de una hora)* pero es recomendable ejecutarlo para asegurar de que su equipo no se alteró por una amenaza. Para obtener instrucciones sobre la ejecución de un Análisis de todo el equipo consulte el capítulo Análisis de AVG.

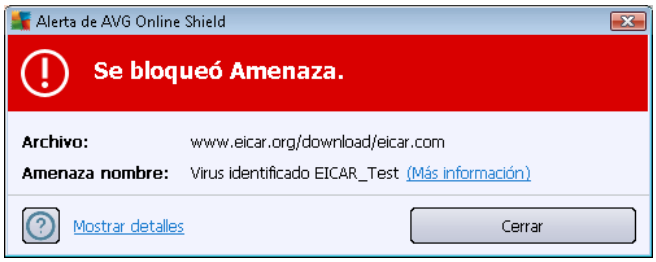
4.4. Análisis Eicar

Para confirmar que **AVG Internet Security 2012** 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 antivirus EICAR]*). Puede descargar el virus EICAR del sitio Web www.eicar.com. Allí también encontrará toda la información necesaria relacionada con el análisis EICAR.

Intente descargar el archivo ***eicar.com*** y guárdelo en el disco local. Inmediatamente después de que confirme que desea descargar el archivo de análisis, Online Shield (*que forma parte del componente Link Scanner*), reaccionará con una advertencia. Esta notificación demuestra que AVG

se ha instalado correctamente en su equipo.



Desde el sitio Web http://www.eicar.com también puede descargar la versión comprimida del "virus" EICAR (*por ejemplo, con el formato eicar_com.zip*). Online Shield permite descargar este archivo y guardarlo en el disco local, pero Protección residente (*que forma parte del componente Anti-Virus*), detectará el "virus" cuando intente descomprimirlo.

Si AVG no identifica el archivo de análisis EICAR como un virus, deberá comprobar nuevamente la configuración del programa.

4.5. Configuración predeterminada de AVG

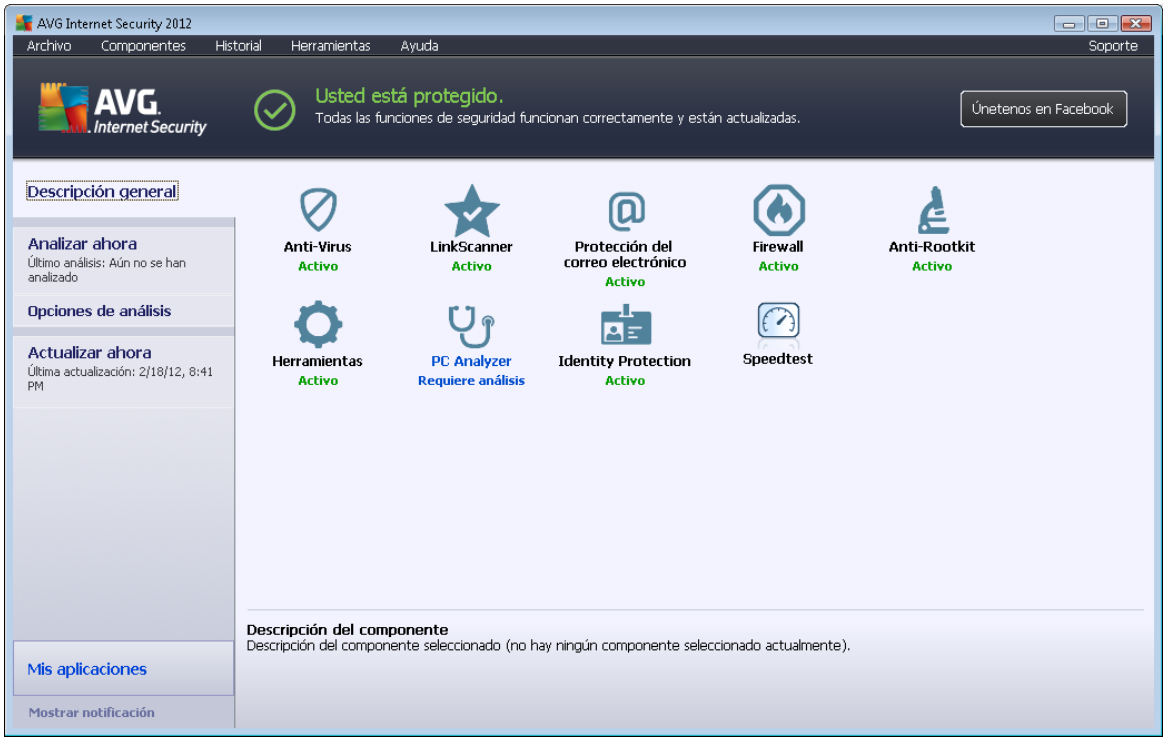
La configuración predeterminada (*es decir, la configuración de la aplicación inmediatamente después de la instalación*) de **AVG Internet Security 2012** está definida por el proveedor de software para que todos los componentes y funciones proporcionen un rendimiento óptimo.

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

Se pueden efectuar pequeñas modificaciones de la configuración de los componentes de AVG directamente desde la interfaz del usuario del componente concreto. Si considera que debe cambiar la configuración de AVG para que se adapte mejor 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 cuadro de diálogo Configuración avanzada de AVG que aparece.

5. Interfaz del usuario de AVG

AVG Internet Security 2012 se abre con la ventana principal:



La ventana principal se divide en varias secciones:

- ***Menú del sistema*** *(línea del sistema superior en la ventana)* es la navegación estándar que le permite tener acceso a todos los componentes, servicios y funciones de **AVG Internet Security 2012** - detalles >>
- ***Información del estado de seguridad*** *(sección superior de la ventana)* le proporciona información acerca del estado actual de **AVG Internet Security 2012** - detalles >>
- ***Estamos en Facebook*** *(sección superior derecha de la ventana)*: este botón le permite unirse a la comunidad de AVG en Facebook. Sin embargo, el botón solo aparece en caso de que todos los componentes funcionen correctamente *(para obtener más detalles sobre cómo reconocer el estado de los componentes AVG consulte el capítulo Información del estado de seguridad)*
- ***Vínculos rápidos*** *(sección izquierda de la ventana)* le permite tener acceso rápido a las tareas más importantes y que se utilizan con mayor frecuencia de **AVG Internet Security 2012** - detalles >>
- ***Mis aplicaciones*** *(sección inferior izquierda de la ventana)* abre una descripción general de las aplicaciones adicionales disponibles para **AVG Internet Security 2012**: LiveKive, Family Safety y PC Tune Up
- ***Descripción general de los componentes*** *(sección central de la ventana)* ofrece una

descripción general de todos los componentes instalados en **AVG Internet Security 2012** - detalles >>

- ***Icono de la bandeja del sistema*** *(esquina inferior derecha del monitor, en la bandeja del sistema)* indica el estado actual de **AVG Internet Security 2012** - detalles >>

- ***Gadget de AVG*** *(barra lateral de Windows, compatible con Windows Vista/7)* permite un acceso rápido al análisis y la actualización de **AVG Internet Security 2012** - detalles >>

5.1. Menú del sistema

El ***menú del sistema*** es el método de navegación estándar que se utiliza en todas las aplicaciones Windows. Está situado horizontalmente en la parte superior de la ventana principal de **AVG Internet Security 2012**. 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:

5.1.1. Archivo

- ***Salir***: cierra la interfaz del usuario de **AVG Internet Security 2012**. Sin embargo, la aplicación de AVG continuará funcionando en segundo plano y su equipo seguirá estando protegido.

5.1.2. 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 del usuario:

- ***Descripción general del sistema***: permite ir al cuadro de diálogo predeterminado de la interfaz del usuario con la descripción general de todos los componentes instalados y su estado

- ***Anti-Virus*** detecta virus, spyware, gusanos, troyanos y archivos ejecutables o bibliotecas no deseados dentro del sistema y le protege de adware malicioso. Detalles >>

- ***LinkScanner*** le protege de ataques basados en Web mientras busca y navega por Internet: detalles >>

- ***Protección del correo electrónico*** comprueba sus mensajes de correo electrónico entrante para detectar SPAM y bloquea virus, ataques de "phishing" (robo de datos personales) u otras amenazas. Detalles >>

- ***Firewall*** controla todas las comunicaciones en cada puerto de la red, protegiéndole contra ataques maliciosos y bloqueando todos los intentos de intrusión. Detalles >>

- ***Anti-Rootkit*** analiza en busca de rootkits peligrosos, ocultos dentro de aplicaciones, controladores y bibliotecas. Detalles >>

- ***Herramientas del sistema*** ofrece un resumen detallado del entorno de AVG e información del sistema operativo. Detalles >>

- ***PC Analyzer*** proporciona información sobre el estado del equipo. Detalles >>

- ***Identity Protection*** protege constantemente sus activos digitales contra amenazas nuevas y desconocidas. Detalles >>

- ***Remote Administration*** sólo se muestra en AVG Business Edition si especificó durante el proceso de instalación que desea tener este componente instalado

5.1.3. Historial

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

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

- Detección mediante Protección del correo electrónico: abre un cuadro de diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente Protección del correo electrónico

- Hallazgos de Online Shield: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por el servicio Online Shield del componente LinkScanner

- 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 del historial de todas las acciones de **AVG Internet Security 2012** registradas

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

5.1.4. Herramientas

- Analizar equipo: realiza 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...***: le permite ejecutar una evaluación a pedido sobre un único archivo específico. Haga clic en esta opción para abrir una nueva ventana con la estructura de árbol de su disco. Seleccione el archivo deseado y confirme la ejecución del análisis.

- Actualizar: ejecuta automáticamente el proceso de actualización de **AVG Internet Security 2012**.

- ***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, como en situaciones en que no existe

una conexión a Internet disponible (*por ejemplo, su equipo se encuentra infectado y está desconectado de Internet, su equipo está conectado a una red sin acceso a Internet, etc.*). En la nueva ventana abierta, seleccione la carpeta donde guardó el archivo de actualización anteriormente y ejecute el proceso de actualización.

- Configuración avanzada...: abre el cuadro de diálogo Configuración avanzada de AVG, en el cual es posible editar la configuración de AVG Internet Security 2012. Generalmente, se recomienda mantener la configuración predeterminada de la aplicación como se encuentra definida por el distribuidor del software.

- Configuración del Firewall...: abre un cuadro de diálogo independiente para la configuración avanzada del componente Firewall.

5.1.5. Ayuda

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

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

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

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

- ***Reactivar***: abre el cuadro de diálogo ***Activar AVG*** con la información introducida en el cuadro de diálogo Personalizar AVG del proceso de instalación. Dentro de este cuadro de diálogo puede introducir el número de licencia para reemplazar el número de venta (*el cual ha instalado con AVG*), o para reemplazar el número de licencia antiguo (*por ejemplo, cuando se actualiza a un nuevo producto AVG*).

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

Nota**: si utiliza la versión de prueba de* **AVG Internet Security 2012**, *los dos últimos elementos aparecen como* ***Comprar ahora *y* ***Activar***, *con lo que puede comprar la versión completa del programa inmediatamente. Para* **AVG Internet Security 2012** *instalado con un número de venta, los elementos aparecen como* ***Registrar*** *y* ***Activar**.*

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

5.1.6. Soporte

El vínculo ***Soporte*** abre un nuevo cuadro de diálogo ***Información*** con todos los tipos de información que podría necesitar cuando intenta encontrar ayuda. El cuadro de diálogo incluye datos básicos sobre el programa AVG instalado (*programa/versión de base de datos*), detalles de la licencia y una lista de vínculos de soporte rápidos.

El cuadro de diálogo ***Información*** está dividido en seis pestañas:

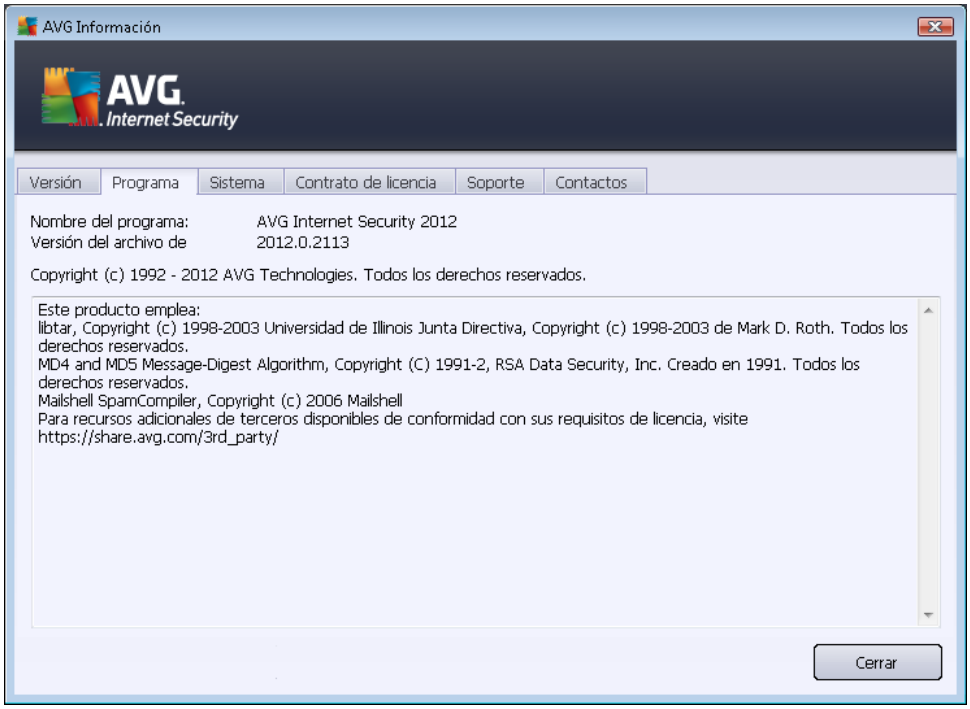
La pestaña ***Versión*** está dividida en tres secciones:

- ***Información de soporte***: proporciona información acerca de la versión de **AVG Internet Security 2012**, la versión de la base de datos de virus, la versión de la base de datos de Anti-Spam y la versión de LinkScanner.

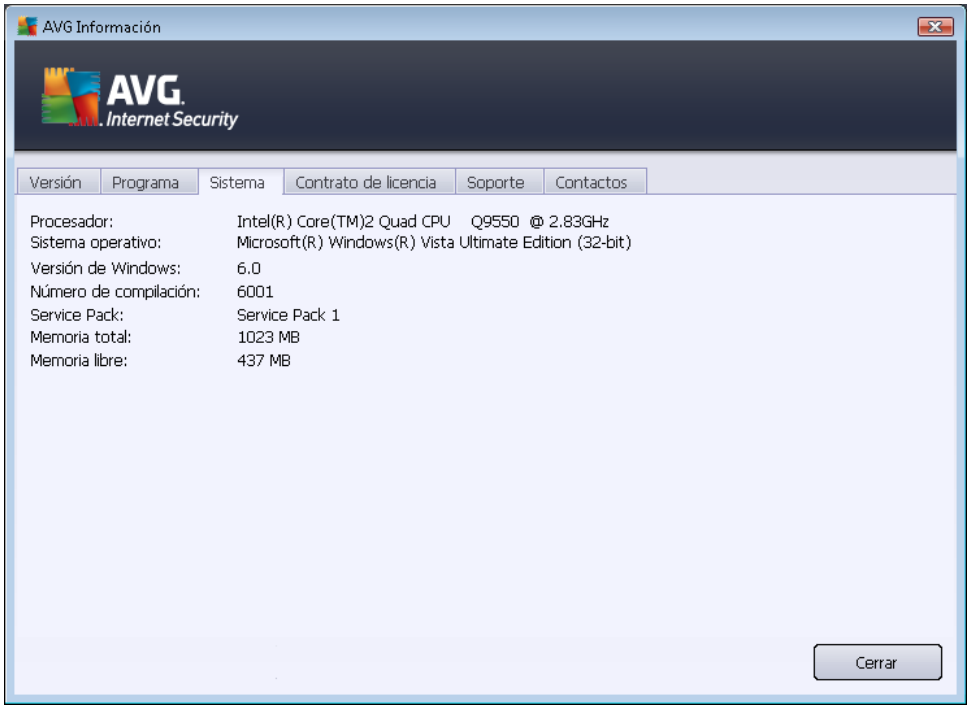
- ***Información del usuario***: proporciona información acerca del usuario y la compañía con licencia.

- ***Detalles de la licencia***: proporciona información sobre su licencia *(nombre del producto, tipo de licencia, número de licencia, fecha de vencimiento y número de puestos*). En esta sección, también puede utilizar el vínculo ***Registrarse*** para registrar su **AVG Internet Security 2012** en línea; de esta manera, podrá utilizar el soporte técnico de AVG completo. Asimismo, utilice el vínculo ***Reactivar*** para abrir el cuadro de diálogo ***Active AVG***: introduzca su número de licencia en el campo respectivo para sustituir su número de venta *(el que utiliza durante la instalación de AVG Internet Security 2012)* o para cambiar su número de licencia actual por otro *(p. ej., al actualizar a una versión superior de AVG).*

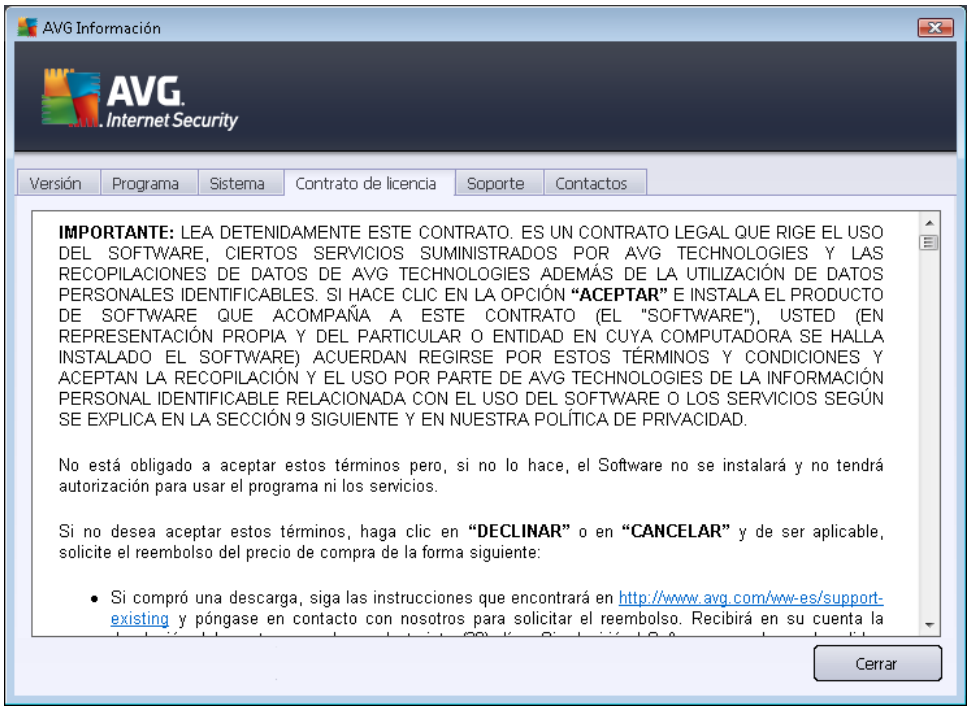
En la pestaña ***Programa*** puede encontrar información acerca de la versión de archivo del programa de **AVG Internet Security 2012** y sobre el código de terceros usado en el producto:



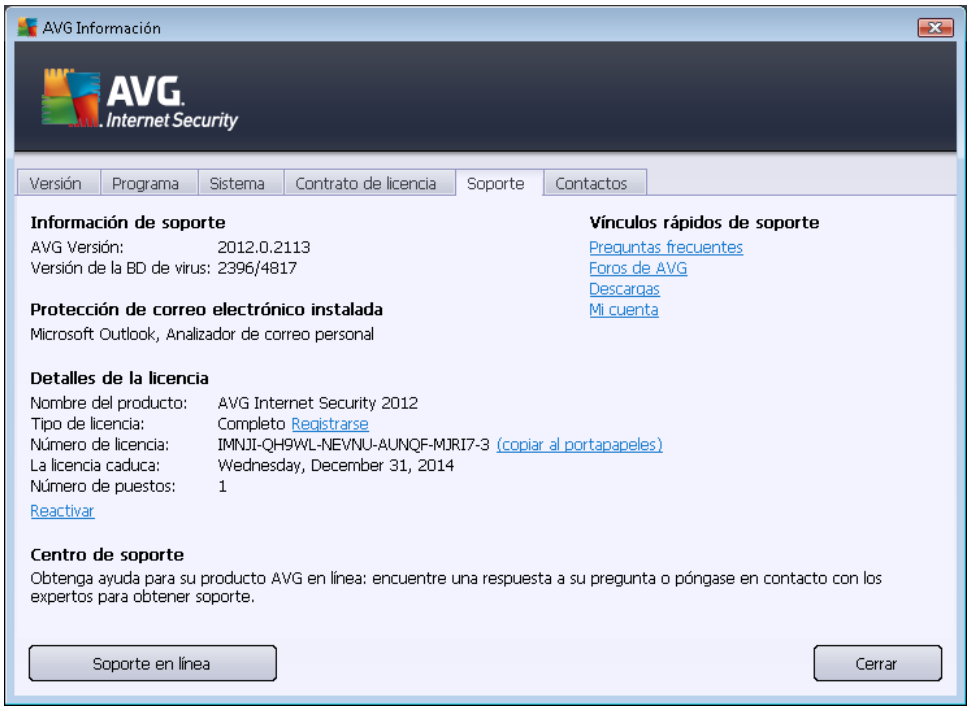
La pestaña ***Sistema*** ofrece una lista de parámetros de su sistema operativo *(tipo de procesador, sistema operativo y su versión, número de compilación, Service Packs utilizados, tamaño de memoria total y tamaño de memoria disponible)*:



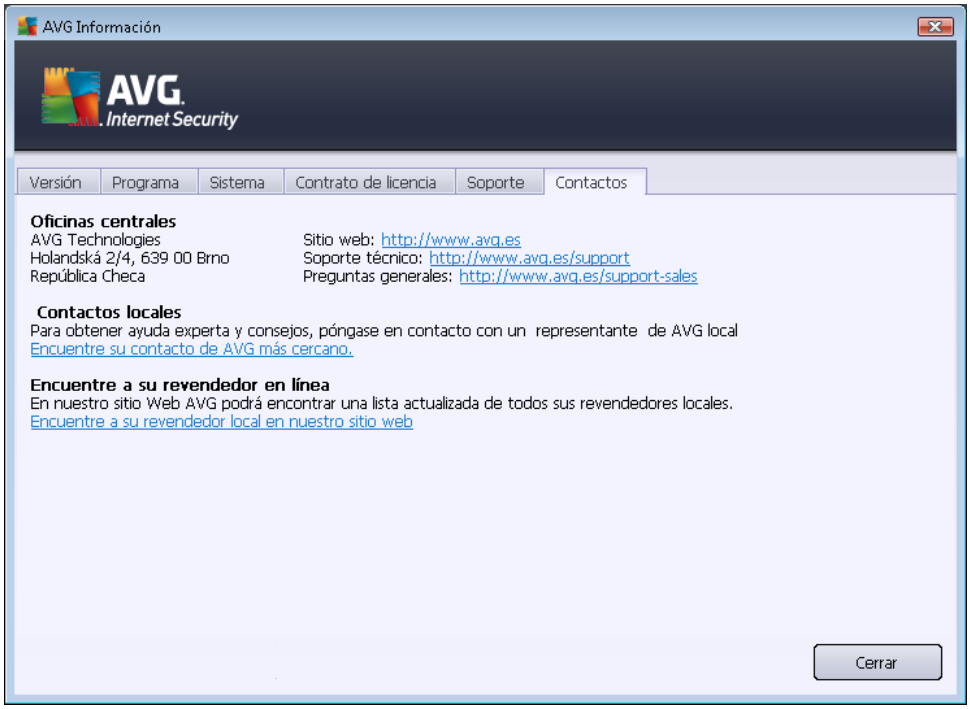
En la pestaña ***Contrato de licencia***, puede leer el texto completo del contrato de licencia entre usted y AVG Technologies:



La pestaña ***Soporte*** incluye una lista de todas las posibilidades de contacto con el servicio de atención al cliente. También proporciona vínculos al sitio Web de AVG (http://www.avg.com/), foros de AVG, preguntas frecuentes, etc. Asimismo, puede encontrar información que podría utilizar mientras se pone en contacto con el equipo de atención al cliente:



La pestaña ***Contactos*** proporciona una lista de todos los contactos de AVG Technologies y también de los contactos de los representantes locales y revendedores de AVG:



5.2. Información del estado de seguridad

La sección ***Información del estado de seguridad*** está situada en la parte superior de la ventana principal de **AVG Internet Security 2012**. En esta sección siempre encontrará información sobre el estado de seguridad actual de su **AVG Internet Security 2012**. Consulte la descripción general de los iconos que posiblemente se muestran en esta sección, y su significado:

 - El icono verde indica que ***AVG Internet Security 2012 está completamente operativo***. Su equipo está totalmente protegido, actualizado y todos los componentes instalados funcionan correctamente.

 - El icono amarillo indica que ***uno o más componentes están configurados de manera incorrecta*** y debería prestar atención a su configuración o a sus propiedades. No hay problemas críticos en **AVG Internet Security 2012** y probablemente ha optado por desactivar algunos componentes por alguna razón. Aún está protegido. Sin embargo, preste atención a la configuración de los componentes con problemas. Podrá ver su nombre en la sección ***Información del estado de seguridad***

El icono amarillo aparece también si, por algún motivo, ha decidido ignorar el estado de error del componente. La opción ***Ignorar el estado del componente*** está disponible en el menú

contextual, *que se abre cuando se hace clic con el botón secundario del mouse* sobre el icono del componente respectivo en la descripción general de los componentes de la ventana principal de **AVG Internet Security 2012**. Seleccione esta opción para expresar que es consciente del estado de error del componente pero que, por alguna razón, desea conservar su **AVG Internet Security 2012** de esta manera y no desea que se le advierta mediante el icono de la bandeja del sistema. Puede ser necesario utilizar esta opción en una situación específica, pero es muy recomendable desactivar la opción ***Ignorar el estado del componente*** a la mayor brevedad posible.

De forma alternativa, el icono amarillo también se mostrará si su **AVG Internet Security 2012** requiere reiniciar el equipo (***es necesario reiniciar***). Preste atención a esta advertencia y reinicie su equipo utilizando el botón ***Reiniciar ahora***.

 - El icono naranja indica que ***AVG Internet Security 2012 se encuentra en estado crítico***. Uno o varios componentes no funcionan correctamente y **AVG Internet Security 2012** 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.

En caso de que AVG Internet Security 2012 no esté configurado para un rendimiento óptimo, aparece un nuevo botón llamado Reparar (de forma alternativa, Reparar todo si el problema concierne a más de un componente) junto a la información de estado de seguridad. Presione el botón para iniciar un proceso automático de confirmación y configuración del programa. Se trata de una forma fácil de configurar AVG Internet Security 2012 para un rendimiento óptimo y alcanzar el máximo nivel de seguridad.

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. De otra manera, su equipo estará en peligro.

Nota: *la información del estado de AVG Internet Security 2012 también se puede obtener en cualquier momento del icono de la bandeja del sistema.*

5.3. Vínculos rápidos

Los ***vínculos rápidos*** están ubicados en el lado izquierdo de la interfaz del usuario de **AVG Internet Security 2012**. Estos vínculos le permiten un acceso inmediato a las funciones más importantes y de uso más común de la aplicación, es decir, análisis y actualizaciones. Los vínculos rápidos están disponibles en todos los cuadros de diálogo de la interfaz del usuario:

Los ***vínculos rápidos*** están divididos gráficamente en tres secciones:

- ***Analizar ahora***: de forma predeterminada, este botón proporciona información sobre el último análisis ejecutado *(p. ej., el tipo de análisis y la fecha de la última ejecución)*. Haga clic en el comando ***Analizar ahora*** para ejecutar de nuevo el mismo análisis. Si desea ejecutar otro análisis, haga clic en el vínculo ***Opciones de análisis***. De esta forma se abre la interfaz de análisis de AVG, donde puede ejecutar análisis, programarlos o editar sus parámetros. *(Para obtener información detallada, consulte el capítulo Análisis de AVG)*

- ***Opciones de análisis*** : utilice este vínculo para cambiar entre cualquier cuadro de diálogo abierto de AVG y la ventana predeterminada con una descripción general de todos los componentes instalados. *(Para obtener información detallada, consulte Descripción general de los componentes)*

- ***Actualizar ahora***: este vínculo proporciona la fecha y la hora de la última actualización ejecutada. Presione este botón para ejecutar el proceso de actualización inmediatamente y seguir su progreso. *(Para obtener información detallada, consulte el capítulo Actualizaciones de AVG)*

Los ***vínculos rápidos*** están disponibles en todo momento en la interfaz del usuario de AVG. Una vez que emplea un vínculo rápido para ejecutar un proceso específico, bien un análisis o una actualización, la aplicación cambia a un nuevo cuadro de diálogo pero los vínculos rápidos aún están disponibles. Además, como el proceso de ejecución se representa gráficamente en el árbol de navegación, tiene un control completo sobre todos los procesos que se ejecutan en ese momento en **AVG Internet Security 2012**.

5.4. Descripción general de los componentes

Secciones de Descripción general de los componentes

La sección ***Descripción general de los componentes*** se encuentra en la parte central de la **interfaz del usuario de** AVG Internet Security 2012. La sección se divide en dos partes:

- ***Descripción general de todos los componentes instalados***, que consta de paneles gráficos correspondientes a todos los componentes instalados. Cada panel está marcado con el icono del componente y proporciona información sobre si el componente respectivo está activo o inactivo en ese momento.

- ***La descripción del componente*** se encuentra en la parte inferior de este cuadro de diálogo. La descripción explica brevemente la funcionalidad básica del componente. Además, proporciona la información sobre el estado actual del componente seleccionado.

Lista de componentes instalados

En **AVG Internet Security 2012,** la sección ***Descripción general de los componentes*** contiene información sobre los siguientes componentes:

- ***Anti-Virus*** detecta virus, spyware, gusanos, troyanos y archivos ejecutables o bibliotecas

no deseados dentro del sistema y le protege de adware malicioso. Detalles >>

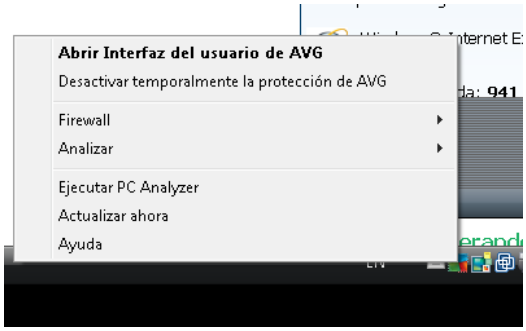
- ***LinkScanner*** le protege de ataques basados en Web mientras busca y navega por Internet: detalles >>
- ***Protección del correo electrónico*** comprueba sus mensajes de correo electrónico entrante para detectar SPAM y bloquea virus, ataques de "phishing" (robo de datos personales) u otras amenazas. Detalles >>
- ***Firewall*** controla todas las comunicaciones en cada puerto de la red, protegiéndole contra ataques maliciosos y bloqueando todos los intentos de intrusión. Detalles >>
- ***Anti-Rootkit*** analiza en busca de rootkits peligrosos, ocultos dentro de aplicaciones, controladores y bibliotecas. Detalles >>
- ***Herramientas del sistema*** ofrece un resumen detallado del entorno de AVG e información del sistema operativo. Detalles >>
- ***PC Analyzer*** es un analizador que proporciona información sobre el estado del equipo. Detalles >>
- ***Identity Protection*** protege constantemente sus activos digitales contra amenazas nuevas y desconocidas. Detalles >>
- ***Remote Administration*** sólo se muestra en AVG Business Edition si especificó durante el proceso de instalación que desea tener este componente instalado

Acciones accesibles

- ***Mueva el mouse sobre 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 del usuario.
- ***Haga un solo clic en el icono de cualquier componente*** para abrir la interfaz propia del componente con una lista de datos estadísticos básicos.
- ***Haga clic con el botón secundario del mouse sobre el icono de un componente*** para expandir un menú contextual con varias opciones:
  - ***Abrir***: haga clic en esta opción para abrir el cuadro de diálogo propio del componente *(igual que con un solo clic en el icono del componente)*.
  - ***Ignorar el estado del componente***: seleccione esta opción para expresar que es consciente del estado de error del componente pero que por alguna razón desea conservar este estado y no desea que se le advierta mediante el icono en la bandeja de sistema.
  - ***Abrir en Configuración avanzada***: esta opción sólo está disponible para algunos componentes, concretamente los que permiten una configuración avanzada.

5.5. Icono en la bandeja de sistema

El ***icono de la bandeja del sistema de AVG*** *(en la barra de tareas de Windows, esquina inferior derecha del monitor)* indica el estado actual de su **AVG Internet Security 2012**. Está visible en todo momento en la bandeja del sistema, tanto si la interfaz del usuario de **AVG Internet Security 2012** está abierta como si no:



Visualización del icono de la bandeja del sistema de AVG

- Si aparece de color completo sin elementos agregados, el icono indica que todos los componentes de **AVG Internet Security 2012** están activos y funcionando totalmente. Sin embargo, el icono puede mostrarse también de esta forma en situaciones en las que uno de los componentes no está funcionando totalmente pero el usuario ha decidido que se ignore el estado del componente. *(Con la confirmación de la opción Ignorar el estado del componente, expresa que es consciente del estado de error del componente pero que, por algún motivo, desea mantenerlo así y no desea que se le advierta de la situación).*

- El icono con un signo de exclamación indica que un componente *(o incluso varios componentes)* se encuentran en estado de error. Preste siempre atención a tales advertencias e intente corregir el problema de configuración de un componente que no está configurado correctamente. Para realizar los cambios en la configuración del componente, haga doble clic en el icono de la bandeja del sistema para abrir la interfaz del usuario de la aplicación. Para obtener información detallada acerca de qué componentes se encuentran en estado de error, consulte la sección Información del estado de seguridad.

- El icono de la bandeja del sistema se puede mostrar también a colores con un haz de luz que parpadea o gira. Esta versión gráfica señaliza un proceso de actualización actualmente ejecutado.

- La visualización alternativa de un icono a colores con una flecha significa que se está ejecutando uno de los análisis de **AVG Internet Security 2012**.

Información del icono de la bandeja del sistema de AVG

El ***icono de la bandeja del sistema de AVG*** informa además de las actividades actuales que tienen lugar en su **AVG Internet Security 2012**, y de los posibles cambios de estado en el

programa (*p. ej., ejecución automática de un análisis o de una actualización programados, Interruptor de perfil del Firewall, cambio de estado de un componente, ocurrencia de estado de error, etc.*) mediante una ventana emergente que se abre desde el icono en la bandeja de sistema de:

Acciones disponibles desde el icono de la bandeja del sistema de AVG

El ***icono de la bandeja del sistema de AVG*** se puede utilizar también como vínculo de acceso rápido a la interfaz del usuario de **AVG Internet Security 2012**, con sólo hacer doble clic en él. Al hacer clic con el botón secundario en el icono se abre un pequeño menú contextual con las opciones siguientes:

- ***Abrir Interfaz del usuario de AVG***: haga clic aquí para abrir la interfaz del usuario de **AVG Internet Security 2012**.
- ***Desactivar temporalmente la protección de AVG***: la opción le permite desactivar la protección completa que usted realizó**AVG Internet Security 2012** anteriormente. Recuerde que no debe usar esta opción si no es absolutamente necesario. En la mayoría de los casos, no es necesario desactivar antes **AVG Internet Security 2012**de instalar nuevo software o controladores, ni siquiera si el instalador o el asistente de software le sugiere que cierre los programas y aplicaciones que se estén ejecutando para asegurarse de que no se producen interrupciones no deseadas durante el proceso de instalación. Si tiene que desactivar temporalmente **AVG Internet Security 2012**, debe volver a activarlo en cuanto termine. Si está conectado a Internet o a una red durante el tiempo que el software antivirus está desactivado, su equipo será vulnerable ante los ataques.
- ***Firewall***: haga clic aquí para abrir el menú contextual de opciones de configuración del Firewall, donde podrá editar los parámetros más importantes: estado del Firewall (*Firewall activado/Firewall desactivado/Modo de emergencia*), cambio al modo de juego y perfiles de Firewall.
- ***Análisis***: haga clic aquí para abrir el menú contextual de análisis predefinidos (*Análisis de todo el equipo* y *Análisis de archivos/carpetas*) y seleccione el análisis que corresponda; se iniciará inmediatamente.
- ***Análisis en ejecución...*** Este elemento se muestra sólo si se está ejecutando un análisis en ese momento en el equipo. Para este análisis puede establecer la prioridad, o detener o pausar el análisis que se está ejecutando. Además, se pueden realizar las siguientes acciones: *Establecer prioridad para todos los análisis, Pausar todos los análisis* o *Detener todos los análisis*.
- ***Ejecutar PC Analyzer***: haga clic aquí para iniciar el componente PC Analyzer.
- ***Actualizar ahora***: inicia inmediatamente una actualización.
- ***Ayuda***: abre el archivo de ayuda de la página de inicio.

5.6. AVG Advisor

AVG Advisor es una función de rendimiento que supervisa todos los procesos en ejecución dentro de su PC para detectar posibles problemas y que, además, ofrece consejos sobre cómo evitarlos. ***AVG Advisor*** está visible en forma de un cuadro de diálogo emergente que se desliza sobre la bandeja del sistema.

AVG Advisor puede aparecer en las siguientes situaciones:

- El navegador de Internet que utiliza se está quedando sin memoria, lo que puede hacer que el equipo funcione más lento *(Los navegadores de Internet que AVG Advisor admite son Internet Explorer, Chrome, Firefox, Opera y Safari);*
- Un proceso en ejecución en su PC está consumiendo una gran cantidad de memoria y hace que el equipo funcione más lento;
- Su equipo está a punto de conectarse automáticamente a una red WiFi desconocida.

En cada una de estas situaciones, ***AVG Advisor*** le advierte de los posibles problemas que se pueden ocasionar y proporciona el nombre y el icono del proceso o de la aplicación en conflicto. Además, ***AVG Advisor*** sugiere los pasos que se deben tomar para evitar los posibles problemas.

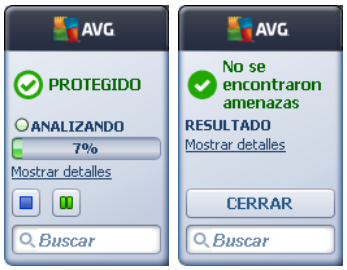
5.7. Gadget de AVG

El gadget de AVG se muestra en el escritorio de Windows (*barra lateral de Windows*). Esta aplicación sólo es compatible con los sistemas operativos Windows Vista y Windows 7. ***El gadget de AVG*** ofrece un acceso inmediato a las funciones más importantes de **AVG Internet Security 2012**, por ejemplo, análisis y actualización:

Acceso rápido a análisis y actualizaciones

Si es necesario, ***el gadget de AVG*** le permite ejecutar un análisis o una actualización de manera inmediata:

- ***Analizar ahora***: haga clic en el vínculo ***Analizar ahora*** para iniciar el análisis de todo el equipo directamente. Puede ver el progreso del proceso de análisis en la interfaz del usuario alternativa del gadget. Una breve descripción general de las estadísticas proporciona información sobre el número de objetos analizados, las amenazas detectadas y las amenazas reparadas. Durante el análisis, siempre puede pausar o detener el proceso de análisis. Para obtener información detallada sobre los resultados del análisis, consulte el cuadro de diálogo estándar Descripción general de los resultados del análisis, que puede abrirse directamente desde el gadget mediante la opción ***Mostrar detalles*** *(los resultados del análisis correspondientes se enumerarán en Análisis de gadgets de la barra lateral)*.



- ***Actualizar ahora***: haga clic en el vínculo ***Actualizar ahora*** para iniciar la actualización de **AVG Internet Security 2012** directamente desde el gadget:

Acceso a las redes sociales

El ***gadget de AVG*** también proporciona un vínculo rápido que le conecta a las principales redes sociales. Utilice el botón respectivo para conectarse a las comunidades de AVG en Twitter, Facebook o LinkedIn:

- ***Vínculo a Twitter***: abre una nueva interfaz del ***gadget de AVG*** en la que se proporciona un resumen de los últimos suministros de AVG publicados en Twitter. Siga el vínculo ***Ver todos los suministros de Twitter de AVG*** para abrir el navegador de Internet en una ventana nueva; irá directamente al sitio Web de Twitter, en concreto a la página

dedicada a las noticias relacionadas con AVG:

- ***Vínculo a Facebook*** : abre el navegador de Internet con el sitio Web de Facebook, específicamente en la página de la ***comunidad de AVG***.

- ***LinkedIn***: esta opción sólo está disponible para la instalación en red (*es decir, cuando ha instalado AVG usando una licencia para alguna de las ediciones Business de AVG*), y abre su navegador de Internet en el sitio Web de ***AVG SMB Community*** dentro de la red social LinkedIn.

Otras funciones con acceso a través del gadget

- ***PC Analyzer*** : abre la interfaz del usuario en el componente PC Analyzer e inmediatamente comienza el análisis.

- ***Cuadro de búsqueda***: escriba una palabra clave y obtenga inmediatamente los resultados de la búsqueda en una nueva ventana que se abre con su navegador Web predeterminado.

6. Componentes de AVG

6.1. Anti-Virus

El componente ***Anti-Virus*** es uno de los elementos principales de su **AVG Internet Security 2012** y en él se combinan varias funciones esenciales de un programa de seguridad:

- Motor de análisis
- Protección residente
- Protección Anti-Spyware

6.1.1. Motor de análisis

El motor de análisis que es la base del componente ***Anti-Virus*** analiza todos los archivos y su actividad *(abrir/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 en la Bóveda de virus.

La función importante de la protección de AVG Internet Security 2012 es que ningún virus conocido se puede ejecutar en el equipo.

Métodos de detección

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 antivirus puede detectar un virus nuevo y desconocido si éste contiene algunas características típicas de los virus ya existentes. ***Anti-Virus*** utiliza los siguientes métodos de detección:

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

Dado que hay casos en que una tecnología por sí sola podría no llegar a detectar o identificar un virus, el ***Anti-Virus*** combina varias tecnologías para garantizar que su equipo esté protegido frente estas amenazas. **AVG Internet Security 2012** puede también analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas en el sistema. Llamamos a estas amenazas programas potencialmente no deseados *(diversos tipos de spyware, adware etc.)*. Además, **AVG Internet Security 2012** 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.

AVG Internet Security 2012 proporciona protección ininterrumpida para su equipo.

6.1.2. Protección residente

AVG Internet Security 2012 le proporciona protección continua en forma de lo que se llama protección residente. El componente ***Anti-Virus*** analiza cada uno de los archivos *(con extensiones específicas o sin extensiones)* que se abre, guarda o copia. Protege las áreas del sistema del equipo y los medios extraíbles (*discos flash, etc.*). Cuando descubre un virus en un archivo al que se está teniendo acceso, detiene la operación que se está realizando y no permite que el virus se active. Normalmente, ni siquiera advertirá el proceso dado que la protección residente se ejecuta "en segundo plano". Sólo recibirá notificaciones cuando se encuentren amenazas; al mismo tiempo, el ***Anti-Virus*** bloquea la activación de la amenaza y la elimina.

La protección residente se carga en la memoria de su equipo durante el inicio del sistema, y es vital que la mantenga activada todo el tiempo.

6.1.3. Protección Anti-Spyware

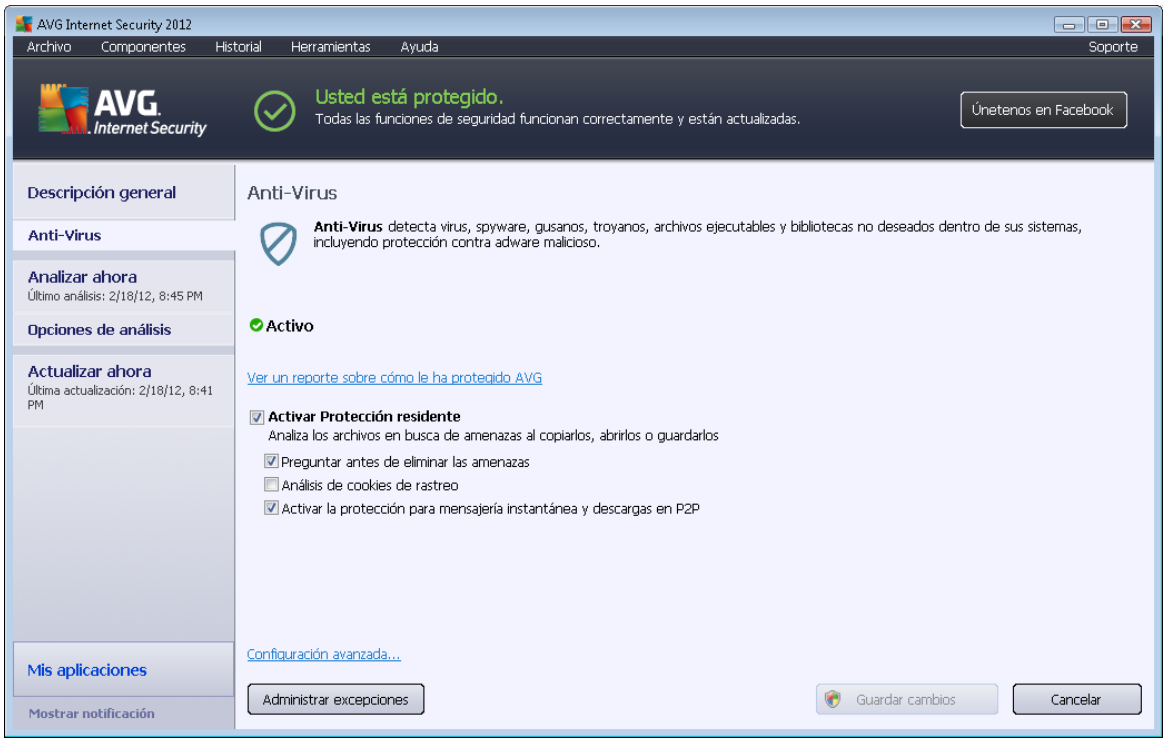
Anti-Spyware consta de una base de datos de spyware que se utiliza para identificar los tipos conocidos de definiciones de spyware. Los expertos en spyware de AVG trabajan constantemente para identificar y describir los últimos patrones de spyware tan pronto emergen, y agregan las definiciones a la base de datos. Mediante el proceso de actualización, estas nuevas definiciones se descargan en su equipo, para que siempre pueda estar protegido, incluso contra los tipos de spyware más recientes. ***Anti-Spyware*** le permite analizar completamente su equipo en busca de malware/spyware. También detecta malware inactivo y no peligroso, esto es, malware que se ha descargado pero que no se ha activado aún.

¿Qué es el spyware?

El spyware generalmente se define como un tipo de malware, esto es, un software que recopila información del equipo del usuario sin su conocimiento ni consentimiento. 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.

6.1.4. Interfaz de Anti-Virus

La interfaz del componente ***Anti-Virus*** ofrece una breve descripción del funcionamiento de este componente, información sobre su estado actual *(Activo)* y opciones básicas de configuración:



Opciones de configuración

Este cuadro de diálogo proporciona algunas opciones básicas de configuración de las funciones disponibles en el componente ***Anti-Virus***. A continuación encontrará una breve descripción de ellas:

- ***Ver un reporte en línea sobre cómo le ha protegido AVG***: este vínculo le redirige a una página específica del sitio Web de AVG (http://www.avg.com/). En esta página puede encontrar una descripción general con datos estadísticos detallados de todas las actividades de **AVG Internet Security 2012** realizadas en su equipo en un periodo de tiempo especificado y en total.

- ***Activar Protección residente***: esta opción le permite activar y desactivar fácilmente la protección residente. Protección residente analiza los archivos mientras se copian, se abren o se guardan. Cuando se detecte una amenaza de virus o de cualquier tipo, se le advertirá inmediatamente. De forma predeterminada, la función está activada y se recomienda mantenerla así. Con la protección residente activada puede decidir cómo se deben tratar las infecciones que sea posible detectar.

    - ***Preguntar antes de eliminar las amenazas***: deje marcada la opción para confirmar que desea que se le pregunte cada vez que se detecte una amenaza antes de que esta se mueva a la Bóveda de virus. Esta opción no tiene impacto sobre el nivel de

seguridad, y sólo refleja sus preferencias.

- ***Analizar cookies de rastreo***: con independencia de las opciones anteriores, puede decidir si desea analizar cookies de rastreo. *(Las cookies son paquetes de texto enviados por un servidor a un navegador Web y después enviados de regreso sin cambios por el navegador 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.)* En algunos casos específicos puede activar esta opción para alcanzar los máximos niveles de seguridad, sin embargo, esta opción está desactivada de manera predeterminada.

- ***Activar protección para mensajería instantánea y descargas en P2P***: marque este elemento si desea verificar que la comunicación a través de la mensajería instantánea (*por ejemplo, ICQ, MSN Messenger, etc.*) no contenga virus.

- ***Configuración avanzada***...: haga clic en el vínculo para ir al cuadro de diálogo respectivo de Configuración avanzada de **AVG Internet Security 2012**. En este cuadro de diálogo puede editar de forma detallada la configuración del componente. No obstante, tenga en cuenta que, de forma predeterminada, todos los componentes están configurados de modo que **AVG Internet Security 2012** proporcione un rendimiento óptimo y la máxima seguridad. A no ser que haya un motivo real para hacerlo, se recomienda mantener la configuración predeterminada.

Botones de control

En este cuadro de diálogo puede utilizar los siguientes botones de control:

- ***Administrar excepciones***: abre un nuevo cuadro de diálogo llamado ***Protección residente - Excepciones***. También se puede obtener acceso a la configuración de excepciones del análisis de la Protección residente desde el menú principal, siguiendo la secuencia Configuración avanzada / Anti-Virus / Protección residente / Excepciones *(para obtener una descripción detallada, consulte el capítulo respectivo)*. En este cuadro de diálogo puede especificar los archivos y carpetas que se deben excluir del análisis de la Protección residente. Si no es absolutamente necesario, le recomendamos no excluir ningún elemento. El cuadro de diálogo proporciona los siguientes botones de control:

  - *Agregar ruta de acceso*: especifique el directorio *(o directorios)* que se deben excluir del análisis seleccionándolos uno a uno en el árbol de navegación del disco local.

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

  - *Editar elemento*: permite editar la ruta de acceso especificada a un archivo o una carpeta que se ha seleccionado.

  - *Eliminar elemento*: le permite eliminar la ruta de acceso a un elemento seleccionado de la lista.

  - *Editar lista*: le permite editar toda la lista de excepciones en un nuevo cuadro de

diálogo que funciona como un editor de texto estándar.

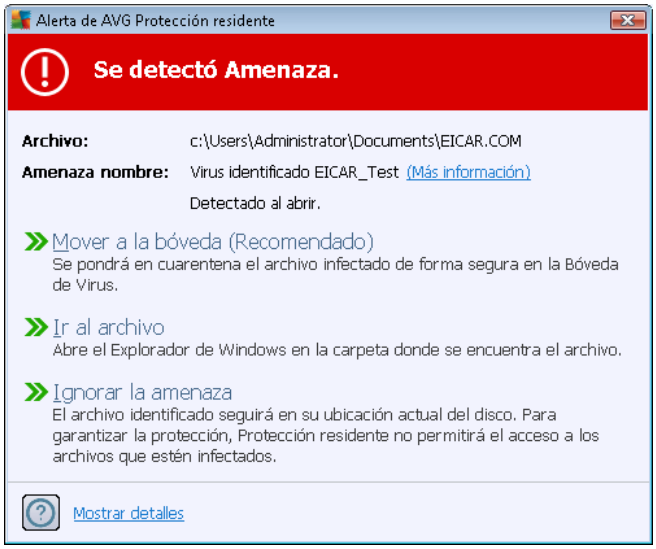
- ***Aplicar***: permite guardar todos los cambios realizados en la configuración del componente en este cuadro de diálogo y volver a la interfaz del usuario principal de **AVG Internet Security 2012** (*descripción general de los componentes*).

- ***Cancelar***: permite cancelar todos los cambios realizados en la configuración del componente en este cuadro de diálogo. No se guardará ningún cambio. Volverá a la interfaz del usuario principal de **AVG Internet Security 2012** (*descripción general de los componentes*).

6.1.5. Detecciones de Protección residente

Amenaza detectada

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



En este cuadro de diálogo de advertencia, verá datos sobre el archivo que se detectó y se designó como infectado (*Nombre del archivo*), el nombre de la infección reconocida (*Nombre de la amenaza*) y un vínculo a la enciclopedia de virus, donde podrá encontrar información detallada sobre la infección detectada, si se conoce (*Más información*).

Además, debe decidir qué acción se debe realizar ahora. Hay varias opciones alternativas disponibles. ***Tenga en cuenta que, en determinadas condiciones (el tipo de archivo infectado y dónde se encuentra), no todas las opciones están siempre disponibles.***

- ***Reparar***: este botón sólo aparece si se puede reparar la infección detectada. A continuación se elimina del archivo y restaura el archivo al estado original. Si el propio archivo es un virus, utilice esta función para eliminarlo (*es decir, enviarlo a la Bóveda de virus*)

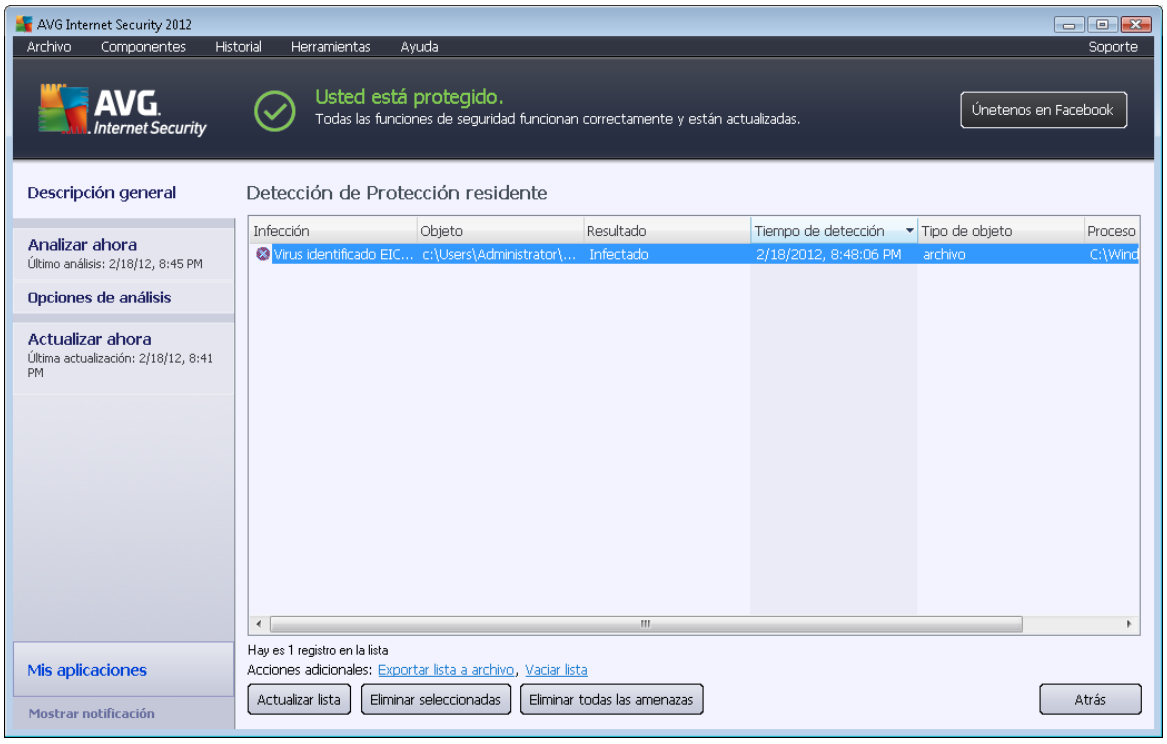
- ***Mover a la Bóveda (Recomendado)***: el virus será movido a la Bóveda de virus
- ***Ir al archivo***: esta opción lo redirige a la ubicación del objeto sospechoso (*abre una ventana nueva del Explorador de Windows*)
- ***Ignorar la amenaza***: recomendamos ampliamente NO utilizar esta opción, a menos que tenga una muy buena razón para hacerlo.

Nota: *es posible que el tamaño del objeto detectado exceda el límite de espacio libre en la Bóveda de virus. Si es así, aparecerá un mensaje para informarle del problema cuando intente mover el objeto infectado a la Bóveda de virus. De todos modos, puede editar el tamaño de la Bóveda de virus. Este tamaño está definido como un porcentaje ajustable del tamaño real de su disco duro. Para aumentar el tamaño de la Bóveda de virus, vaya al cuadro de diálogo Bóveda de virus dentro de Configuración avanzada de AVG, utilizando la opción "Limitar el tamaño de la Bóveda de virus".*

En la sección inferior del cuadro de diálogo encontrará el vínculo ***Mostrar detalles***: haga clic sobre él para abrir una ventana emergente con información detallada sobre el proceso que se estaba ejecutando cuando se detectó la infección, y la identificación del proceso.

Descripción general de las detecciones de Protección residente

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



La ***Detección de la Protección residente*** ofrece una descripción general de los objetos que detectó

la Protección residente, evaluados como peligrosos y reparados o movidos a la Bóveda de virus. Para cada objeto detectado se proporciona la siguiente información:

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

En la parte inferior del cuadro de 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*** le lleva de vuelta al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*).

6.2. LinkScanner

LinkScanner le protege contra el creciente número de amenazas fugaces que aparecen en la Web. Estas amenazas pueden esconderse en cualquier tipo de sitio Web, desde gubernamentales y de marcas grandes y reconocidas hasta de negocios pequeños, y rara vez permanecen allí por más de 24 horas. ***LinkScanner*** le protege analizando las páginas que están detrás de los vínculos de cualquier página Web que esté viendo, y se asegura de que sean seguras en el único momento en que verdaderamente importa: cuando está por hacer clic sobre ellas.

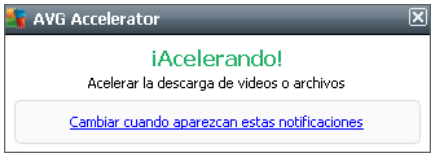
LinkScanner no está diseñado para proteger plataformas de servidor.

La tecnología ***LinkScanner*** consta de las siguientes funciones principales:

- Search-Shield contiene una lista de los sitios Web *(direcciones URL)* que se sabe que son peligrosos. Al realizar una búsqueda con Google, Yahoo! JP, eBay, Twitter, Digg, SlashDo, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask y Seznam, todos los resultados de la búsqueda se comprueban según esta lista y aparece un icono de veredicto (*para los resultados de búsqueda de Yahoo! sólo se muestran iconos de veredicto del tipo "sitio Web vulnerable"*).
- Surf-Shield analiza el contenido de los sitios Web que visita, independientemente de la dirección del sitio. Aunque Search-Shield *no detecte alguno de estos sitios Web (p. ej., un sitio malicioso que se haya creado recientemente o un sitio que antes estaba limpio pero que ahora contiene malware*), Surf-Shield lo detectará y lo bloqueará cuando intente visitarlo.
- Online Shield funciona como protección en tiempo real al navegar por Internet. Analiza el contenido de las páginas Web visitadas y los archivos que puedan contener incluso antes

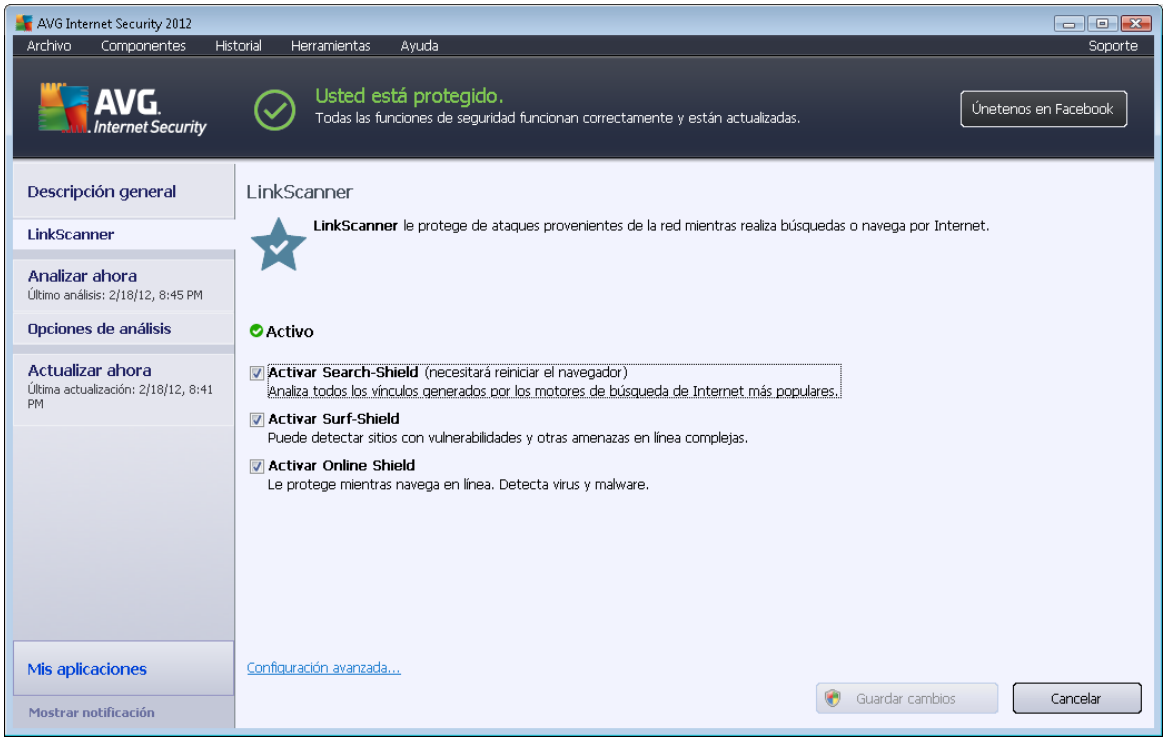
de que se visualicen en el navegador o de que se descarguen en el equipo. Online Shield detecta virus y spyware contenidos en la página que va a visitar y detiene la descarga inmediatamente para que ninguna amenaza llegue a su equipo.

- ***AVG Accelerator*** mejora la reproducción de video en línea y facilita la realización de descargas adicionales. Cuando el proceso de aceleración de video está en curso, se le notificará mediante la ventana emergente de la bandeja del sistema.



6.2.1. Interfaz de LinkScanner

El cuadro de diálogo principal del componente LinkScanner proporciona una breve descripción de sus funciones e información sobre su estado actual *(Activo)*:



En la parte inferior del cuadro de diálogo hay disponibles algunas opciones de configuración básicas del componente:

- ***Activar Search-Shield*** (*activado de forma predeterminada*): quite la marca del cuadro sólo si tiene un buen motivo para desactivar la funcionalidad de Search Shield.

- ***Activar Surf-Shield*** (*activado de forma predeterminada*): protección activa (*en tiempo real*) contra sitios de explotación cuando se obtiene acceso a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario accede

a ellos a través de un navegador Web (*o cualquier otra aplicación que utilice HTTP*).

- ***Activar Online Shield*** (*activado de forma predeterminada*): análisis en tiempo real de las páginas Web que va a visitar para detectar posibles virus o spyware. Si se detectan, la descarga se detiene inmediatamente para que ninguna amenaza llegue a su equipo.

6.2.2. Detecciones de Search-Shield

Al realizar búsquedas en Internet con ***Search-Shield*** activado, todos los resultados de búsqueda que devuelven los motores de búsqueda más populares (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg y SlashDot*) se evalúan para buscar vínculos peligrosos o sospechosos. Mediante la comprobación de estos vínculos y la marcación de los vínculos malos, LinkScanner muestra una advertencia antes de hacer clic en los vínculos peligrosos o sospechosos; así puede estar seguro de que sólo visitará sitios Web seguros.

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

 La página vinculada es segura.

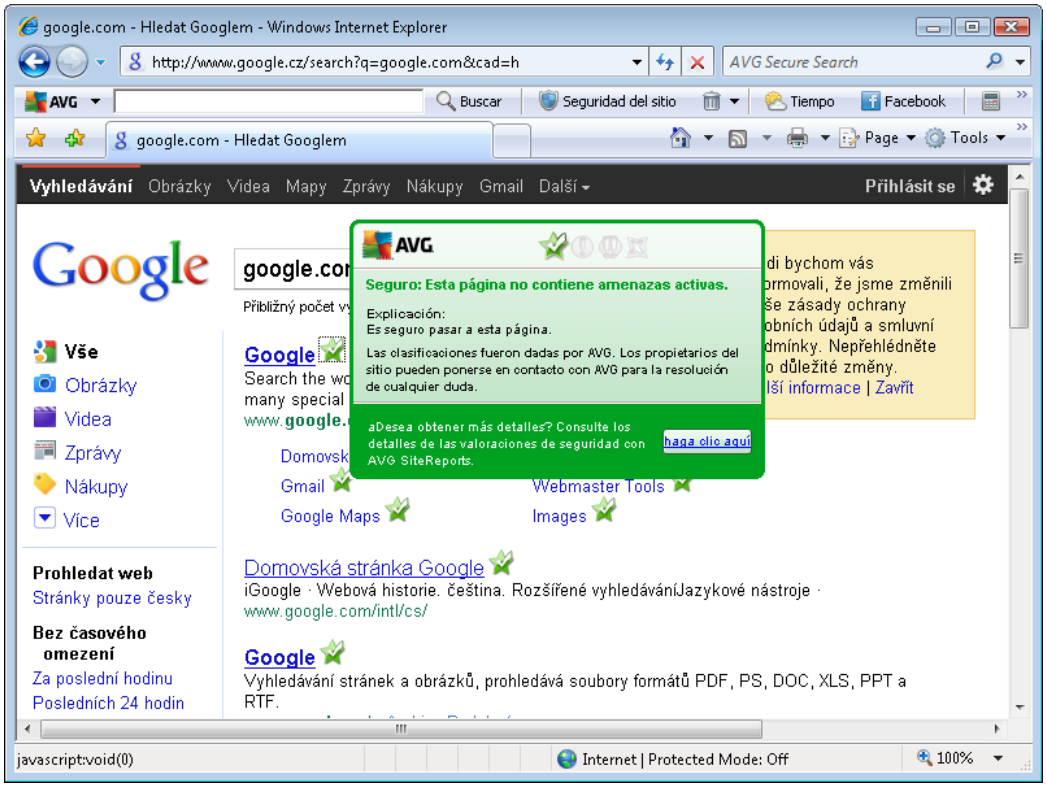
 La página vinculada no contiene amenazas pero es algo sospechosa (*origen o motivos cuestionables, por lo tanto no recomendable para realizar compras por Internet, etc.*).

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

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

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

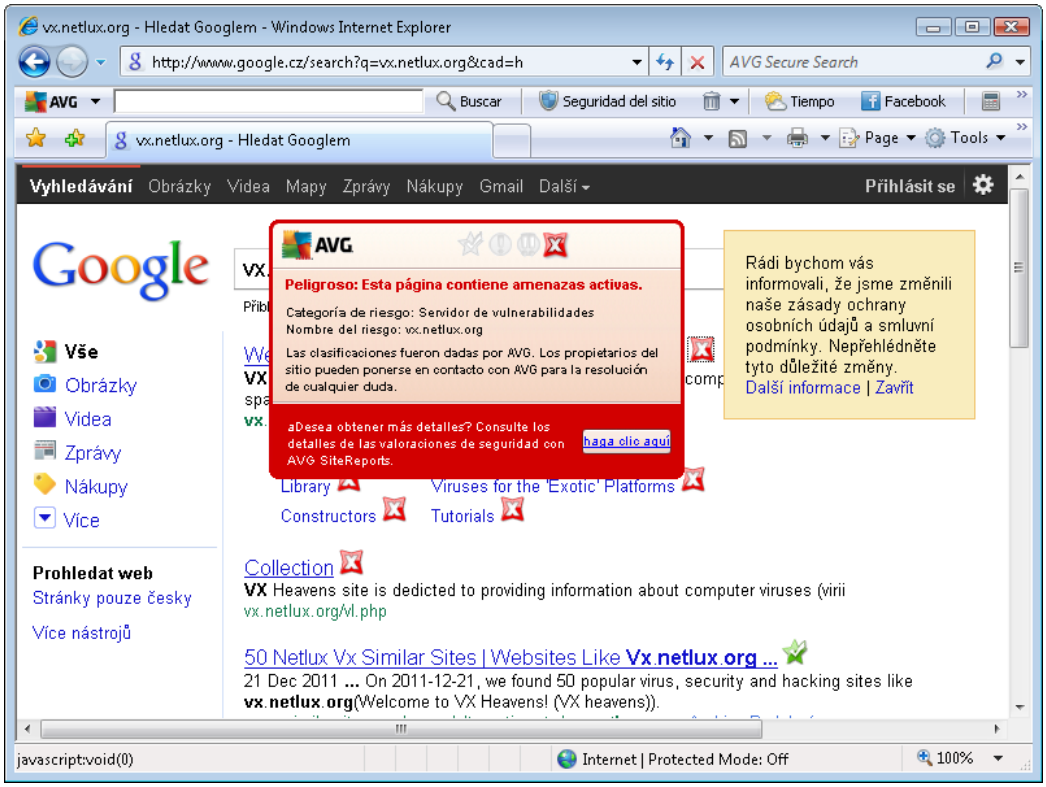
Al desplazarse sobre un icono de calificación se mostrarán detalles acerca del vínculo en cuestión. La información incluye detalles adicionales acerca de la amenaza (*si los hay*):



6.2.3. Detecciones de Surf-Shield

Esta poderosa protección bloqueará el contenido malicioso de cualquier página que intente abrir, y evitará que se descargue en su equipo. Con esta característica activada, al hacer clic en un vínculo o escribir la URL de un sitio peligroso se evitará que se abra la página Web, protegiéndolo 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, LinkScanner no permitirá que su navegador la muestre.

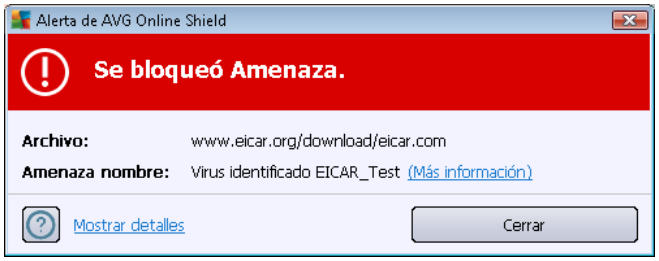
Si encuentra un sitio Web malicioso, LinkScanner le advertirá dentro del navegador Web con un mensaje similar al siguiente:



Entrar en este sitio Web es muy arriesgado y no es recomendable.

6.2.4. Detecciones de Online Shield

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

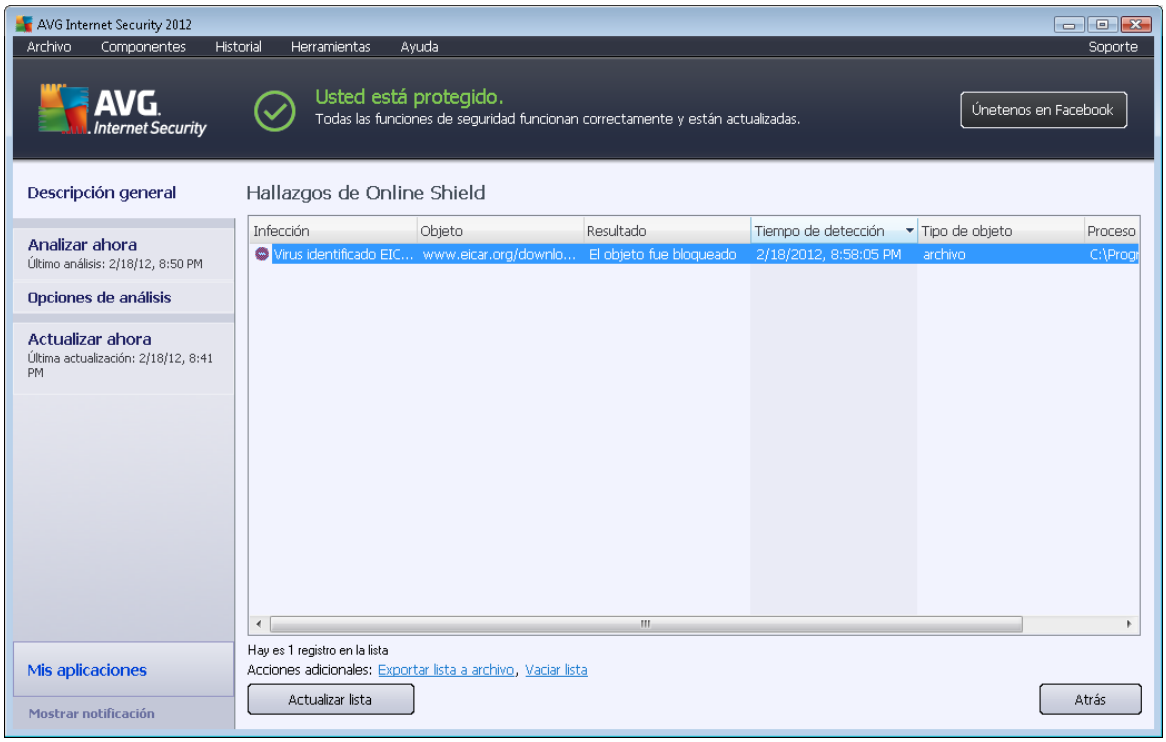


En este cuadro de diálogo de advertencia, verá datos sobre el archivo que se detectó y se designó como infectado (*Nombre del archivo*), el nombre de la infección reconocida (*Nombre de la amenaza*) y un vínculo a la enciclopedia de virus, donde podrá encontrar información detallada sobre la infección detectada (*si se conoce*). El cuadro de diálogo proporciona los siguientes botones:

- ***Mostrar detalles***: haga clic en el botón ***Mostrar detalles*** para abrir una nueva ventana emergente donde podrá encontrar información acerca del proceso que se estaba ejecutando cuando se detectó la infección, y la identificación del proceso.

- ***Cerrar***: haga clic en el botón para cerrar el mensaje de advertencia.

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



Para cada objeto detectado se proporciona la siguiente información:

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

En la parte inferior del cuadro de 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 a un archivo (***Exportar lista a archivo***) y eliminar todas las entradas en los objetos detectados (***Vaciar lista***).

Botones de control

- ***Actualizar lista***: actualiza la lista de hallazgos detectados por ***Online Shield***
- ***Atrás***: vuelve al cuadro de diálogo principal de AVG predeterminado *(descripción general de los componentes)*

6.3. Protección del correo electrónico

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

El componente ***Protección del correo electrónico*** es el responsable de analizar cada mensaje de correo electrónico, enviado o recibido; cada vez que se detecta un virus en un mensaje de correo electrónico, éste se transfiere a la Bóveda de virus inmediatamente. El componente también puede filtrar determinados tipos de archivos adjuntos de correo electrónico, así como agregar un texto de certificación a los mensajes no infectados. ***Protección del correo electrónico*** consta de dos funciones principales:

- Analizador de correos electrónicos
- Anti-Spam

6.3.1. Analizador de correos electrónicos

El Analizador de correo electrónico personal analiza automáticamente los correos electrónicos entrantes/salientes. Puede utilizarlo con los clientes de correo electrónico que no tienen su propio complemento de AVG (*pero también se puede utilizar para analizar mensajes de correo electrónico para clientes de correo electrónico compatibles con AVG con un complemento específico, como Microsoft Outlook, The Bat y Mozilla Thunderbird*). Principalmente, se utilizará con aplicaciones de correo electrónico como Outlook Express, Incredimail, etc.

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

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

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

Bóveda de virus de forma inmediata. Después se pasa el mensaje al cliente de correo.

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

El Analizador de correos electrónicos no está diseñado para plataformas de servidor.

6.3.2. Anti-Spam

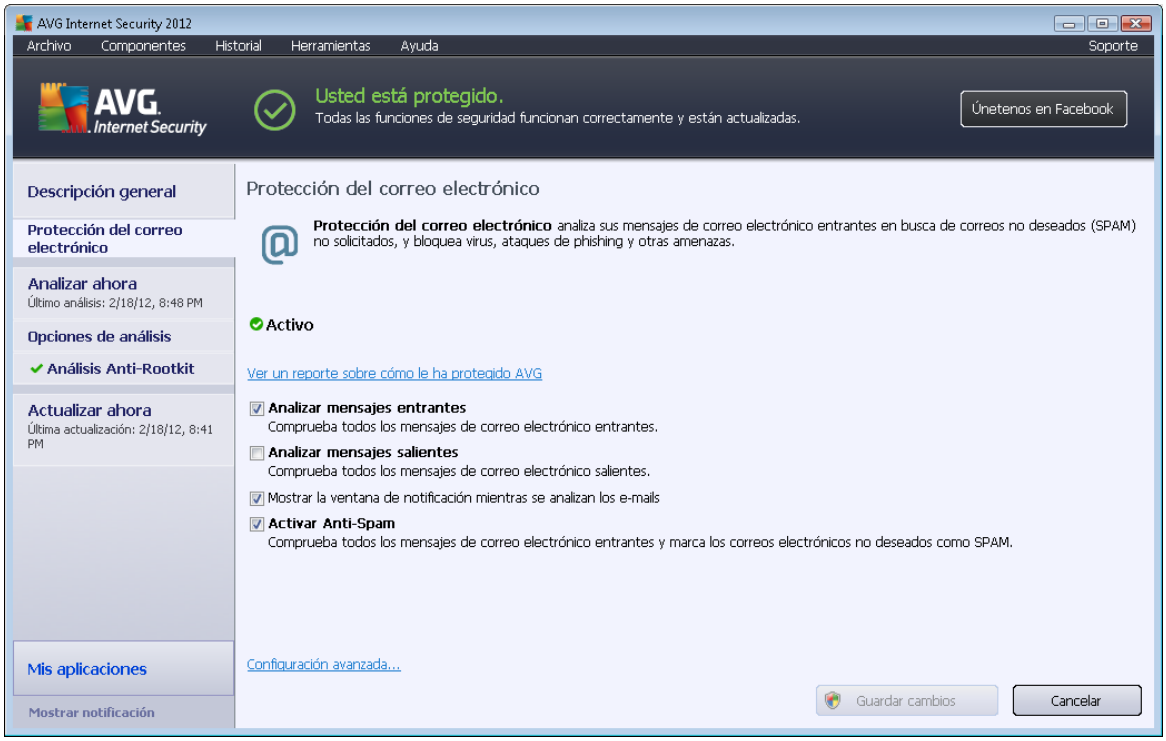
¿Cómo funciona el Anti-Spam?

Anti-Spam comprueba todos los mensajes de correo electrónico entrantes y marca los no deseados como spam. ***Anti-Spam*** puede modificar el asunto del correo electrónico (*identificado como spam*) agregando una cadena de texto especial. Luego puede filtrar fácilmente sus mensajes en el cliente de correo electrónico. El componente ***Anti-Spam*** usa varios métodos de análisis para procesar cada mensaje y ofrece la mayor protección posible contra mensajes de correo electrónico no deseados. ***Anti-Spam*** utiliza una base de datos que se actualiza regularmente para la detección del spam. También es posible usar servidores RBL (*bases de datos públicas con direcciones de correo electrónico de "spammers conocidos"*), así como agregar manualmente direcciones de correo electrónico a la Lista blanca (*nunca marcar como spam*) y a la Lista negra (*marcar siempre como spam*).

¿Qué es el spam?

El término spam hace referencia al correo electrónico no solicitado, la mayoría publicitando un producto o servicio, que se envía de forma masiva a un gran número de direcciones de correo al mismo tiempo, lo que llena los buzones de correo de los destinatarios. Los correos de spam no son correos comerciales legítimos cuyos consumidores hayan dado su consentimiento. El spam no es sólo irritante, sino que también puede ser una fuente de virus o contenido ofensivo.

6.3.3. Interfaz de protección del correo electrónico



En el cuadro de diálogo ***Protección del correo electrónico***, puede encontrar un breve texto con una descripción de las funciones del componente e información sobre su estado actual *(Activo)*. Utilice el vínculo ***Ver un reporte en línea sobre cómo le ha protegido AVG*** para revisar estadísticas detalladas de las actividades y detecciones de **AVG Internet Security 2012** en una página del sitio Web de AVG específicamente dedicada a ello (http://www.avg.com/).

Configuración básica de Protección del correo electrónico

En el cuadro de diálogo ***Protección del correo electrónico***, puede seguir editando algunas funciones básicas del componente:

- ***Analizar mensajes entrantes*** *(activado de forma predeterminada)*: seleccione esta casilla de verificación para especificar que todos los correos electrónicos entregados en la cuenta deben analizarse en busca de virus.
- ***Analizar mensajes salientes*** *(desactivado de forma predeterminada)*: seleccione esta casilla de verificación para confirmar que todo el correo electrónico enviado desde su cuenta se debe analizar en busca de virus.
- ***Mostrar ventana de notificación cuando se estén analizando correos electrónicos*** *(activado de forma predeterminada)*: marque este elemento para confirmar que desea que se le informe mediante el cuadro de diálogo de notificación que aparece sobre el icono de AVG en la bandeja del sistema durante el análisis del correo electrónico.

- ***Activar Anti-Spam*** *(activado de forma predeterminada)*: marque este elemento para especificar que desea filtrar el correo entrante para evitar recibir correo no solicitado.

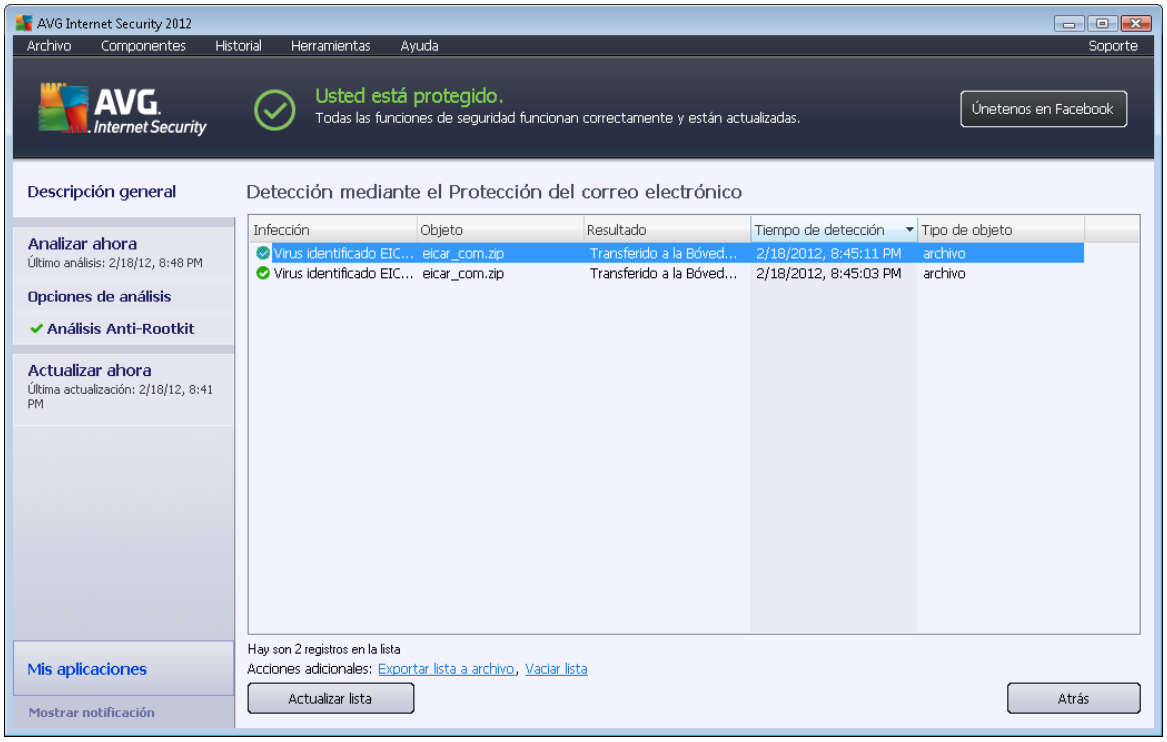
El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración. Si necesita cambiar la configuración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

Botones de control

Los botones de control disponibles en el cuadro de diálogo ***Protección del correo electrónico*** son:

- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo
- ***Cancelar***: presione este botón para volver al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*)

6.3.4. Detecciones del analizador de correos electrónicos



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

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

En la parte inferior del cuadro de 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 a un archivo (***Exportar lista a archivo***) y eliminar todas las entradas en los objetos detectados (***Vaciar lista***).

Botones de control

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

- ***Actualizar lista***: actualiza la lista de amenazas detectadas.
- ***Atrás***: le lleva al cuadro de diálogo mostrado anteriormente.

6.4. Firewall

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

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

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

Los equipos que no están protegidos por un firewall se vuelven blancos fáciles para los hackers informáticos y para el robo de datos.

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

firewall en su equipo y desactive los demás; así se elimina el riesgo de posibles conflictos y cualquier problema relacionado con esto.

6.4.1. Principios de Firewall

En **AVG Internet Security 2012**, el ***Firewall*** controla todo el tráfico en cada puerto de red de su equipo. El ***Firewall***, de acuerdo con las reglas definidas, evalúa las aplicaciones que están ejecutándose en el equipo *(y desean conectarse a Internet o a una red local)* o las que abordan su equipo desde el exterior para intentar conectarse a él. Para cada una de estas aplicaciones, el ***Firewall*** permite o prohíbe la comunicación en los puertos de red. De forma predeterminada, si la aplicación es desconocida *(es decir, no tiene reglas de Firewall definidas), el* ***Firewall*** le preguntará si desea permitir o bloquear el intento de comunicación.

El Firewall AVG no está diseñado para plataformas de servidor.

El Firewall AVG puede:

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

6.4.2. Perfiles de Firewall

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

Perfiles disponibles

- ***Permitir todo***: un perfil de sistema de Firewall que ha preestablecido el fabricante y siempre se encuentra presente. Al activar este perfil, se permite toda la comunicación a través de la red y no se aplican reglas de políticas de seguridad, como si la protección del Firewall estuviera desactivada (todas las aplicaciones se permiten, pero los paquetes continúan siendo analizados; para desactivar por completo cualquier filtrado necesita deshabilitar el Firewall). Este perfil de sistema no puede duplicarse, eliminarse, y su configuración no puede modificarse.
- ***Bloquear todo***: un perfil de sistema de Firewall que ha preestablecido el fabricante y siempre se encuentra presente. Cuando este perfil está activado, se bloquea toda la comunicación de red, y el equipo no estará disponible para las redes externas y tampoco podrá comunicarse con ellas. El perfil de sistema no puede duplicarse, eliminarse, y su configuración no puede ser cambiada.

- ***Perfiles personalizados***: los perfiles personalizados permiten aprovechar el cambio automático de perfiles, que es especialmente útil si se conecta a diferentes redes de forma regular *(por ejemplo, con un equipo portátil).* Los perfiles personalizados se generan automáticamente después de la instalación de **AVG Internet Security 2012** y cubren las necesidades específicas de las reglas de políticas del Firewall. Se encuentran disponibles los siguientes perfiles personalizados:

    - ***Conectado directamente a Internet***: adecuado para equipos de escritorio o portátiles conectados directamente a Internet, sin ninguna protección adicional. Esta opción también es recomendable cuando conecta su equipo portátil a varias redes desconocidas y probablemente inseguras (*por ejemplo, un café Internet, una habitación de hotel, etc.*). Las reglas de política de Firewall más estrictas de este perfil garantizan que el equipo esté correctamente protegido.

    - ***Equipo en un dominio***: adecuado para los equipos dentro de una red local, por ejemplo, corporativa o escolar. Se asume que la red está administrada por un profesional y protegida por algunas medidas adicionales, por lo que el nivel de seguridad puede ser menor que para los casos anteriormente mencionados, permitiendo la obtención de acceso a carpetas compartidas, unidades de disco, etc.

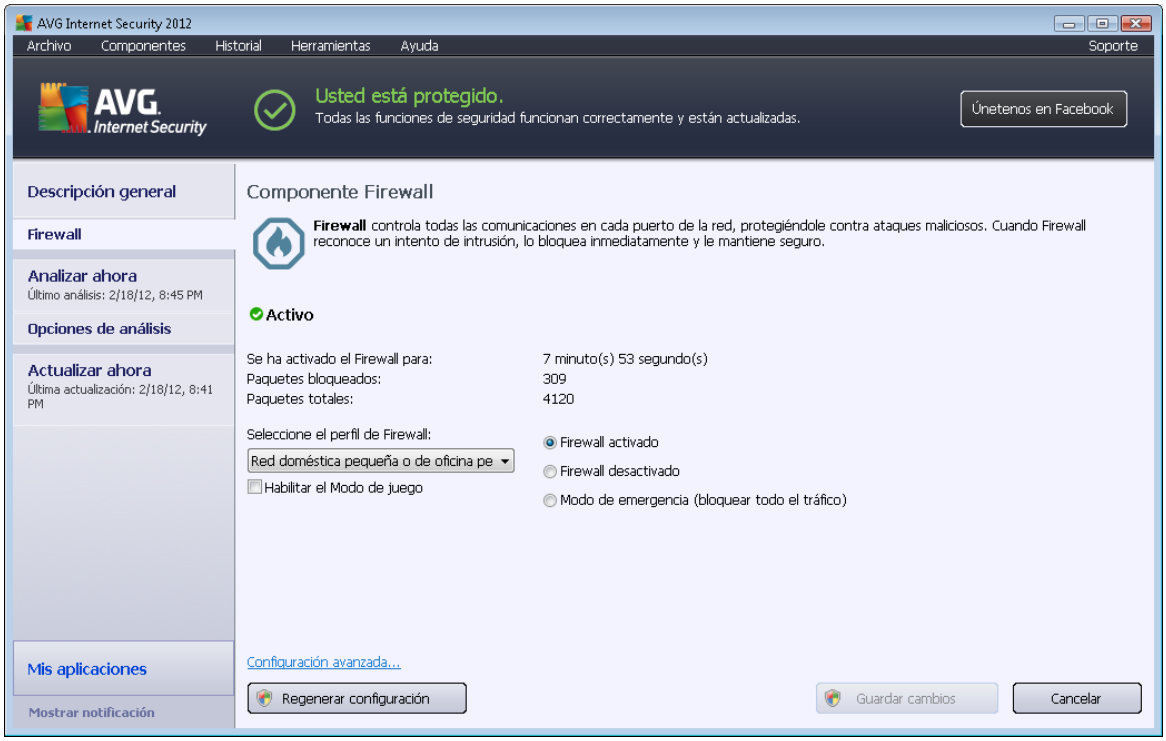
    - ***Red doméstica pequeña o de oficina pequeña***: adecuado para equipos en redes pequeñas, por ejemplo, en casa o en una oficina pequeña. Normalmente, este tipo de red no tiene un administrador "central" y sólo está formada por varios equipos conectados entre sí, que a menudo comparten una impresora, un escáner o un dispositivo similar, lo que debe reflejarse en las reglas del Firewall.

Cambio de perfiles

La función de cambio de perfil permite al Firewall cambiar automáticamente al perfil definido al utilizar un adaptador de red determinado o al conectarse a un cierto tipo de red. Si aún no se ha asignado un perfil al área de red, hasta la siguiente conexión a esa área, el Firewall mostrará un cuadro de diálogo que solicitará asignar un perfil. Puede asignar los perfiles a todas las áreas o interfaces de redes locales y especificar la configuración más detalladamente en el cuadro de diálogo Perfiles de áreas y adaptadores, donde también puede desactivar la característica si no desea utilizarla (*posteriormente, para cualquier tipo de conexión, se utilizará el perfil predeterminado*).

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

6.4.3. Interfaz de Firewall



El cuadro de diálogo principal denominado ***Componente Firewall*** proporciona información básica acerca de la funcionalidad del componente, su estado *(Activo)* y una breve descripción general de las estadísticas del componente:

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

Configuración básica del Firewall

- ***Seleccione el perfil de Firewall***: en el menú desplegable, seleccione uno de los perfiles definidos (*para obtener una descripción detallada de cada perfil y su uso recomendado, consulte el capítulo Perfiles de Firewall*)
- ***Habilitar el Modo de juego***: seleccione esta opción para garantizar que al ejecutar aplicaciones de pantalla completa (*juegos, presentaciones, películas, etc.*), el Firewall no mostrará cuadros de diálogo donde se le pregunte si desea permitir o bloquear la comunicación con aplicaciones desconocidas. Si en ese momento una aplicación desconocida intenta comunicarse mediante la red, el Firewall permitirá o bloqueará

automáticamente el intento de acuerdo a la configuración que existe en el perfil actual. ***Nota:*** cuando está activado el modo de juego, todas las tareas programadas (análisis y actualizaciones) se posponen hasta que se cierra la aplicación.

- Además, en esta sección de configuración básica puede seleccionar entre tres opciones alternativas que definen el estado actual del componente Firewall:

    - ***Firewall activado*** *(activada de forma predeterminada)*: seleccione esta opción para permitir la comunicación a aquellas aplicaciones que tienen la asignación de 'permitido' en el conjunto de reglas definido dentro del perfil de Firewall seleccionado.

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

    - ***Modo de emergencia (bloquear todo el tráfico)***: seleccione esta opción para bloquear todo el tráfico en todos los puertos de red; el Firewall continuará en ejecución, pero se detendrá todo el tráfico de red.

Nota: *el proveedor del software ha configurado todos los componentes de AVG Internet Security 2012 para que ofrezcan 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 cambios en la configuración. Si necesita cambiar la configuración del Firewall, seleccione el elemento del menú del sistema* ***Herramientas/Configuración del Firewall*** *y edite la configuración del Firewall en el cuadro de diálogo Configuración del Firewall que se abre.*

Botones de control

- ***Regenerar configuración***: presione este botón para sobrescribir la configuración actual del Firewall y para volver a la configuración predeterminada según la detección automática.

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

- ***Cancelar***: presione este botón para volver al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*).

6.5. Anti-Rootkit

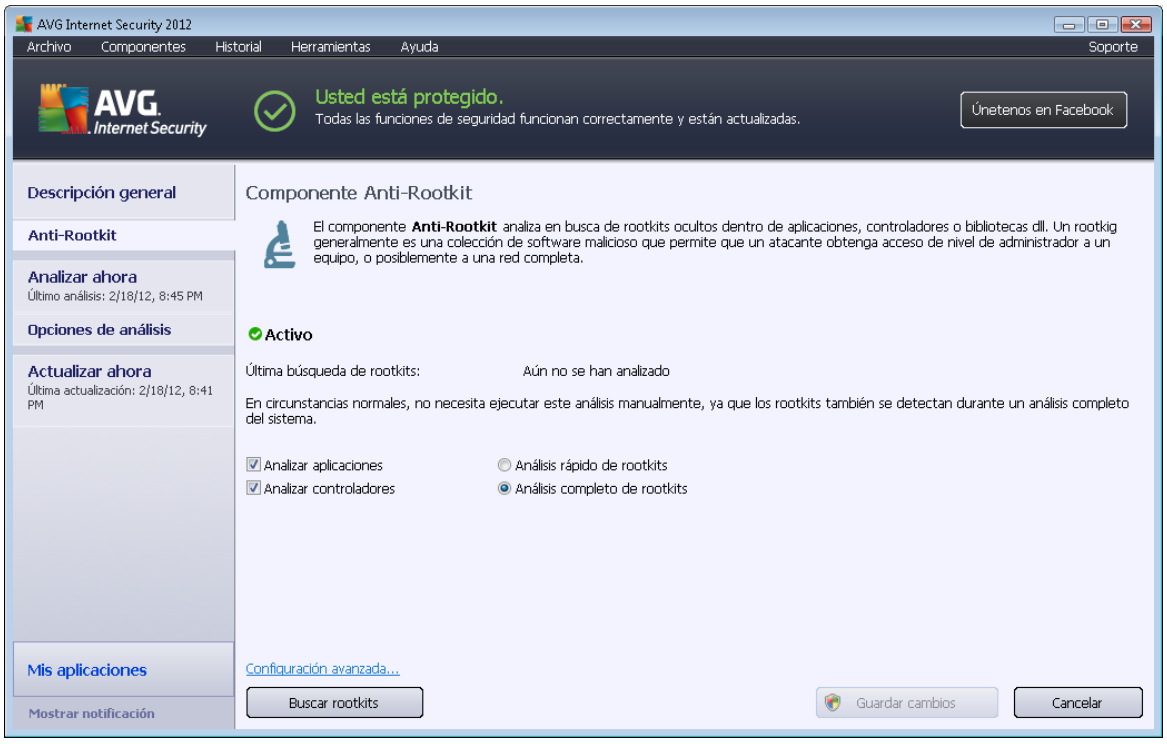
Anti-Rootkit es una herramienta especializada que detecta y elimina con eficacia los rootkits peligrosos, es decir, los programas y las tecnologías que pueden camuflar la presencia de software malicioso en el equipo. ***Anti-Rootkit*** puede detectar rootkits según un conjunto de reglas predefinido. Tenga en cuenta que se detectan todos los rootkits (*no sólo los infectados*). Si ***Anti-Rootkit*** encuentra un rootkit, no significa necesariamente que el rootkit está infectado. En ocasiones, los rootkits se utilizan como controladores o forman parte de aplicaciones correctas.

¿Qué es un rootkit?

Un rootkit es un programa diseñado para tomar el control fundamental de un sistema informático,

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

6.5.1. Interfaz de Anti-Rootkit



El cuadro de diálogo ***Anti-Rootkit*** proporciona una breve descripción de la funcionalidad del componente, informa de su estado actual *(Activo)* y también aporta información sobre la última vez que se realizó un análisis de ***Anti-Rootkit*** (*Última búsqueda de rootkits; la evaluación de rootkit es un proceso predeterminado que se ejecuta dentro del Análisis de todo el equipo*). El cuadro de diálogo ***Anti-Rootkit*** también proporciona el vínculo Herramientas/Configuración avanzada. Utilice el vínculo para ir al entorno de configuración avanzada del componente ***Anti-Rootkit***.

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 cambios en la configuración.

Configuración básica de Anti-Rootkit

En la parte inferior del cuadro de diálogo, 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 controladores***

También puede seleccionar el modo de análisis de rootkits:

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

Botones de control

- ***Buscar rootkits***: como el análisis de rootkits no es un elemento implícito del 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 todos los cambios efectuados en esta interfaz y regresar al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*).
- ***Cancelar***: presione este botón para regresar al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*) sin guardar los cambios realizados.

6.6. Herramientas del sistema

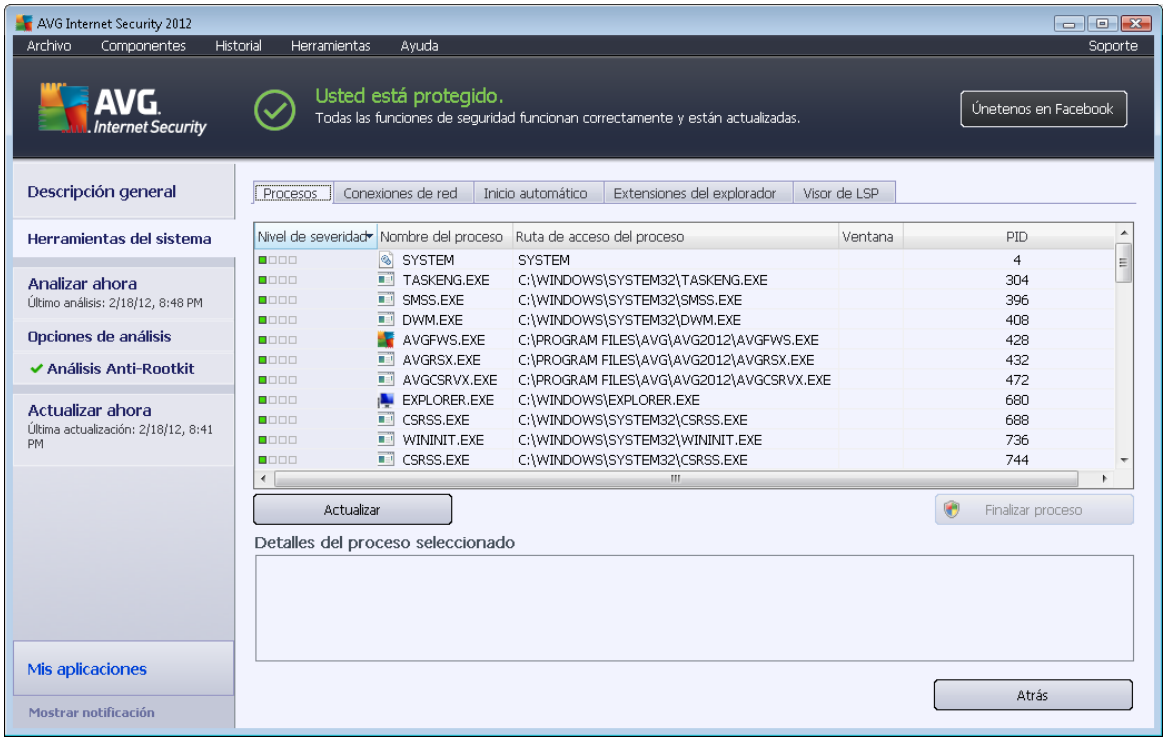
Herramientas del sistema hace referencia a las herramientas que ofrecen un resumen detallado del entorno **AVG Internet Security 2012** y el sistema operativo. El componente muestra una descripción general de:

- Procesos: lista de procesos (*(por ejemplo, aplicaciones en ejecución)*) que están activos actualmente en el equipo
- Conexiones de red: lista de las conexiones de red activas actualmente
- Inicio automático: lista de todas las aplicaciones que se ejecutan al iniciar el sistema Windows
- Extensiones del navegador: lista de los plugins o complementos (*p. ej. aplicaciones*) instalados en el navegador de Internet
- Visor de LSP: lista de los proveedores de servicio por niveles (*LSP*)

Las descripciones generales también pueden editarse, si bien esto sólo se recomienda para

los usuarios con mucha experiencia.

6.6.1. Procesos



El cuadro de diálogo ***Procesos*** contiene una lista de los procesos (*aplicaciones en ejecución*) actualmente activos en el equipo. La lista se divide en varias columnas:

- ***Nivel de severidad***: identificación gráfica de la severidad del proceso correspondiente en una escala de cuatro niveles desde menos importante (■□□□) hasta crítico (■■■■)
- ***Nombre del proceso***: indica el nombre del proceso activo
- ***Ruta de acceso del proceso***: ruta física de acceso del proceso activo
- ***Ventana***: si corresponde, indica el nombre de la aplicación que figura en la ventana
- ***PID***: número de identificación del proceso, es un identificador de procesos internos único en Windows

Botones de control

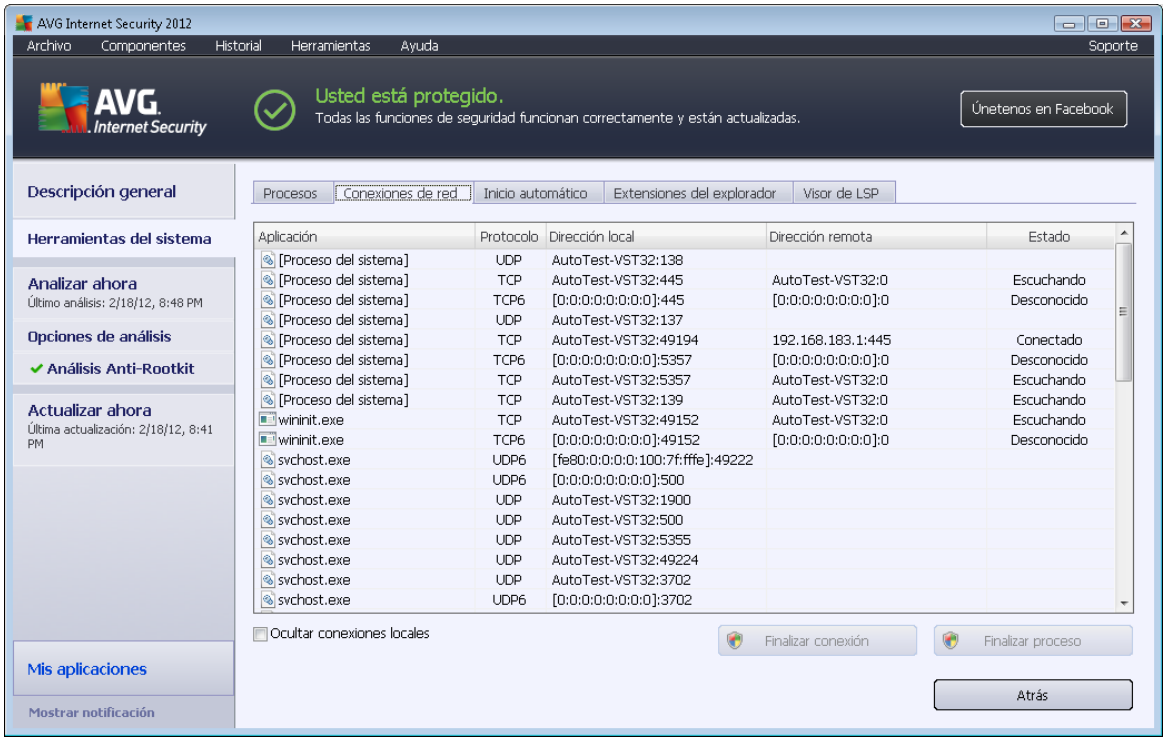
Los botones de control disponibles en la pestaña ***Procesos*** son los siguientes:

- ***Actualizar***: actualiza la lista de procesos de acuerdo con el estado actual
- ***Finalizar proceso***: puede seleccionar una o más aplicaciones y después finalizarlas

presionando este botón. ***Le recomendamos encarecidamente que no finalice ninguna aplicación, a menos que tenga plena seguridad de que representa una amenaza verdadera.***

- ***Atrás***: le lleva al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*)

6.6.2. Conexiones de red



El cuadro de diálogo ***Conexiones de red*** contiene una lista de las conexiones actualmente activas. La lista se divide en las siguientes columnas:

- ***Aplicación***: nombre de la aplicación relacionada con la conexión (*con la excepción de Windows 2000 donde la información no está disponible*)
- ***Protocolo***: tipo de protocolo de transmisión utilizado para la conexión:
  - TCP: protocolo que se utiliza en conjunto con el protocolo de Internet (IP) para transmitir información a través de Internet.
  - UDP: protocolo TCP alternativo
- ***Dirección local***: dirección IP del equipo local y número de puerto utilizado
- ***Dirección remota***: dirección IP del equipo remoto y número del puerto al que está conectado. De ser posible, también buscará el nombre de host del equipo remoto.

- ***Estado***: indica el estado actual más probable (*Conectado, Servidor debe cerrarse, Escuchar, Cierre activo finalizado, Cierre pasivo, Cierre activo*)

Para elaborar una lista que incluya sólo las conexiones externas, seleccione la casilla de verificación ***Ocultar conexiones locales*** en la sección inferior del cuadro de diálogo, debajo de la lista.

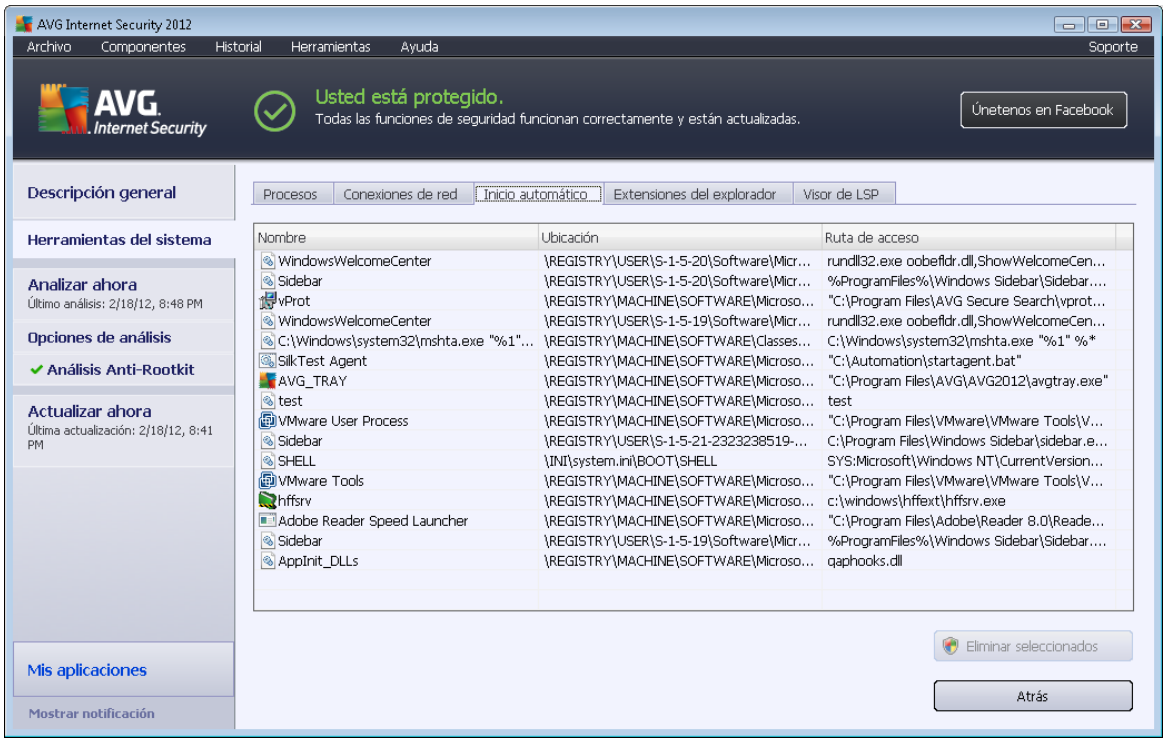
Botones de control

Los botones de control disponibles en la pestaña ***Conexiones de red*** son los siguientes:

- ***Finalizar conexión***: cierra una o más conexiones seleccionadas en la lista
- ***Finalizar proceso***: cierra una o más aplicaciones relacionadas con las conexiones seleccionadas en la lista
- ***Atrás***: vuelve al cuadro de diálogo principal de AVG predeterminado (descripción general de los componentes)

En ocasiones sólo es posible finalizar las aplicaciones que figuran actualmente como "conectadas". Le recomendamos que no finalice ninguna conexión, a menos que tenga plena seguridad de que representa una amenaza verdadera.

6.6.3. Inicio automático



El diálogo ***Inicio automático*** muestra una lista de todas las aplicaciones que se ejecutan durante

el inicio del sistema Windows. A menudo, muchas aplicaciones de malware se agregan automáticamente a sí mismas a la entrada del registro de inicio.

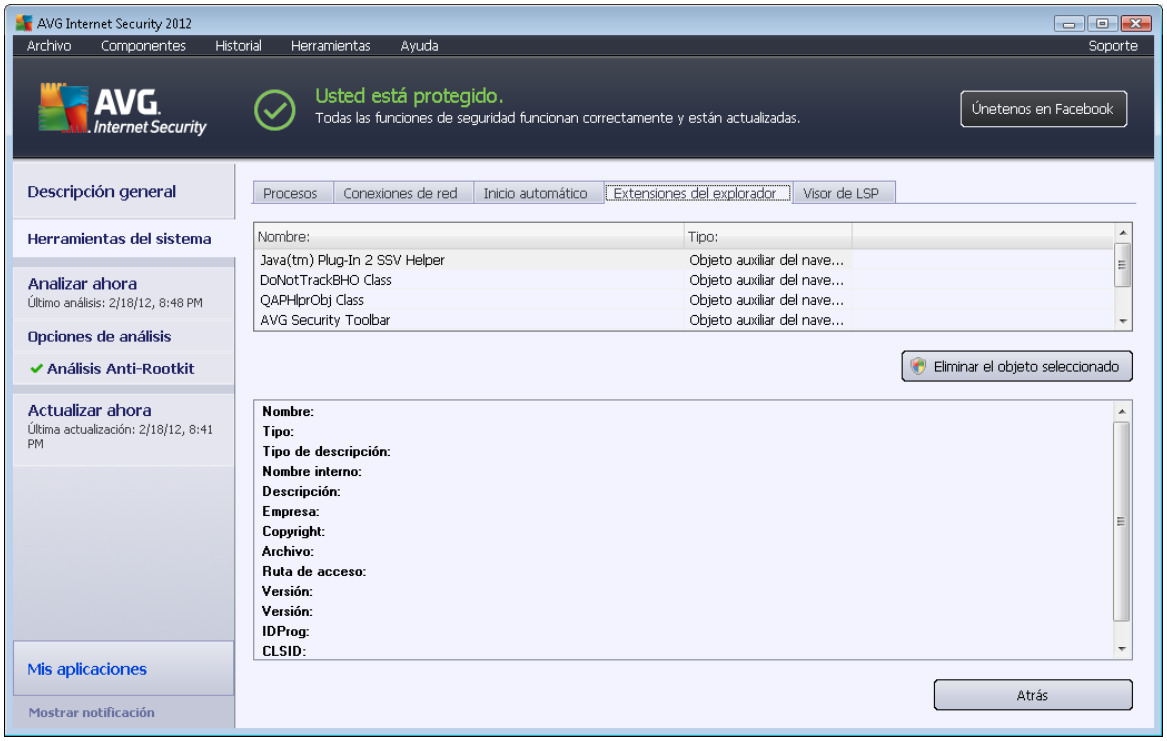
Botones de control

Los botones de control disponibles en la pestaña ***Inicio automático*** son los siguientes:

- ***Eliminar seleccionados***: presione el botón para eliminar una o varias entradas seleccionadas.
- ***Atrás***: le lleva al cuadro de diálogo principal de AVG *predeterminado (descripción general de los componentes).*

Le recomendamos que no elimine ninguna aplicación de la lista, a menos que tenga plena seguridad de que representa una amenaza verdadera.

6.6.4. Extensiones del navegador



El cuadro de diálogo ***Extensiones del navegador*** contiene una lista de plugins o complementos (*es decir, aplicaciones*) instalados dentro de su navegador de Internet. Esta lista puede contener tanto plugins comunes como programas que sean potencialmente maliciosos. Haga clic en un objeto de la lista para obtener información detallada acerca del complemento seleccionado que se mostrará en la sección inferior del cuadro de diálogo.

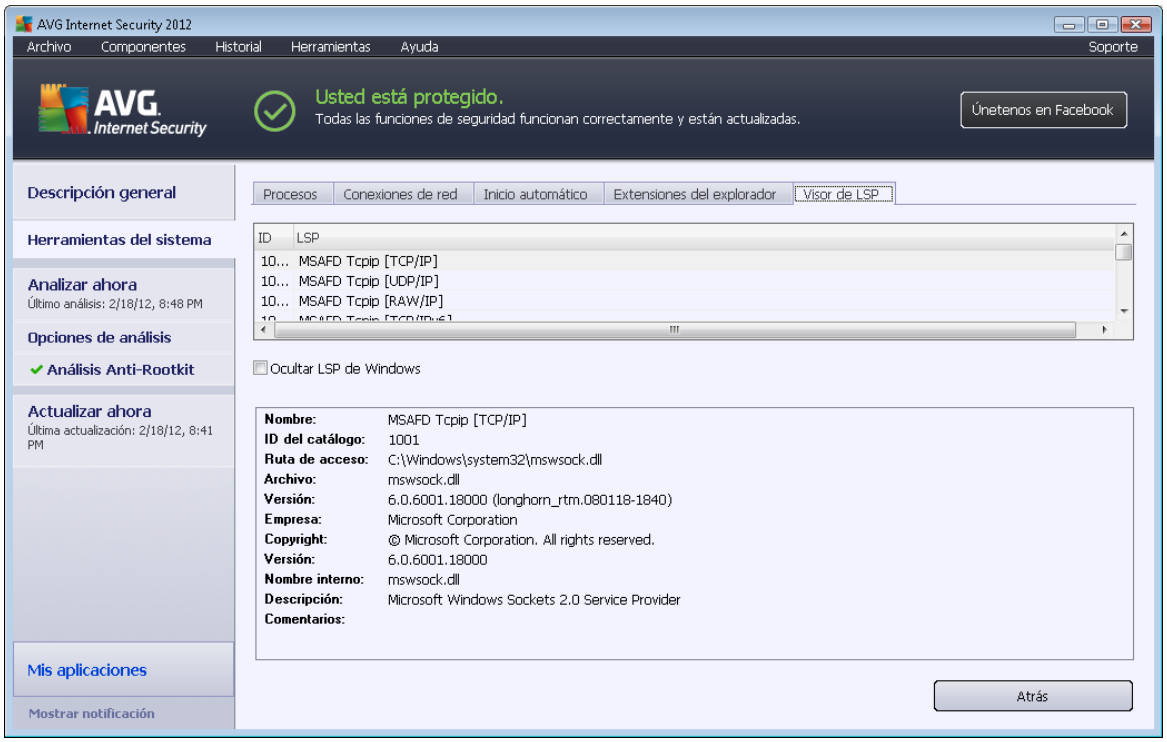
Botones de control

Los botones de control disponibles en la pestaña ***Extensiones del navegador*** son los siguientes:

- ***Eliminar el objeto seleccionado***: elimina el complemento resaltado de la lista. ***Le recomendamos que no elimine ningún complemento de la lista, a menos que tenga plena seguridad de que representa una amenaza verdadera.***

- ***Atrás***: le lleva al cuadro de diálogo principal de AVG *predeterminado (descripción general de los componentes).*

6.6.5. Visor de LSP



El cuadro de diálogo ***Visor de LSP*** muestra una lista de proveedores de servicio por niveles (LSP).

Un ***Proveedor de servicio por niveles*** (LSP) es un controlador del sistema vinculado a los servicios de red del sistema operativo Windows. Tiene acceso a todos los datos que ingresan al equipo o salen de él, y cuenta con la capacidad de poder modificar esos datos. Es necesario contar con algunos de estos LSP a fin de que Windows pueda conectarse a otros equipos, incluido Internet. No obstante, algunas aplicaciones de malware también se instalan a sí mismas como LSP y, así, obtienen acceso a todos los datos que su equipo transmite. Por ello, esta revisión le permitirá analizar todas las posibles amenazas presentadas por los LSP.

Bajo ciertas circunstancias, también es posible reparar los LSP que se hayan dañado (*por ejemplo, si se ha eliminado el archivo, pero las entradas del registro permanecen intactas*). Cuando se descubre un LSP que se puede reparar, aparecerá un nuevo botón que le permitirá solucionar el problema.

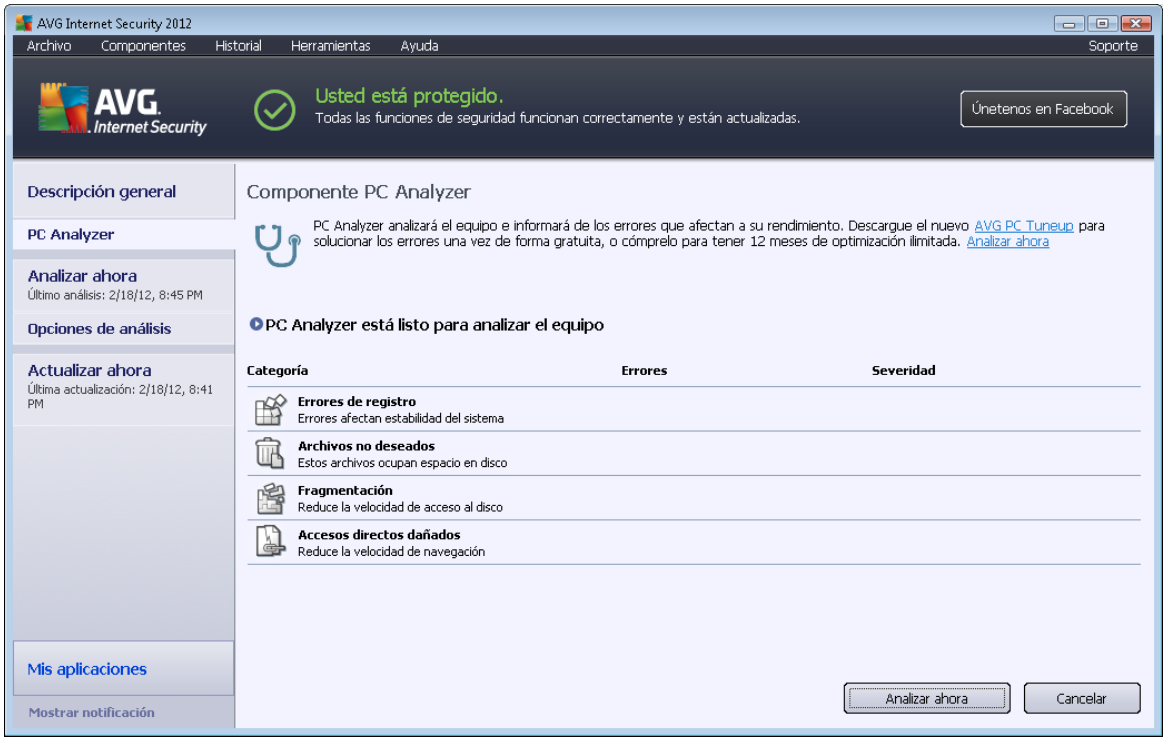
Botones de control

Los botones de control disponibles en la pestaña ***Visor de LSP*** son los siguientes:

- ***Ocultar LSP de Windows***: para incluir LSP de Windows en la lista, quite la marca de este elemento.
- ***Atrás***: le lleva al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*).

6.7. PC Analyzer

El componente ***PC Analyzer*** puede analizar el equipo para detectar problemas del sistema y puede proporcionarle una descripción general clara de lo que podría estar afectando al rendimiento general de su equipo. En la interfaz del usuario del componente puede ver un gráfico dividido en cuatro líneas que hacen referencia a las categorías correspondientes: errores de registro, archivos no deseados, fragmentación y accesos directos rotos:

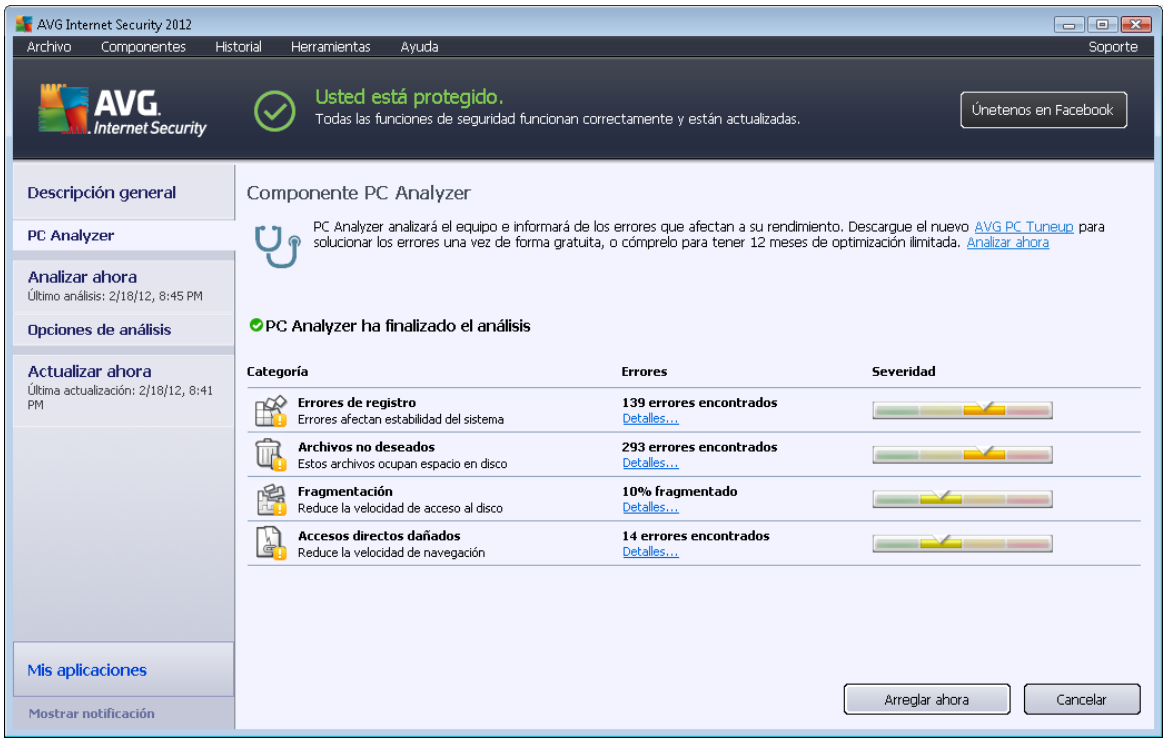


- ***Errores en el registro*** mostrará el número de errores en el Registro de Windows. Debido a que corregir el Registro exige un conocimiento más profundo, no recomendamos que intente solucionar los errores usted mismo.
- ***Archivos no deseados*** proporcionará el número de archivos sin los que se puede trabajar perfectamente. Normalmente se tratará de varios tipos de archivos temporales, así como de archivos de la Papelera de reciclaje.

- ***Fragmentación*** calculará el porcentaje del disco duro que está fragmentado, es decir, que se ha utilizado durante mucho tiempo de forma que la mayoría de los archivos ahora están separados en distintas partes del disco físico. Puede utilizar alguna herramienta de desfragmentación para solucionarlo.

- ***Accesos directos dañados*** le notificará si hay accesos directos que ya no funcionan, que llevan a ubicaciones no existentes, etc.

Para iniciar el análisis del sistema, presione el botón ***Analizar ahora***. Posteriormente podrá ver el progreso del análisis y los resultados directamente en el gráfico:



En la descripción general de los resultados se proporciona el número de problemas del sistema detectados (***Errores***) divididos según las categorías correspondientes analizadas. Los resultados del análisis también se mostrarán gráficamente en un eje en la columna ***Severidad***.

Botones de control

- ***Analizar ahora*** (*se muestra antes de que se inicie el análisis*): presione este botón para ejecutar el análisis del equipo inmediatamente

- ***Reparar ahora*** (*se muestra cuando el análisis ha terminado*): presione el botón para ir al sitio Web de AVG (http://www.avg.com/), en la página en la que se proporciona información detallada y actualizada sobre el componente ***PC Analyzer***

- ***Cancelar***: presione este botón para detener el análisis en ejecución o para volver al cuadro de diálogo principal de AVG predeterminado (*descripción general de los componentes*)

cuando el análisis se haya completado

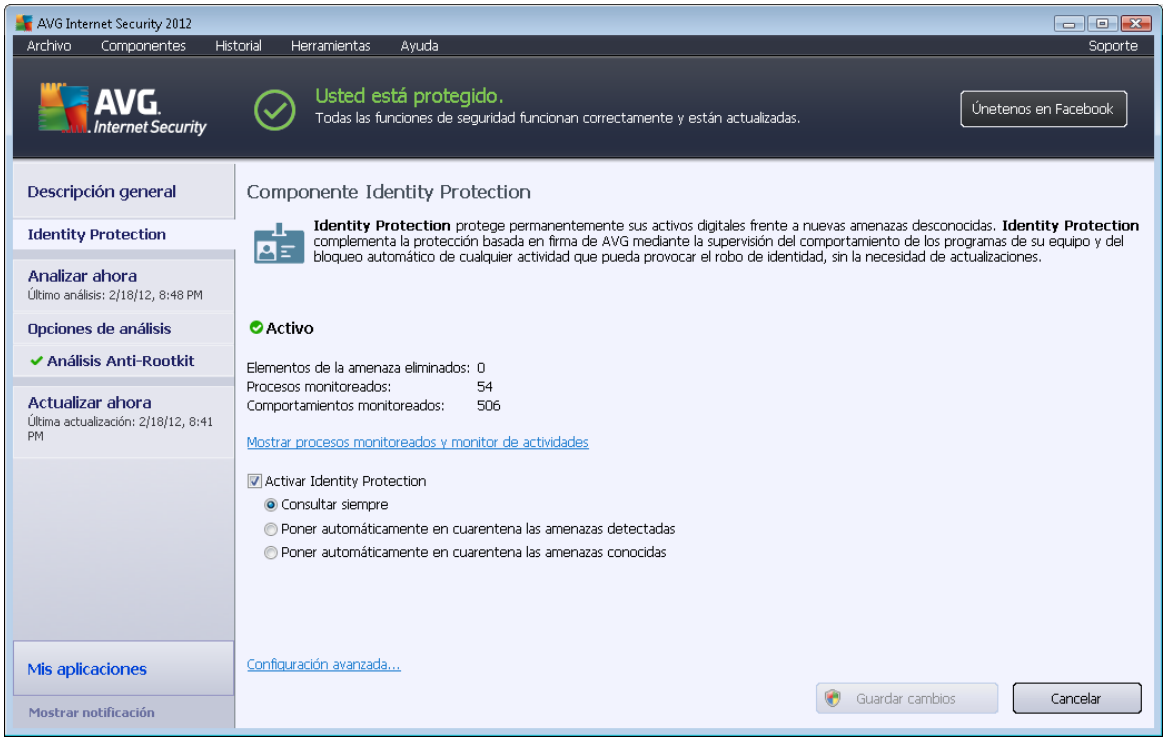
6.8. Identity Protection

Identity Protection es un componente anti-malware que ofrece protección contra todo tipo de malware (*spyware, bots, robo de identidad, ...*) mediante tecnologías conductuales que proporcionan protección día cero frente a nuevos virus. ***Identity Protection*** va dirigido a prevenir posibles robos de contraseñas, detalles de cuentas bancarias, números de tarjeta de crédito y otros datos digitales personales de valor ocasionados por toda clase de software malicioso (*malware*) en su equipo. Asegura que todos los programas que se ejecuten en su equipo o en su red compartida funcionen correctamente. ***Identity Protection*** detecta y bloquea comportamientos sospechosos de forma continua, y protege su equipo de cualquier malware nuevo.

Identity Protection da a su equipo protección en tiempo real contra amenazas nuevas e incluso desconocidas. Supervisa todos los procesos *(incluso los ocultos)* y más de 285 comportamientos diferentes, y puede determinar si está ocurriendo algo malicioso dentro de su sistema. Por este motivo, hasta puede mostrar amenazas que aún no están descritas en la base de datos de virus. Cuando una parte de código desconocida llega a su equipo, inmediatamente se comprueba si tiene un comportamiento malicioso y se realiza un seguimiento. Si se considera que el archivo es malicioso, ***Identity Protection*** eliminará el código, lo trasladará a la Bóveda de virus y deshará los cambios que hayan podido realizarse en el sistema *(inyecciones de código, cambios del registro, apertura de puertos, etc.)*. No es necesario iniciar un análisis para estar protegido. Esta tecnología es muy proactiva, raras veces necesita actualización y siempre está de guardia.

Identity Protection es una protección complementaria a Anti-Virus. Se recomienda encarecidamente tener instalados ambos componentes para que su equipo cuente con la protección más completa.

6.8.1. Interfaz de Identity Protection



El cuadro de diálogo Identity Protection proporciona una breve descripción de las funciones básicas del componente, su estado *(Activo)* y algunos datos estadísticos:

- ***Elementos de amenaza eliminados***: proporciona el número de aplicaciones detectadas como malware y eliminadas
- ***Procesos monitoreados***: número de aplicaciones actualmente en ejecución que monitorea IDP
- ***Comportamientos monitoreados***: número de acciones específicas en ejecución dentro de las aplicaciones monitoreadas

Más abajo encontrará el vínculo Mostrar procesos monitoreados y monitor de actividades que le llevará a la interfaz del usuario del componente Herramientas del sistema, donde puede ver una descripción general detallada de todos los procesos monitoreados.

Configuración básica de Identity Protection

En la parte inferior del cuadro de diálogo, puede editar varias funciones básicas del componente:

- ***Activar Identity Protection*** (*activada de forma predeterminada*): seleccione esta opción para activar el componente IDP y para abrir más opciones de edición.

  En algunos casos, ***Identity Protection*** puede indicar que un archivo legítimo es sospechoso

o peligroso. Dado que ***Identity Protection*** detecta amenazas según el comportamiento de éstas, esto suele producirse cuando un programa intenta supervisar presiones de teclas, instalar otros programas o cuando se instala un controlador nuevo en el equipo. Por lo tanto, seleccione una de las siguientes opciones especificando el comportamiento del componente ***Identity Protection*** en caso de detectarse una actividad sospechosa:

  - ***Consultar siempre***: si se detecta una aplicación como malware, se le preguntará si se debe bloquear (*esta opción está activada de forma predeterminada y se recomienda no cambiarla a menos que tenga una razón real para hacerlo*)
  - ***Poner automáticamente en cuarentena las amenazas detectadas***: todas las aplicaciones detectadas como malware se bloquearán automáticamente
  - ***Poner automáticamente en cuarentena las amenazas conocidas***: sólo se bloquearán aquellas aplicaciones que se detectan con absoluta certeza como malware

- ***Configuración avanzada...***: haga clic en el vínculo para ir al cuadro de diálogo respectivo de Configuración avanzada de **AVG Internet Security 2012**. En este cuadro de diálogo puede editar de forma detallada la configuración del componente. No obstante, tenga en cuenta que, de forma predeterminada, todos los componentes están configurados de modo que **AVG Internet Security 2012** proporcione un rendimiento óptimo y la máxima seguridad. A no ser que haya un motivo real para hacerlo, se recomienda mantener la configuración predeterminada.

Botones de control

Los botones de control disponibles dentro de la interfaz de ***Identity Protection*** son:

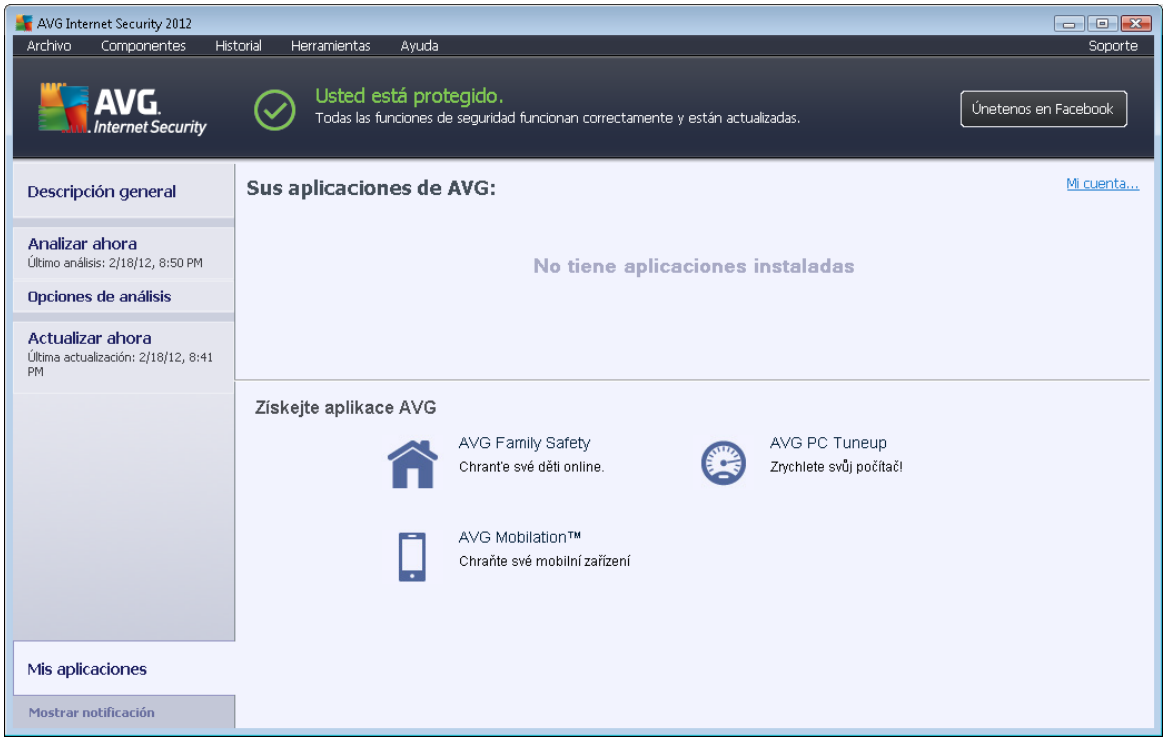
- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo
- ***Cancelar***: presione este botón para volver al cuadro de diálogo principal de AVG ***predeterminado*** (*descripción general de los componentes*)

6.9. Remote Administration

El componente ***Remote Administration*** sólo se muestra en la interfaz del usuario de **AVG Internet Security 2012** si ha instalado la versión Business Edition de su producto *(para obtener información acerca de la licencia usada en la instalación, consulte la pestaña Versión del cuadro de diálogo Información que se puede abrir a través del elemento de menú del sistema Soporte)*. Para obtener una descripción detallada de las opciones y funciones del componente en el sistema AVG Remote Administration, consulte la documentación específica dedicada a este tema exclusivamente. Esta documentación está disponible para su descarga en el sitio Web de AVG (http://www.avg.com/), en la sección ***Centro de soporte / Descarga / Documentación***.

7. Mis aplicaciones

El cuadro de diálogo ***Mis aplicaciones*** *(se puede acceder mediante el botón Mis aplicaciones directamente desde el cuadro de diálogo principal de AVG)* proporciona una descripción general de las aplicaciones independientes de AVG, instaladas en su equipo o listas para instalarse de forma opcional.



El cuadro de diálogo se divide en dos secciones:

- ***Sus aplicaciones de AVG***: proporciona una descripción general de todas las aplicaciones independientes de AVG que ya están instaladas en su equipo;
- ***Obtener aplicaciones de AVG***: ofrece una descripción general de las aplicaciones independientes de AVG en las que usted puede estar interesado. Estas aplicaciones están listas para instalarse. La oferta cambia dinámicamente en base a su licencia, ubicación y otros criterios. Para obtener información detallada sobre estas aplicaciones, consulte el sitio Web de AVG (http://www.avg.com/).

A continuación, encontrará un breve resumen de todas las aplicaciones disponibles y una breve explicación sobre su función:

7.1. AVG Family Safety

AVG Family Safety le ayuda a proteger a sus hijos de sitios Web, contenido multimedia y búsquedas en línea inadecuados, y le brinda reportes sobre su actividad en línea. ***AVG Family Safety*** utiliza una tecnología de análisis de secuencias de teclas para supervisar las actividades de sus hijos, tanto en salas de chat como en redes sociales. Si detecta palabras, frases o contenido

utilizados para ofrecer un trato vejatorio a los niños en línea, se le notificará inmediatamente por SMS o correo electrónico. Esta aplicación le permite establecer el nivel adecuado de protección para cada uno de sus hijos y supervisarlos de manera individual mediante inicios de sesión únicos.

Para obtener información detallada, visite la página Web dedicada de AVG, donde también puede descargar el componente inmediatamente. Para hacerlo, puede utilizar el vínculo AVG Family Safety del cuadro de diálogo Mis aplicaciones.

7.2. AVG LiveKive

AVG LiveKive es específico para las copias de resguardo en línea en servidores seguros. ***AVG LiveKive*** realiza automáticamente una copia de resguardo de todos sus archivos, fotos y música en un lugar seguro, para que pueda compartirlos con su familia y amigos y tener acceso a ellos desde cualquier dispositivo con acceso a Internet, incluidos los dispositivos iPhone y Android. Entre las funciones de ***AVG LiveKive*** se encuentran las siguientes:

- Medida de seguridad en caso de que su equipo y/o disco duro resulten dañados
- Acceso a sus datos desde cualquier dispositivo conectado a Internet
- Organización sencilla
- Compartir con cualquier persona que autorice

Para obtener información detallada, visite la página Web dedicada de AVG, donde también puede descargar el componente inmediatamente. Para hacerlo, puede utilizar el vínculo AVG LiveKive del cuadro de diálogo Mis aplicaciones.

7.3. AVG Mobilation

AVG Mobilation protege su teléfono celular de virus y malware, y también le proporciona la capacidad de realizar un seguimiento de su teléfono inteligente de forma remota si se encuentra separado de él. Entre las funciones de ***AVG Mobilation*** se encuentran las siguientes:

- *Analizador de archivos* permite analizar la seguridad de los archivos en diferentes ubicaciones de almacenamiento;
- *Task Killer* permite detener una aplicación en caso de que el dispositivo se bloquee o funcione lento;
- *Bloqueador de aplicaciones* permite bloquear y proteger una o más aplicaciones con contraseñas para evitar el uso indebido;
- *Tune Up* recopila varios parámetros del sistema *(medidor de batería, uso del almacenamiento, ubicación y tamaño de la instalación de las aplicaciones, etc.)* en una sola vista centralizada para ayudarle a controlar el rendimiento del sistema;
- *Copia de resguardo de aplicaciones* permite realizar copias de resguardo de las aplicaciones en la tarjeta de memoria y recuperarlas más tarde;

- *Spam and Scam* permite marcar los mensajes instantáneos como spam y notificar sitios Web con virus;
- *Wipe personal data* borra sus datos personales de manera remota en caso de que le roben el teléfono;

- *Navegación segura en Internet* ofrece supervisión en tiempo real de las páginas Web que visita.

Para obtener información detallada, visite la página Web dedicada de AVG, donde también puede descargar el componente inmediatamente. Para hacerlo, puede utilizar el vínculo AVG Mobilation del cuadro de diálogo Mis aplicaciones.

7.4. AVG PC Tune Up

La aplicación AVG PC Tune Up es una herramienta avanzada para el análisis detallado y la corrección del sistema, respecto a cómo podría mejorarse la velocidad y el rendimiento general del equipo. ***Entre las funciones de AVG PC Tune Up*** se encuentran las siguientes:

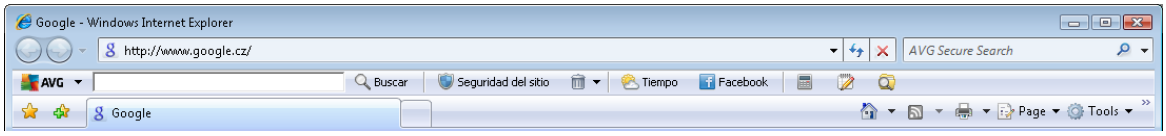
- *Limpiador del disco*: elimina archivos no deseados que hacen que el equipo funcione más lento.
- *Desfragmentador del disco*: desfragmenta las unidades de disco y optimiza la colocación de los archivos del sistema.
- *Limpiador del registro*: repara errores del registro para aumentar la estabilidad del PC.
- *Desfragmentador del registro*: compacta el registro eliminando vacíos que consumen memoria.
- *Doctor del disco*: detecta sectores dañados, clústeres perdidos y errores de directorio, y los arregla.
- *Optimizador de Internet*: adapta la configuración predeterminada a una conexión a Internet específica.
- *Borrador de rastros*: elimina el historial de uso del equipo y de Internet.
- *Limpiador de disco*: borra el espacio libre de los discos para evitar la recuperación de datos confidenciales.
- *Destructor de archivos*: borra archivos seleccionados de un disco o una memoria USB de modo que no se puedan recuperar.
- *Recuperación de archivos*: recupera archivos borrados por accidente de discos, memorias USB o cámaras.
- *Buscador de archivos duplicados*: le ayuda a encontrar y eliminar archivos duplicados que desperdician espacio en el disco.

- *Administrador de servicios*: desactiva servicios innecesarios que ralentizan el equipo.
- *Administrador de inicio*: permite a un usuario administrar programas que se inician automáticamente al arrancar Windows.
- *Administrador de desinstalación*: desinstala por completo los programas de software que ya no necesita.
- *Administrador de cambios*: permite a un usuario ajustar centenares de opciones de configuración ocultas de Windows.
- *Administrador de tareas*: ofrece una lista de todos los procesos y servicios en ejecución y los archivos bloqueados.
- *Explorador del disco*: muestra qué archivos ocupan más espacio en un equipo.
- *Información del sistema*: proporciona información detallada sobre el hardware y el software instalado.

Para obtener información detallada, visite la página Web dedicada de AVG, donde también puede descargar el componente inmediatamente. Para hacerlo, puede utilizar el vínculo AVG PC Tune Up del cuadro de diálogo Mis aplicaciones.

8. AVG Security Toolbar

AVG Security Toolbar es una herramienta que colabora estrechamente con el componente LinkScanner y que le ofrece la máxima seguridad mientras navega por Internet. En **AVG Internet Security 2012**, la instalación de ***AVG Security Toolbar*** es opcional; durante el proceso de instalación se le invita a decidir si se debe instalar el componente. ***AVG Security Toolbar*** está disponible directamente en su navegador de Internet. Por el momento, los navegadores de Internet admitidos son Internet Explorer (*versión 6.0 y superior*) y/o Mozilla Firefox (*versión 3.0 y superior*). No se admite ningún otro navegador *(en caso de que utilice un navegador de Internet alternativo, como Avant Browser, puede producirse un comportamiento inesperado)*.



AVG Security Toolbar consta de los siguientes elementos:

- ***Logotipo de AVG*** con el menú desplegable:
  - ***Utilizar AVG Secure Search***: le permite buscar directamente desde ***AVG Security Toolbar*** usando el motor de ***AVG Secure Search***. Como el servicio Search-Shield comprueba continuamente todos los resultados de búsqueda, puede sentirse completamente seguro cuando navegue por Internet.
  - ***Nivel actual de amenaza***: abre la página Web del laboratorio de virus con una visualización gráfica del nivel de amenaza actual en Internet.
  - ***Laboratorios AVG de amenazas***: abre el sitio Web del ***Laboratorio AVG de amenazas*** específico *(en http://www.avgthreatlabs.com)* donde puede encontrar información sobre la seguridad y el nivel de amenaza actual en línea de varios sitios Web.
  - ***Ayuda de la barra de herramientas***: abre la ayuda en línea donde se describe todo el funcionamiento de ***AVG Security Toolbar***.
  - ***Enviar comentarios del producto***: abre una página Web con un formulario que puede rellenar para darnos su opinión acerca de ***AVG Security Toolbar***.
  - ***Acerca de...***: abre una nueva ventana con información acerca de la versión de ***AVG Security Toolbar*** actualmente instalada.
- ***Campo de búsqueda*** : realiza búsquedas en Internet mediante ***AVG Security Toolbar*** para estar completamente seguro y protegido, dado que todos los resultados de búsqueda mostrados son cien por ciento seguros. Escriba la palabra clave o una frase en el campo de búsqueda y presione el botón ***Buscar*** *(o Intro)*. Todos los resultados de búsqueda se comprueban continuamente mediante el servicio Search-Shield *(dentro del componente Link Scanner)*.
- ***Seguridad de sitio***: este botón abre un nuevo diálogo con información sobre el nivel de la amenaza actual (*Actualmente seguro*) de la página que está visitando. Este breve resumen se puede ampliar y muestra detalles completos de todas las actividades de seguridad relacionadas

con la página directamente en la ventana del navegador (*Ver informe completo*):

- ***Eliminar***: el botón de la papelera de reciclaje ofrece un menú desplegable desde donde puede seleccionar si desea eliminar información de navegación, descargas, formularios en línea, o si desea eliminar todo su historial de búsquedas de una vez.

- ***Tiempo***: este botón abre un nuevo cuadro de diálogo con información acerca del tiempo actual en su ubicación, junto con la previsión del tiempo para los próximos dos días. Esta información se actualiza periódicamente, cada 3-6 horas. En este cuadro de diálogo, puede cambiar la ubicación deseada manualmente y decidir si desea ver la información de temperatura en grados Celsius o Fahrenheit.

- ***Facebook***: este botón le permite conectarse a la red social Facebook directamente desde ***AVG Security Toolbar***.

- Botones de acceso directo para el acceso rápido a estas aplicaciones: ***Calculadora***, ***Bloc de notas***, ***Explorador de Windows***.

9. AVG Do Not Track

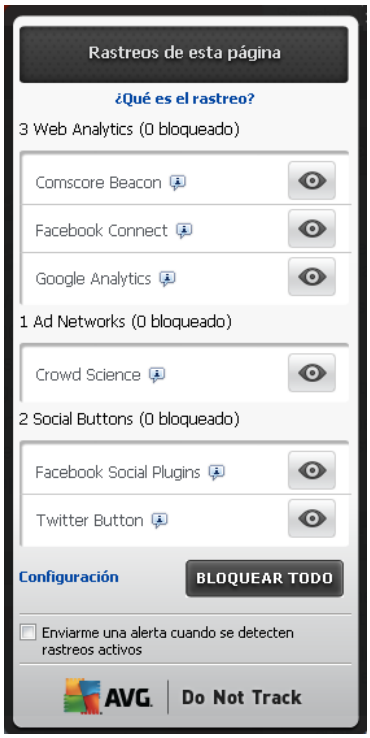
AVG Do Not Track le ayuda a identificar los sitios web que recopilan datos acerca de sus actividades en línea. Un icono en su navegador muestra los sitos Web o los anunciantes que recopilan datos acerca de sus actividades y le da la posibilidad de permitir o no esta práctica.

- ***AVG Do Not Track*** le proporciona información adicional sobre la política de privacidad de cada servicio respectivo, además de un enlace directo para excluirse del servicio, si se encuentra disponible.
- Además, ***AVG Do Not Track*** admite el protocolo W3C DNT para notificar automáticamente a los sitios que no desea que realicen seguimiento de sus actividades. Esta notificación está habilitada de manera predeterminada, pero se puede modificar en cualquier momento.
- ***El servicio de AVG Do Not Track*** se facilita bajo estos términos y condiciones.
- ***AVG Do Not Track*** está habilitado de manera predeterminada, pero puede deshabilitarse fácilmente en cualquier momento. Puede encontrar instrucciones en el artículo de las Preguntas frecuentes que trata cómo deshabilitar la función AVG Do Not Track.
- Para obtener más información sobre ***AVG Do Not Track***, visite nuestro sitio web.

Actualmente, la función ***AVG Do Not Track*** es compatible con Mozilla Firefox, Chrome e Internet Explorer. *(En Internet Explorer, el icono AVG Do Not Track se encuentra a la derecha de la barra de comandos. Si tiene algún problema para visualizar el icono AVG Do Not Track con la configuración predeterminada del navegador, asegúrese de tener activada la barra de comandos. Si, aún axial, no puede ver el icono, arrastre la barra de comandos hacia la izquierda para visualizar todos los iconos y botones disponibles en esa barra de herramientas.)*

9.1. Interfaz de AVG Do Not Track

Mientras está en línea, ***AVG Do Not Track*** lo advierte rápidamente cuando se detecta cualquier tipo de actividad de recopilación de datos. Visualizará el siguiente cuadro de diálogo:



Todos los servicios de recopilación de datos detectados se enumeran según el nombre en el resumen ***Rastreadores en esta página***. Son tres los tipos de actividades de recopilación de datos que reconoce ***AVG Do Not Track***:

- ***Análisis de web*** *(permitidos en forma predeterminada):* servicios empleados para mejorar el rendimiento y la experiencia del sitio web respectivo. En esta categoría encontrará servicios como Google Analytics, Omniture o Yahoo Analytics. Recomendamos que no bloquee los servicios de análisis de web, ya que es posible que el sitio web no funcione en la forma prevista.

- ***Botones sociales*** *(permitidos en forma predeterminada):* elementos diseñados para mejorar la experiencia en las redes sociales. Estos elementos los incluyen las redes sociales en el sitio que se visita. Pueden recopilar datos sobre su actividad en línea si ha iniciado sesión. Algunos ejemplos de botones sociales son: plugins sociales de Facebook, el botón de Twitter, Google +1.

- ***Redes publicitarias*** *(algunas están bloqueadas de manera predeterminada):* servicios que recopilan o comparten datos sobre su actividad en línea en varios sitios, ya sea directa o indirectamente, para ofrecerle publicidad personalizada en lugar de publicidad basada en contenido. Esto se determina en función de la política de privacidad de cada red publicitaria según se encuentre disponible en sus sitios Web. Algunas redes publicitarias están bloqueadas de manera predeterminada.

Nota: *según los servicios que se ejecutan en segundo plano en el sitio web, es posible que alguna de las tres secciones descritas arriba no aparezcan en el diálogo de AVG Do Not Track.*

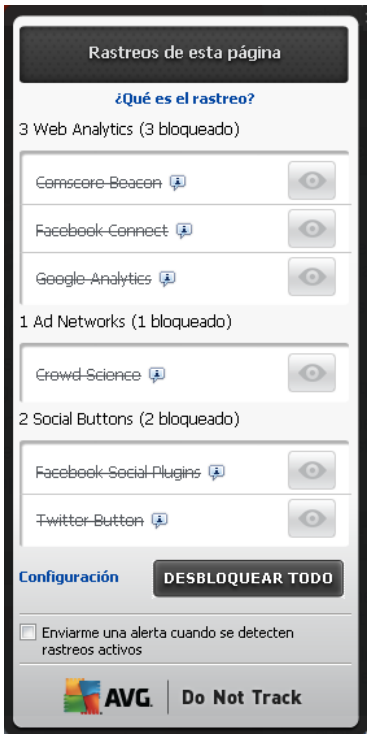
El diálogo también contiene dos hipervínculos:

- ***¿Qué es el rastreo?*** : haga clic en este vínculo en la sección superior del diálogo para llegar a la página web que proporciona una explicación detallada sobre los principios de rastreo y una descripción de los tipos de rastreo específicos.
- ***Configuración*** : haga clic en este vínculo en la sección inferior del diálogo para llegar a la página web en la que puede ajustar la configuración específica de varios parámetros ***AVG Do Not Track*** *(ver el capítulo Configuración de AVG Do Not Track para obtener información detallada)*

9.2. Información sobre los procesos de seguimiento

La lista de servicios de recopilación de datos detectados informa sólo el nombre del servicio específico. Para realizar una decisión experta acerca del bloqueo o el acceso del servicio correspondiente, es posible que necesite más información. Mueva su mouse sobre el elemento de la lista en cuestión. Aparecerá un icono de información con detalles sobre el servicio. Podrá aprender si el servicio recopila sus datos personales u otros datos disponibles; sabrá si esos datos se comparten con otros terceros y si los datos se almacenan para un posible uso posterior.

En la sección inferior del icono de información podrá ver el hipervínculo ***Política de privacidad*** que lo redirige al sitio web dedicado a la política de privacidad del servicio detectado respectivo.

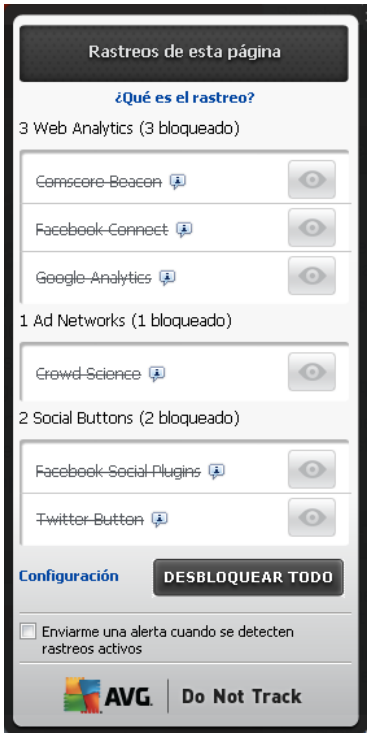


9.3. Bloqueo de los procesos de seguimiento

Con las listas de todos los análisis web, redes publicitarias o botones sociales, ahora tiene la opción de controlar qué servicios se deben bloquear. Tiene dos opciones:

- ***Bloquear todos***: al seleccionar este botón en la sección inferior del diálogo, indica expresamente que no desea ninguna actividad de recopilación de datos. *(Sin embargo, tenga en cuenta que esta acción quizás afecte la funcionalidad en la página web respectiva en la que el servicio funciona.)*

- Si no desea bloquear de una vez todos los servicios detectados, puede especificar si desea bloquear o permitir cada servicio individualmente. Puede permitir que algunos de los sistemas detectados se ejecuten *(por ej., los análisis web):* estos sistemas usan los datos recopilados para optimizar sus sitios web y de esta forma ayudan a mejorar el entorno común de Internet para todos los usuarios. Sin embargo, puede, al mismo tiempo, bloquear todas las actividades de recopilación de datos de los procesos clasificados como redes publicitarias. Simplemente haga clic en el icono junto al servicio respectivo para bloquear la recopilación de datos *(el nombre del proceso aparecerá tachado)* o para volver a permitir la recopilación de datos.

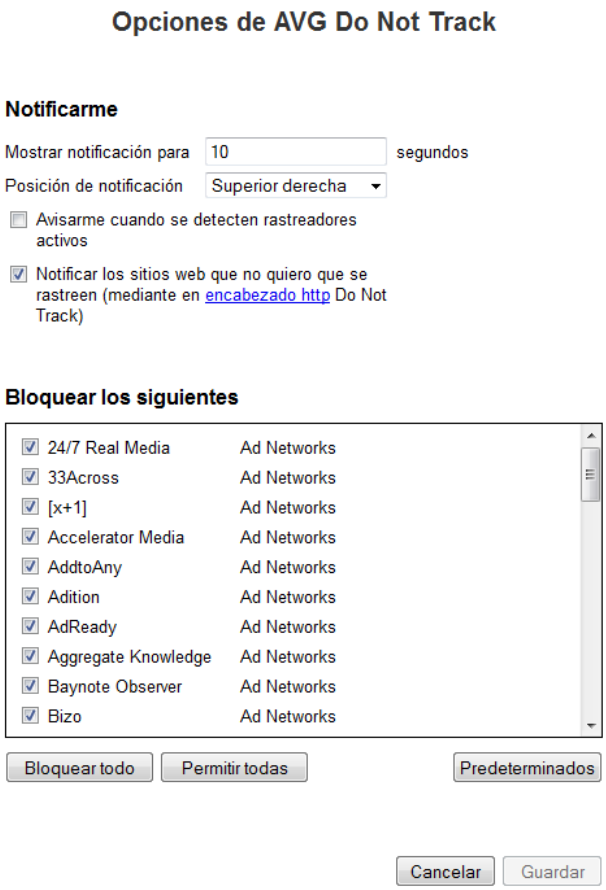


9.4. Configuración de AVG Do Not Track

Directamente en el diálogo ***AVG Do Not Track***, ya solo una opción de configuración: en la parte inferior puede ver la casilla de verificación ***Deseo recibir alertas cuando se detecten rastreadores activos***. Por defecto, esta opción está desmarcada. Marque la casilla de verificación para confirmar que desea que se le notifique cada vez que ingrese en una página web con un nuevo servicio de

recopilación de datos que aún no se haya bloqueado. Si está marcada, cuando ***AVG Do Not Track*** detecta un nuevo servicio de recopilación de datos en la página que está visitando, le muestra el diálogo de notificación en la pantalla. De lo contrario, sólo podrá saber si se ha detectado un servicio nuevo mediante el icono de ***AVG Do Not Track*** *(que se encuentra en la barra de comandos de su navegador)*, ya que éste cambiará de color, de verde a amarillo.

Sin embargo, en la parte inferior del diálogo de ***AVG Do Not Track***, encontrará el vínculo de ***Configuración***. Haga clic en el enlace para que se lo redireccione a la página web dedicada en la que puede especificar sus ***Opciones de AVG Do Not Track*** detalladas:



- ***Posición de notificación*** *(arriba a la derecha, por defecto)*: abra el menú desplegable para indicar en qué posición desea que aparezca el diálogo de ***AVG Do Not Track*** en su monitor.

- ***Mostrar notificación durante*** *(10 por defecto)*: en este campo, debe definir cuánto tiempo *(en segundos)*desea que la notificación de ***AVG Do Not Track*** permanezca visible en su pantalla. Puede especificar un número del 0 al 60 segundos *(si indica 0, no aparecerá la notificación en su pantalla)*.

- ***Avisarme cuando se detecten rastreadores activos****(apagado por defecto)*: marque esta casilla para confirmar que desea que se le notifique cada vez que ingrese a una página web

con un nuevo servicio de recopilación de datos que aún no ha sido bloqueado. Si está marcada, cuando ***AVG Do Not Track*** detecta un nuevo servicio de recopilación de datos en la página que está visitando, le muestra el diálogo de notificación en la pantalla. De lo contrario, sólo podrá saber si se ha detectado un servicio nuevo mediante el icono de ***AVG Do Not Track*** *(que se encuentra en la barra de comandos de su navegador)*, ya que éste cambiará de color, de verde a amarillo.

- ***Notificar a los sitios web que no deseo que rastreen mis actividades*** *(activada por defecto)**:*** mantenga esta opción activada si desea que ***AVG Do Not Track*** les informe a los proveedores de un servicio de recopilación de datos detectado que usted no desea que rastreen sus actividades.

- ***Bloquear las siguientes*** *(todos los servicios de recopilación de datos enumerados permitidos por defecto)*: en esta sección, puede ver un cuadro con una lista de servicios de recopilación de datos que pueden clasificarse como redes publicitarias. Por defecto, ***AVG Do Not Track*** bloquea ciertas redes publicitarias automáticamente y es decisión suya bloquear el resto o permitirlo. Para ello, haga clic en el botón ***Bloquear todos*** debajo de la lista.

Los botones de control disponibles dentro de la página de ***Opciones de AVG Do Not Track*** son las siguientes:

- ***Bloquear todos***: haga clic en este botón para bloquear directamente todos los servicios del cuadro de arriba que se clasifican como Redes publicitarias;

- ***Permitir todos***: haga clic en este botón para desbloquear directamente todos los servicios del cuadro de arriba que se clasifican como Redes publicitarias que se habían boqueado;

- ***Predeterminados***: haga clic en este botón para descartar todas las configuraciones personalizadas y restablecer la configuración predeterminada;

- ***Guardar***: haga clic en este botón para aplicar y guardar todos los datos de configuración especificados;

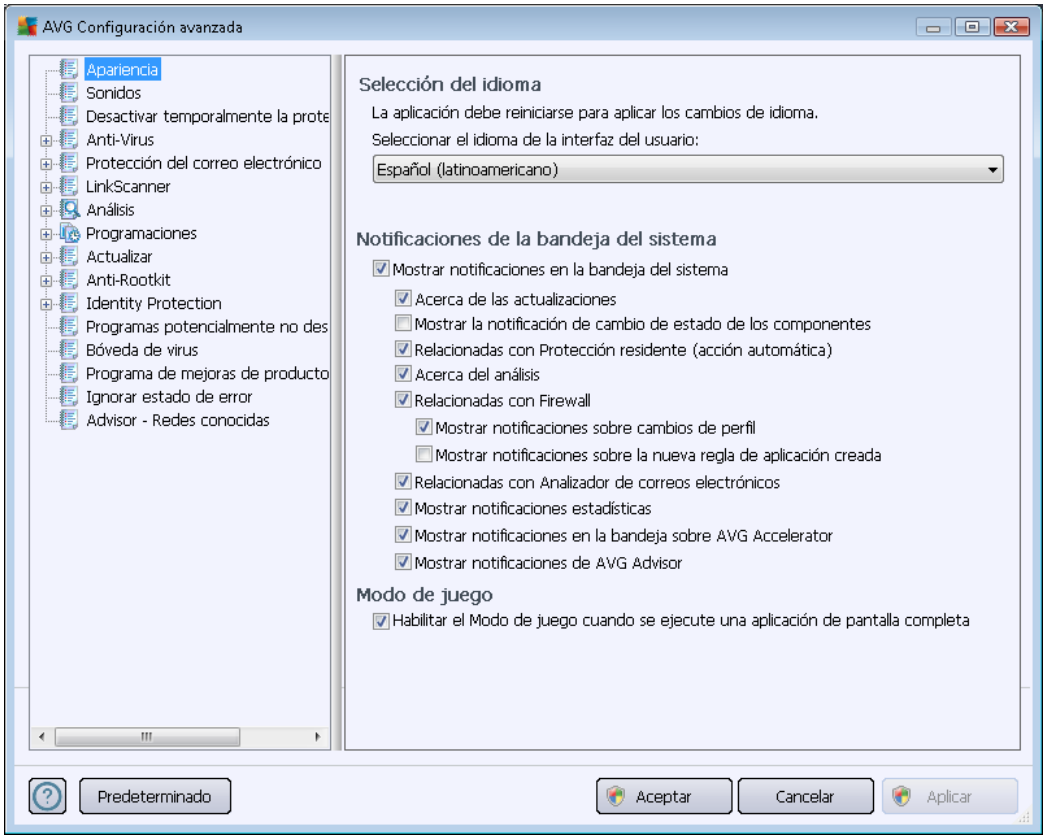
- ***Cancelar***: haga clic en este botón para cancelar todos los datos de configuración especificados anteriormente.

10. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG Internet Security 2012** se abre en una ventana nueva denominada ***Configuración avanzada de AVG***. La ventana está dividida en dos secciones: la parte izquierda ofrece una navegación organizada en forma de árbol hacia las opciones de configuración del programa. Seleccione el componente del que desea cambiar la configuración (*o su parte específica*) para abrir el diálogo de edición en la sección del lado derecho de la ventana.

10.1. Apariencia

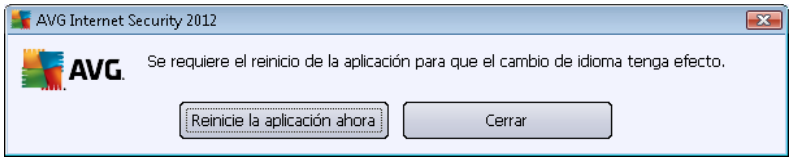
El primer elemento del árbol de navegación, ***Apariencia***, hace referencia a la configuración general de la interfaz del usuario de **AVG Internet Security 2012** y proporciona unas cuantas opciones básicas del comportamiento de la aplicación:



Selección del idioma

En la sección ***Selección del idioma*** puede seleccionar el idioma deseado en el menú desplegable. Este será el idioma que se utilice en toda la interfaz del usuario de **AVG Internet Security 2012**. El menú desplegable sólo ofrece los idiomas que haya seleccionado con anterioridad para instalarse durante el proceso de instalación (*consulte el capítulo Opciones personalizadas*), además del inglés (*que se instala automáticamente de forma predeterminada*). Para terminar de cambiar el idioma de su **AVG Internet Security 2012** debe reiniciar la aplicación. Por favor siga estos pasos:

- En el menú desplegable, seleccione el idioma deseado de la aplicación.
- Para confirmar la selección, presione el botón ***Aplicar*** *(esquina inferior derecha del cuadro de diálogo).*
- Presione el botón ***Aceptar*** para confirmar.
- Se abre un nuevo cuadro de diálogo que le informa de que para cambiar el idioma de la aplicación debe reiniciar su **AVG Internet Security 2012**
- Presione el botón ***Reinicie la aplicación ahora*** para aceptar el reinicio del programa y espere un momento a que el cambio de idioma surta efecto:



Notificaciones de la bandeja del sistema

En esta sección, puede suprimir la visualización de las notificaciones de la bandeja del sistema sobre el estado de la aplicación **AVG Internet Security 2012**. De forma predeterminada, se permite la visualización de las notificaciones del sistema. Se recomienda encarecidamente mantener esta configuración. Las notificaciones del sistema informan, entre otras cosas, de la ejecución del proceso de actualización o de análisis, o del cambio de estado de un componente de **AVG Internet Security 2012**. Es importante que ponga atención a estos anuncios.

Sin embargo, si por alguna razón decide que no desea que se muestren este tipo de notificaciones, o que sólo desea ver algunas de ellas *(relacionadas con un componente específico de AVG Internet Security 2012)*, puede definir y especificar sus preferencias seleccionando/quitando la marca de selección de las siguientes opciones:

- ***Mostrar notificaciones en la bandeja del sistema*** *(activada de manera predeterminada)*: de forma predeterminada se muestran todas las notificaciones. Quite la marca de selección de este elemento para desactivar completamente la visualización de todas las notificaciones del sistema. Cuando se encuentra activado, puede también seleccionar qué notificaciones en concreto deben visualizarse:
  - ***Acerca de las actualizaciones*** *(activada de forma predeterminada)*: decida si debe visualizarse información sobre la ejecución, el progreso y la finalización del proceso de actualización de **AVG Internet Security 2012**.
  - ***Mostrar la notificación de cambio de estado de los componentes*** *(desactivada de forma predeterminada)*: 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 notifica un problema en cualquier componente de **AVG Internet Security 2012**.

- ***Relacionadas con Protección residente (acción automática)*** *(activada de forma predeterminada)*: decida si debe visualizarse o suprimirse la información relativa a los procesos de guardado, copia y apertura de archivos (*esta configuración sólo se muestra si la opción Autoreparar de la Protección residente está activada*).

- ***Acerca del análisis*** *(activada de forma predeterminada)*: decida si debe visualizarse información sobre la ejecución automática del análisis programado, su progreso y resultados.

- ***Relacionadas con Firewall*** *(activada, de forma predeterminada)*: decida si debe visualizar información relativa al estado y los procesos relacionados con el Firewall, por ejemplo, las advertencias de activación/desactivación del componente, el posible bloqueo del tráfico, etc. . Este elemento proporciona dos opciones de selección más específicas *(para obtener una explicación detallada de cada una de ellas, consulte el capítulo Firewall de este documento)*:

  - ***Mostrar notificaciones sobre cambios de perfil*** *(activada de forma predeterminada)*: le informa de los cambios automáticos de los perfiles de Firewall.

  - ***Mostrar notificaciones sobre la nueva regla de aplicación creada*** *(desactivada de forma predeterminada)*: le informa de la creación automática de reglas de Firewall para nuevas aplicaciones en función de una lista de aplicaciones seguras.

- ***Relacionadas con Analizador de correos electrónicos*** *(activada de forma predeterminada)*: decida si debe visualizarse información sobre el análisis de todos los mensajes de correo electrónico entrantes y salientes.

- ***Mostrar notificaciones estadísticas*** *(activada de forma predeterminada)*: mantenga la opción seleccionada para permitir la notificación regular de revisión de estadísticas en la bandeja del sistema.

- ***Mostrar notificaciones en la bandeja sobre AVG Accelerator*** *(activada de forma predeterminada)*: decida si debe visualizarse información acerca de las actividades de ***AVG Accelerator***. ***AVG Accelerator*** es un servicio que mejora la reproducción de video en línea y que facilita la realización de descargas adicionales.

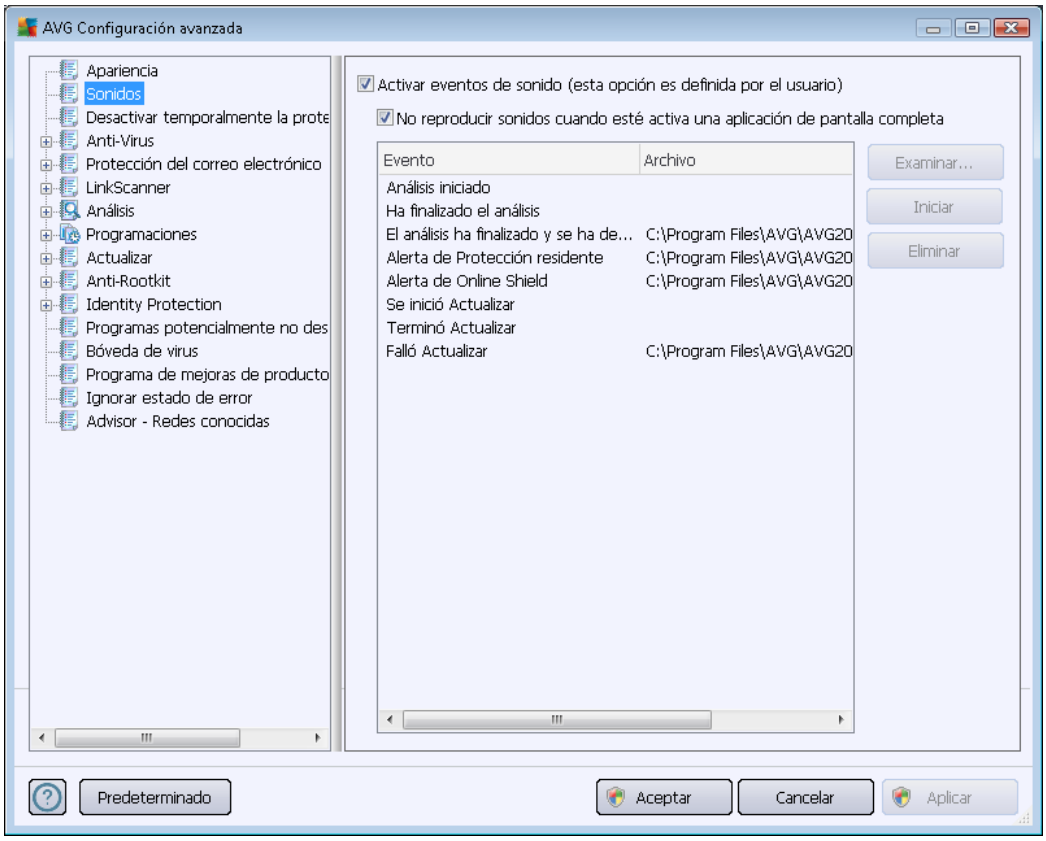
- ***Mostrar notificaciones de rendimiento de AVG Advisor*** *(activada de forma predeterminada)*: ***AVG Advisor*** vigila el rendimiento de los navegadores de Internet compatibles *(Internet Explorer, Chrome, Firefox, Opera y Safari)* y le informa en caso de que su navegador consuma una cantidad de memoria superior a la recomendada. En esta situación, el rendimiento de su equipo podría ralentizarse de forma importante, y se le aconseja que reinicie el navegador de Internet para aumentar la velocidad de los procesos. Deje activado el elemento ***Mostrar notificaciones de rendimiento de AVG Advisor*** para estar informado.

Modo de juego

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

10.2. Sonidos

En el cuadro de diálogo ***Sonidos***, puede especificar si desea que se le informe acerca de acciones específicas de **AVG Internet Security 2012** mediante una notificación sonora:



La configuración sólo es válida para la cuenta de usuario actual, es decir, cada usuario del equipo puede tener su propia configuración de sonido. Si desea permitir la notificación sonora, mantenga seleccionada la opción ***Activar eventos de sonido*** (*la opción está activada de forma predeterminada*) para activar la lista de todas las acciones pertinentes. Además, puede seleccionar la opción ***No reproducir sonidos cuando esté activa una aplicación de pantalla completa*** para suprimir la notificación sonora en situaciones en que podría resultar molesta *(consulte también la sección Modo de juego del capítulo Configuración avanzada/Apariencia de este documento)*.

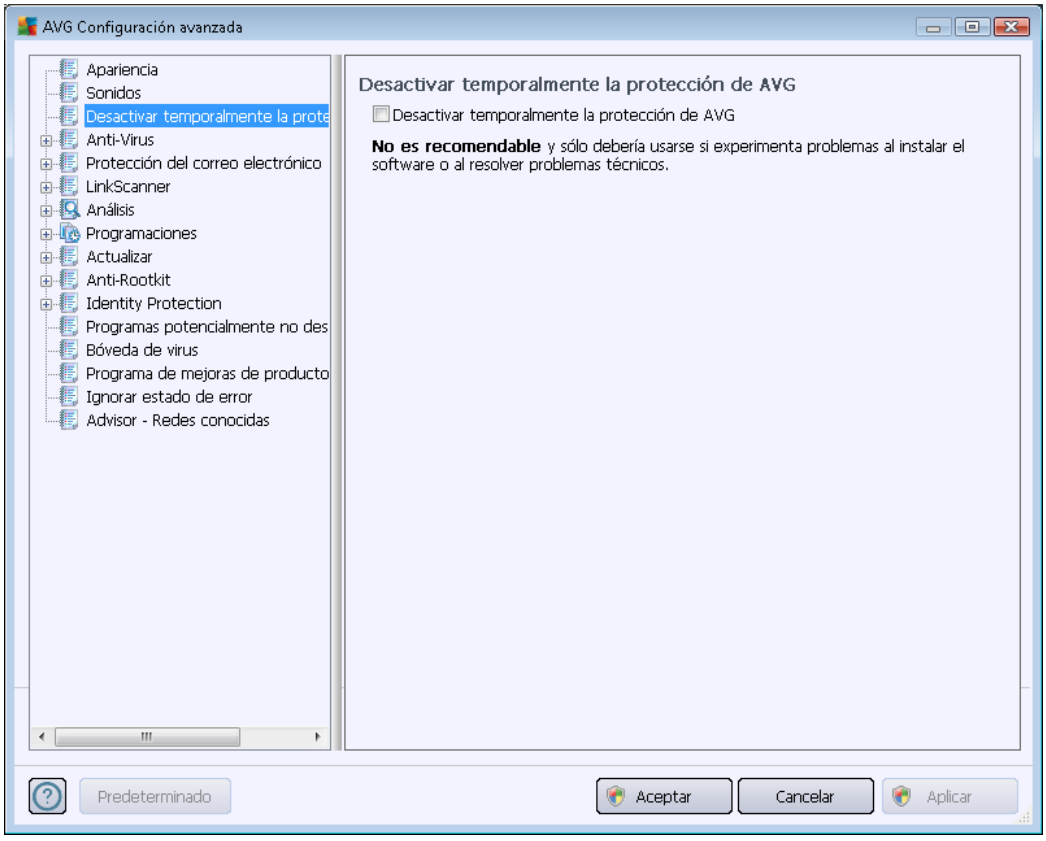
Botones de control

- ***Examinar***: una vez que ha seleccionado el evento respectivo de la lista, utilice el botón ***Examinar*** para buscar en el disco el archivo de sonido deseado que desea asignarle. *(Tenga en cuenta que por el momento sólo se admiten archivos de sonido *.wav.)*
- ***Reproducir***: para escuchar el sonido seleccionado, resalte el evento en la lista y presione el botón ***Reproducir***.
- ***Eliminar***: utilice el botón ***Eliminar*** para eliminar el sonido asignado a un evento específico.

10.3. Desactivar temporalmente la protección de AVG

En el cuadro de diálogo ***Desactivar temporalmente la protección de AVG*** tiene la opción de desactivar toda la protección que proporciona **AVG Internet Security 2012** a la vez.

Recuerde que no debe usar esta opción si no es absolutamente necesario.



En la mayoría de los casos, ***no es necesario*** desactivar **AVG Internet Security 2012** antes de instalar nuevo software o controladores, ni siquiera si el instalador o el asistente de software le sugiere que cierre los programas y aplicaciones que se estén ejecutando para asegurarse de que no se producen interrupciones no deseadas durante el proceso de instalación. Si realmente experimenta problemas durante la instalación, intente primero desactivar la protección residente (*Activar Protección residente*). Si tiene que desactivar temporalmente **AVG Internet Security 2012**, debe volver a activarlo en cuanto termine. Si está conectado a Internet o a una red durante el tiempo que el software antivirus está desactivado, su equipo será vulnerable ante los ataques.

Cómo desactivar la protección de AVG

- Marque la casilla de verificación ***Desactivar temporalmente la protección de AVG*** y presione el botón ***Aplicar*** para confirmar su elección
- En el cuadro de diálogo ***Desactivar temporalmente la protección de AVG*** recién abierto, especifique por cuánto tiempo desea desactivar su **AVG Internet Security 2012**. De forma

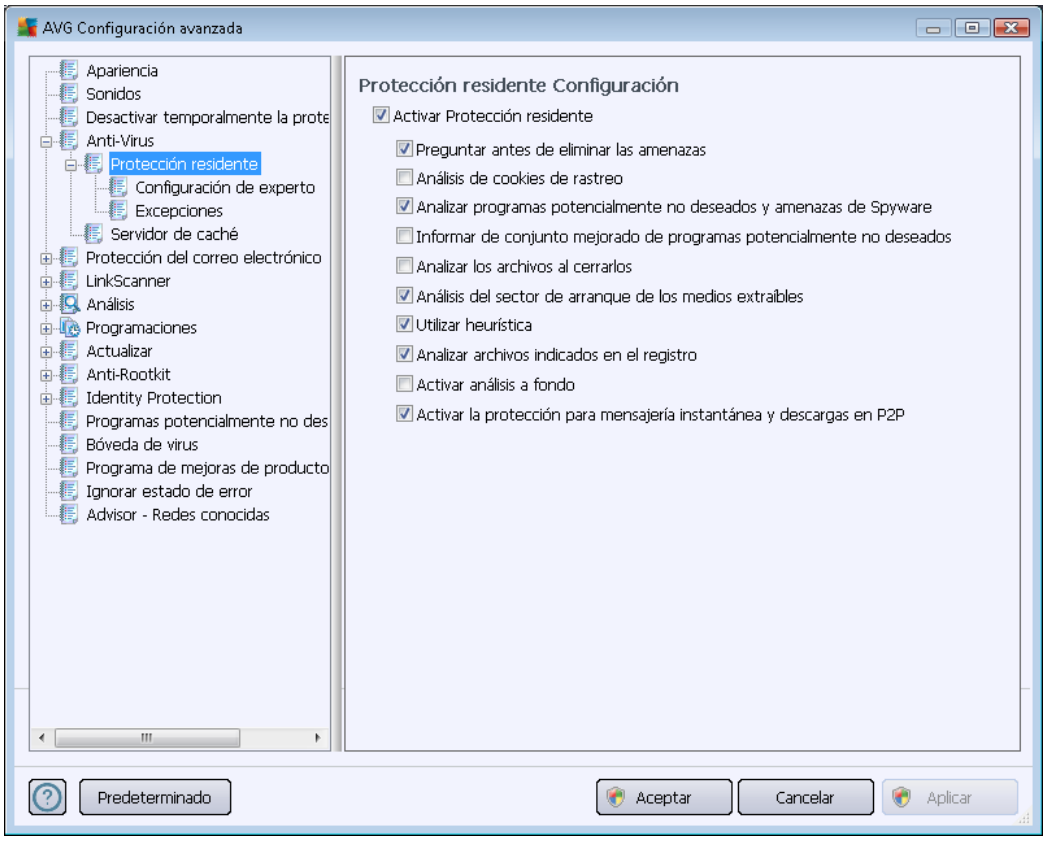
predeterminada, la protección permanece desactivada durante 10 minutos, que deberían ser suficientes para cualquier tarea común, como la instalación de nuevo software, etc. Tenga en cuenta que el límite de tiempo inicial que se puede configurar es de 15 minutos y que, por motivos de seguridad, no se puede sustituir por un valor personalizado. Transcurrido el periodo de tiempo especificado, todos los componentes desactivados se activarán de nuevo de forma automática.

10.4. Anti-Virus

El componente ***Anti-Virus*** protege el equipo continuamente de todos los tipos de virus y spyware conocidos *(incluido el denominado malware inactivo y no peligroso, es decir, malware que se ha descargado, pero que no se ha activado aún)*.

10.4.1. Protección residente

Protección residente realiza la protección activa de archivos y carpetas contra virus, spyware y otro malware.



En el cuadro de diálogo ***Configuración de Protección residente***, puede activar o desactivar completamente la protección residente seleccionando o deseleccionando el elemento ***Activar Protección residente*** (*esta opción está activada de forma predeterminada*). Además, puede seleccionar qué funciones de la protección residente se deben activar:

- ***Preguntar antes de eliminar las amenazas***(*activado de forma predeterminada*): seleccione esta opción para que la Protección residente no realice ninguna acción de manera automática; si la selecciona, muestra un diálogo que describe la amenaza detectada y le permite decidir qué debe hacer. Si deja la casilla sin seleccionar, **AVG Internet Security 2012** reparará la infección automáticamente y, si no es posible, el objeto se moverá a la Bóveda de virus.

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

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

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

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

- ***Analizar los archivos al cerrarlos*** (*desactivada de forma predeterminada*): el análisis al c errar garantiza que AVG analiza los objetos activos (por ejemplo, aplicaciones, documentos, etc.) cuando se abren y también cuando se cierran; esta función le ayuda a proteger el equipo frente a algunos tipos de virus sofisticados.

- ***Análisis del sector de arranque de los medios extraíbles*** (*activada de manera predeterminada*)

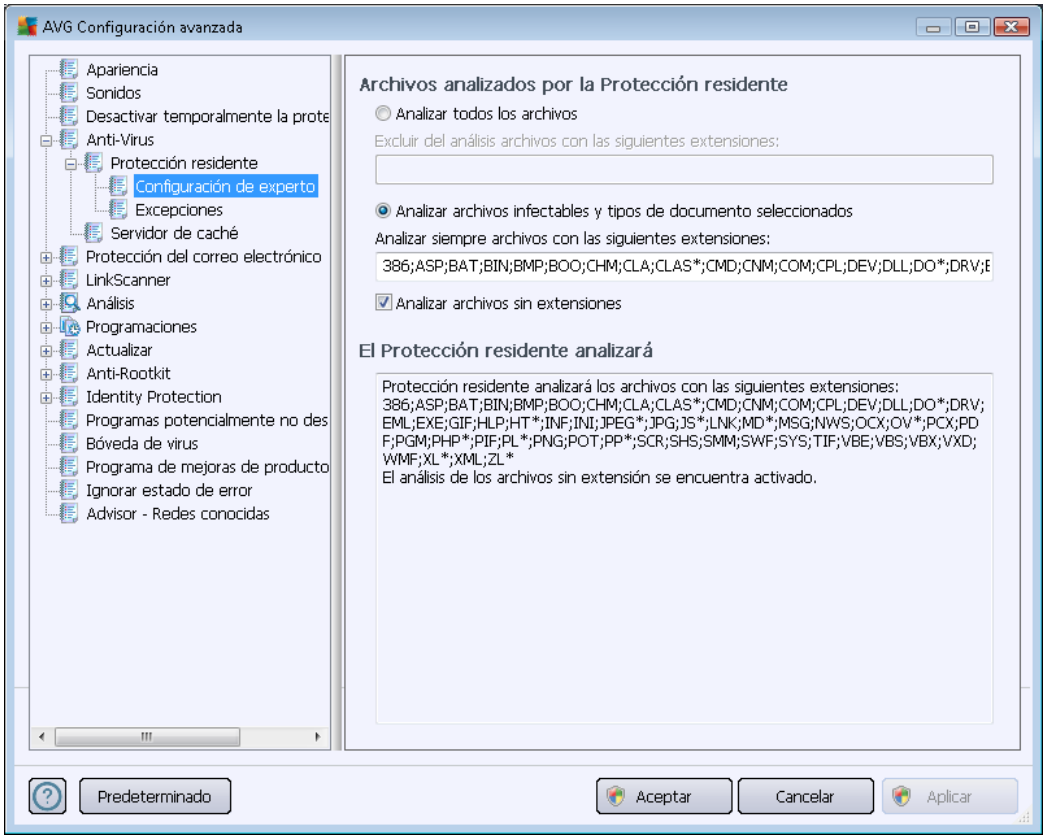
- ***Utilizar heurística*** (*activada de forma predeterminada*): el análisis heurístico se utilizará para la detección (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).

- ***Analizar archivos indicados en el registro*** (*activado de manera predeterminada*): este parámetro define que AVG analizará todos los archivos ejecutables añadidos al registro de inicio para evitar que una infección conocida se ejecute durante el siguiente inicio del equipo.

- ***Activar análisis a fondo*** (*desactivada de forma predeterminada*): en determinadas situaciones (*en un estado de extrema emergencia*) puede marcar esta opción para activar los algoritmos más minuciosos, que comprobarán a fondo todos los objetos remotamente amenazantes. Pero recuerde que este método consume mucho tiempo.

- ***Activar la protección para mensajería instantánea y descargas en P2P*** (*activado de forma predeterminada*): seleccione este elemento si desea comprobar que la comunicación de mensajería instantánea (*p. ej., ICQ, MSN Messenger, etc.*) y las descargas punto a punto (P2P) estén libres de virus.

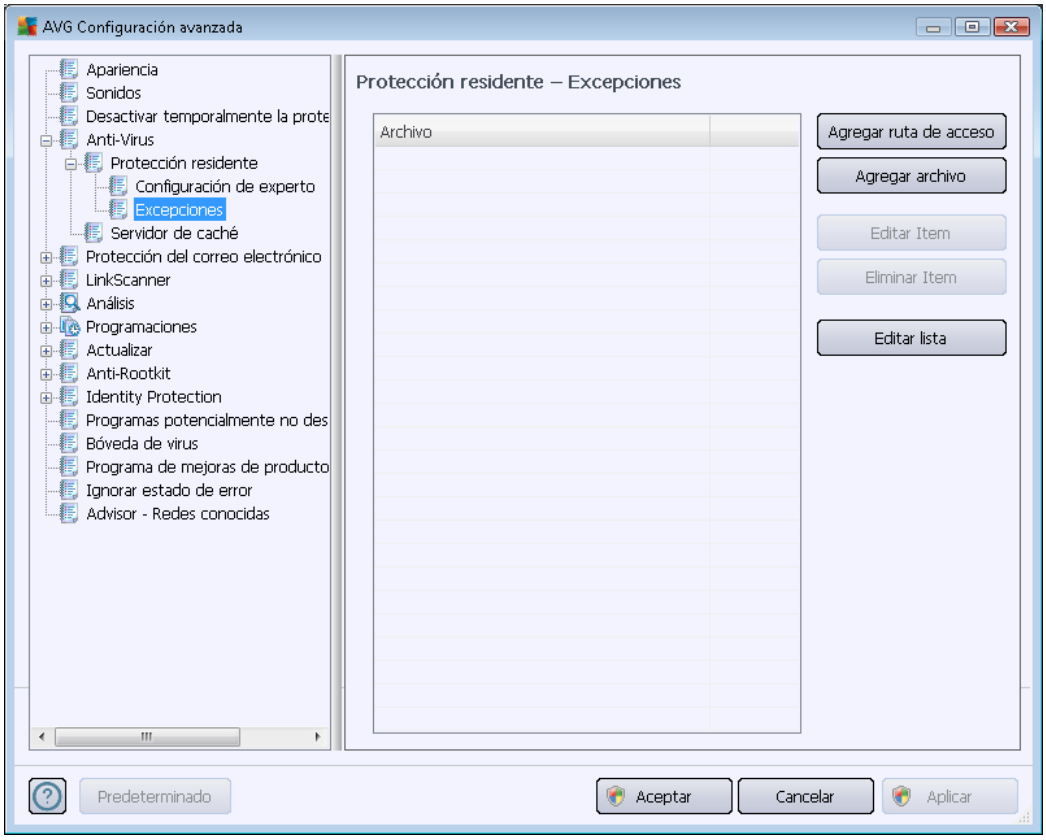
En el cuadro de diálogo ***Archivos analizados por Protección residente*** es posible configurar qué archivos se van a analizar (*por medio de las extensiones específicas*):



Marque la casilla de verificación respectiva para decidir si desea ***Analizar todos los archivos*** o solamente ***Analizar archivos infectables y tipos de documento seleccionados***. Si eligió la última opción, puede especificar además una lista de extensiones que definen los archivos que se deben excluir del análisis y una lista de extensiones de archivo que determinan los archivos que se deben analizar siempre.

Seleccione la opción ***Analizar archivos sin extensiones*** (*activada de forma predeterminada*) para asegurarse de que incluso los archivos sin extensión y los de formato desconocido se analicen con la Protección residente. Recomendamos mantener esta característica activada, ya que los archivos sin extensión son sospechosos.

La sección posterior denominada ***Protección residente analizará*** también resume la configuración actual y muestra una descripción general detallada de lo que analizará la ***Protección residente***.



El cuadro de diálogo ***Protección residente: Excepciones*** ofrece la posibilidad de definir archivos o carpetas que deben excluirse del análisis de la ***Protección residente***.

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

Botones de control

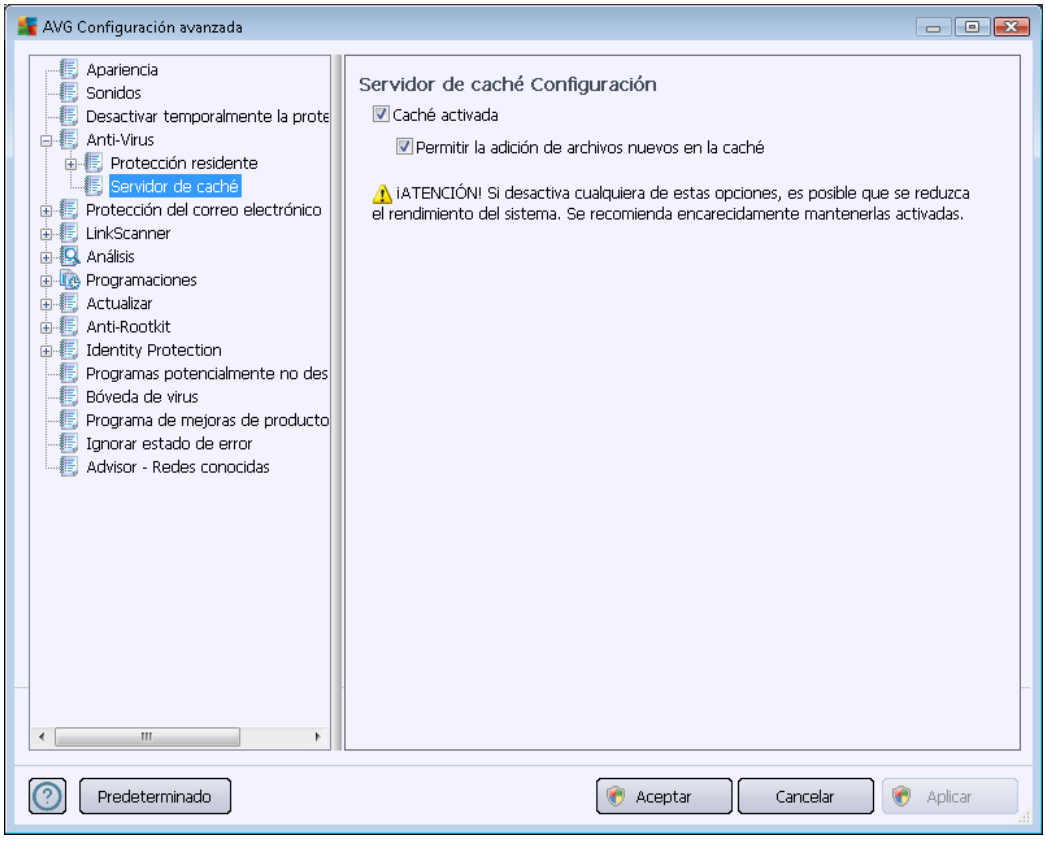
El cuadro de diálogo proporciona los siguientes botones de control:

- ***Agregar ruta de acceso***: especifica el directorio o directorios que deben excluirse del análisis seleccionándolos uno por uno en el árbol de navegación del disco local
- ***Agregar archivo***: especifica los archivos que deben excluirse del análisis seleccionándolos uno por uno en el árbol de navegación del disco local
- ***Editar elemento***: permite editar la ruta de acceso especificada a un archivo o una carpeta que se ha seleccionado
- ***Eliminar elemento***: le permite eliminar la ruta de acceso a un elemento seleccionado de la lista
- ***Editar lista***: le permite editar toda la lista de excepciones en un nuevo cuadro de diálogo

que funciona como un editor de texto estándar

10.4.2. Servidor de caché

El cuadro de diálogo ***Configuración del servidor de caché*** hace referencia al proceso del servidor de caché diseñado para aumentar la velocidad de todos los tipos de análisis de **AVG Internet Security 2012**:



El servidor de caché recopila y mantiene información de los archivos confiables (*se considera que un archivo es confiable si está firmado con una firma digital de un origen de confianza*). Estos archivos se consideran automáticamente seguros y no es necesario analizarlos de nuevo, por lo que se omiten durante el análisis.

El cuadro de diálogo ***Configuración del servidor de caché*** ofrece las siguientes opciones de configuración:

- ***Caché activada*** (*activada de forma predeterminada*): quite la marca de la casilla para desactivar el ***Servidor de caché*** y vacíe la memoria caché. Tenga en cuenta que el análisis puede ralentizar y reducir el rendimiento general de su equipo, porque primero se analizarán todos y cada uno de los archivos en uso en busca de virus y spyware.

- ***Permitir la adición de archivos nuevos en la caché*** (*activada de forma predeterminada*): quite la marca de la casilla para dejar de agregar archivos en la memoria caché. Se guardarán y usarán todos los archivos ya almacenados en caché hasta que el

almacenamiento en caché se desactive completamente o hasta la siguiente actualización de la base de datos de virus.

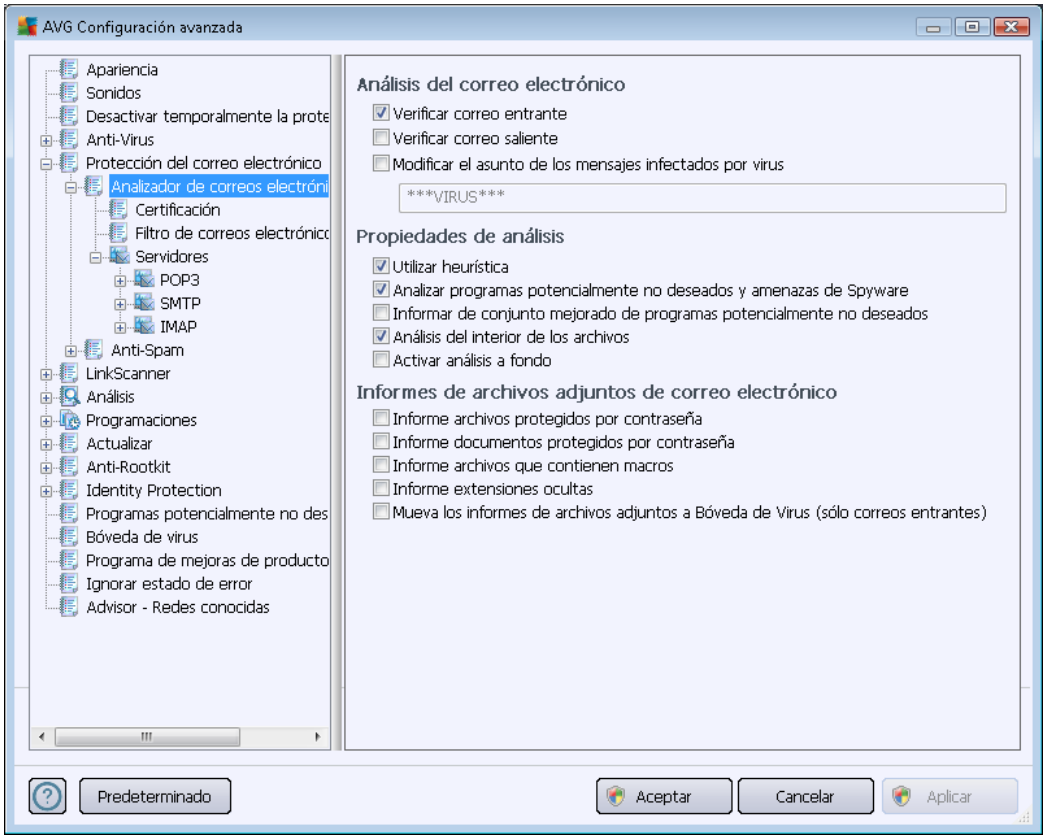
A no ser que tenga un buen motivo para desactivar el servidor de caché, se recomienda encarecidamente que mantenga la configuración predeterminada y deje ambas opciones activadas. De lo contrario, podría experimentar una disminución significativa de la velocidad y el rendimiento del sistema.

10.5. Protección del correo electrónico

En la sección ***Protección del correo electrónico***, puede editar la configuración detallada del Analizador de correos electrónicos y de Anti-Spam:

10.5.1. Analizador de correos electrónicos

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



Análisis del correo electrónico

En esta sección puede establecer la siguiente configuración básica para los mensajes de correo electrónico entrantes o salientes:

- ***Verificar correo entrante*** (*activada de forma predeterminada*): marque esta opción para activar o desactivar la opción de análisis de todos los mensajes de correo electrónico

enviados a su cliente de correo

- ***Verificar correo saliente*** (*desactivada de forma predeterminada*): marque esta opción para activar o desactivar la opción de analizar todos los correos electrónicos enviados desde su cuenta

- ***Modificar el asunto de los mensajes infectados por virus*** (*desactivada de forma predeterminada*): si desea que se le avise si el mensaje de correo electrónico analizado se detectó como infeccioso, marque este elemento y escriba el texto que desea en el campo de texto. Entonces este texto se agregará al campo "Asunto" de cada mensaje de correo electrónico detectado con el fin de facilitar la identificación y el filtrado. El valor predeterminado es ***VIRUS***, y recomendamos conservarlo.

Propiedades de análisis

En esta sección puede especificar cómo deben analizarse los mensajes de correo electrónico:

- ***Utilizar método heurístico*** (*activada de forma predeterminada*): seleccione esta opción para utilizar el método de detección heurístico al analizar mensajes de correo electrónico. Cuando esta opción está activada, se pueden filtrar los archivos adjuntos de correo electrónico no sólo por extensión sino que también se considerará el contenido real del archivo adjunto. El filtro se puede establecer en el cuadro de diálogo Filtro de correos electrónicos.

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

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

- ***Analizar el interior de los archivos*** (*activada de forma predeterminada*): seleccione esta opción para analizar el contenido de los archivos adjuntos a los mensajes de correo electrónico.

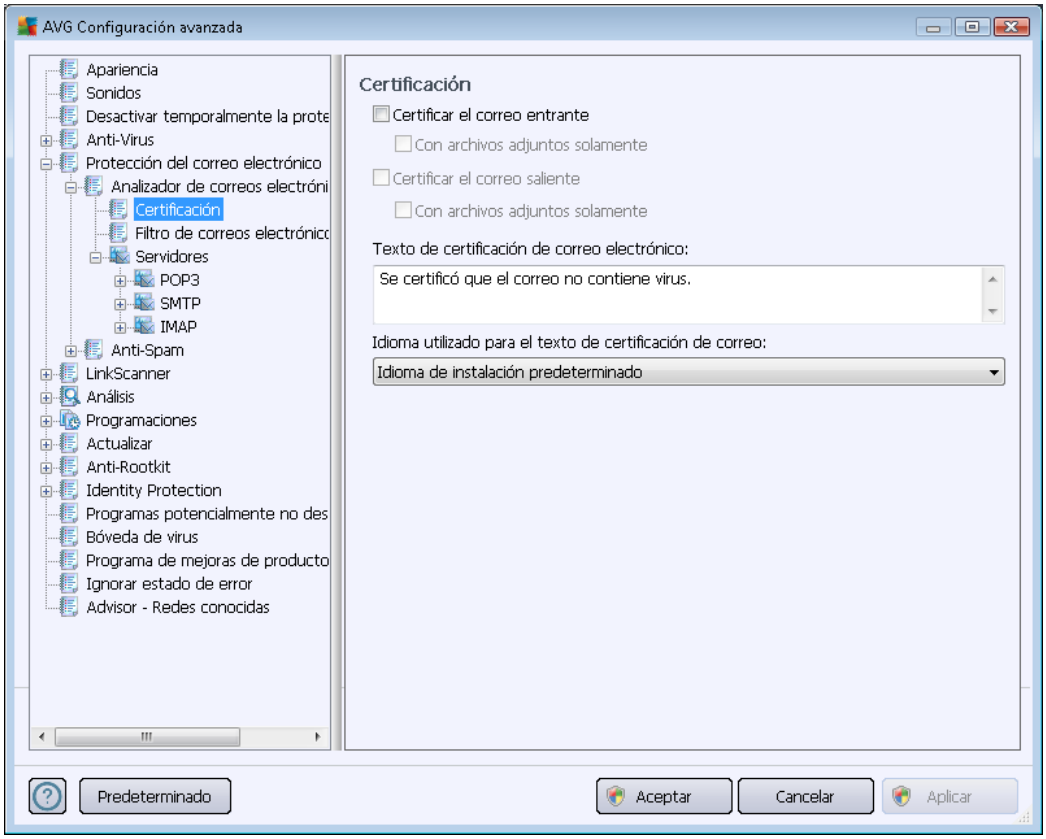
- ***Activar análisis a fondo*** (*desactivada de forma predeterminada*): en determinadas situaciones (*por ejemplo, sospechas de que el equipo está infectado por un virus o una vulnerabilidad*), puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

Informes de archivos adjuntos de correo electrónico

En esta sección se pueden establecer reportes adicionales acerca de archivos potencialmente peligrosos o sospechosos. Tenga en cuenta que no se mostrará ningún cuadro de diálogo de advertencia, sólo se agregará un texto de certificación al final del mensaje de correo electrónico, y todos esos reportes se enumerarán en el cuadro de diálogo Detección mediante el Analizador de correos electrónicos:

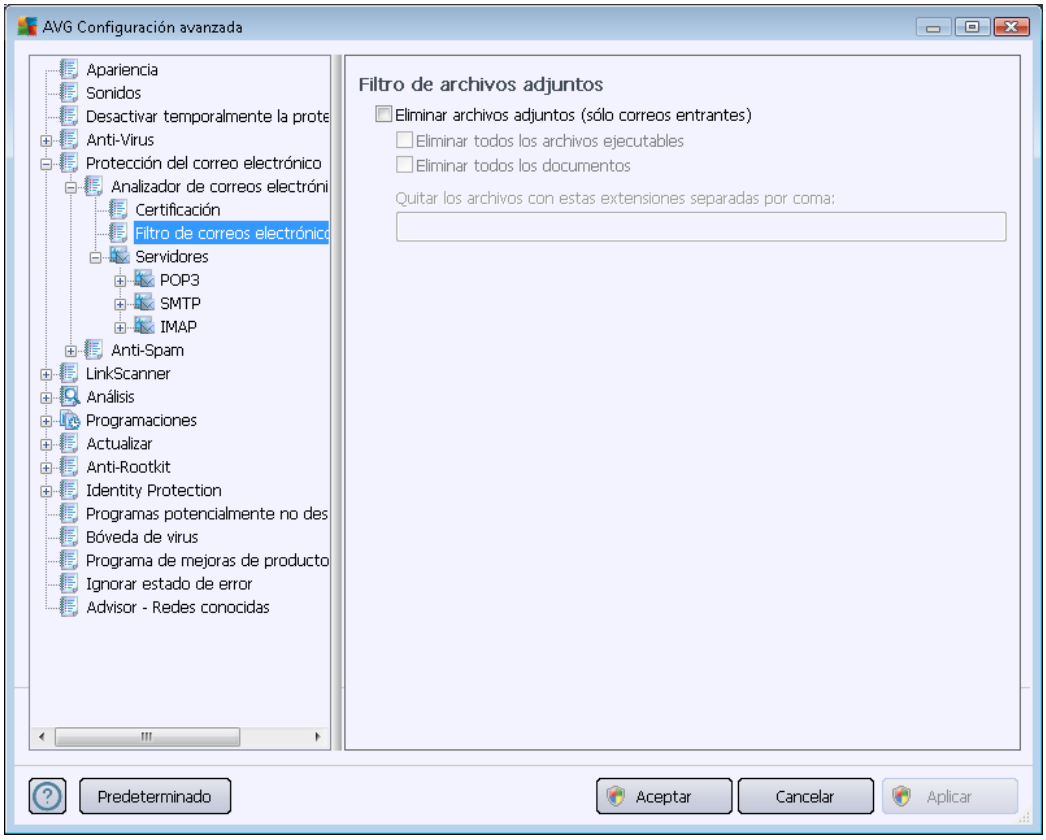
- ***Informar de los archivos protegidos por contraseña***: los archivos (*ZIP, RAR, etc.*) protegidos por contraseña no se pueden analizar en busca de virus; seleccione la casilla para informar de ellos como potencialmente peligrosos.
- ***Informar acerca de los documentos protegidos por contraseña***: no es posible analizar los documentos protegidos por contraseña en busca de virus; seleccione la casilla para informar de ellos como potencialmente peligrosos.
- ***Informar acerca de los archivos que contienen macros***: una macro es una secuencia predefinida de pasos encaminados a hacer que ciertas tareas sean más fáciles para el usuario *(las macros de MS Word son ampliamente conocidas*). Como tal, una macro puede contener instrucciones potencialmente peligrosas, y podría ser útil seleccionar la casilla para garantizar que los archivos con macros se reporten como sospechosos.
- ***Informar acerca de las extensiones ocultas***: las extensiones ocultas pueden hacer, por ejemplo, que un archivo ejecutable sospechoso "algo.txt.exe" parezca un archivo de texto simple inofensivo "algo.txt"; seleccione la casilla para informar de estos archivos como potencialmente peligrosos.
- ***Mueva los informes de archivos adjuntos a Bóveda de virus***: especifique si desea que se le notifique mediante correo electrónico acerca de los archivos protegidos con contraseña, los documentos protegidos por contraseña, los archivos que contienen macros y los archivos con extensión oculta detectados como un dato adjunto del mensaje del correo electrónico analizado. Si durante el análisis se identifica un mensaje en estas condiciones, defina si el objeto infeccioso detectado se debe mover a la Bóveda de virus.

En el cuadro de diálogo ***Certificación*** puede marcar las casillas de verificación específicas para decidir si desea certificar el correo entrante (***Certificar el correo entrante***) y/o el correo saliente (***Certificar el correo saliente***). Para cada una de estas opciones puede especificar además el parámetro ***Con archivos adjuntos solamente*** para que la certificación sólo se agregue a los mensajes de correo electrónico con archivos adjuntos:



De forma predeterminada, el texto de certificación consta de información básica que indica *Se certificó que el correo no contiene virus.* Sin embargo, esta información se puede ampliar o cambiar según sus necesidades: escriba el texto de certificación deseado en el campo ***Texto de certificación de correo electrónico***. En la sección ***Idioma utilizado para el texto de certificación de correo***, puede definir además el idioma en que se debe mostrar la parte de certificación generada automáticamente (*Se certificó que el correo no contiene virus*).

Nota: *tenga en cuenta que solo se mostrará en el idioma solicitado el texto predeterminado, y que el texto personalizado no se traducirá automáticamente.*



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

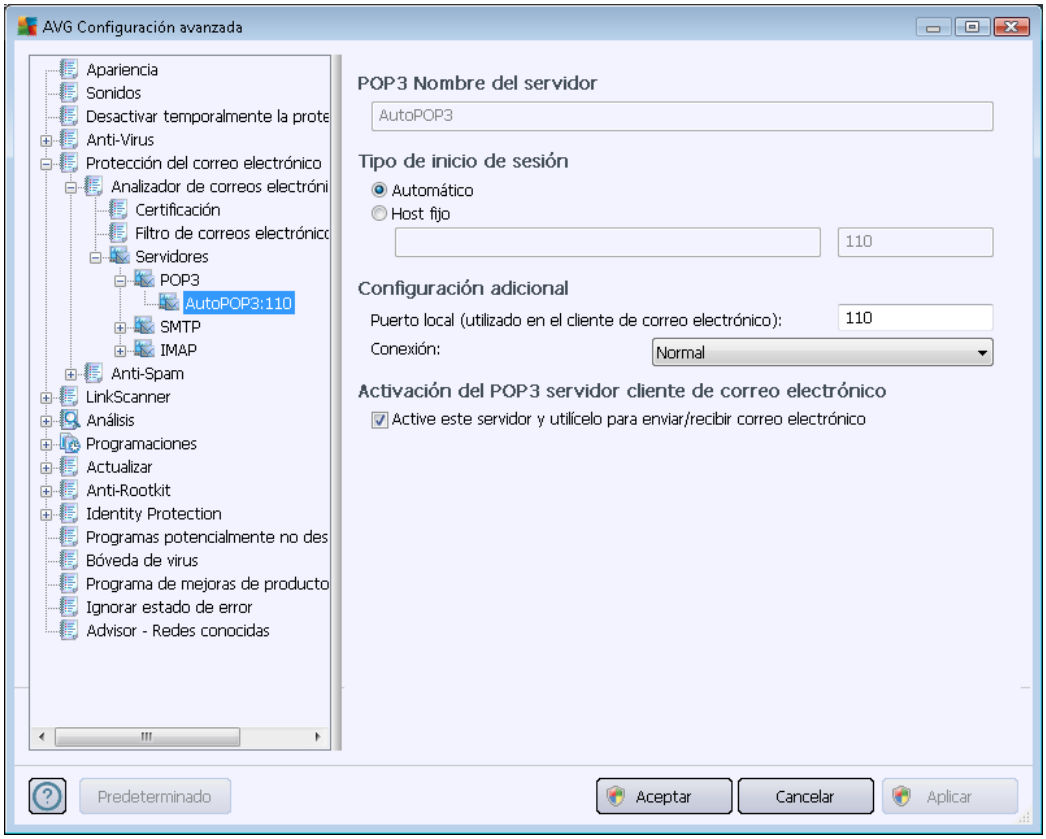
- ***Quitar todos los archivos ejecutables***: se eliminarán todos los archivos *.exe
- ***Quitar todos los documentos***: se eliminarán todos los archivos *.doc, *.docx, *.xls y *.xlsx
- ***Eliminar los archivos con las siguientes extensiones separadas por coma***: se eliminarán todos los archivos con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

En la sección ***Servidores***, puede editar los parámetros de los servidores de Analizador de correos electrónicos:

- Servidor POP3
- Servidor SMTP

- Servidor IMAP

Además, con el botón ***Agregar nuevo servidor***, puede definir un nuevo servidor para el correo entrante y saliente.



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

- ***Nombre del servidor POP3***: en este campo podrá especificar el nombre de los servidores nuevos (*para agregar un servidor POP3, haga clic con el botón secundario del mouse en el elemento POP3 del menú de navegación de la izquierda*). Para el servidor "AutoPOP3" creado automáticamente, este campo está desactivado.

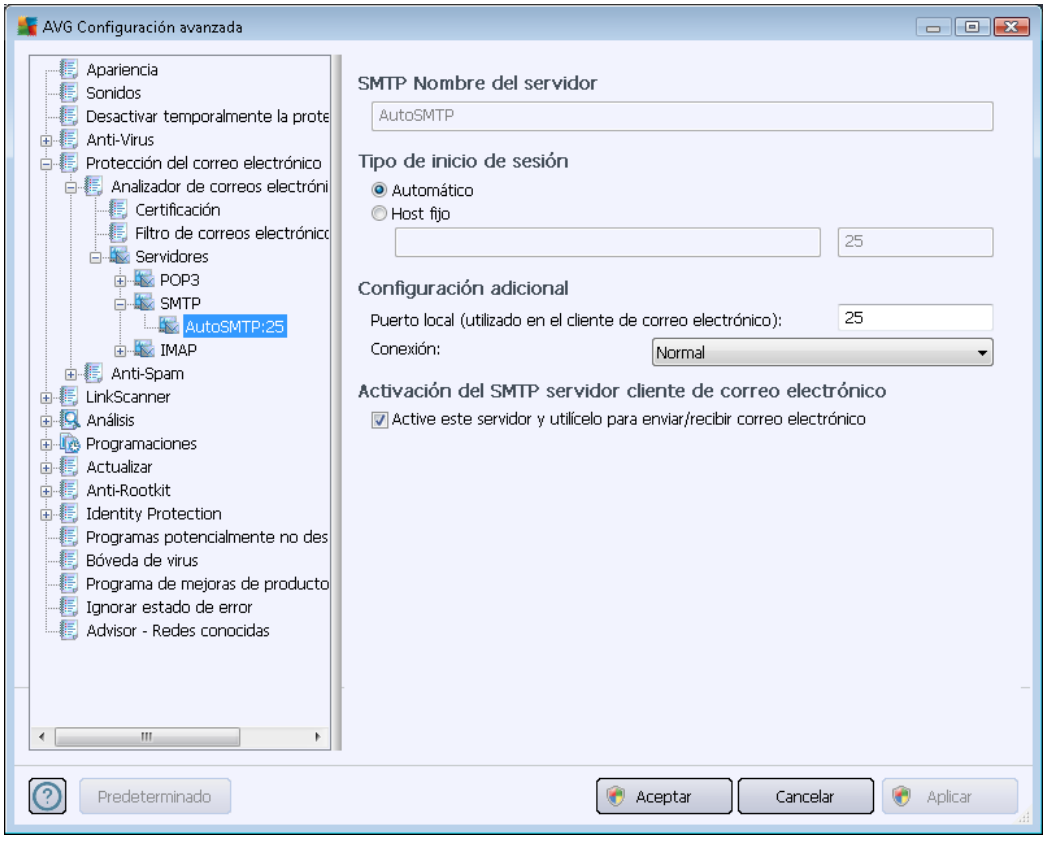
- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo entrante:

  - ***Automático***: el inicio de sesión se realizará de manera automática, de acuerdo con la configuración del cliente de correo electrónico.

  - ***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 sin cambiar. Como nombre, puede utilizar un nombre de dominio (

por ejemplo, pop.acme.com), así como 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 mayor 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.
  - ***Conexión***: en el menú desplegable, puede especificar la clase de conexión que desea utilizar (*normal/SSL/SSL predeterminado*). 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***: seleccione o quite la marca de selección de este elemento para activar o desactivar el servidor POP3 especificado



En este cuadro de diálogo (*al que se obtiene acceso mediante* ***Servidores / SMTP***) puede

configurar un nuevo servidor para el Analizador de correos electrónicos utilizando el protocolo SMTP para el correo saliente:

- ***Nombre del servidor SMTP***: en este campo podrá especificar el nombre de los servidores recién agregados (*para agregar un servidor SMTP, haga clic con el botón secundario del mouse en el elemento SMTP del menú de navegación de la izquierda*). Para el servidor "AutoSMTP" creado automáticamente, este campo está desactivado.

- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo saliente:

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

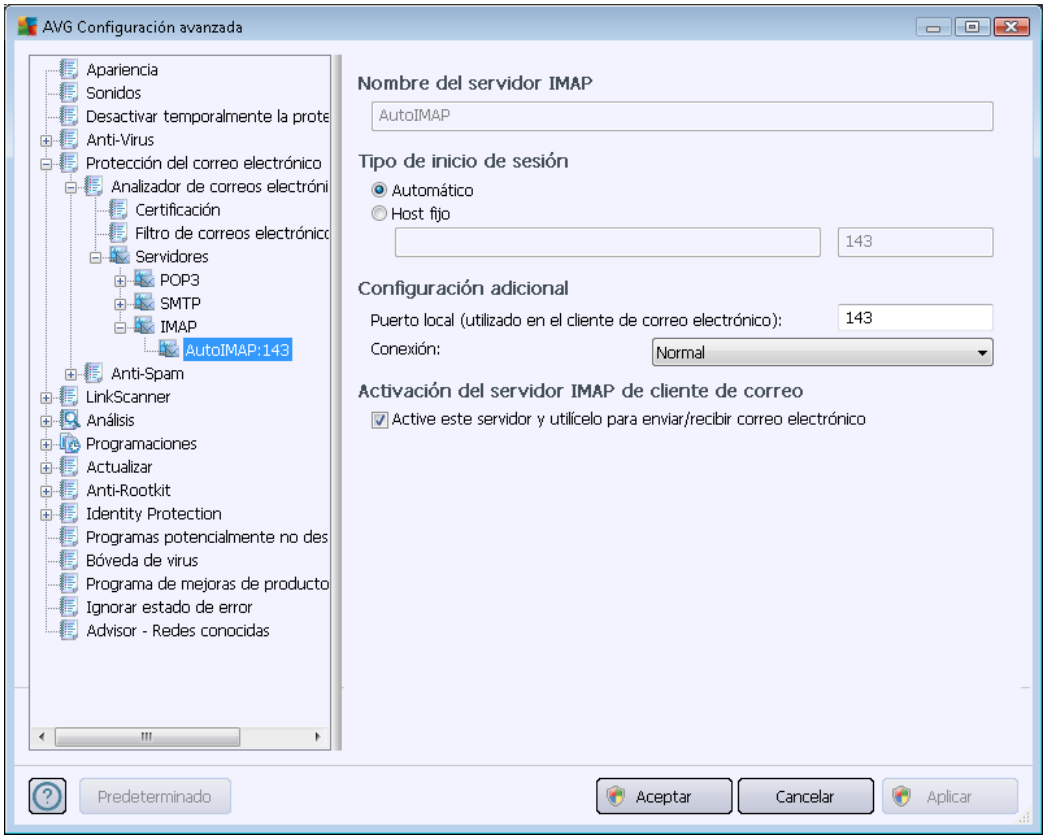
    - ***Host fijo***: en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, smtp.acme.com*), así como una dirección IP (*por ejemplo, 123.45.67.89*). Si 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 el 25.

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

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

    - ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/SSL predeterminado*). 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 SMTP en el cliente de correo electrónico***: seleccione o quite la marca de selección de este elemento para activar o desactivar el servidor SMTP especificado anteriormente



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

- ***Nombre del servidor IMAP***: en este campo podrá especificar el nombre de los servidores recién agregados (*para agregar un servidor IMAP, haga clic con el botón secundario del mouse en el elemento IMAP del menú de navegación de la izquierda*). Para el servidor "AutoIMAP" creado automáticamente, este campo está desactivado.

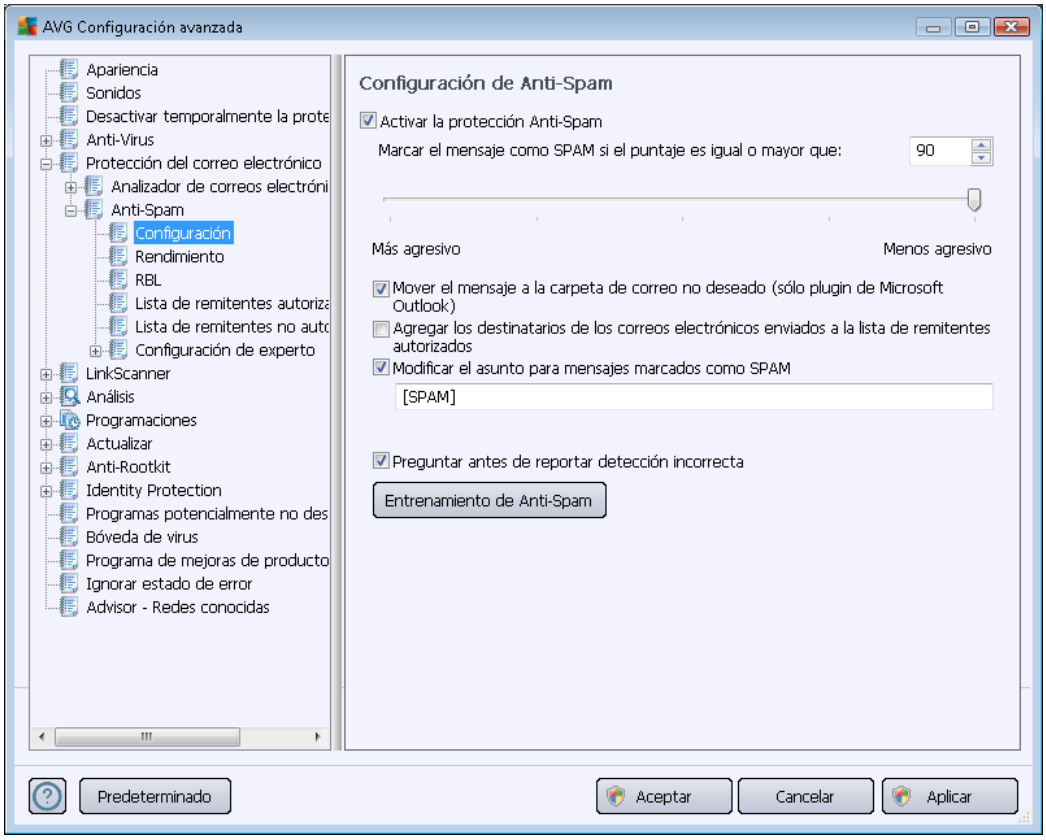
- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo saliente:

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

    - ***Host fijo***: en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, smtp.acme.com*), así como 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, imap.acme.com:8200*). El puerto estándar para comunicaciones IMAP es el 143.

- ***Configuración adicional***: especifica los parámetros con mayor detalle:
    - ***Puerto local***: especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Posteriormente deberá especificar en su aplicación de correo este puerto como puerto para la comunicación IMAP.
    - ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/SSL predeterminado*). 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 IMAP en el cliente de correo electrónico***: seleccione o quite la marca de esta casilla para activar o desactivar el servidor IMAP especificado anteriormente.

10.5.2. Anti-Spam



En el cuadro de diálogo ***Configuración de Anti-Spam***, puede seleccionar o quitar la selección de la casilla de verificación ***Activar la protección Anti-Spam*** para permitir o prohibir el análisis anti-spam de la comunicación por correo electrónico. Está opción está activada de forma predeterminada, y como siempre, se recomienda conservar esta configuración a menos que tenga una razón real para cambiarla.

A continuación, puede seleccionar medidas de puntaje más o menos agresivas. El filtro ***Anti-Spam*** asigna a cada mensaje un puntaje (*es decir, el grado de similitud del contenido del mensaje con el SPAM*) en función de varias técnicas de análisis dinámicas. Puede ajustar la configuración ***Marcar el mensaje como spam si el puntaje es mayor que*** escribiendo el valor o moviendo el control deslizante hacia la izquierda o hacia la derecha (*el rango de valores es de 50 a 90*).

Normalmente, recomendamos definir el umbral en un valor comprendido entre 50 y 90 o, si no está muy seguro, en 90. A continuación se muestra una descripción general del umbral de puntaje:

- ***Valores 80-90***: se filtrarán los mensajes de correo electrónico que probablemente sean spam. También se filtrarán, por equivocación, mensajes que no son spam.
- ***Valores 60-79***: se considera una configuración bastante agresiva. Se filtrarán los mensajes de correo electrónico que probablemente son spam. Es probable que también se incluyan mensajes que no lo son.
- ***Valores 50-59***: configuración muy agresiva. Los mensajes de correo electrónico que no son spam probablemente se consideren mensajes de spam. Este umbral no se recomienda para uso normal.

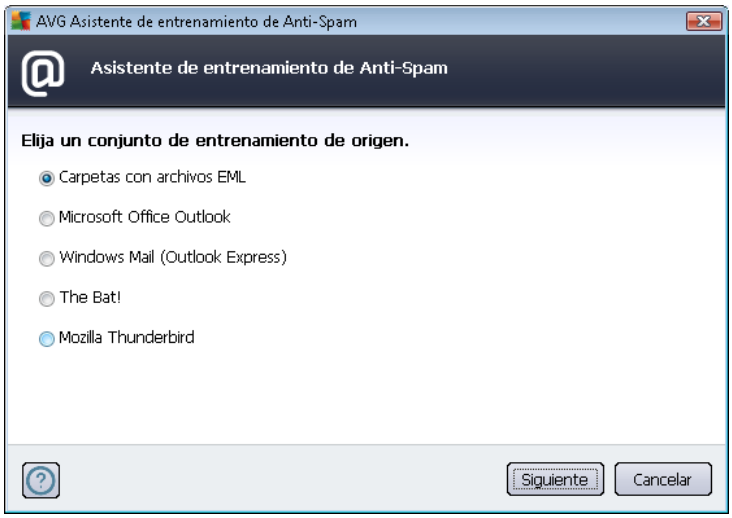
En el cuadro de diálogo ***Configuración de Anti-Spam***, puede definir de modo adicional cómo deben tratarse los mensajes de correo electrónico de spam detectados:

- ***Mover el mensaje a la carpeta de correo no deseado*** *(solo complemento de Microsoft Outlook)*: seleccione esta casilla de verificación para especificar que cada mensaje de spam detectado se debe mover automáticamente a la carpeta de correo no deseado específica del cliente de correo electrónico MS Outlook. En este momento, la función no es compatible con otros clientes de correo.
- ***Agregar los destinatarios de los correos electrónicos enviados a la lista de remitentes autorizados*** (lista blanca): seleccione esta casilla para confirmar que todos los destinatarios de los correos electrónicos enviados son confiables, y que todos los mensajes recibidos desde sus direcciones de correo electrónico pueden ser entregados.
- ***Modificar el asunto de los mensajes marcados como SPAM***: seleccione esta casilla de verificación si desea que todos los mensajes detectados como spam se marquen con una palabra o un carácter en el campo de asunto del mensaje de correo electrónico; el texto deseado se puede escribir en el campo de texto que se activa.
- ***Preguntar antes de reportar detección incorrecta***: siempre y cuando durante el proceso de instalación haya aceptado participar en el Programa de mejora de productos. De ser así, permitió informar de las amenazas detectadas a AVG. Los reportes se realizan automáticamente. Sin embargo, puede marcar esta casilla de verificación para confirmar que desea que se le pregunte antes de informar a AVG de cualquier spam detectado para asegurarse de que el mensaje se debía clasificar realmente como spam.

Botones de control

Entrenamiento de Anti-Spam: este botón abre el Asistente de entrenamiento de Anti-Spam que se describe en detalle en el siguiente capítulo.

El primer diálogo del ***Asistente de entrenamiento de Anti-Spam*** le pide que seleccione el origen de los mensajes de correo electrónico que desea utilizar para entrenar. Normalmente, deseará utilizar los correos electrónicos que se han marcado incorrectamente como SPAM, o los mensajes spam que no se han reconocido.



Existen las siguientes opciones entre las cuales elegir:

- ***Un cliente de correo electrónico específico***: si utiliza uno de los clientes de correo electrónico listados (*MS Outlook, Outlook Express, The Bat!*), simplemente seleccione la opción respectiva.

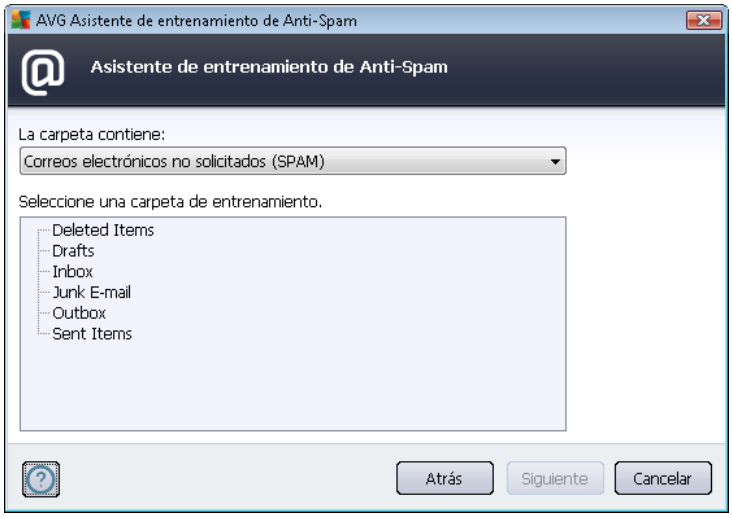
- ***Carpeta con archivos EML***: si utiliza cualquier otro programa de correo electrónico, primero debe guardar los mensajes en una carpeta específica (*en formato .eml*) o estar seguro de que conoce la ubicación de las carpetas de mensajes del cliente de correo electrónico. A continuación seleccione ***Carpeta con archivos EML***, lo cual le permitirá ubicar la carpeta deseada en el siguiente paso

Para un proceso de entrenamiento más rápido y fácil, es buena idea clasificar los correos electrónicos en las carpetas de antemano, de esta manera la carpeta que utilizará para entrenamiento contiene únicamente los mensajes de entrenamiento (deseados, o no deseados). Sin embargo, ésto no es necesario, ya que podrá filtrar los correos electrónicos más adelante.

Seleccione la opción adecuada y haga clic en ***Siguiente*** para que el asistente continúe.

El cuadro de diálogo que se muestra en este paso depende de su selección anterior.

Carpetas con archivos EML



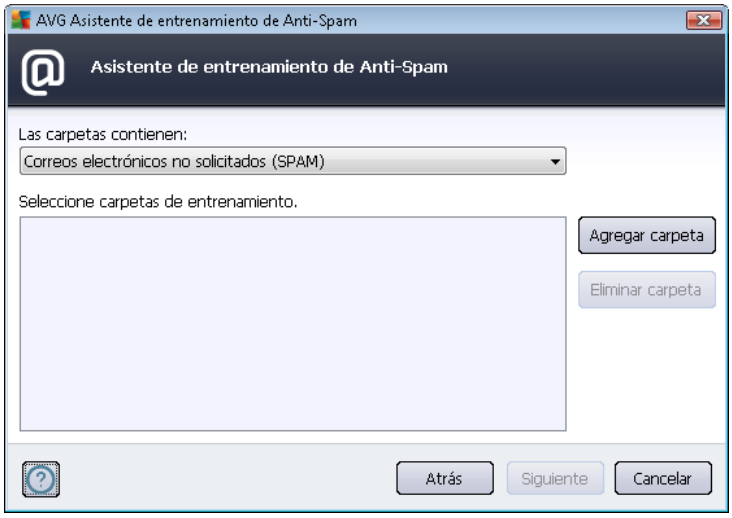
En este cuadro de diálogo, seleccione la carpeta con los mensajes que desea utilizar para entrenamiento. Presione el botón ***Agregar carpeta*** para ubicar la carpeta con los archivos .eml (*mensajes de correo electrónico guardados*). La carpeta seleccionada se mostrará a continuación en el cuadro de diálogo.

En el menú desplegable ***Las carpetas contienen***, establezca una de las siguientes dos opciones: la carpeta seleccionada contiene mensajes deseados (*HAM*) o contiene mensajes no solicitados (*SPAM*). Tenga en cuenta que podrá filtrar los mensajes en el siguiente paso, de manera que la carpeta no tiene que contener sólo los correos electrónicos de entrenamiento. También puede eliminar carpetas seleccionadas no deseadas de la lista haciendo clic en el botón ***Eliminar carpeta*** .

Cuando haya terminado, haga clic en ***Siguiente*** y continúe con Opciones de filtro de mensaje.

Especifique el cliente de correo electrónico

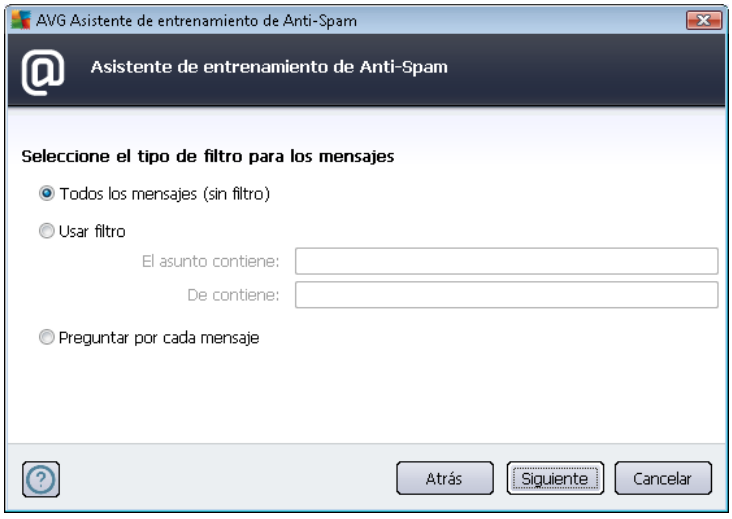
Una vez que haya confirmado una de las opciones, aparecerá el nuevo cuadro de diálogo.



Nota: *en el caso de Microsoft Office Outlook, se le pedirá que seleccione primero el perfil de MS Office Outlook.*

En el menú desplegable ***Las carpetas contienen***, establezca una de las siguientes dos opciones: la carpeta seleccionada contiene mensajes deseados (*HAM*) o contiene mensajes no solicitados (*SPAM*). Tenga en cuenta que podrá filtrar los mensajes en el siguiente paso, de manera que la carpeta no tiene que contener sólo los correos electrónicos de entrenamiento. En la sección principal del cuadro de diálogo ya se muestra un árbol de navegación del cliente de correo electrónico seleccionado. Localice la carpeta deseada en el árbol y resáltela con el mouse.

Cuando haya terminado, haga clic en ***Siguiente*** y continúe con Opciones de filtro de mensaje.



En este cuadro de diálogo, puede establecer los filtros para los mensajes de correo electrónico.

- ***Todos los mensajes (sin filtro)***: si está seguro de que la carpeta seleccionada contiene sólo mensajes que desea utilizar para el entrenamiento, seleccione la opción ***Todos los***

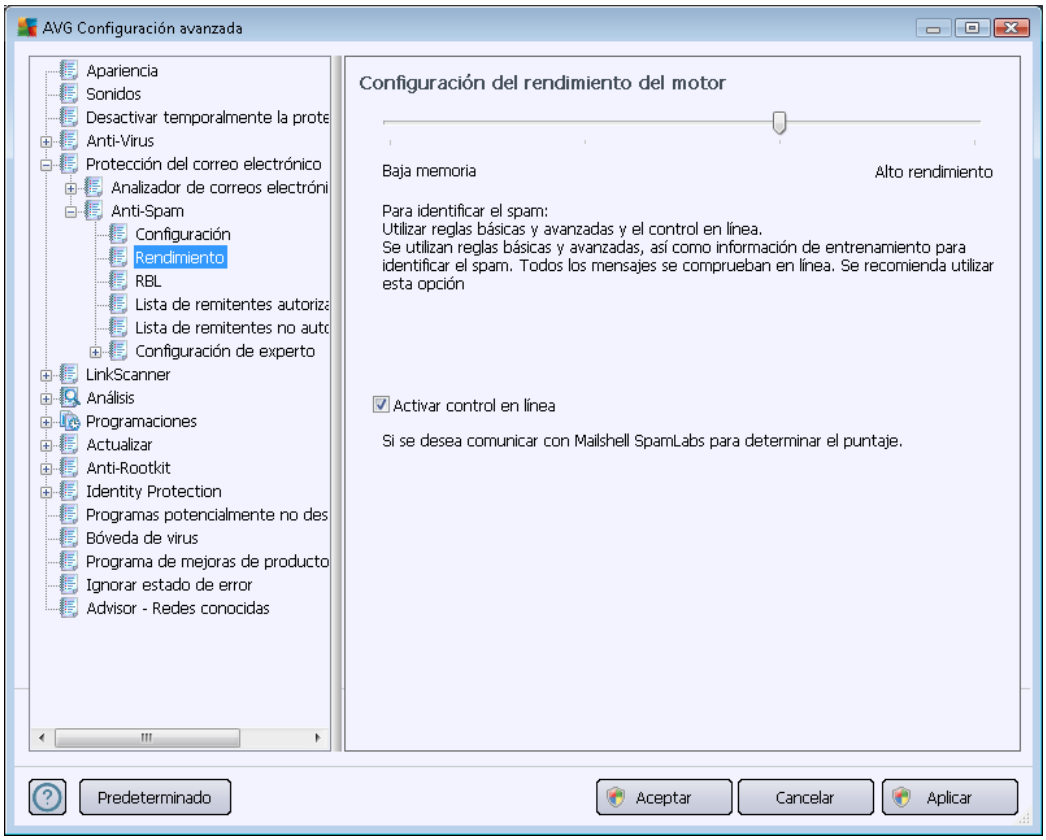
mensajes (sin filtro).

- ***Usar filtro***: si desea un filtrado más avanzado, seleccione la opción ***Usar filtro***. Puede escribir una palabra (*nombre*), parte de una palabra o frase que deba buscarse en los campos de asunto y remitente. Todos los mensajes que contengan exactamente los criterios se utilizarán para el entrenamiento, sin preguntar en cada uno. Cuando llena ambos campos de texto, las direcciones que corresponden a sólo una de las dos condiciones también se utilizarán.

- ***Preguntar por cada mensaje***: si no está seguro de cuáles son los mensajes que se encuentran en la carpeta y desea que el asistente le pregunte qué hacer con cada mensaje *(para que pueda determinar si debe utilizarse para el entrenamiento o no)*, seleccione la opción ***Preguntar por cada mensaje***.

Cuando haya seleccionado la opción adecuada, haga clic en ***Siguiente***. El siguiente cuadro de diálogo será únicamente informativo, para indicar que el asistente está listo para procesar los mensajes. Para iniciar el entrenamiento, haga clic en el botón ***Siguiente*** nuevamente. El entrenamiento comenzará de acuerdo con las condiciones previamente seleccionadas.

El cuadro de diálogo ***Configuración del rendimiento del motor*** (*vinculado mediante el elemento* ***Rendimiento*** *del área de navegación izquierda*) ofrece la configuración de rendimiento del componente ***Anti-Spam***:



Mueva el control deslizante a la izquierda o la derecha para cambiar el nivel del rendimiento del análisis, que varía entre los modos ***Baja memoria*** y ***Alto rendimiento***.

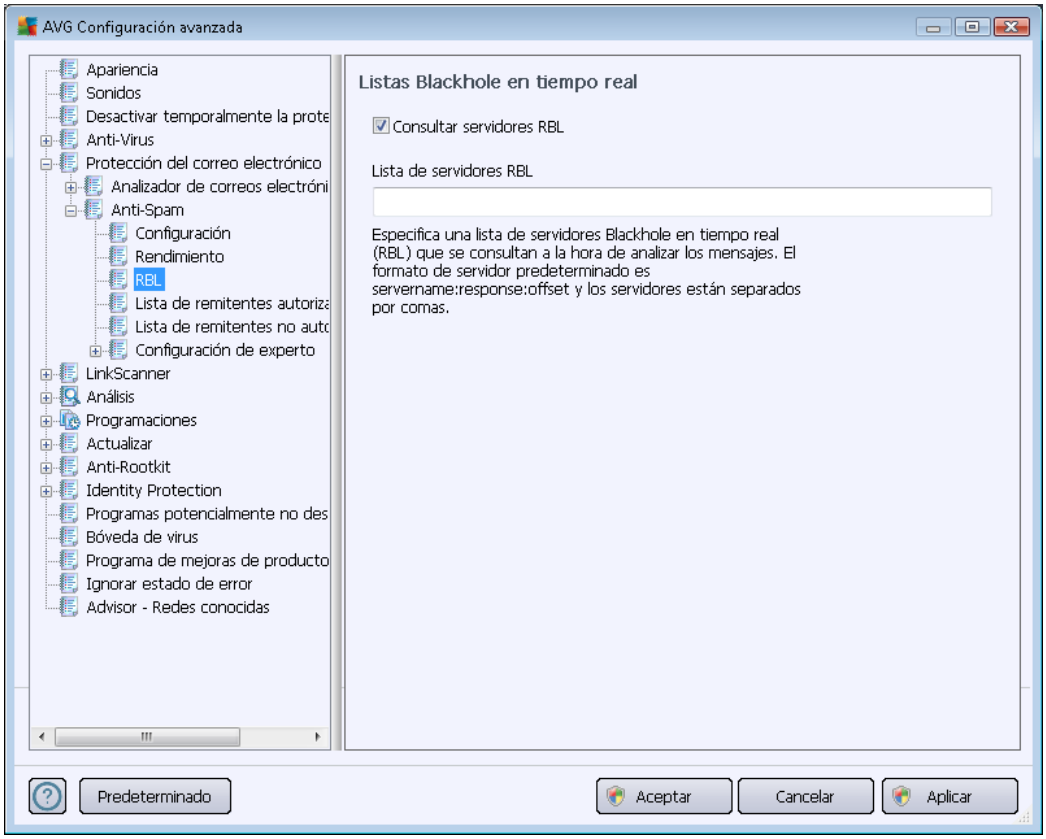
- ***Baja memoria***: durante el proceso de análisis para identificar spam, no se utilizará ninguna regla. Sólo se utilizarán los datos de aprendizaje para identificarlo. Este modo no se recomienda para los equipos de uso común, excepto si el hardware del equipo es muy pobre.

- ***Alto rendimiento***: este modo utiliza una gran cantidad de memoria. Durante el proceso de análisis para identificar spam, se utilizarán las funciones siguientes: reglas y caché de base de datos de spam, reglas básicas y avanzadas, direcciones IP y bases de datos que suelen emitir spam.

El elemento ***Activar control en línea*** está seleccionado de modo predeterminado. El resultado es una detección más precisa de spam mediante la comunicación con servidores Mailshell, es decir, los datos analizados se compararán con las bases de datos Mailshell en línea.

Por lo general, se recomienda mantener la configuración predeterminada y cambiarla únicamente si existe un motivo válido para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración.

El elemento ***RBL*** abre un cuadro de diálogo llamado ***Listas Blackhole en tiempo real*** donde puede activar o desactivar la función ***Consultar servidores RBL***:

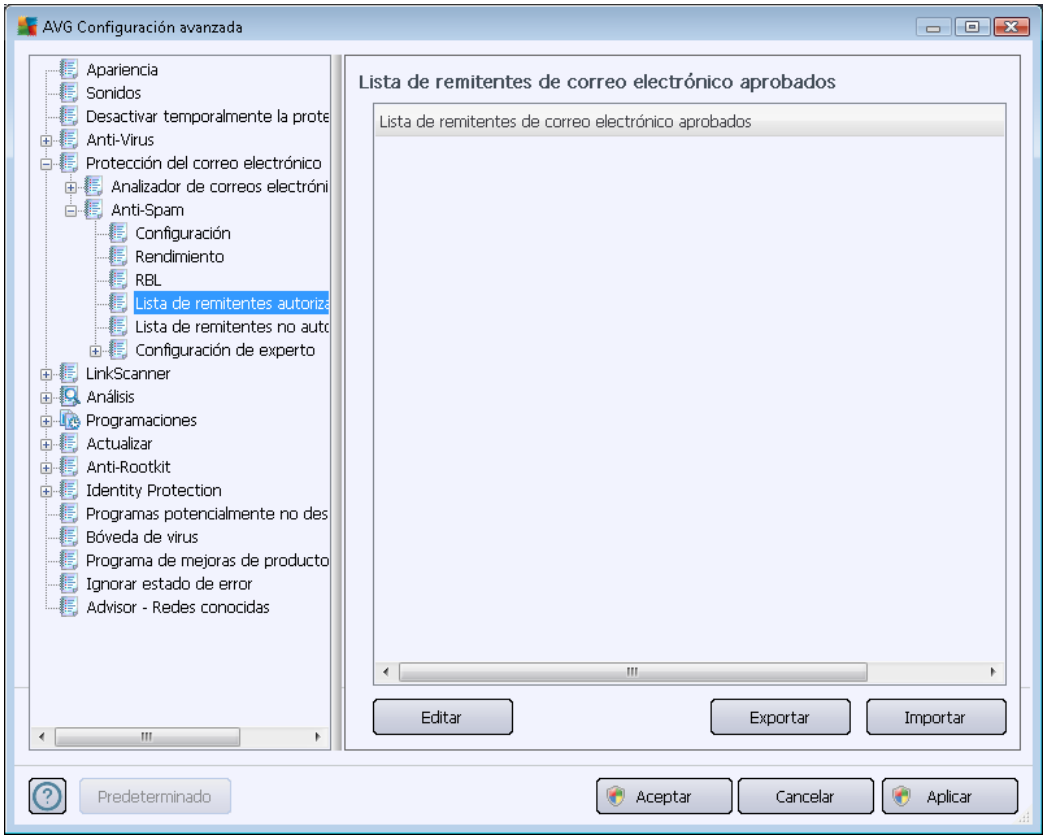


El servidor RBL (*Lista Blackhole en tiempo real*) es un servidor DNS con una base de datos extensa de remitentes conocidos que envían spam. Cuando se habilita esta función, todos los mensajes de correo electrónico se comparan con la base de datos del servidor RBL y se marcan como spam si resultan idénticos a cualquiera de las entradas de la base de datos. Las bases de datos de servidores RBL contienen las "fingerprints" (huellas digitales) del spam actualizadas hasta el último momento para brindar una detección de correo no deseado óptima y precisa. Esta función resulta particularmente útil para usuarios que reciben grandes cantidades de spam que el motor Anti-Spam no suele detectar.

La ***Lista de servidores RBL*** le permite definir las ubicaciones de servidores RBL específicos (*tenga en cuenta que la habilitación de esta función puede, en algunos sistemas y configuraciones, ralentizar el proceso de recepción de correo electrónico dado que cada mensaje se debe comprobar en la base de datos del servidor RBL).*

No se envían datos personales al servidor.

El elemento ***Lista de remitentes autorizados*** abre un cuadro de diálogo llamado ***Lista de remitentes de correo electrónico aprobados*** con una lista global de direcciones de correo electrónico de remitentes y nombres de dominio cuyos mensajes nunca deben considerarse como spam.



En la interfaz de edición, puede compilar una lista de remitentes de los cuales está seguro que nunca le enviarán mensajes no deseados (spam). También puede compilar una lista de nombres de

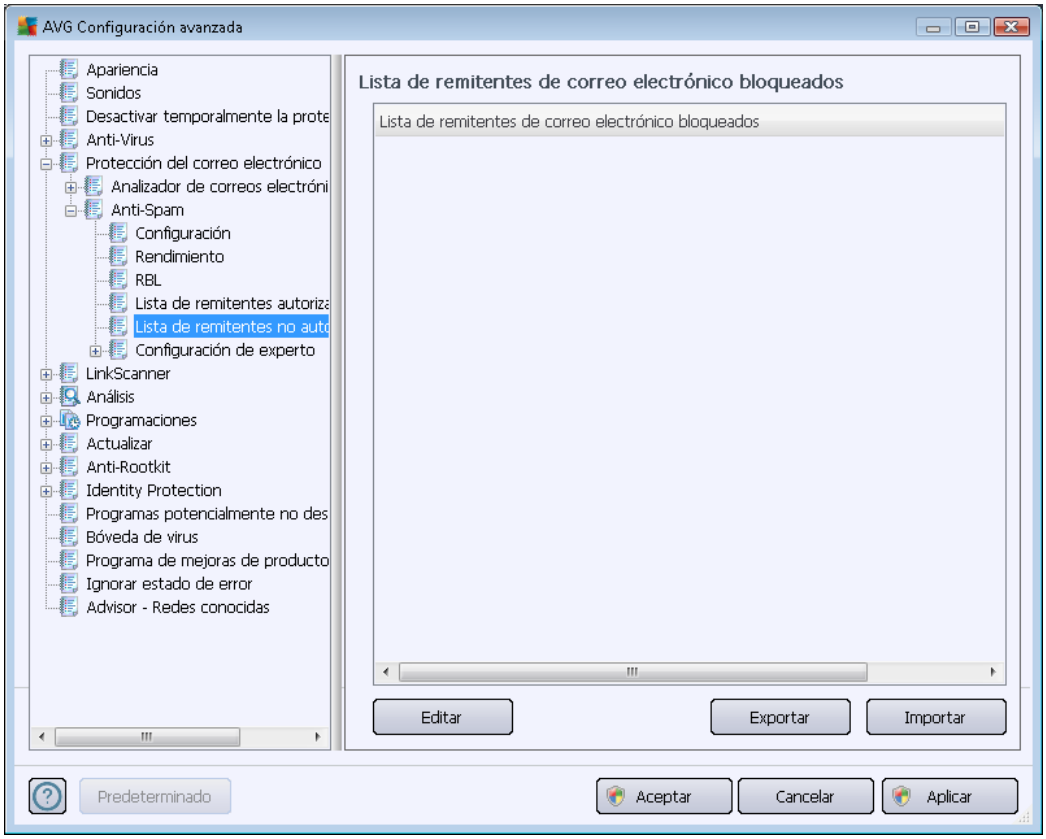
dominio completos (*por ejemplo, avg.com*), que sabe que no generan mensajes de spam. Una vez que tenga preparada la lista con los nombres de los remitentes y/o dominios, puede introducirlos por cualquiera de los siguientes métodos: mediante entrada directa de cada dirección de correo electrónico o importando toda la lista de direcciones de una vez.

Botones de control

Están disponibles los siguientes botones de control:

- ***Editar***: presione este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (*también puede emplear el método de copiar y pegar*). Inserte un elemento por línea (*remitente, nombre de dominio*).
- ***Exportar***: si decide exportar los registros por algún motivo, puede hacerlo presionando este botón. Se guardarán todos los registros en un archivo de sólo texto.
- ***Importar***: si ya tiene preparado un archivo de texto con direcciones de correo electrónico o nombres de dominio, puede importarlo seleccionando este botón. El archivo debe contener sólo un elemento (*dirección, nombre de dominio*) por línea.

El elemento ***Lista de remitentes no autorizados*** (lista negra) abre un cuadro de diálogo con una lista global de direcciones de correo electrónico de remitentes y nombres de dominios bloqueados cuyos mensajes siempre se marcarán como spam.



En la interfaz de edición, puede indicar una lista de remitentes que considera que le enviarán mensajes no deseados (*spam*). También puede compilar una lista de nombres de dominio completos (*como, por ejemplo, spammingcompany.com*) que cree que pueden enviarle mensajes de spam o que ya se los envían. Todos los mensajes de correo electrónico de las direcciones y los dominios de la lista se identificarán como spam. Una vez que tenga preparada la lista con los nombres de los remitentes y/o dominios, puede introducirlos por cualquiera de los siguientes métodos: mediante entrada directa de cada dirección de correo electrónico o importando toda la lista de direcciones de una vez.

Botones de control

Están disponibles los siguientes botones de control:

- ***Editar***: presione este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (*también puede emplear el método de copiar y pegar*). Inserte un elemento por línea (*remitente, nombre de dominio*).
- ***Exportar***: si decide exportar los registros por algún motivo, puede hacerlo presionando este botón. Se guardarán todos los registros en un archivo de sólo texto.
- ***Importar***: si ya tiene preparado un archivo de texto con direcciones de correo electrónico o nombres de dominio, puede importarlo seleccionando este botón.

La rama Configuración avanzada contiene amplias opciones de configuración para el componente Anti-Spam. Estas opciones están diseñadas exclusivamente para usuarios experimentados, generalmente administradores de red que necesitan configurar la protección anti-spam con mayor detalle para obtener la mejor protección de los servidores de correo electrónico. Por ello, no hay ayuda adicional disponible para los cuadros de diálogo individuales; sin embargo, hay una breve descripción de cada opción respectiva directamente en la interfaz del usuario.

Es altamente recomendable no cambiar ninguna configuración a menos que esté completamente familiarizado con todas las configuraciones avanzadas de Spamcatcher (MailShell Inc.). Cualquier cambio inapropiado puede dar lugar a un rendimiento deficiente o a un funcionamiento incorrecto de los componentes.

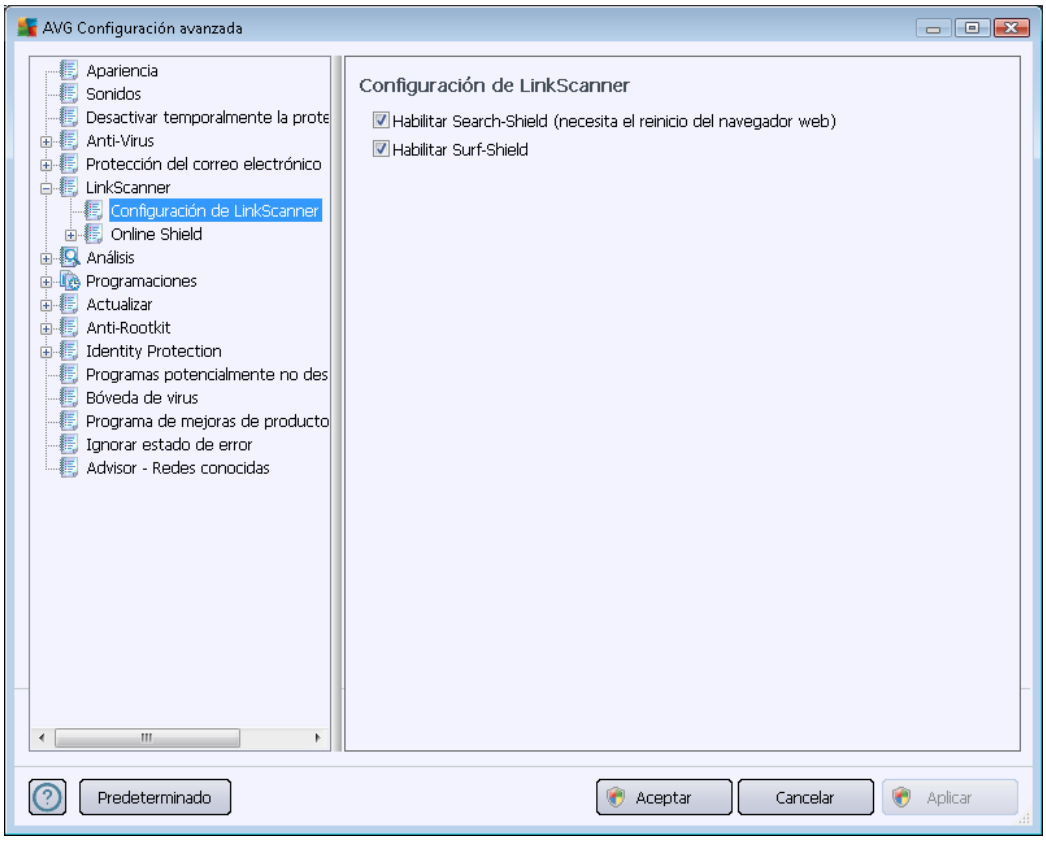
Si aún cree que necesita cambiar la configuración de Anti-Spam a un nivel muy avanzado, siga las instrucciones que se proporcionan directamente en la interfaz del usuario. Generalmente, en cada cuadro de diálogo encontrará una sola función específica que se puede editar (su descripción siempre está incluida en el mismo cuadro de diálogo):

- ***Caché***: huella digital, reputación del dominio, LegitRepute
- ***Entrenamiento***: entradas máximas de palabras, umbral de auto-entrenamiento, peso
- ***Filtro***: lista de idiomas, lista de países, IP aprobadas, IP bloqueadas, países bloqueados, juegos de caracteres bloqueados, remitentes con identidad suplantada
- ***RBL***: servidores RBL, aciertos múltiples, umbral, tiempo de espera, IP máximas
- ***Conexión a Internet***: tiempo de espera, servidor proxy, autenticación de servidor proxy

10.6. LinkScanner

10.6.1. Configuración de LinkScanner

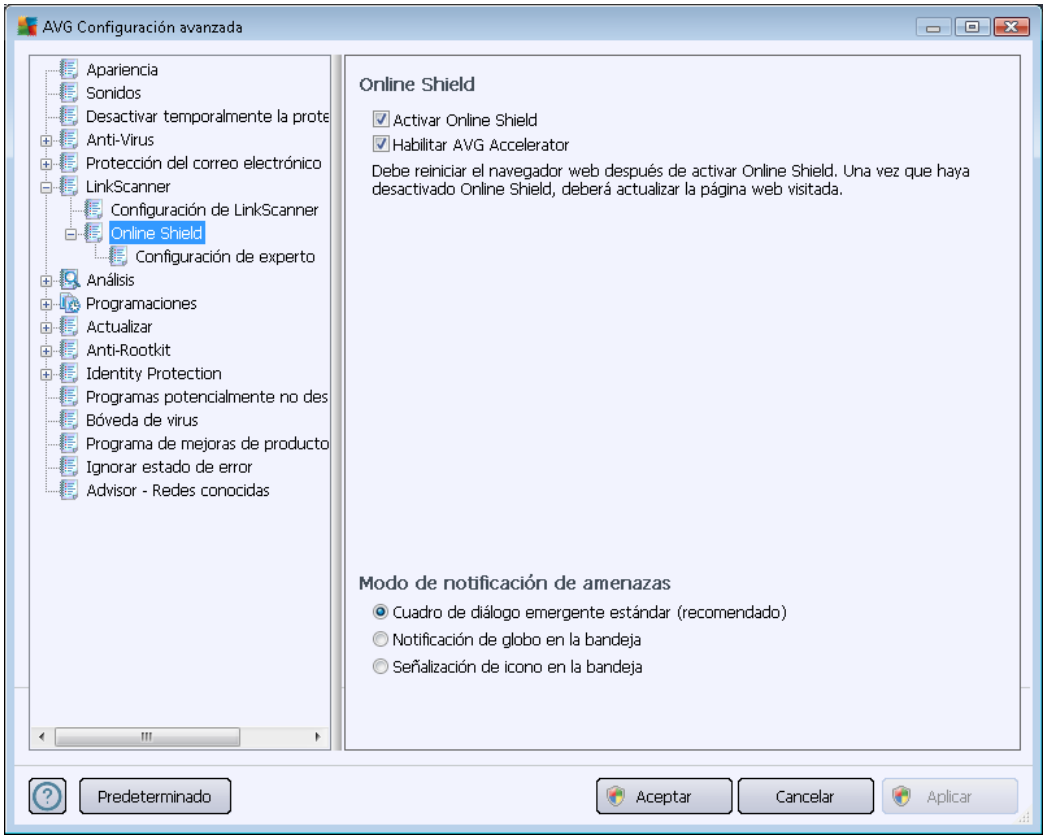
El cuadro de diálogo ***Configuración de LinkScanner*** le permite activar o desactivar las funciones básicas de LinkScanner:



- ***Habilitar Search-Shield*** (*activado de forma predeterminada*): iconos de evaluación y notificación sobre las búsquedas realizadas con Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot al comprobar por adelantado el contenido de los sitios devueltos por el motor de búsqueda.

- ***Habilitar Surf-Shield*** (*activado de forma predeterminada*): protección activa (*en tiempo real*) contra sitios de explotación cuando se obtiene acceso a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario accede a ellos a través de un navegador Web (*o cualquier otra aplicación que utilice HTTP*).

10.6.2. Online Shield



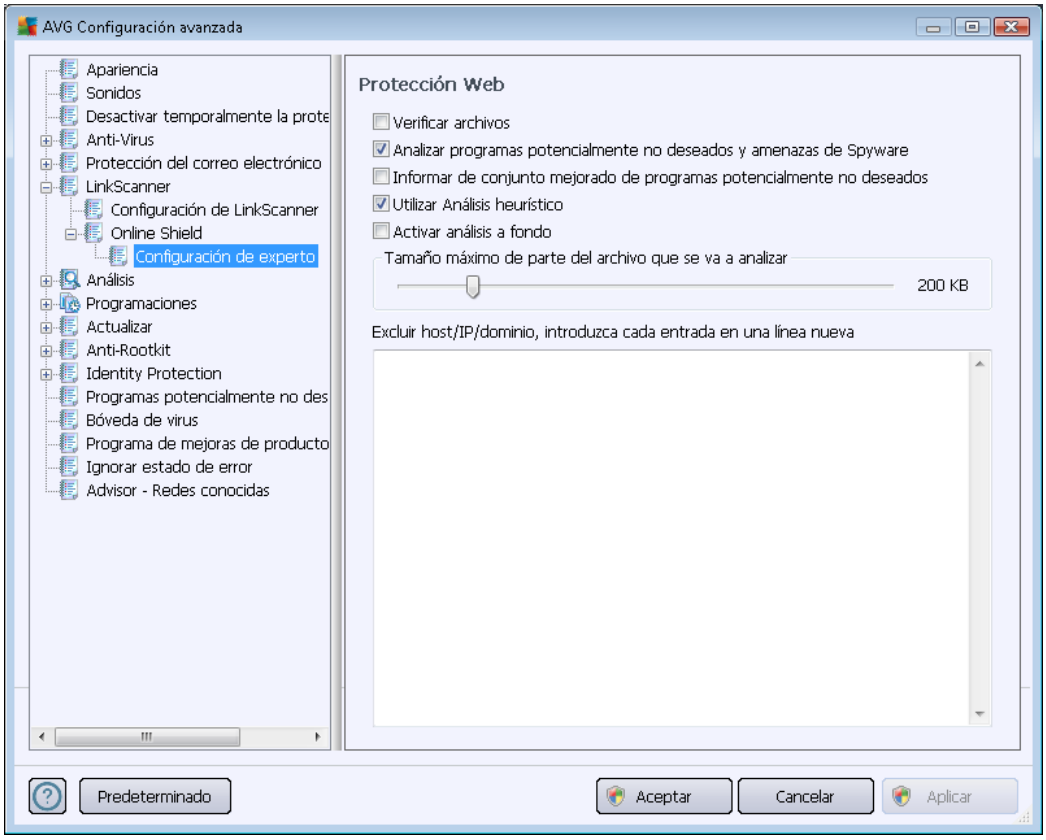
El cuadro de diálogo ***Online Shield*** ofrece las siguientes opciones:

- ***Activar Online Shield*** *(activada de forma predeterminada)*: activa o desactiva el servicio entero ***Online Shield***. Para ver la configuración avanzada de ***Online Shield***, continúe con el siguiente cuadro de diálogo llamado Protección Web.

- ***Activar AVG Accelerator*** *(activada de forma predeterminada):* activa o desactiva el servicio ***AVG Accelerator*** que permite una mejor reproducción de video en línea y facilita la realización de descargas adicionales.

Modo de notificación de amenazas

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



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

- ***Habilitar Protección Web***: esta opción confirma que ***Online Shield*** debe analizar el contenido de las páginas Web. Mientras esta opción esté seleccionada (*valor predeterminado*), podrá activar o desactivar estos elementos:
    - ***Examinar archivos***: (*desactivado de manera predeterminada*): analiza el contenido de los archivos que pudieran existir en la página Web que se visualizará.
    - ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione esta opción para activar el motor Anti-Spyware y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
    - ***Informar de conjunto mejorado de programas potencialmente no deseados***: (*desactivada de manera predeterminada*): seleccione esta opción para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden

emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

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

- ***Activar análisis a fondo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

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

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

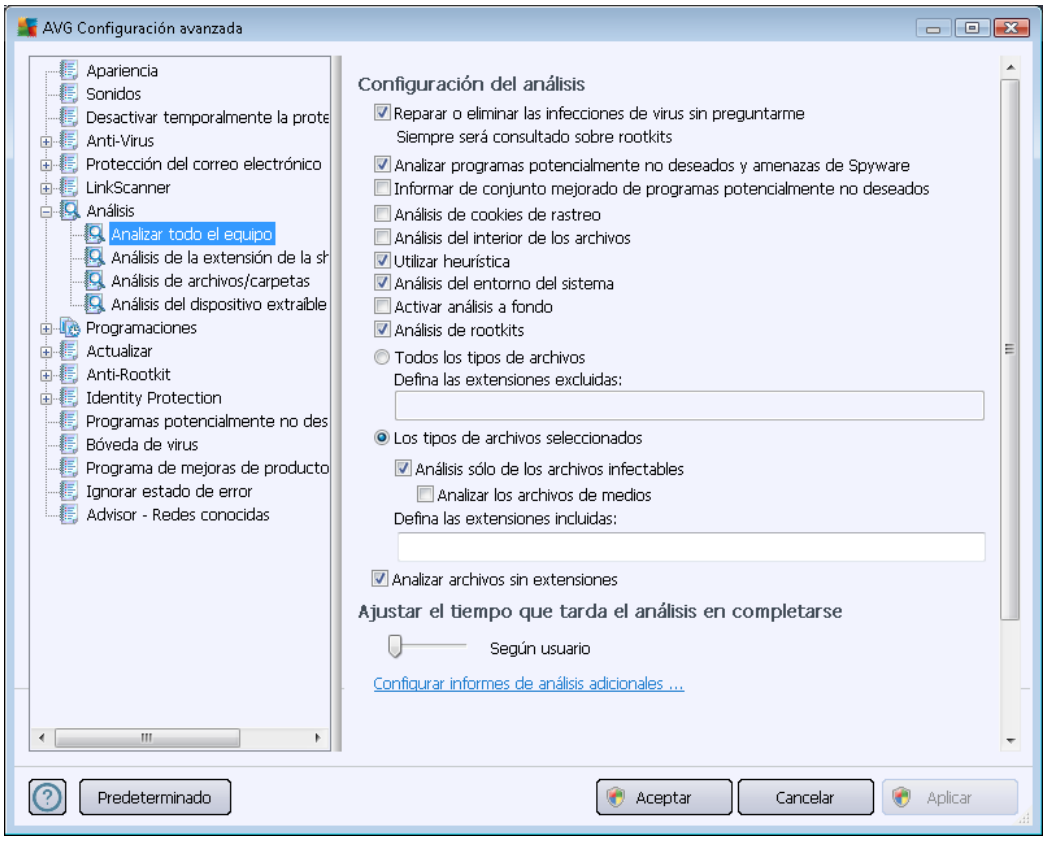
10.7. Análisis

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

- ***Análisis de 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
- ***Análisis de archivos/carpetas***: análisis estándar predefinido de áreas seleccionadas del equipo
- ***Análisis del dispositivo extraíble***: análisis específico de dispositivos extraíbles conectados a su equipo

10.7.1. Análisis de todo el equipo

La opción ***Análisis de todo el equipo*** le permite editar los parámetros de uno de los análisis predefinidos por el proveedor de software, el 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 las infecciones de virus sin preguntarme*** (*activado de manera predeterminada*): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.

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

- ***Informar de conjunto mejorado de programas potencialmente no deseados*** (

desactivada de forma predeterminada): seleccione esta opción para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

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

- ***Analizar el interior de los archivos*** (*activado de manera predeterminada*): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos (por ejemplo, ZIP, RAR...

- ***Utilizar método heurístico*** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) 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.

- ***Activar análisis a fondo*** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

- ***Analizar en busca de rootkits*** (*activado de manera predeterminada*): el análisis Anti-Rootkit busca en su equipo posibles rootkits, es decir, programas y tecnologías que cubran la actividad de malware en su equipo. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

Después sería conveniente decidir si desea analizar

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

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

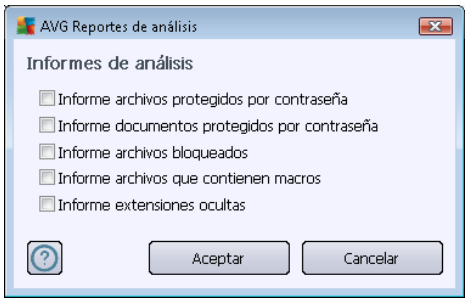
- De manera opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben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

Ajustar el tiempo que tarda el análisis en completarse

Dentro de la sección ***Ajustar el tiempo que tarda el análisis en completarse*** 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 *según usuario* de empleo automático de recursos. Si desea que el análisis se realice a más velocidad, tardará menos tiempo pero el uso de recursos del sistema aumentará de modo notable durante el análisis y el resto de actividades del equipo se ralentizará (*esta opción se puede emplear cuando el equipo está encendido pero no hay nadie trabajando en él*). Por otra parte, puede reducir el uso de recursos del sistema prolongando la duración del análisis.

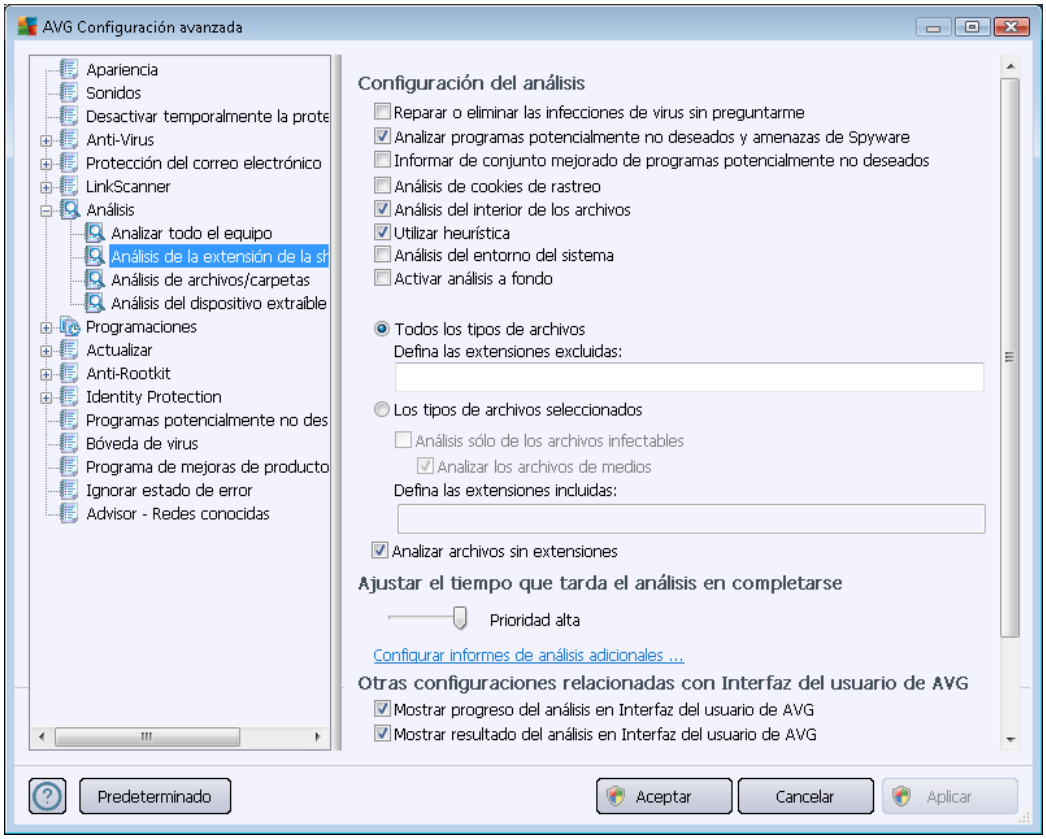
Configurar informes de análisis adicionales ...

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



10.7.2. Análisis de la extensión de la shell

De modo parecido al anterior elemento, Análisis de todo el equipo, este elemento denominado ***Análisis de la 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:



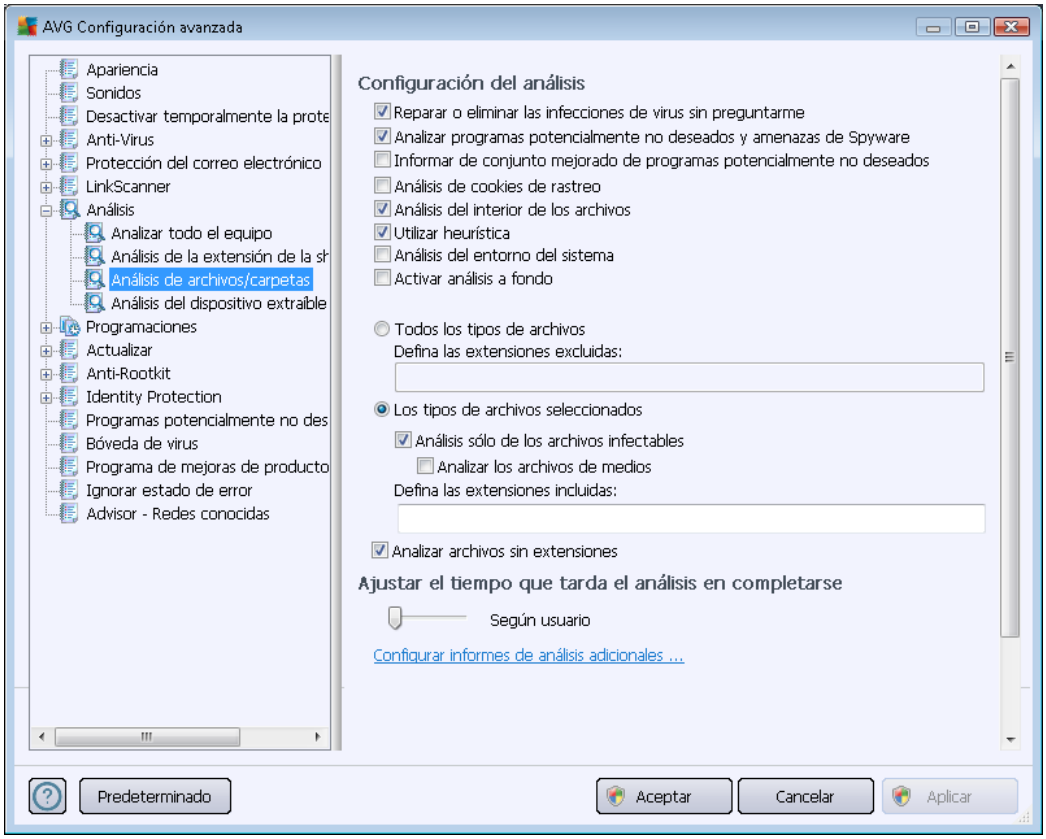
La lista de parámetros muestra parámetros idénticos a los que están disponibles en el Análisis de todo el equipo. Sin embargo, la configuración predeterminada es diferente (*por ejemplo, el análisis de todo el equipo no comprueba de manera predeterminada los archivos, pero sí analiza el entorno del sistema, mientras que con el análisis de extensión de la shell es al revés*).

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

En comparación con el cuadro de diálogo Análisis de todo el equipo, el cuadro de diálogo ***Análisis de la extensión de la shell*** también incluye la sección llamada ***Otras configuraciones relacionadas con Interfaz del usuario de AVG***, donde podrá especificar si desea que se pueda obtener acceso al progreso y a los resultados del análisis desde la interfaz del usuario de AVG. Asimismo, puede definir que el resultado del análisis sólo se muestre en caso de que se detecte una infección durante el análisis.

10.7.3. Análisis de archivos/carpetas

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

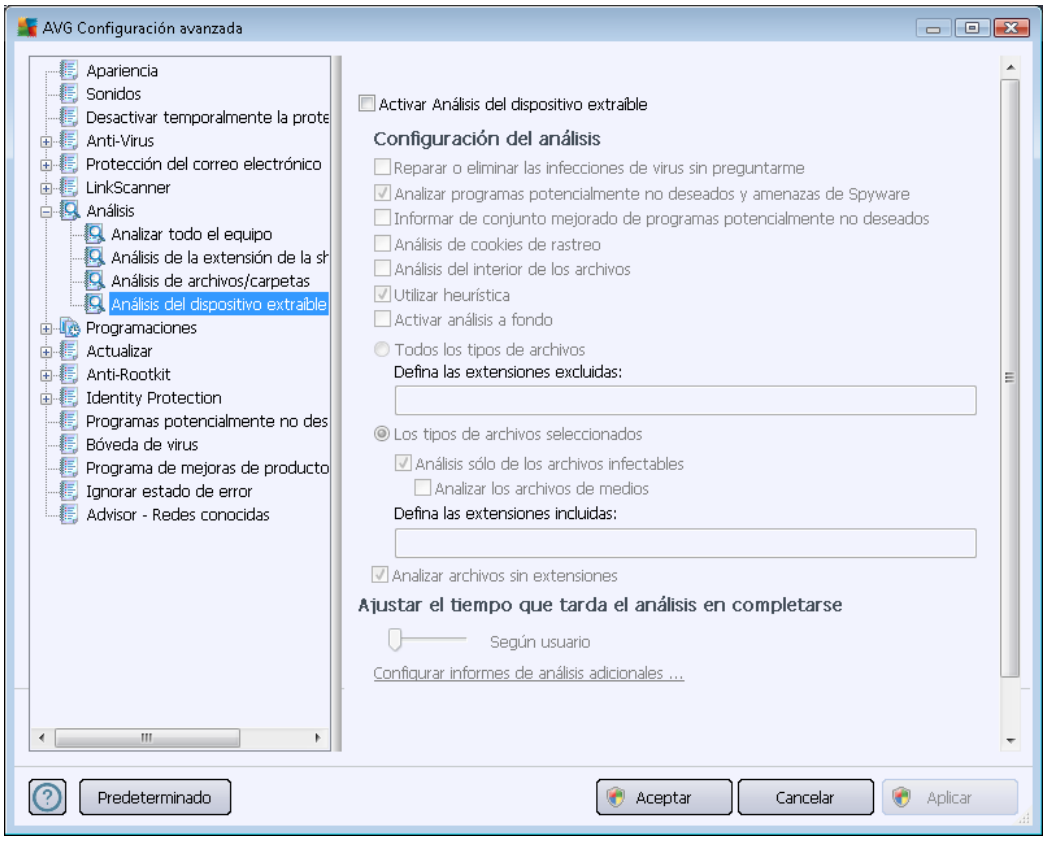


Todos los parámetros definidos en este cuadro de diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con Análisis de archivos/carpetas.

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

10.7.4. Análisis del dispositivo extraíble

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

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

10.8. Programaciones

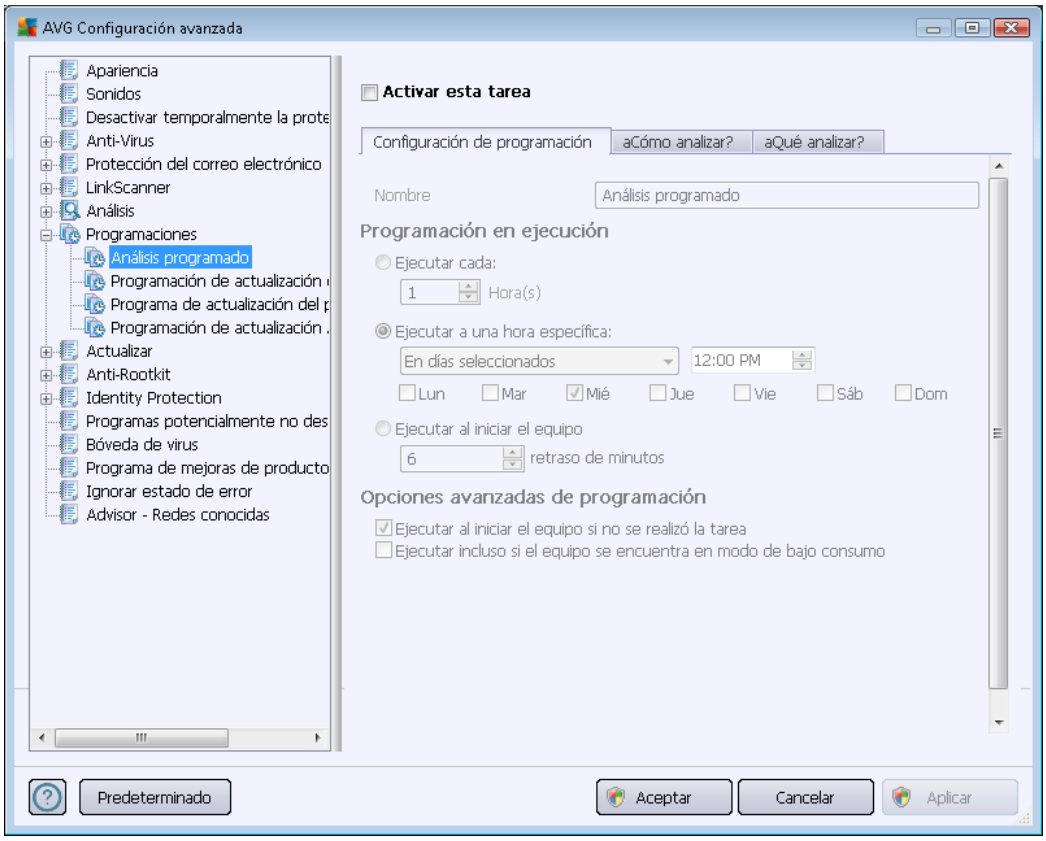
En la sección ***Programas*** puede editar la configuración predeterminada de:

- Análisis programado
- Programación de actualización de las definiciones
- Programación de actualización del programa

- Programación de actualización de Anti-Spam

10.8.1. Análisis programado

Los parámetros del análisis programado se pueden editar (*o se puede configurar una nueva programación*) en tres pestañas. En cada pestaña puede seleccionar o cancelar la selección del elemento ***Activar esta tarea*** para desactivar de forma temporal el análisis programado y volverlo a activar cuando sea necesario:



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

Ejemplo: *no es adecuado llamar al análisis por el nombre "Nuevo análisis" o "Mi análisis" ya que estos nombres no hacen referencia a lo que el análisis realmente comprueba. 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 cuadro de diálogo puede definir con más detalle los siguientes parámetros del análisis:

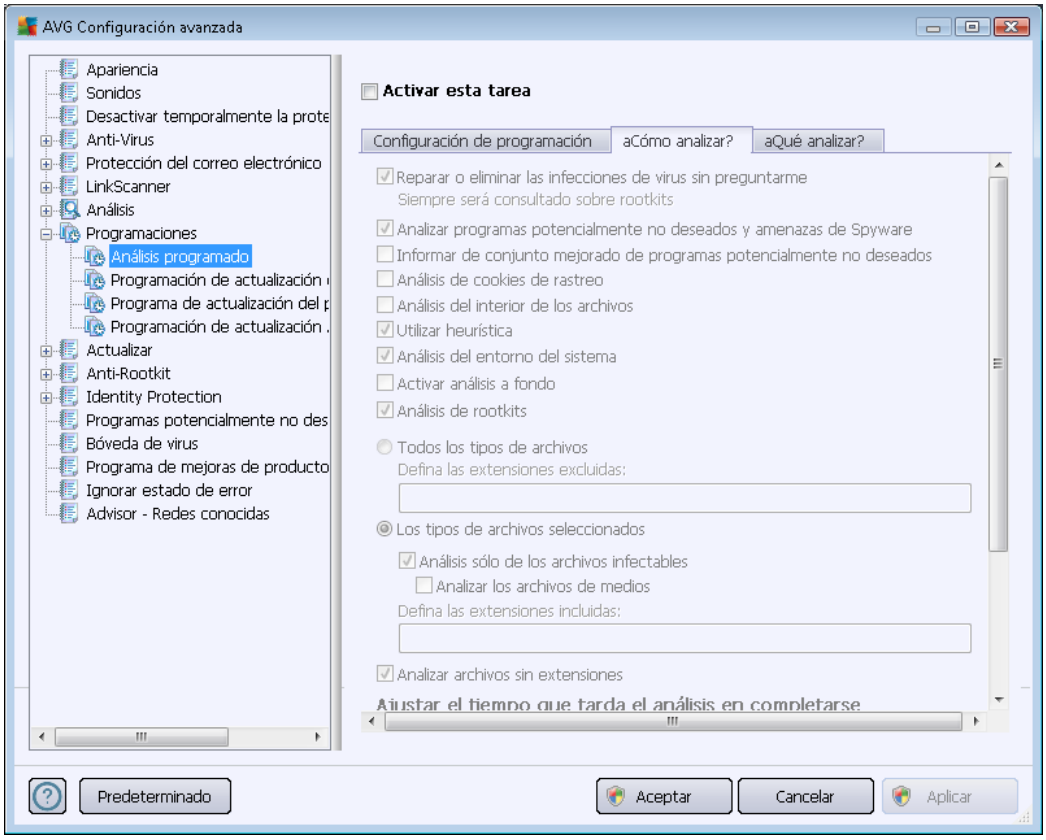
Programación en ejecución

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

Opciones avanzadas de programación

Esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado. Una vez que se inicia el análisis programado en la hora que se especificó, se le informará de este hecho mediante una ventana emergente que se abre sobre el icono en la bandeja de sistema AVG:

A continuación aparece un nuevo icono de la bandeja del sistema AVG (*a todo color y brillante*) informando de 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 contextual donde puede decidir pausar o detener la ejecución del análisis, y también cambiar la prioridad del análisis que se está ejecutando en ese momento.



En la pestaña ***Cómo analizar*** se encontrará una lista de parámetros de análisis que de manera opcional se pueden activar o 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 las infecciones de virus sin preguntarme*** *(activada de forma predeterminada):* si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.

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

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

forma predeterminada está desactivada.

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

- ***Analizar el interior de los archivos*** (*desactivado 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, etc.

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

- ***Analizar el entorno del sistema*** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.

- ***Activar análisis a fondo*** (*desactivado de forma predeterminada):* en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

- ***Analizar en busca de rootkits*** *(activado de forma predeterminada):* Anti-Rootkit busca en su equipo posibles rootkits, es decir, programas y tecnologías que cubran la actividad de malware en su equipo. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

Después sería conveniente decidir si desea analizar

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

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

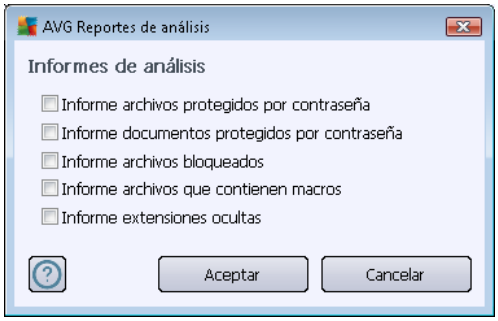
- De manera opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben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

Ajustar el tiempo que tarda el análisis en completarse

Dentro de la sección ***Ajustar el tiempo que tarda el análisis en completarse*** 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 *según usuario* de empleo automático de recursos. Si desea que el análisis se realice a más velocidad, tardará menos tiempo, pero el uso de recursos del sistema aumentará de modo notable durante el análisis y el resto de actividades del equipo se ralentizará (*esta opción se puede emplear cuando el equipo está encendido pero no hay nadie trabajando en él*). Por otro lado, puede reducir el uso de recursos del sistema prolongando la duración del análisis.

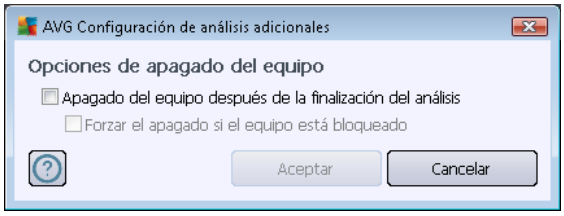
Configurar informes de análisis adicionales

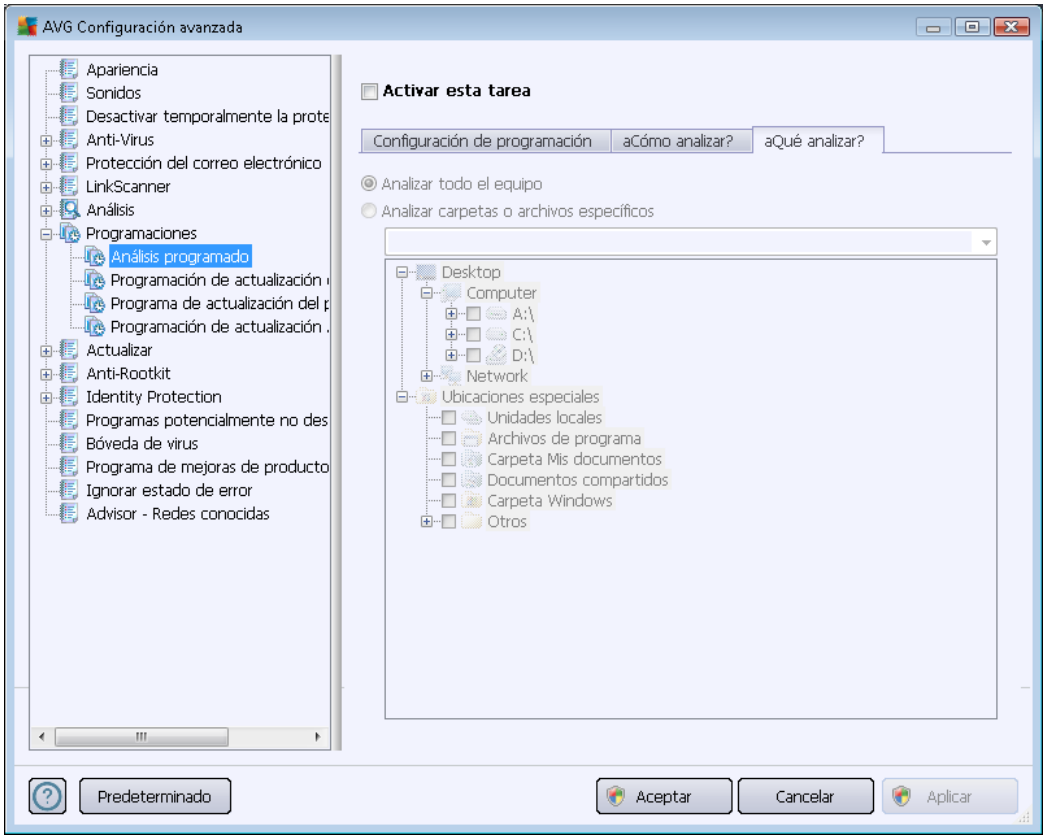
Haga clic en el vínculo ***Configurar informes de análisis adicionales...*** para abrir una ventana de diálogo denominada ***Informes de análisis*** donde puede marcar varios elementos para definir de qué hallazgos se debería informar:



Configuración de análisis adicional

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

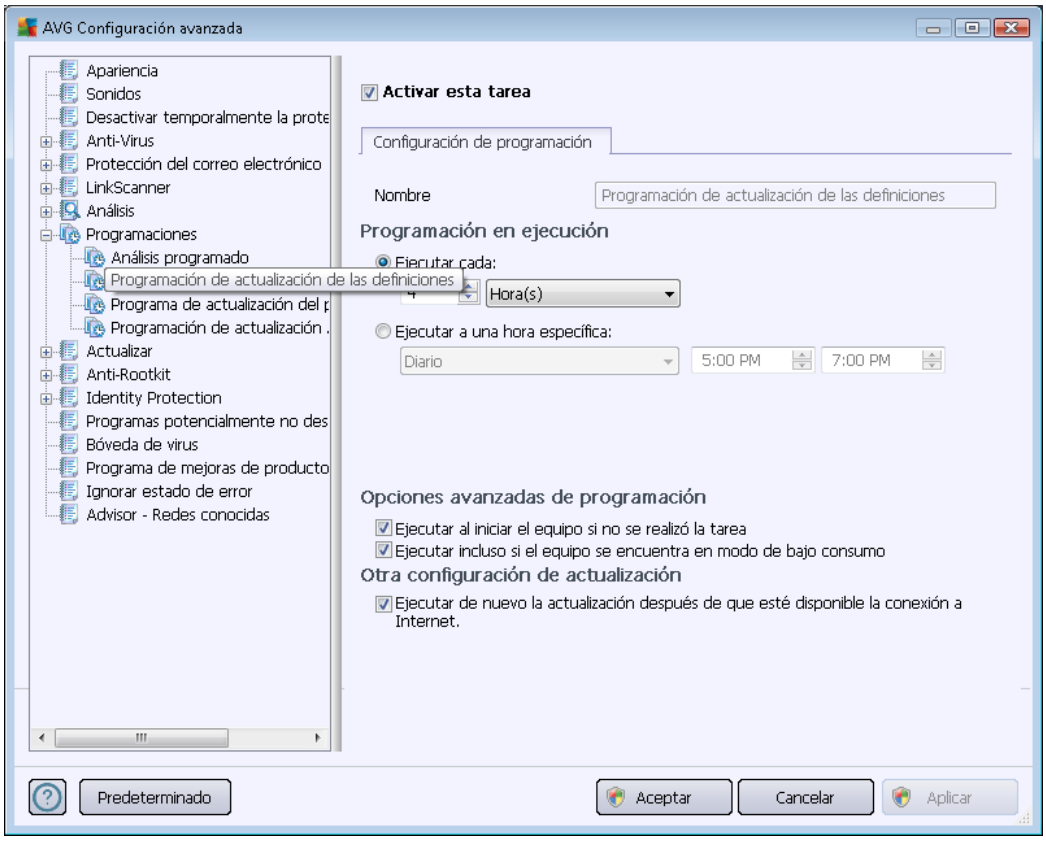




En la pestaña ***Qué analizar*** puede definir si desea programar el análisis de todo el equipo o el análisis de archivos/carpetas. Si selecciona analizar archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activará la estructura de árbol visualizada y podrá especificar las carpetas que se analizarán.

10.8.2. Programación de actualización de las definiciones

Si es ***realmente necesario***, puede quitar la marca del elemento ***Activar esta tarea*** para desactivar de forma temporal la actualización programada de las definiciones y volverla a activar más adelante:



En este cuadro de diálogo, puede configurar algunos parámetros detallados de la programación de actualización de las definiciones. En el campo de texto denominado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

Programación en ejecución

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

Opciones avanzadas de programación

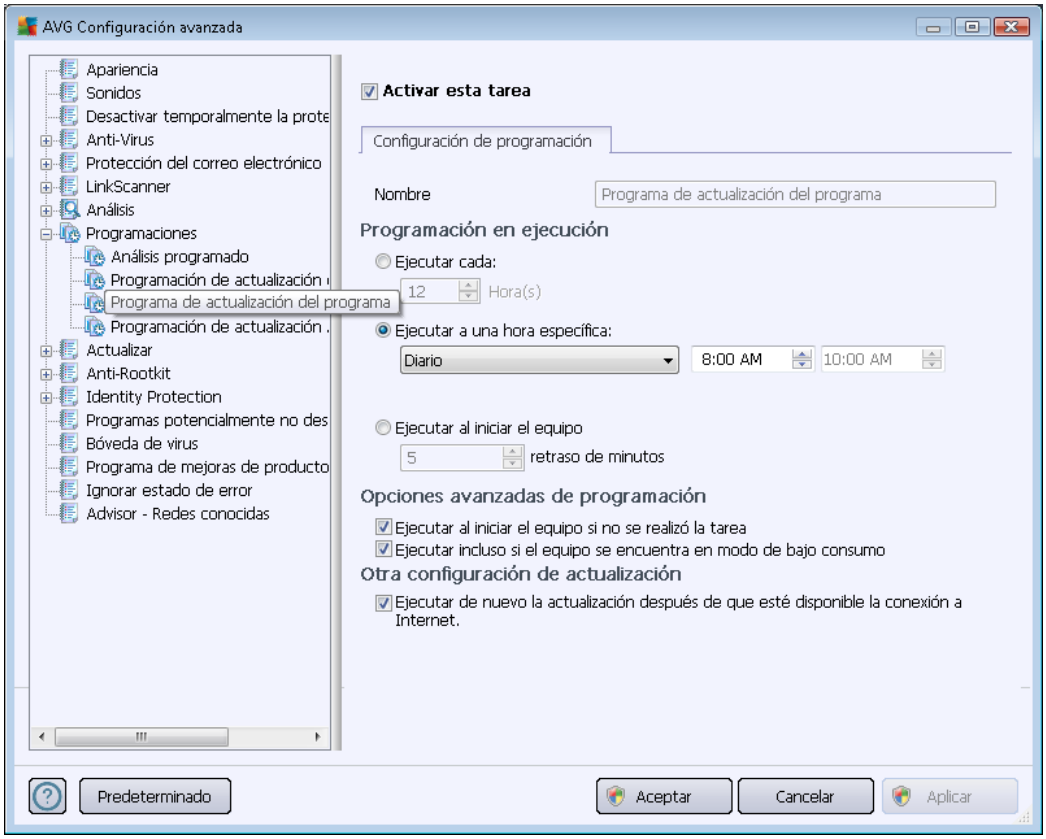
Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización de las definiciones si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

Otra configuración de actualización

Finalmente, seleccione la opción ***Ejecutar de nuevo la actualización después de que esté disponible la conexión a Internet*** para asegurarse de que, en caso de que se interrumpa la conexión a Internet y se detenga el proceso de actualización, éste se vuelva a iniciar tan pronto se restablezca. Una vez que se ejecuta la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el icono de la bandeja del sistema AVG (*siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo Configuración avanzada/Apariencia*).

10.8.3. Programación de actualización del programa

Si es ***realmente necesario***, puede quitar la marca del elemento ***Activar esta tarea*** para desactivar de forma temporal la actualización programada y volverla a activar más adelante:



En el campo de texto denominado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

Programación en ejecución

Aquí, especifique los intervalos de tiempo para la ejecución de la actualización del programa recién programada. El tiempo se puede definir con la ejecución repetida de la actualización después de un

cierto periodo de tiempo (***Ejecutar cada ...***), definiendo una fecha y hora exactas (***Ejecutar a una hora específica ...***) o posiblemente definiendo un evento con el que se debe asociar la ejecución de la actualización (***Acción basada en el inicio del equipo***).

Opciones avanzadas de programación

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

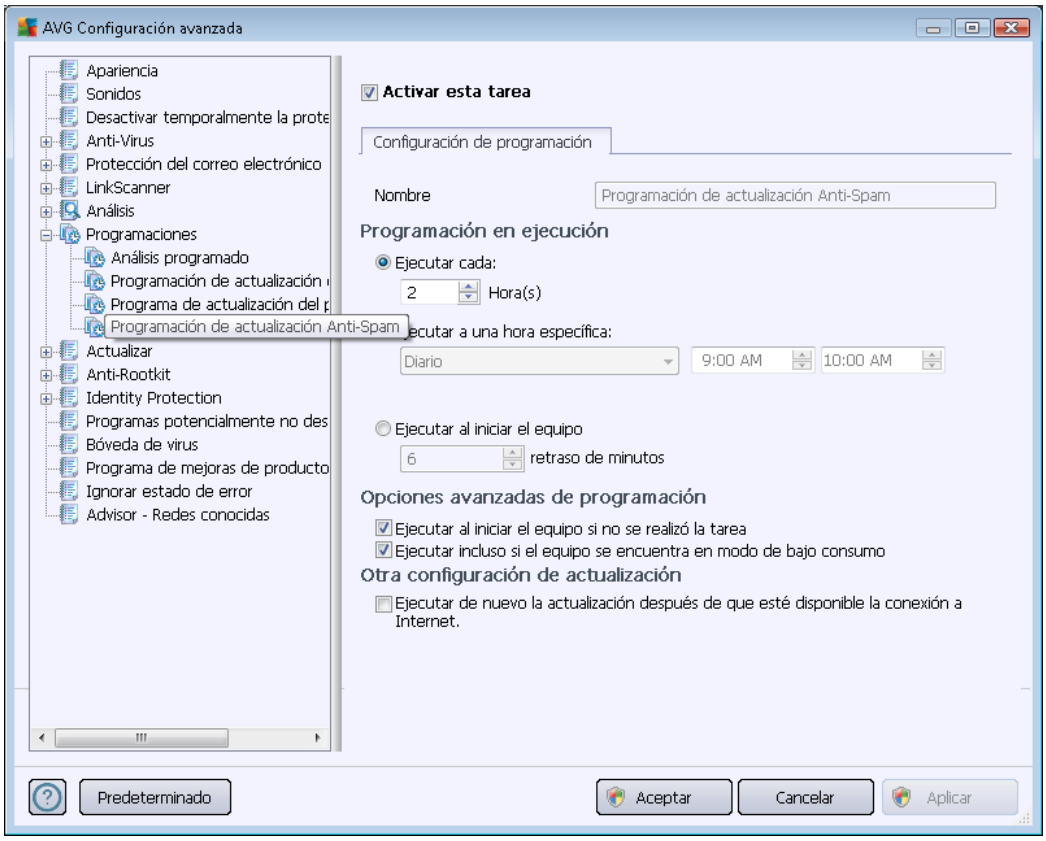
Otra configuración de actualización

Seleccione la opción ***Ejecutar de nuevo la actualización después de que esté disponible la conexión a Internet*** para asegurarse de que en caso de interrupción del proceso de actualización debido a una falla en la conexión a Internet, el proceso se reinicie inmediatamente después de recuperarla. Una vez que se ejecuta la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el icono de la bandeja del sistema AVG (*siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo Configuración avanzada/Apariencia*).

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

10.8.4. Programación de actualización de Anti-Spam

Si es realmente necesario, puede quitar la marca del elemento ***Activar esta tarea*** para desactivar de forma temporal la actualización de Anti-Spam programada y volverla a activar más adelante:



En este cuadro de diálogo puede configurar algunos parámetros detallados de la programación de actualización. En el campo de texto denominado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

Programación en ejecución

Aquí, especifique los intervalos de tiempo de ejecución de la actualización recién programada de Anti-Spam. El tiempo se puede definir con la ejecución repetida de la actualización de Anti-Spam tras un periodo de tiempo determinado (***Ejecutar cada...***), estableciendo una fecha y una hora exactas (***Ejecutar a una hora específica***) o estableciendo un evento al que debe estar asociada la ejecución de la actualización (***Acción basada en el inicio del equipo***).

Opciones avanzadas de programación

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

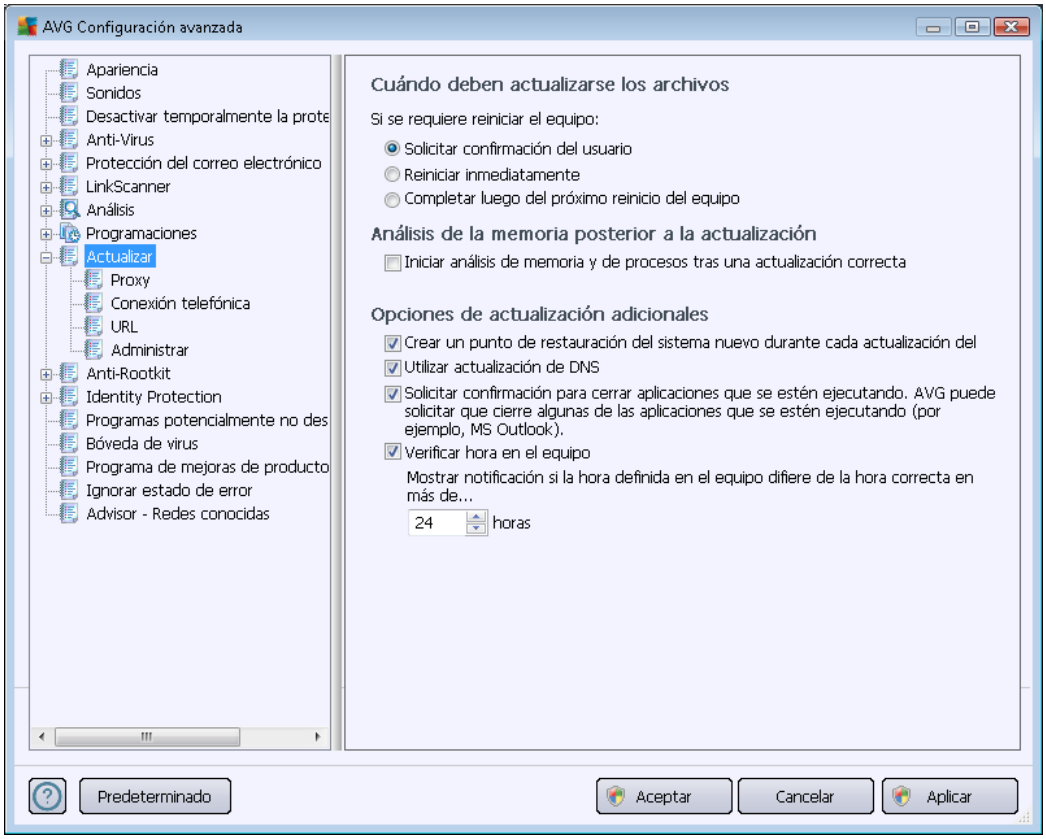
Otra configuración de actualización

Seleccione la opción ***Ejecutar de nuevo la actualización después de que esté disponible la conexión a Internet*** para estar seguro de que si la conexión a Internet se interrumpe y el proceso de actualización de Anti-Spam falla, éste se volverá a ejecutar nuevamente tan pronto como se restaure la conexión a Internet.

Una vez que se inicie 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 cuadro de diálogo Configuración avanzada/Apariencia*) .

10.9. Actualizar

El elemento de navegación ***Actualizar*** abre un nuevo cuadro de 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 tres opciones alternativas para utilizar en caso de que el proceso de actualización requiera un reinicio del equipo. Se puede programar la finalización de la

actualización para el próximo reinicio del equipo, o bien se puede ejecutar el reinicio inmediatamente:

- ***Solicitar confirmación del usuario*** *(activada de forma predeterminada)*: 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, y no será necesaria la aprobación del usuario.
- ***Completar luego del próximo reinicio del equipo***: la finalización del proceso de actualización se pospondrá hasta el próximo reinicio del equipo. Tenga en cuenta que esta opción sólo se recomienda si puede estar seguro de que el equipo se reinicia regularmente, al menos diariamente.

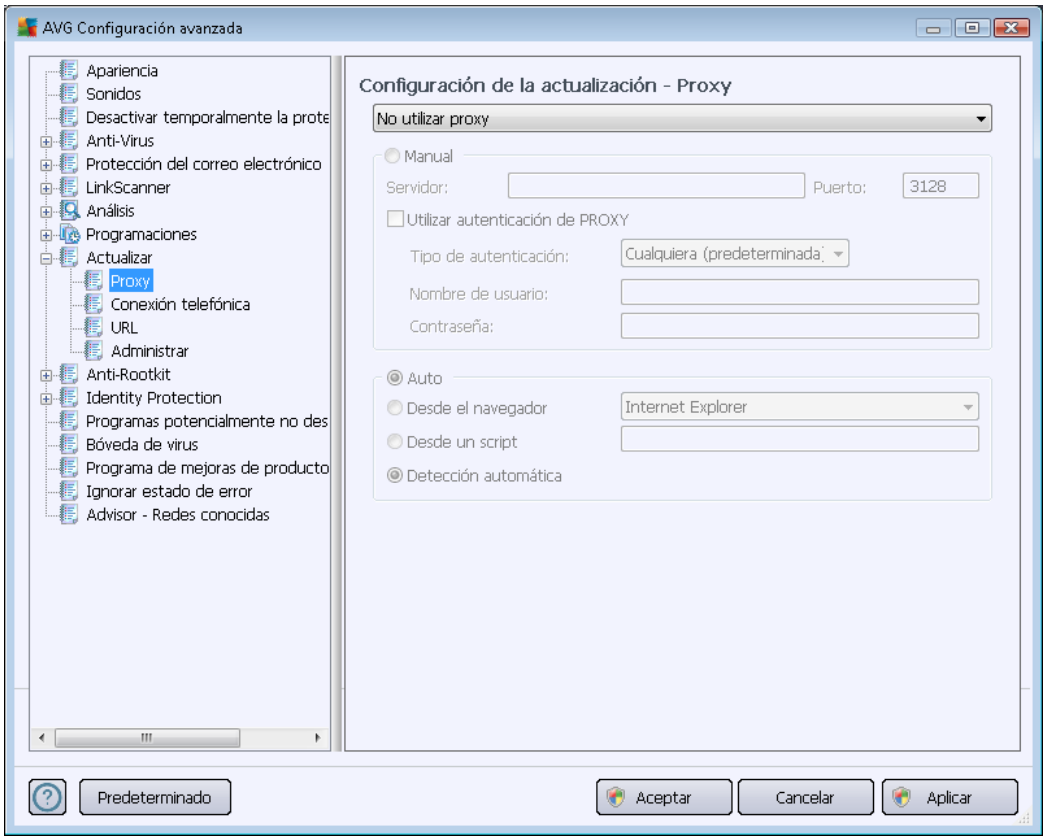
Análisis de la memoria posterior a la actualización

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

Opciones de actualización adicionales

- ***Crear un nuevo punto de restauración del equipo durante cada actualización del programa***: antes de iniciar cada actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Se puede obtener acceso a esta opción mediante Inicio/Todos los programas/Accesorios/ Herramientas del sistema/Restaurar sistema, pero se recomienda que sólo los usuarios experimentados realicen cambios. Mantenga esta casilla seleccionada si desea hacer uso de esta funcionalidad.
- ***Utilizar actualización de DNS*** (*activado de manera predeterminada*): si este elemento está marcado, una vez que se inicia la actualización, su **AVG Internet Security 2012** busca la información sobre la última versión de la base de datos de virus y la última versión del programa en el servidor DNS. A continuación, sólo se descargan y aplican los archivos más pequeños e indispensables para la actualización. De esta manera, se minimiza la cantidad de datos que se deben descargar y el proceso de actualización se ejecuta con mayor rapidez.
- ***Solicitar confirmación para cerrar aplicaciones que se estén ejecutando*** (*activado de forma predeterminada*): con este elemento tendrá la seguridad de que ninguna aplicación actualmente en ejecución se cerrará sin su permiso, si esto se requiere para que el proceso de actualización finalice.
- ***Verificar hora en el equipo***: marque esta opción para declarar que desea recibir una notificación en caso de que la hora del equipo difiera por más horas de las especificadas de la hora correcta.

10.9.1. Proxy



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

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

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

Configuración manual

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

- ***Servidor***: especifique la dirección IP del servidor o el nombre del servidor.

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

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

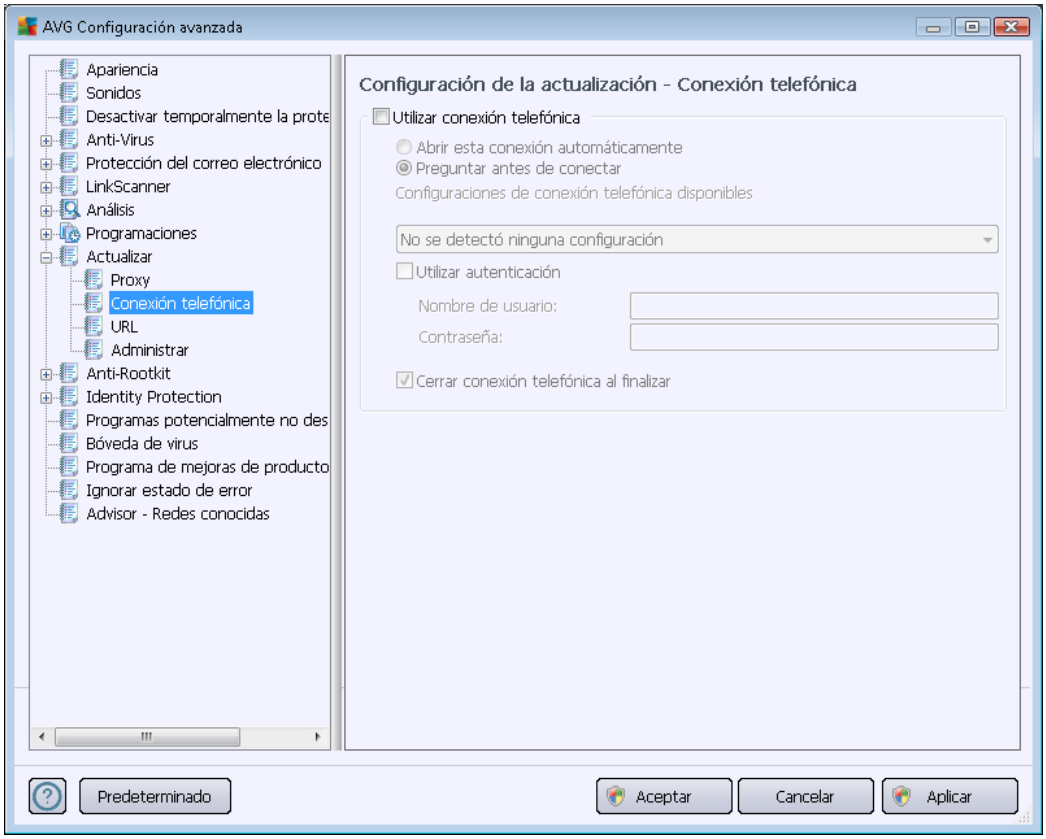
Configuración automática

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

- ***Desde el navegador***: la configuración se obtendrá del navegador de Internet predeterminado
- ***Desde el script***: la configuración se leerá de un script descargado con la dirección de proxy como valor de retorno de la función.
- ***Detección automática***: la configuración se detectará automáticamente desde el servidor proxy

10.9.2. Conexión telefónica

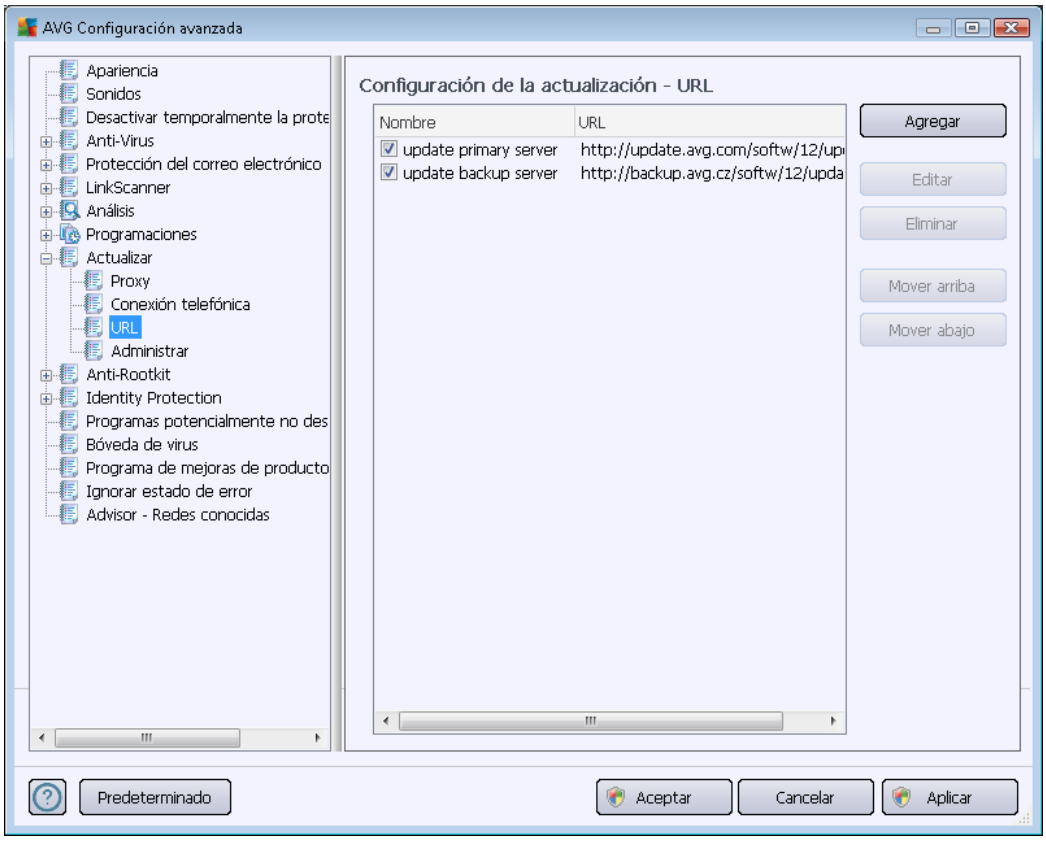
Todos los parámetros definidos de modo opcional en el diálogo ***Actualizar configuración - Conexión telefónica*** hacen referencia a la conexión telefónica a Internet. Los campos del diálogo están inactivos hasta que se selecciona la opción ***Utilizar conexión telefónica***, que los activa:



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

10.9.3. URL

El cuadro de diálogo ***URL*** ofrece una lista de direcciones de Internet desde las que se pueden descargar los archivos de actualización:



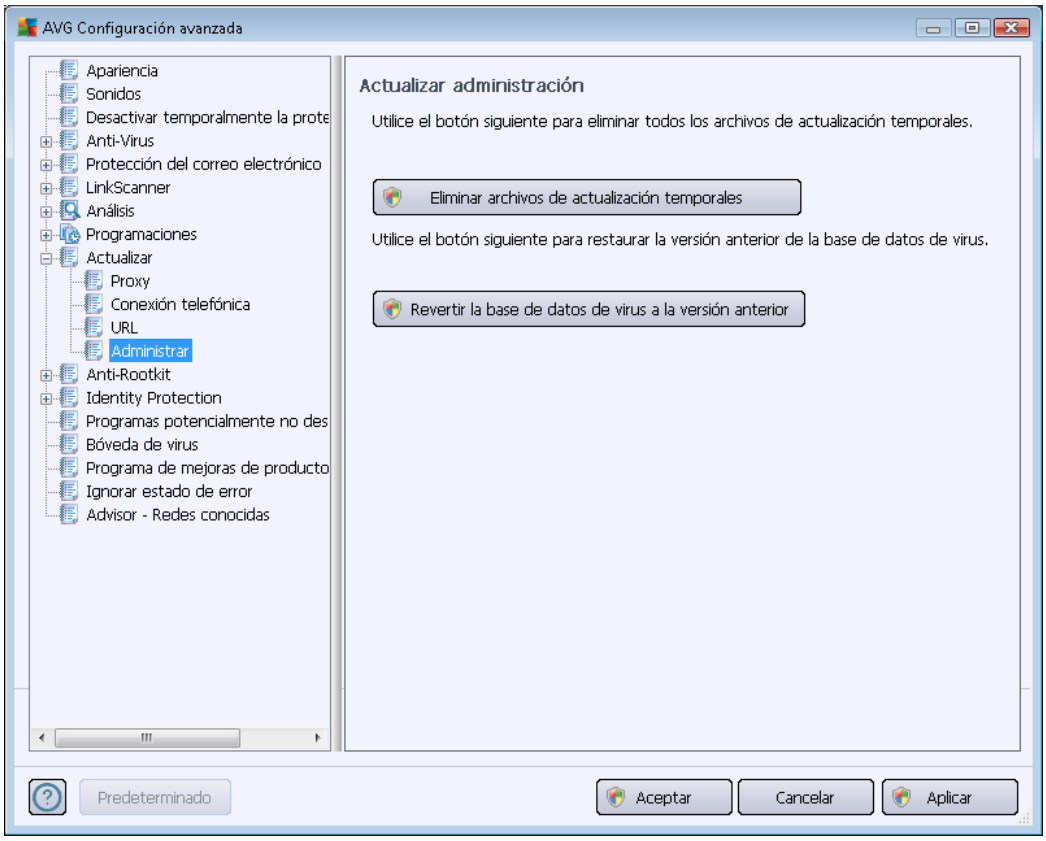
Botones de control

La lista y los elementos se pueden modificar por medio de los siguientes botones de control:

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

10.9.4. Administrar

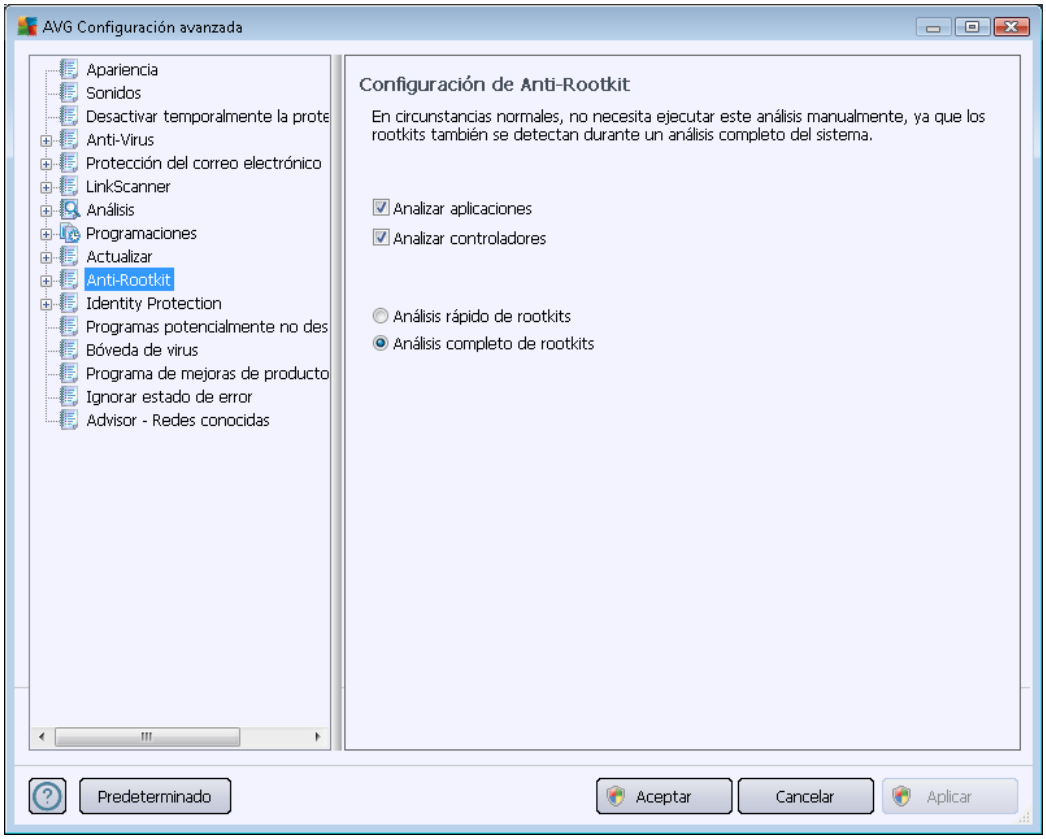
El cuadro de diálogo ***Administración de actualizaciones*** ofrece dos opciones accesibles mediante dos botones:



- ***Eliminar archivos de actualización temporales***: presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada estos archivos se guardan durante 30 días*)
- ***Revertir la base de datos de virus a la versión anterior***: presione este botón para eliminar la última versión de la base de datos de virus del disco duro y volver a la versión anterior guardada (*la nueva versión de la base de datos de virus será parte de la siguiente actualización*).

10.10. Anti-Rootkit

En el cuadro de diálogo ***Configuración de Anti-Rootkit*** puede editar la configuración y los parámetros específicos del análisis del componente Anti-Rootkit. El análisis anti-rootkit es un proceso predeterminado incluido en el Análisis de todo el equipo:



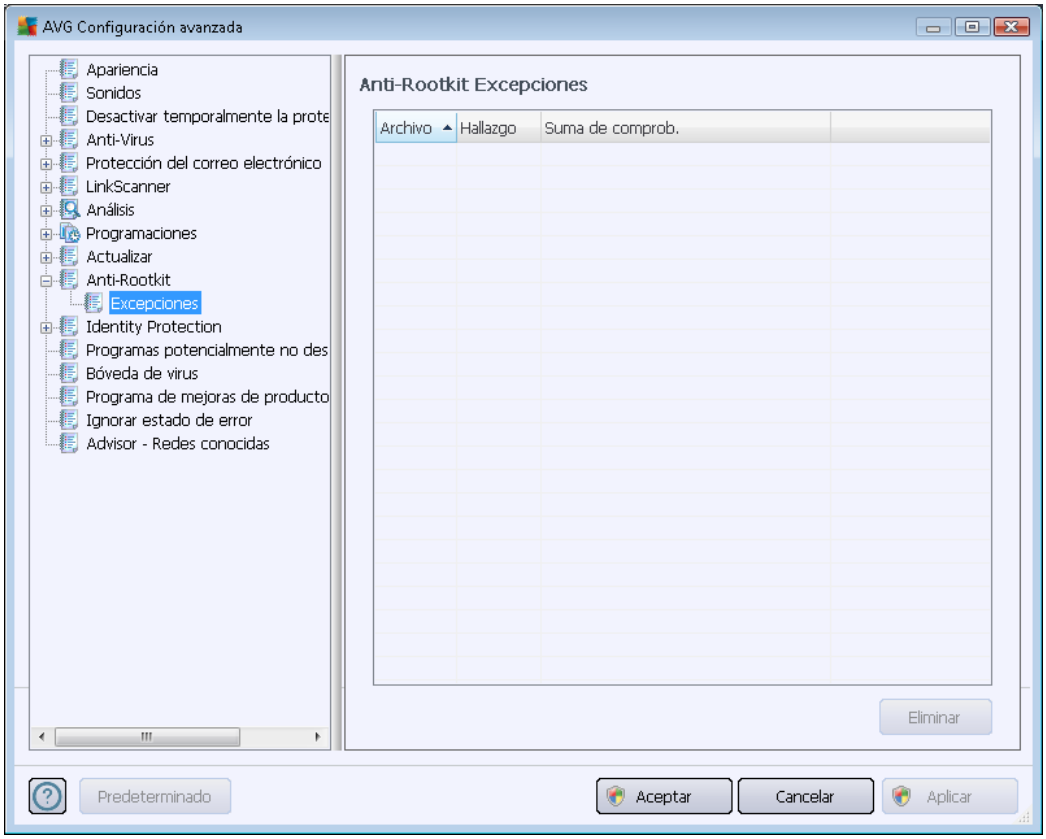
También es posible acceder y editar todas las funciones del componente Anti-Rootkit disponibles en este cuadro de diálogo directamente desde la interfaz del componente Anti-Rootkit.

Analizar aplicaciones y ***Analizar controladores*** le permiten especificar en detalle qué debe incluirse en el análisis anti-rootkit. Esta configuración está diseñada para usuarios avanzados; le recomendamos mantener todas las opciones activadas. También puede seleccionar el modo de análisis de rootkits:

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

10.10.1. Excepciones

En el cuadro de diálogo ***Excepciones de Anti-Rootkit***, puede definir archivos específicos *(por ejemplo, algunos controladores que se pueden detectar de forma falsamente positiva como rootkits)* que se deben excluir de este análisis:

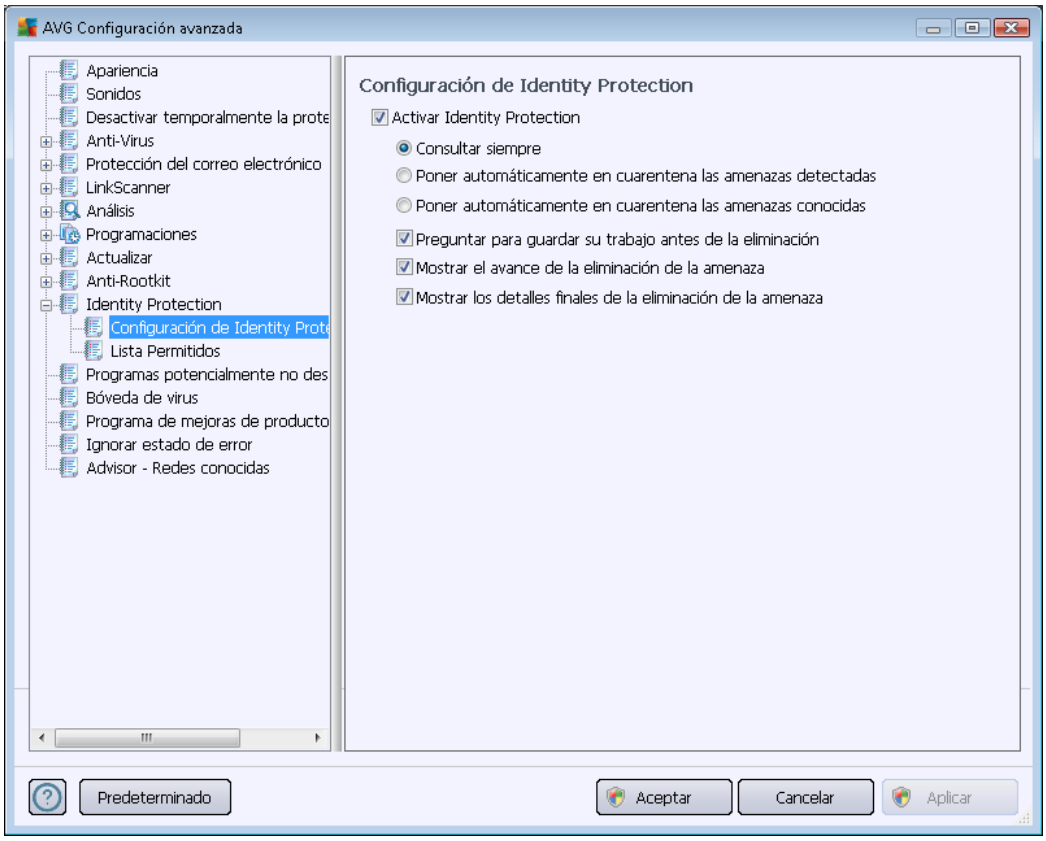


10.11. Identity Protection

Identity Protection es un componente anti-malware que ofrece protección contra todo tipo de malware (*spyware, bots, robo de identidad, etc.*) mediante tecnologías conductuales que proporcionan protección desde el día cero frente a nuevos virus. *(Para obtener una descripción detallada del funcionamiento de los componentes, consulte el capítulo Identity Protection).*

10.11.1. Configuración de Identity Protection

El cuadro de diálogo ***Configuración de Identity Protection*** le permite activar y desactivar las funciones básicas del componente Identity Protection:



Activar Identity Protection (*activada de forma predeterminada*): quite la marca para desactivar el componente Identity Protection.

Sugerimos firmemente no hacer esto a menos que sea absolutamente necesario.

Cuando Identity Protection está activa, se puede especificar qué hacer cuando se detecta una amenaza:

- ***Consultar siempre*** (*activada de forma predeterminada*): cuando se detecte una amenaza se le preguntará si desea ponerla en cuarentena para tener la seguridad de que no se elimine ninguna de las aplicaciones que desee ejecutar.
- ***Poner automáticamente en cuarentena las amenazas detectadas***: seleccione esta casilla de verificación para indicar que desea mover inmediatamente todas las amenazas posibles detectadas al lugar seguro de la Bóveda de virus . Si se mantiene la configuración predeterminada, cuando se detecte una amenaza se le preguntará si desea ponerla en cuarentena para tener la seguridad de que no se elimine ninguna de las aplicaciones que desee ejecutar.
- ***Poner automáticamente en cuarentena las amenazas conocidas***: mantenga este

elemento marcado si desea que todas las aplicaciones detectadas como posible malware se muevan inmediatamente y de forma automática a la Bóveda de virus.

Además, puede asignar elementos concretos para activar de forma opcional más funciones de Identity Protection:

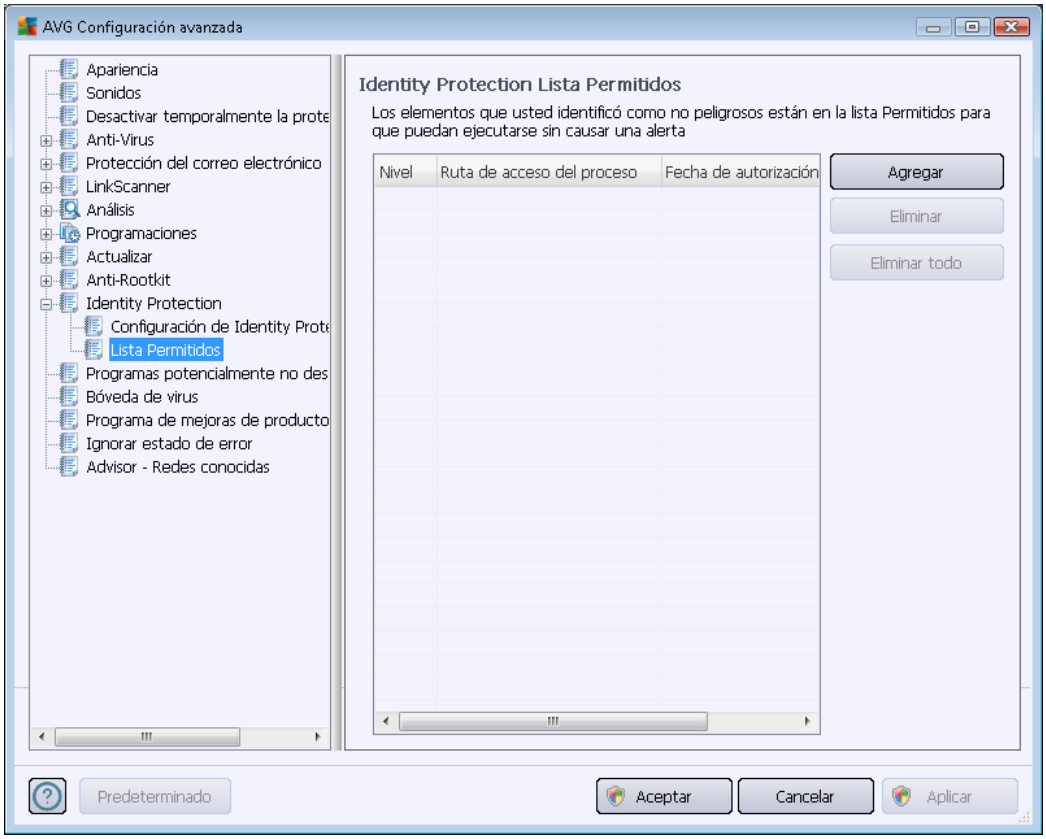
- ***Solicitar guardar el trabajo antes de la eliminación*** (*activada de forma predeterminada*): mantenga este elemento seleccionado si desea que se le avise antes de que la aplicación detectada como posible malware se ponga en cuarentena. En caso de que precisamente sea la aplicación con la que trabaja será necesario guardar el proyecto, ya que podría perderlo. Este elemento está activo de forma predeterminada, y se recomienda encarecidamente conservarlo así.

- ***Mostrar el avance de la eliminación de amenazas*** (*activada de forma predeterminada*): con este elemento activado, cuando se detecta posible malware, se abre un nuevo cuadro de diálogo donde se muestra el progreso del malware puesto en cuarentena.

- ***Mostrar los detalles finales de la eliminación de la amenaza*** (*activada de forma predeterminada*): con este elemento activado, ***Identity Protection*** muestra información detallada acerca de cada objeto puesto en cuarentena (*nivel de severidad, ubicación, etc.*).

10.11.2. Lista Permitidos

Si en el cuadro de diálogo ***Configuración de Identity Protection*** ha decidido mantener el elemento ***Poner automáticamente en cuarentena las amenazas detectadas*** sin seleccionar, cada vez que se detecte malware posiblemente peligroso se le preguntará si se debe eliminar. Si luego asigna la aplicación sospechosa (*detectada según su comportamiento*) como segura y confirma que se debe mantener en el equipo, la aplicación se agregará a la llamada ***Lista Permitidos de Identity Protection*** y no se volverá a notificar como posiblemente peligrosa:



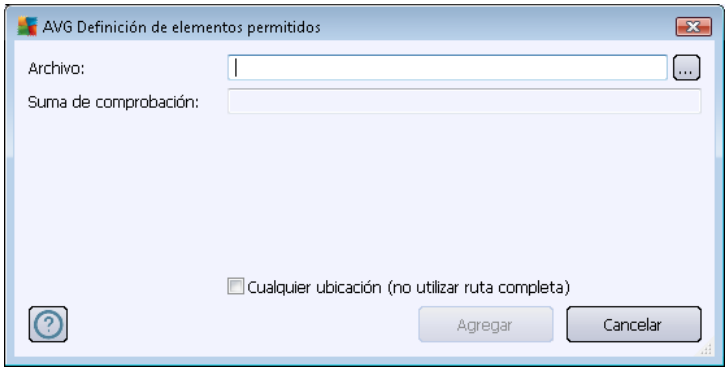
La ***lista Permitidos de Identity Protection*** proporciona la información siguiente sobre cada aplicación:

- ***Nivel***: identificación gráfica de la severidad del proceso correspondiente en una escala de cuatro niveles desde el nivel de menor importancia (■□□□) hasta el nivel crítico (■■■■)
- ***Ruta de acceso del proceso***: ruta de acceso a la ubicación del archivo ejecutable (*proceso*) de la aplicación
- ***Fecha de autorización***: la fecha en que asignó manualmente la aplicación como segura

Botones de control

Los botones de control disponibles en el cuadro de diálogo ***Lista Permitidos de Identity Protection*** son:

- ***Agregar***: presione este botón para agregar una nueva aplicación a la lista Permitidos. Aparece el siguiente cuadro de diálogo emergente:

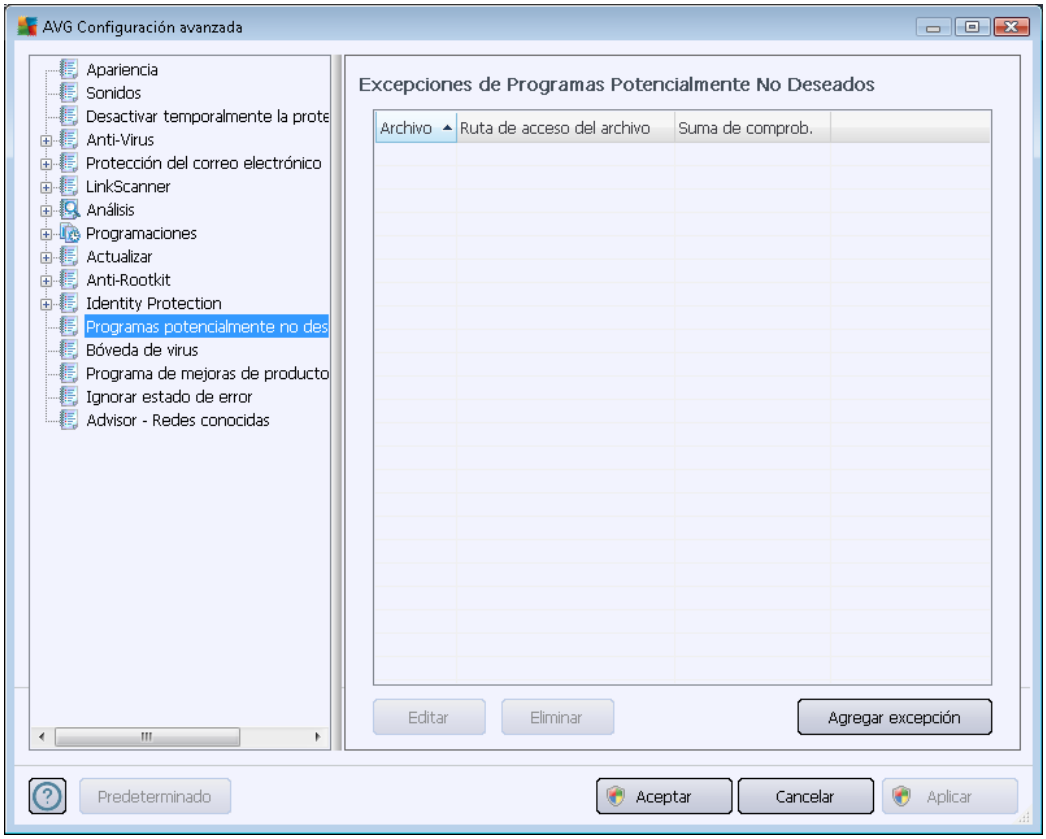


- ***Archivo***: introduzca la ruta completa del archivo (*aplicación*) que desea marcar como excepción
- ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generados automáticamente que permite a AVG distinguir de manera inequívoca los archivos elegidos de otros archivos. La suma de comprobación se genera y se muestra después de haber agregado el archivo correctamente.
- ***Cualquier ubicación (no utilizar ruta completa)***: si desea definir este archivo como excepción sólo para la ubicación específica, deje esta casilla sin seleccionar

- ***Eliminar***: presione este botón para eliminar la aplicación seleccionada de la lista
- ***Eliminar todo***: presione este botón para eliminar todas las aplicaciones de la lista

10.12. Programas potencialmente no deseados

AVG Internet Security 2012 puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas en el sistema. En algunos casos, el usuario puede querer mantener ciertos programas no deseados en el equipo (programas que fueron instalados intencionalmente). Algunos programas, en especial los gratuitos, incluyen adware. **AVG Internet Security 2012** podría detectar este adware y notificarlo 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:



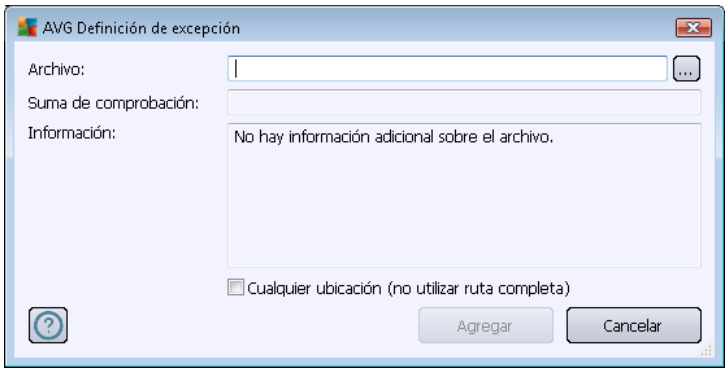
El cuadro de diálogo ***Excepciones de programas potencialmente no deseados*** muestra una lista de excepciones definidas y válidas de programas potencialmente no deseados. Puede editar la lista, eliminar elementos existentes o agregar nuevas excepciones. En la lista, puede encontrar la siguiente información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

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

Botones de control

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

- ***Agregar excepción***: abre un cuadro de diálogo de edición en el cual es posible definir parámetros para una excepción que se creará:



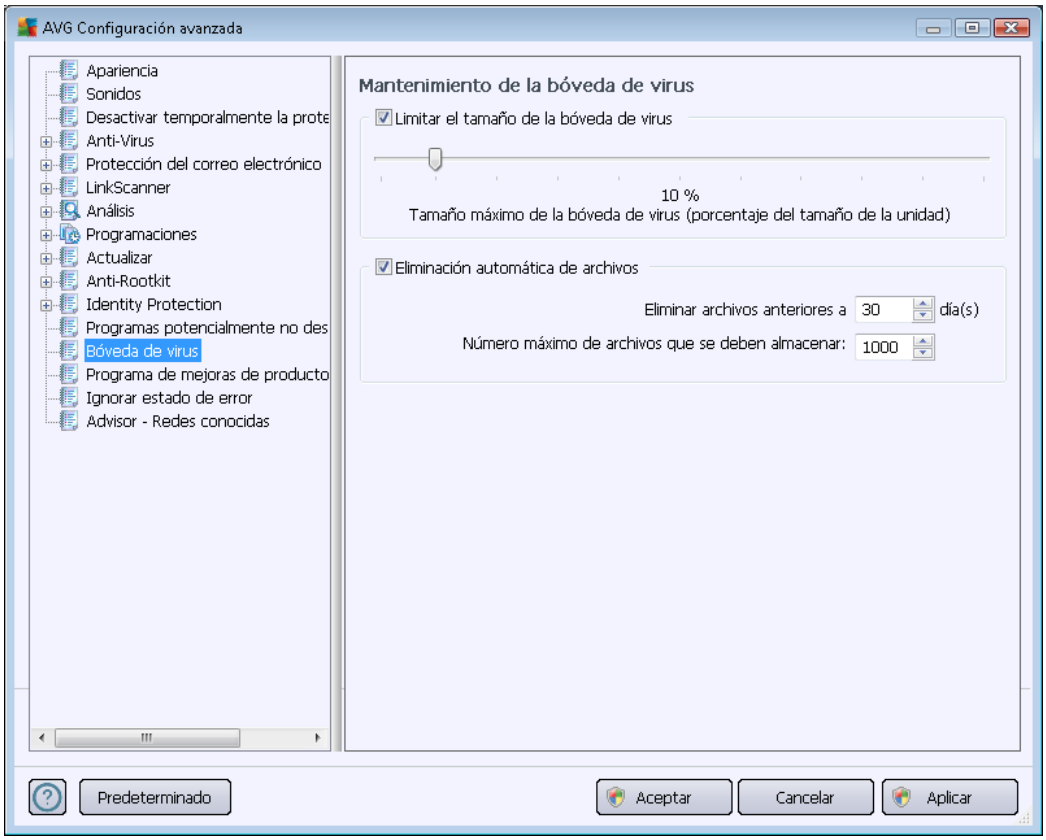
  - ***Archivo***: introduzca la ruta completa del archivo que desea marcar como una excepción

  - ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generados automáticamente que permite a AVG distinguir de manera inequívoca los archivos elegidos de otros archivos. La suma de comprobación 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. *Si la casilla de verificación está marcada, el archivo especificado se define como una excepción independientemente de dónde se encuentre (sin embargo, tendrá que introducir la ruta completa al archivo específico de todas formas; entonces el archivo se usará como único ejemplo en caso que dos archivos del mismo nombre aparezcan en el sistema)*.

10.13. Bóveda de virus



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

- ***Limitar el tamaño de la Bóveda de virus***: utilice el control deslizante para configurar el tamaño máximo de la Bóveda de virus. El tamaño se especifica proporcionalmente en comparación con el tamaño del disco local.

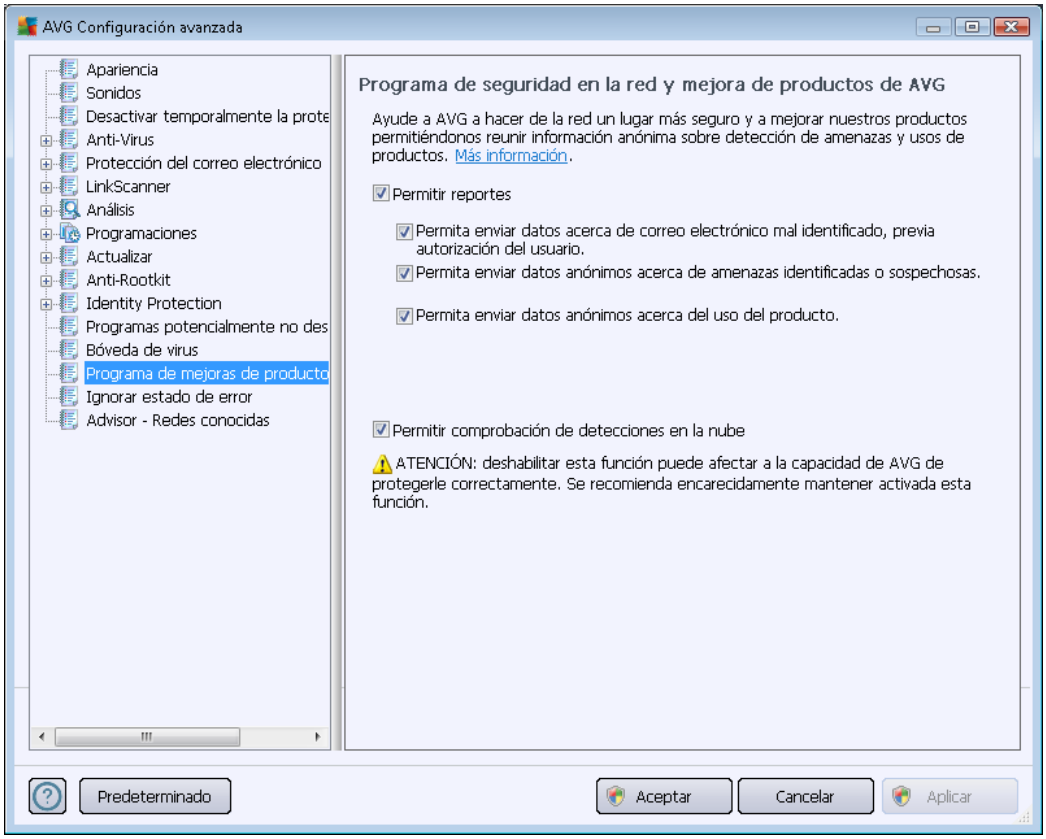
- ***Eliminación automática de archivos***: en esta sección, defina la longitud máxima de tiempo que se almacenarán los objetos en la Bóveda de virus (***Eliminar archivos anteriores a... días***) y el número máximo de archivos que se almacenarán en la Bóveda de virus (***Número máximo de archivos que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

10.14. Programa de mejora de productos

El cuadro de diálogo ***Seguridad en la red y programa de mejora de productos de AVG*** le invita a participar en las mejoras del producto AVG y a ayudarnos a aumentar el nivel general de seguridad en Internet. Mantenga marcada la opción ***Permitir reportes*** para permitir el envío de reportes de las amenazas detectadas a los laboratorios de AVG. Esto ayuda a recopilar información actualizada sobre las últimas amenazas de participantes de todo el mundo y, a cambio, podemos mejorar la protección para todos.

Los reportes se realizan automáticamente, por lo tanto no le causan ninguna molestia, y no

se incluye en ellos ningún dato de identificación personal. Aunque el envío de reportes de las amenazas detectadas es opcional, le pedimos que mantenga activada esta opción puesto que nos ayuda a mejorar la protección para los usuarios de AVG.



En el cuadro de diálogo, están disponibles las siguientes opciones de configuración:

- ***Permitir reportes*** *(activada de forma predeterminada)*: si desea colaborar con nosotros para mejorar **AVG Internet Security 2012**, deje marcada la casilla de verificación. De este modo, se podrán notificar todas las amenazas encontradas a AVG, por lo que podremos recopilar información actualizada sobre malware de todos los participantes repartidos por el mundo y, a cambio, mejorar la protección de todos. Los reportes se realizan automáticamente, por lo tanto no le causan ninguna molestia, y no se incluye en ellos ningún dato de identificación personal.
    - ***Permita enviar datos acerca de correo electrónico mal identificado, previa autorización del usuario*** *(activada de forma predeterminada)*: envíe información sobre mensajes de correo electrónico identificados incorrectamente como spam, o sobre mensajes de spam no detectados por el componente Anti-Spam. Al enviar este tipo de información, se le solicitará su confirmación.
    - ***Permita enviar datos anónimos acerca de amenazas identificadas o sospechosas*** *(activado de forma predeterminada)*: envíe información sobre cualquier código o patrón de conducta sospechoso o definitivamente peligroso *(ya sea un virus, spyware o una página Web maliciosa a la que está intentando obtener*

acceso) detectado en su equipo.

- ***Permita enviar datos anónimos acerca del uso del producto*** *(activado de forma predeterminada)*: envíe datos estadísticos básicos sobre el uso de la aplicación, como el número de detecciones, análisis ejecutados, actualizaciones exitosas o no exitosas, etc.

- ***Permitir la comprobación de las detecciones en la nube*** *(activado de forma predeterminada)*: se comprobará si las amenazas detectadas están realmente infectadas, con el fin de descartar falsos positivos.

Amenazas más comunes

Actualmente, hay muchas más amenazas que los simples virus. Los autores de códigos maliciosos y sitios Web peligrosos son muy innovadores, y frecuentemente surgen nuevos tipos de amenazas, la gran mayoría de las cuales proviene de Internet. Estas son algunas de las más comunes:

- ***Un virus*** es un código malicioso que se copia y propaga por sí solo, frecuentemente sin ser notado hasta que el daño está hecho. Algunos virus son una amenaza seria, eliminando o cambiando deliberadamente los archivos, mientras que otros pueden hacer algo aparentemente inofensivo, como tocar una pieza de música. Sin embargo, todos los virus son peligrosos debido a su capacidad básica para multiplicarse: incluso un virus simple puede apoderarse de toda la memoria del equipo en un instante y causar una falla.

- ***Un gusano*** es una subcategoría de virus que, a diferencia de un virus normal, no necesita un objeto "portador" al que adjuntarse, sino que se envía a sí mismo a otros equipos de manera independiente, normalmente a través del correo electrónico y, como resultado, con frecuencia sobrecarga los servidores de correo electrónico y los sistemas de red.

- ***El spyware*** se define normalmente como una categoría de malware (*malware = cualquier software malicioso, incluyendo programas que contienen virus*), normalmente caballos de Troya, encaminado a robar información personal, contraseñas, números de tarjeta de crédito, o a infiltrarse en un equipo y permitir al atacante controlarlo de manera remota; todo, por supuesto, sin el conocimiento o el consentimiento del propietario del equipo.

- ***Los programas potencialmente no deseados (PUP)*** son un tipo de spyware que puede ser peligroso para su equipo, pero no tiene por qué serlo necesariamente. Un ejemplo específico de un PUP es el adware, un software diseñado para distribuir publicidad, normalmente mostrando ventanas emergentes con anuncios publicitarios; resulta molesto, pero no es realmente nocivo.

- ***Las cookies de rastreo*** también se pueden considerar una clase de spyware, ya que estos pequeños archivos, almacenados en el navegador y enviados automáticamente al sitio Web "primario" cuando lo visita nuevamente, pueden contener datos como su historial de navegación y otra información similar.

- ***Vulnerabilidad*** es un código malicioso que se aprovecha de una falla o vulnerabilidad en un sistema operativo, navegador de Internet u otro programa esencial.

- ***El phishing*** es un intento por conseguir datos personales confidenciales fingiendo ser una

organización confiable y bien conocida. Normalmente, se ponen en contacto con las víctimas potenciales mediante un correo electrónico masivo pidiéndoles, por ejemplo, que actualicen los detalles de su cuenta bancaria. Para hacerlo, se les invita a que sigan el vínculo que se les proporciona, el cual los lleva a un sitio Web del banco falso.

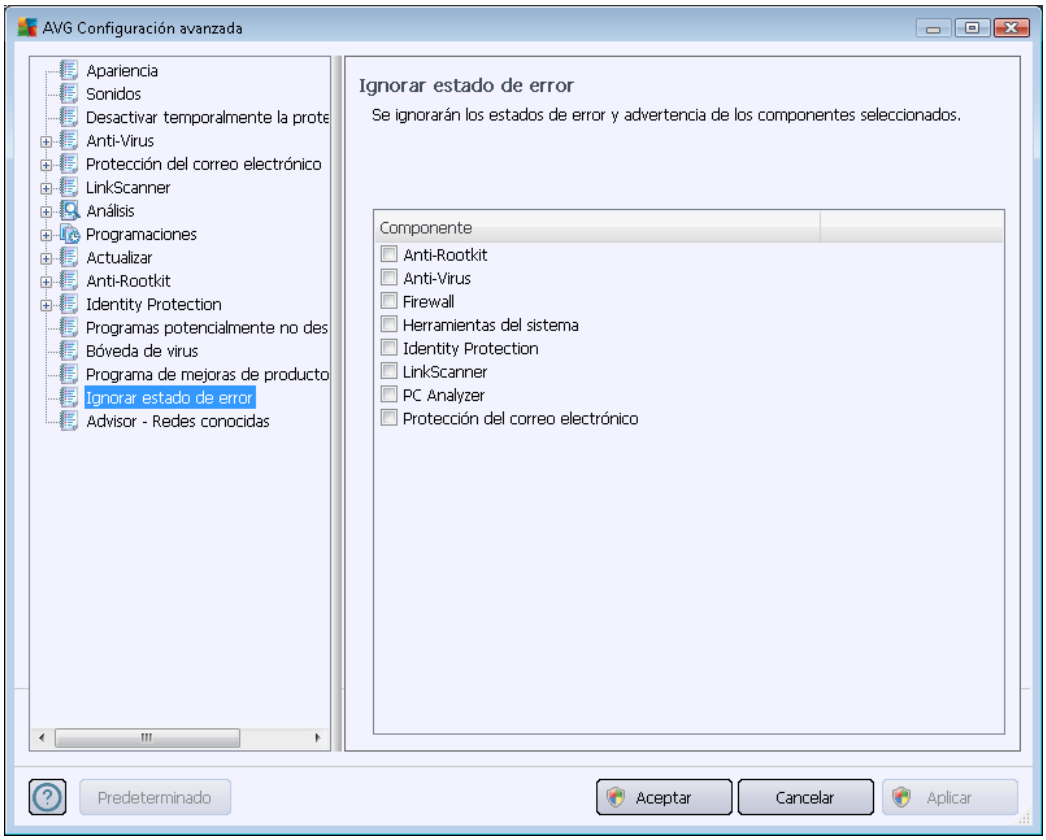
- ***Hoax (engaño)*** es un correo electrónico masivo que contiene información peligrosa, alarmante o sólo molesta e inútil. Muchas de las amenazas anteriores utilizan mensajes de correo electrónico masivo para propagarse.

- ***Los sitios Web maliciosos*** son aquellos que deliberadamente instalan el software malicioso en su equipo, y los sitios objeto de piratería que hacen lo mismo, sólo que estos son sitios Web legítimos que han sido alterados para infectar a los visitantes.

Para protegerle de todos estos tipos diferentes de amenazas, AVG Internet Security 2012 incluye componentes especializados. Para obtener una breve descripción de ellos, consulte el capítulo Descripción general de los componentes.

10.15. Ignorar estado de error

En el cuadro de diálogo ***Ignorar estado de error*** puede marcar aquellos componentes de los que no desea que se le informe:



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

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

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

Puede haber una situación en la cual por alguna razón es necesario desactivar un componente temporalmente (*no es recomendable, se debe intentar conservar todos los componentes activados permanentemente y con la configuración predeterminada, pero esto puede suceder*). En ese caso el icono en la bandeja de sistema informa automáticamente del estado de error del componente. Sin embargo, en este caso específico no podemos hablar de un error real debido a que usted mismo lo introdujo deliberadamente, y está consciente del riesgo potencial. A su vez, una vez que el icono se muestra en color gris, no puede informar realmente de ningún error adicional posible que pueda aparecer.

Para esta situación, dentro del cuadro de 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 *(Ignorar el estado del componente)* también está disponible para componentes específicos directamente desde la descripción general de los componentes en la ventana principal de AVG.

10.16. Advisor - Redes conocidas

El AVG Advisor incluye una función que monitorea redes a las cuales se conecta, y *si detecta una red nueva (con el nombre de una red ya utilizada, lo cual puede generar confusión)* lo notificará y le recomendará que verifique la seguridad de la red. Si decide que es seguro conectarse a la nueva red, también puede guardarla en esta lista; AVG Advisor recordará los atributos únicos de la red *(específicamente la dirección MAC)* y no volverá a mostrar la notificación.

En esta ventana de diálogo, puede comprobar qué redes ha guardado previamente como conocidas. Puede eliminar entradas individuales presionando el botón ***Eliminar***; la red respectiva se considerará como desconocida y potencialmente insegura nuevamente.

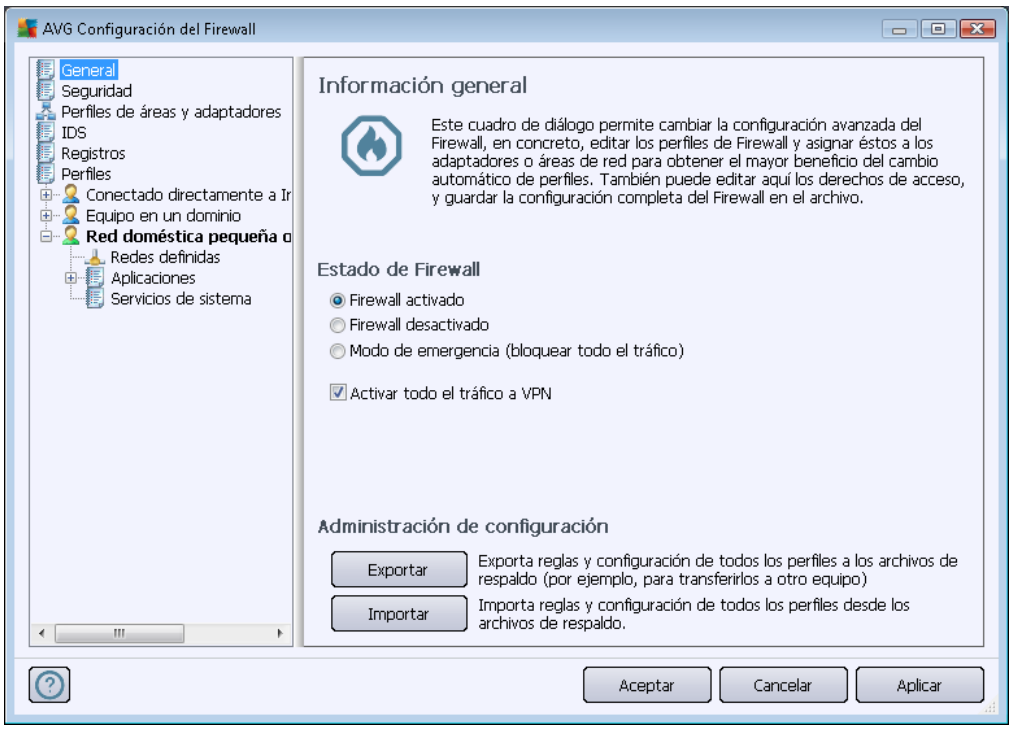
11. Configuración del Firewall

La configuración del Firewall se abre en una nueva ventana donde se pueden establecer parámetros muy avanzados del componente en varios cuadros de diálogo.

No obstante, el proveedor del software ha configurado todos los componentes de AVG Internet Security 2012 para que ofrezcan un rendimiento óptimo. No modifique la configuración predeterminada salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración.

11.1. General

El cuadro de diálogo ***Información general*** está dividido en dos secciones:



Estado del Firewall

En la sección ***Estado del Firewall*** puede cambiar el estado del Firewall cuando sea necesario:

- ***Firewall activado***: seleccione esta opción para permitir la comunicación con aquellas aplicaciones que tienen la asignación de 'permitido' en el conjunto de reglas definido dentro del Perfil de Firewall seleccionado..
- ***Firewall desactivado***: esta opción desactiva el Firewall por completo, se permite todo el tráfico, pero no se analiza.
- ***Modo de emergencia (bloquear todo el tráfico)***: seleccione esta opción para bloquear

todo el tráfico en todos los puertos de red; el Firewall continuará en ejecución, pero se detendrá todo el tráfico de red.

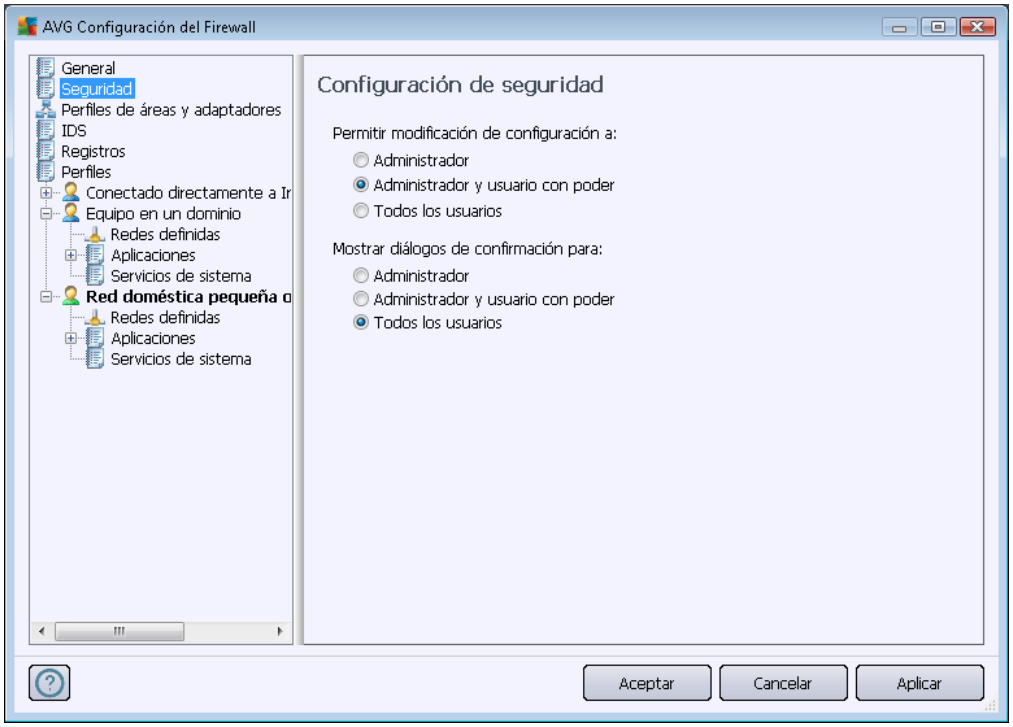
- ***Activar todo el tráfico a VPN*** *(activado de forma predeterminada)*: si utiliza una conexión VPN *(Red privada virtual)* para, por ejemplo, conectarse a su oficina desde su casa, recomendamos seleccionar la casilla. ***Firewall AVG*** busca automáticamente a través de sus adaptadores de red, encuentra los usados para la conexión VPN y permite que todas las aplicaciones se conecten a la red de destino *(esto sólo se aplica a las aplicaciones sin una regla específica de firewall asignada)*. En un sistema estándar con adaptadores de red comunes, este sencillo paso le evita tener que configurar una regla detallada para cada aplicación que necesita usar a través de VPN.

Nota: *para permitir la conexión VPN en todo momento, es necesario permitir la comunicación con los siguientes protocolos del sistema: GRE, ESP, L2TP, PPTP. Esto se puede hacer en el cuadro de diálogo Servicios de sistema.*

Administración de configuración

En la sección ***Administración de configuración*** puede ***exportar*** o ***importar*** la configuración del Firewall; es decir, exportar las reglas del Firewall definidas y la configuración a los archivos de copia de resguardo o, por otro lado, importar todo el archivo de copia de resguardo.

11.2. Seguridad



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

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

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

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

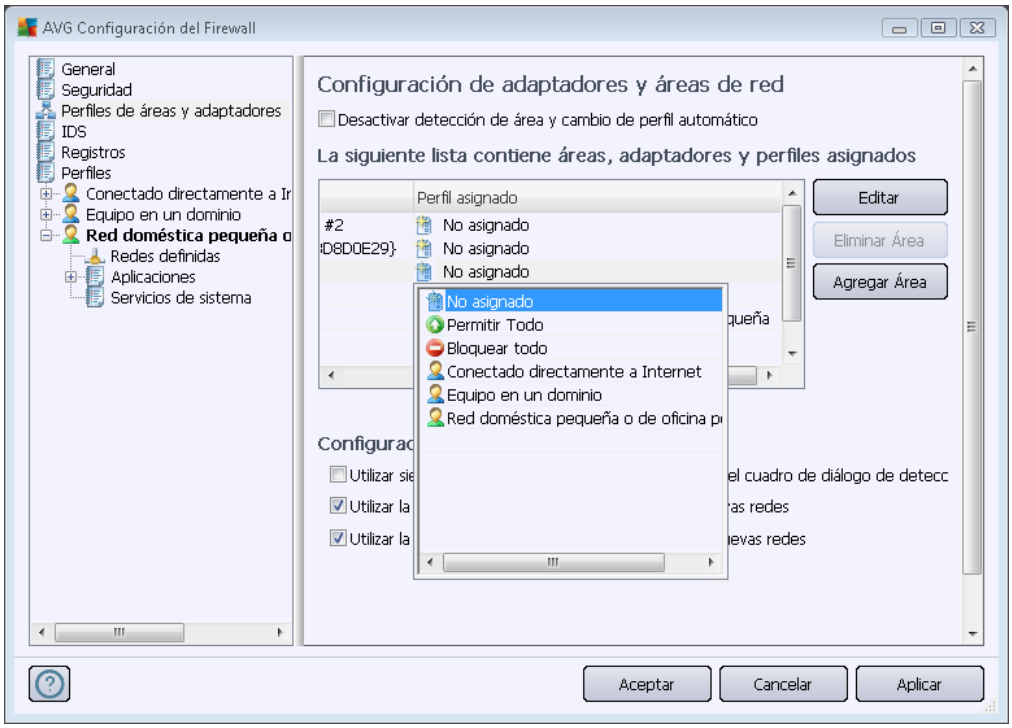
- ***Administrador***: controla el equipo por completo y tiene derecho a asignar a cada usuario a grupos con autoridades específicamente definidas.

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

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

11.3. Perfiles de áreas y adaptadores

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



- ***Desactivar detección de área y cambio de perfil automático*** *(desactivada de forma*

predeterminada): uno de los perfiles definidos puede asignarse a cada tipo de interfaz de red, de forma respectiva a cada área. Si no desea definir perfiles específicos, se utilizará un perfil común. Sin embargo, si decide diferenciar los perfiles y asignarlos a áreas y adaptadores específicos, y después, por alguna razón, desea cambiar esta configuración de forma temporal, haga clic en la opción ***Deshabilitar la detección de área y el cambio automático de perfiles***.

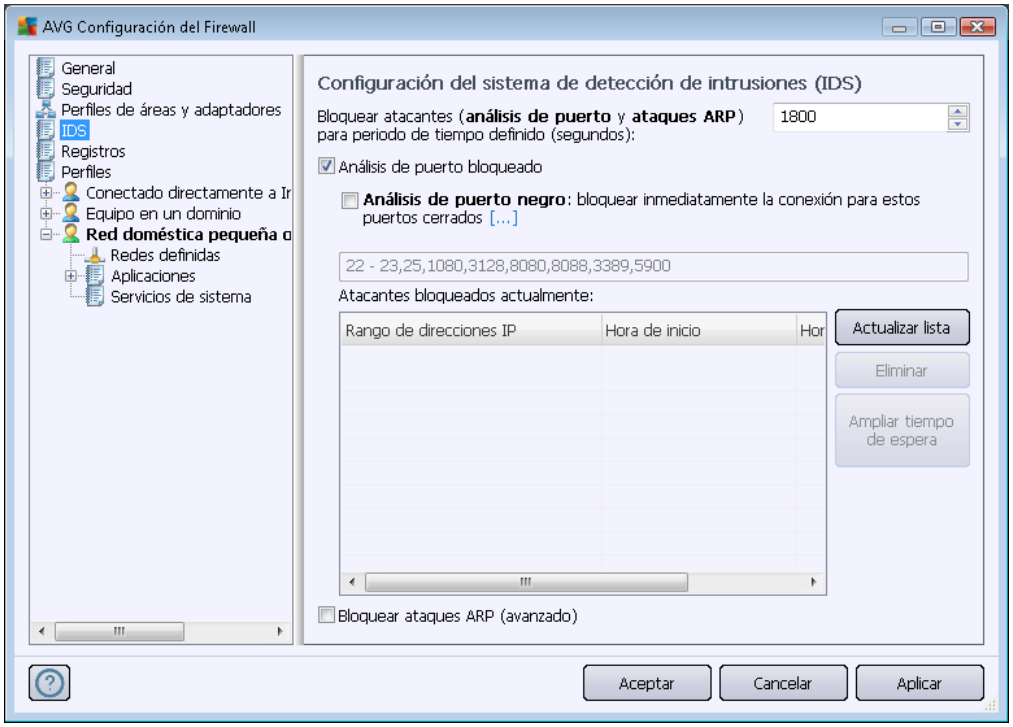
- ***Lista de adaptadores, áreas y perfiles asignados***: en esta lista puede encontrar una descripción general de los adaptadores y áreas detectados. Para cada uno de ellos, puede asignar un perfil específico en el menú de perfiles definidos. Para abrir este menú, haga clic con el botón principal en el elemento respectivo de la lista de adaptadores *(en la columna Perfil asignado)* y seleccione el perfil en el menú contextual.

Configuración avanzada

- ***Utilizar siempre el perfil predeterminado y no mostrar el cuadro de diálogo de detección de nuevas redes***: siempre que el equipo se conecte a una red nueva, el Firewall le alertará y mostrará un cuadro de diálogo en el que se le solicitará que seleccione un tipo de conexión de red y que le asigne un perfil de Firewall. Si no desea que se muestre este cuadro de diálogo, marque esta casilla.
- ***Utilizar la heurística de AVG para la detección de nuevas redes***: permite la recopilación de información sobre redes recién detectadas con el mecanismo propio de AVG (*sin embargo, esta opción sólo está disponible en los sistemas operativos VISTA y superiores*).
- ***Utilizar la heurística de Microsoft para la detección de nuevas redes***: permite obtener información de las redes recién detectadas del servicio de Windows (*esta opción sólo está disponible en Windows Vista y superiores*).

11.4. IDS

El sistema de detección de intrusiones es una función especial de análisis del comportamiento diseñada para identificar y bloquear intentos de comunicación sospechosos en puertos específicos del equipo. Puede configurar los parámetros de IDS en el cuadro de diálogo ***Configuración del sistema de detección de intrusiones (IDS)***:



El cuadro de diálogo ***Configuración del sistema de detección de intrusiones (IDS)*** ofrece estas opciones de configuración:

- ***Bloquear atacantes (análisis de puerto y ataques ARP) para periodo de tiempo definido***: aquí puede especificar cuántos segundos debe estar bloqueado un puerto, siempre que se detecte un intento de comunicación sospechoso en él. De forma predeterminada, el intervalo de tiempo está establecido en 1800 segundos (*30 minutos*).

- ***Análisis de puerto bloqueado*** *(activado de forma predeterminada)*: seleccione la casilla para bloquear los intentos de comunicación en todos los puertos TCP y UDP del equipo procedentes del exterior. Para estos tipos de conexión, se permiten cinco intentos y el sexto se bloquea. Este elemento está activado de forma predeterminada y se recomienda mantener su configuración. Si deja la opción ***Análisis de puerto bloqueado*** activada, habrá disponibles algunas otras opciones de configuración detallada *(de lo contrario, el elemento siguiente estará desactivado)*:

    - ***Análisis de puerto negro***: seleccione la casilla para bloquear inmediatamente cualquier intento de comunicación en los puertos especificados en el campo de texto de abajo. Los distintos puertos o rangos de puertos se deben separar mediante comas. Hay una lista predefinida de puertos recomendados por si desea utilizar esta función.

    - Atacantes bloqueados actualmente: en esta sección se enumeran los intentos de comunicación que el Firewall tiene bloqueados actualmente. El historial completo de los intentos bloqueados se puede visualizar en el cuadro de diálogo Registros (*pestaña Registros de análisis de puertos*).

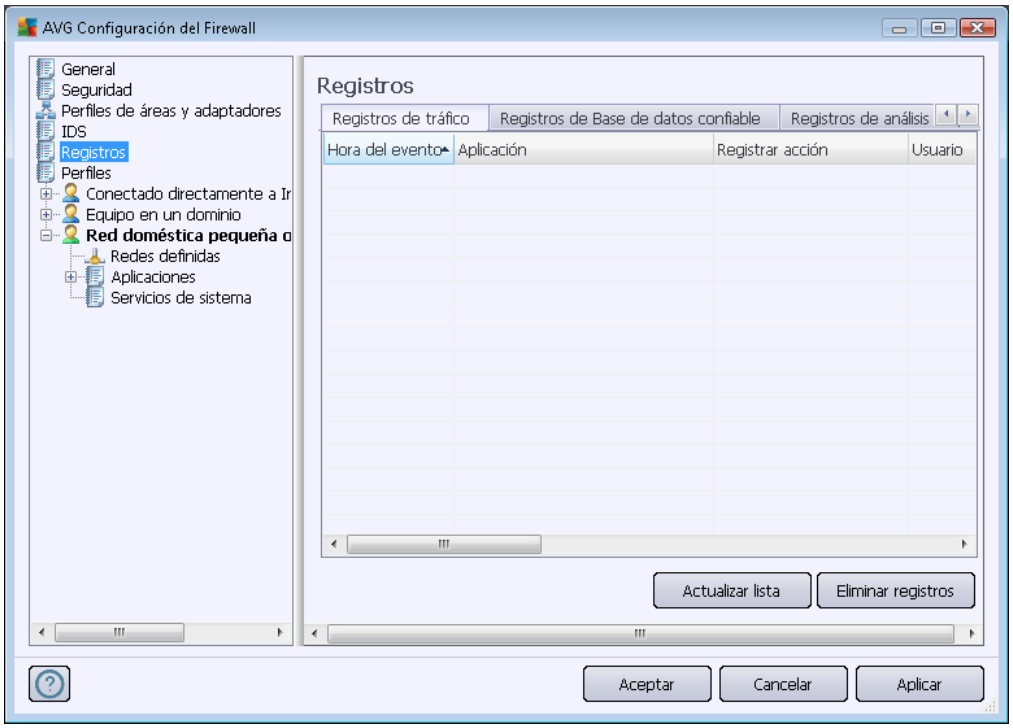
- ***Bloquear ataques ARP (avanzado)*** *(desactivada de forma predeterminada)*: marque esta

opción para activar el bloqueo de intentos de comunicación de tipo especial dentro de una red local detectados por ***IDS*** como potencialmente peligrosos. Se aplica el tiempo establecido en ***Bloquear atacantes para periodo de tiempo definido***. Recomendamos que sólo los usuarios avanzados, familiares con el tipo y el nivel de riesgo de su red, utilicen esta función.

Botones de control

- ***Actualizar lista***: presione este botón para actualizar la lista (*para incluir los últimos intentos bloqueados*)
- ***Eliminar***: presione para cancelar un bloqueo seleccionado
- ***Ampliar tiempo de espera***: presione para prolongar el periodo de tiempo durante el que está bloqueado un intento seleccionado. Aparecerá un nuevo cuadro de diálogo con opciones avanzadas, que permite establecer una fecha y hora específicas o una duración ilimitada.

11.5. Registros



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

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

- ***Registros de Base de datos confiable***: la *Base de datos confiable* es la base de datos interna de AVG que recopila información acerca de aplicaciones certificadas y confiables a las que siempre se les puede permitir comunicarse en línea. La primera vez que una nueva aplicación intenta conectarse a la red (*es decir, aún no existen reglas del firewall especificadas para esta aplicación*), es necesario determinar si se le debe permitir la comunicación con la red. Primero, AVG busca en la *Base de datos confiable* y, si la aplicación se encuentra en la lista, se le concederá automáticamente acceso a la red. Sólo después de que se comprueba que no existe información disponible acerca de la aplicación en la base de datos, se le preguntará en un cuadro de diálogo independiente si desea permitir que la aplicación obtenga acceso a la red.

- ***Registros de análisis de puertos***: proporciona el registro de todas las actividades del sistema de detección de intrusiones.

- ***Registros de ARP***: información de registro sobre el bloqueo de clases especiales de intentos de comunicación dentro de una red local (opción *Bloquear ataques ARP*) detectados por el sistema de detección de intrusiones como potencialmente peligrosos.

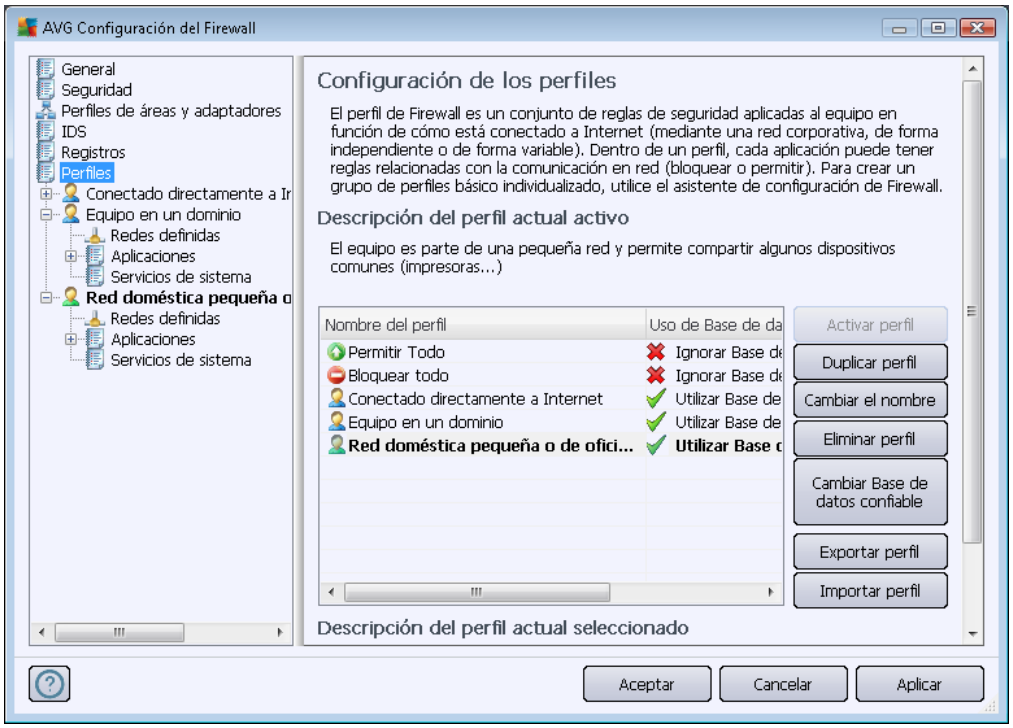
Botones de control

- ***Actualizar lista***: todos los parámetros registrados se pueden organizar de acuerdo al atributo seleccionado: cronológicamente (*fechas*) o alfabéticamente (*otras columnas*); sólo haga clic en el encabezado de la columna respectiva. Utilice el botón ***Actualizar lista*** para actualizar la información actualmente mostrada.

- ***Eliminar registros***: presione este botón para eliminar todas las entradas del gráfico.

11.6. Perfiles

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



Los perfiles del sistema *(Permitir todo, Bloquear todo)* no se pueden editar. Sin embargo, todos los perfiles *personalizados (Conectado directamente a Internet, Equipo en un dominio, Red doméstica pequeña o de oficina pequeña)* se pueden editar luego en este cuadro de diálogo mediante los siguientes botones de control:

- ***Activar perfil***: este botón establece el perfil seleccionado como activo, lo cual significa que el Firewall utilizará el perfil seleccionado para controlar el tráfico de la red.
- ***Duplicar perfil***: crea una copia idéntica del perfil seleccionado; posteriormente es posible editar y cambiar el nombre de la copia para crear un perfil nuevo basado en el original duplicado.
- ***Cambiar el nombre del perfil***: permite definir un nombre nuevo para un perfil seleccionado.
- ***Eliminar perfil***: elimina el perfil seleccionado de la lista.
- ***Cambiar Base de datos confiable***: para el perfil seleccionado puede elegir utilizar la información de la *Base de datos confiable (la Base de datos confiable es una base de datos interna de AVG que recopila información acerca de las aplicaciones confiables y certificadas a las cuales siempre se puede permitir la comunicación en línea.*).
- ***Exportar perfil***: registra la configuración del perfil seleccionado en un archivo que se

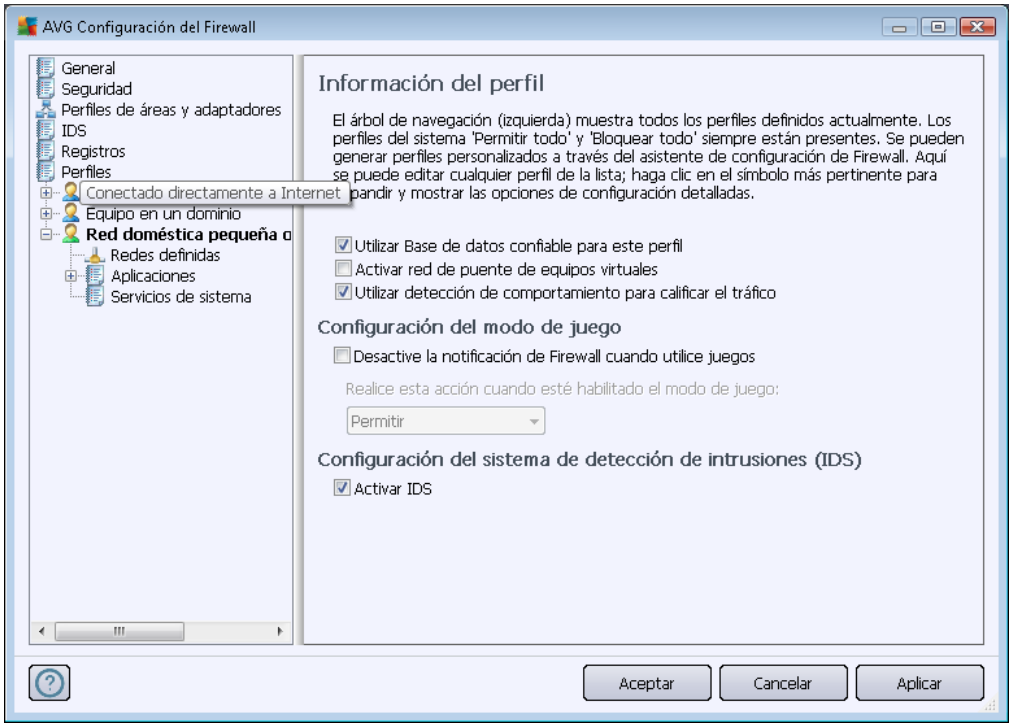
guardará para utilizarse en el futuro.

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

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

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

11.6.1. Información del perfil



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

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

- ***Activar red de puente de equipos virtuales*** (*desactivado de forma predeterminada*): marque este elemento para permitir que las máquinas virtuales de VMware se conecten directamente a la red.

- ***Utilizar detección de comportamiento para calificar el tráfico*** (*activada de forma predeterminada*): marque esta opción para permitir que el Firewall utilice la función Identity Protection al evaluar una aplicación. Identity Protection puede determinar si la aplicación muestra algún comportamiento sospechoso o si se puede confiar en ella y se le debe permitir la comunicación en línea.

Configuración del modo de juego

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

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

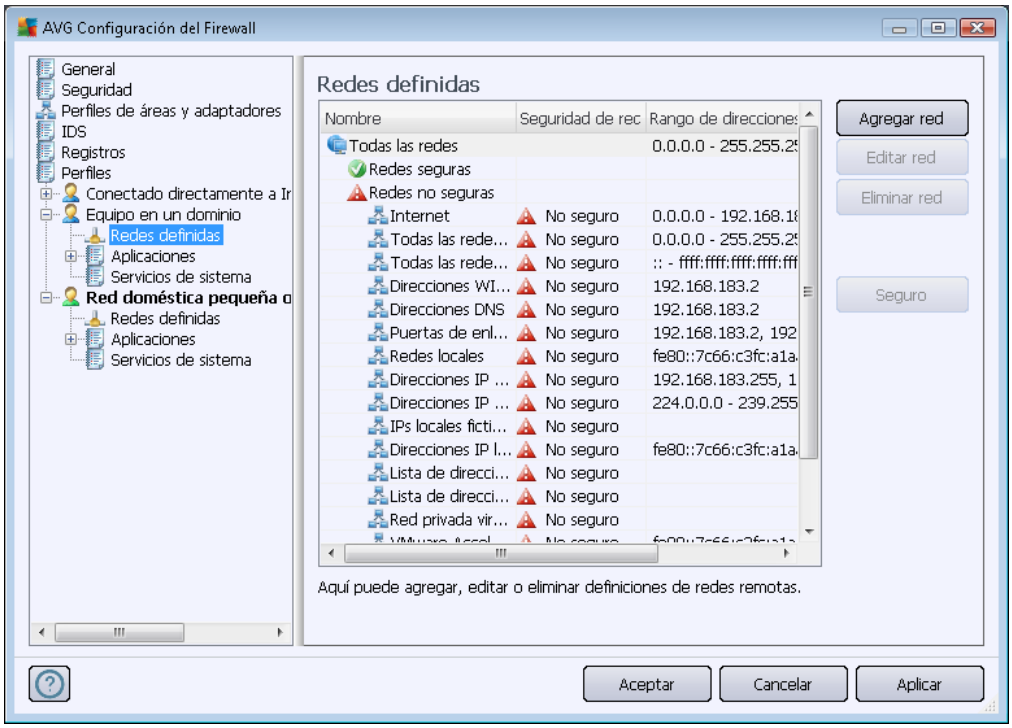
Cuando está activado el modo de juego, todas las tareas programadas (*análisis y actualizaciones*) se posponen hasta que la aplicación se cierra.

Configuración del sistema de detección de intrusiones (IDS)

Marque la casilla de verificación ***Activar IDS*** para activar una función especial de análisis diseñada para identificar y bloquear intentos de comunicación sospechosos a través de determinados puertos de su equipo *(para obtener más detalles sobre la configuración de esta función, consulte el capítulo sobre IDS de esta documentación).*

11.6.2. Redes definidas

El cuadro de diálogo ***Redes definidas*** ofrece una lista de todas las redes a las que está conectado su equipo.

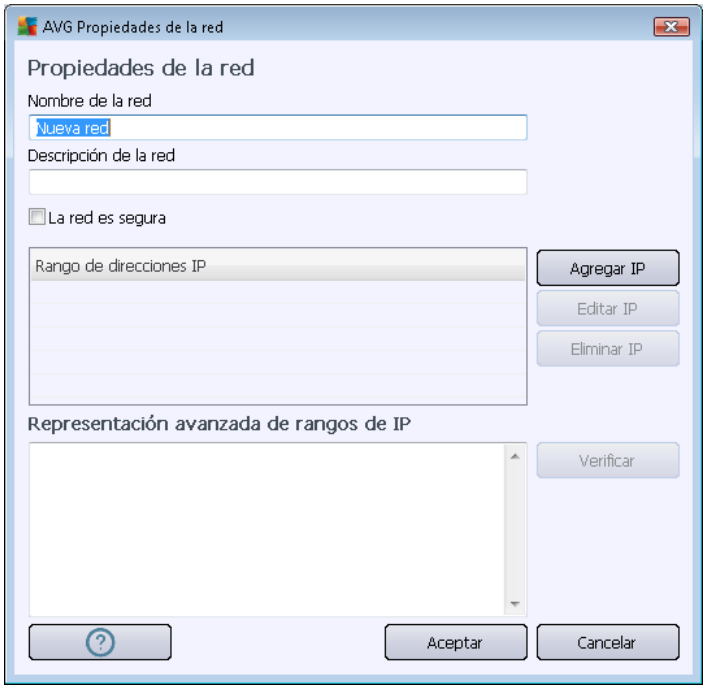


La lista proporciona la siguiente información sobre cada red detectada:

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

Botones de control

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



Dentro de este cuadro de diálogo, puede especificar el ***Nombre de la red***, dar la ***Descripción de la red*** y posiblemente asignar la red como segura. La nueva red puede definirse de forma manual en un cuadro de diálogo independiente que se abre mediante el botón ***Agregar IP*** (de forma alternativa, ***Editar IP***/***Eliminar IP***); dentro de este cuadro de diálogo puede especificar la red utilizando su rango o máscara IP. Para establecer varias redes que deben definirse como parte de una red creada recientemente, puede utilizar la opción ***Representación avanzada de rangos de IP***: introduzca la lista de todas las redes en el campo de texto respectivo (*es compatible con cualquier formato estándar*) y presione el botón ***Verificar*** para asegurarse de que se pueda reconocer el formato. A continuación, presione ***Aceptar*** para confirmar y guardar la información.

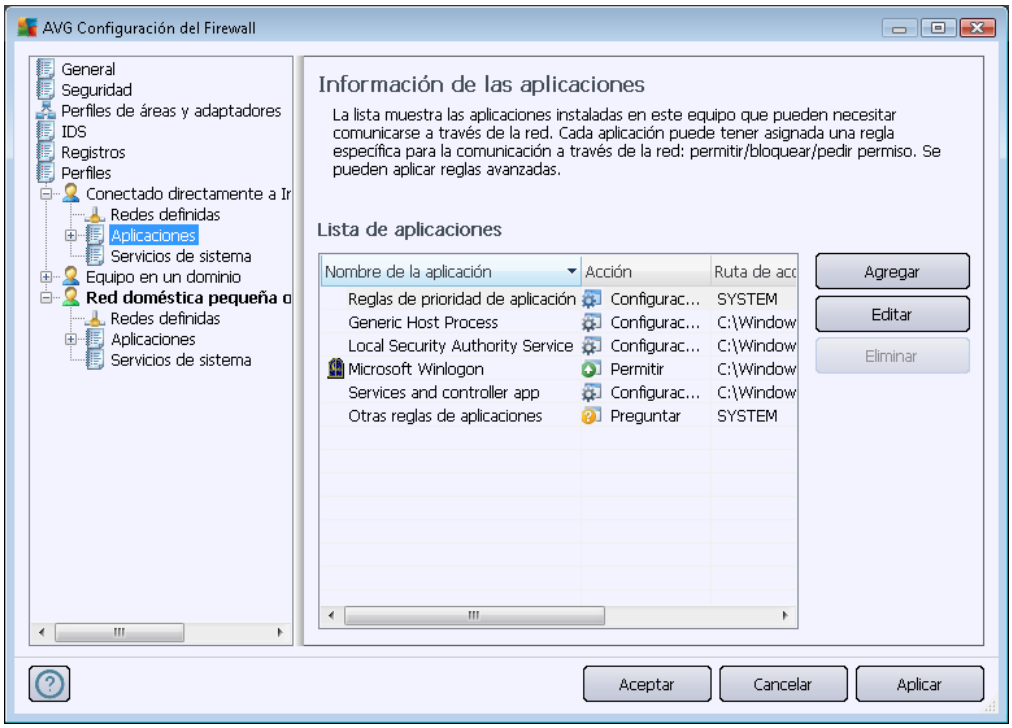
- ***Editar red***: abre la ventana del cuadro de diálogo ***Propiedades de la red*** (*ver arriba*), donde puede editar los parámetros de una red ya definida (*el cuadro de diálogo es idéntico al cuadro de diálogo para agregar una red nueva; consulte la descripción en el párrafo anterior*).

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

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

11.6.3. Aplicaciones

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



Las aplicaciones de la ***Lista de aplicaciones*** son las que se detectaron en su equipo (*y a las que se asignaron acciones respectivas*). Se pueden utilizar los siguientes tipos de acciones:

- - Permitir la comunicación para todas las redes
- - Permitir la comunicación sólo para las redes definidas como seguras
- - Bloquear la comunicación
- - Mostrar cuadro de diálogo de pregunta (*el usuario podrá decidir si desea permitir o bloquear la comunicación cuando la aplicación intente comunicarse a través de la red*)
- - Configuración avanzada definida

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

Por supuesto, también puede definir reglas para la nueva aplicación de forma inmediata: en este

cuadro de diálogo, presione ***Agregar*** e introduzca los detalles de la aplicación.

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

- ***Las reglas prioritarias de aplicaciones*** (*en la parte superior de la lista*) son preferenciales y siempre se aplican antes que las reglas específicas de las aplicaciones.
- ***Otras reglas de aplicaciones*** (*en la parte inferior de la lista*) se utilizan como "último recurso" cuando no se aplican reglas específicas para la aplicación, por ejemplo, para una aplicación desconocida e indefinida. Seleccione la acción que debe activarse cuando dicha aplicación intente comunicarse a través de la red:
  - *Bloquear*: la comunicación siempre estará bloqueada.
  - *Permitir*: se permitirá siempre la comunicación en cualquier red.
  - *Preguntar*: se le invita a decidir si se debe permitir o bloquear la comunicación.

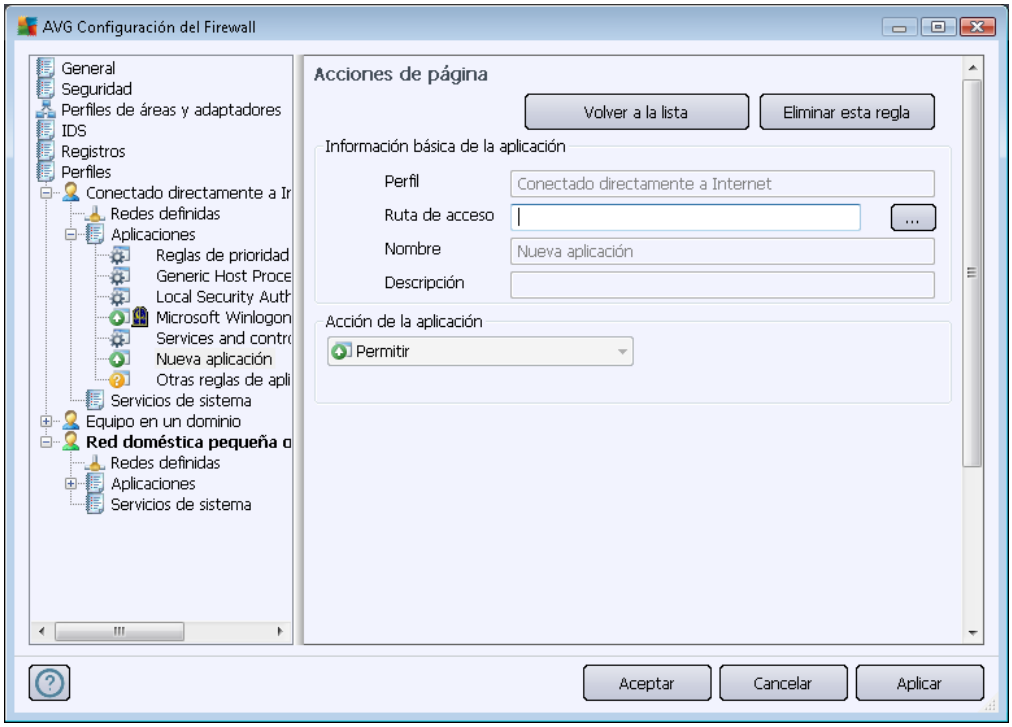
Estos elementos tienen opciones de configuración diferentes a las de las aplicaciones comunes y sólo deben utilizarlos los usuarios experimentados. Se recomienda encarecidamente no modificar la configuración.

Botones de control

La lista puede editarse utilizando los siguientes botones de control:

- ***Agregar***: abre un cuadro de diálogo Acciones de página vacío para definir nuevas reglas de aplicación.
- ***Editar***: abre el mismo cuadro de diálogo Acciones de página con los datos proporcionados para editar el conjunto de reglas de una aplicación existente.
- ***Eliminar***: elimina la aplicación seleccionada de la lista.

En el cuadro de diálogo ***Acciones de página***, puede definir la configuración detallada de la aplicación respectiva:



Botones de control

En la parte superior del cuadro de diálogo existen dos botones de control:

- ***Volver a la lista***: presione este botón para mostrar la descripción general de todas las reglas de aplicaciones definidas.
- ***Eliminar esta regla***: presione este botón para eliminar la regla de aplicación actualmente mostrada. ***Tenga en cuenta que esta acción no puede revertirse.***

Información básica de la aplicación

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

Acción de la aplicación

En el menú desplegable, puede seleccionar la regla de Firewall para la aplicación, por ejemplo, lo

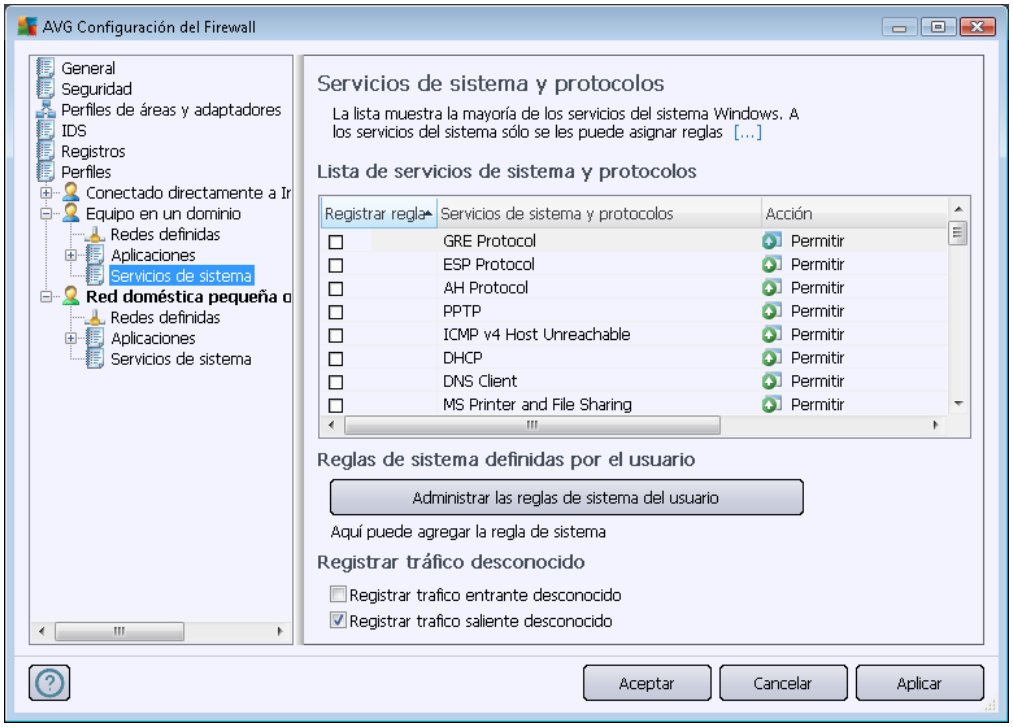
que el Firewall debe hacer cuando la aplicación intenta comunicarse mediante la red:

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

11.6.4. Servicios del sistema

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

El cuadro de diálogo ***Servicios de sistema y protocolos*** muestra los servicios y protocolos estándar de Windows que pueden necesitar comunicarse a través de la red:



Lista de servicios de sistema y protocolos

La tabla tiene las siguientes columnas:

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

Para editar la configuración de cualquier elemento de la lista (*incluidas las acciones asignadas*), haga clic con el botón secundario en el elemento y seleccione ***Editar***. ***La edición de la regla de sistema la deben realizar únicamente usuarios avanzados; se recomienda encarecidamente no editar las reglas de sistema.***

Reglas de sistema definidas por el usuario

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

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

Registrar tráfico desconocido

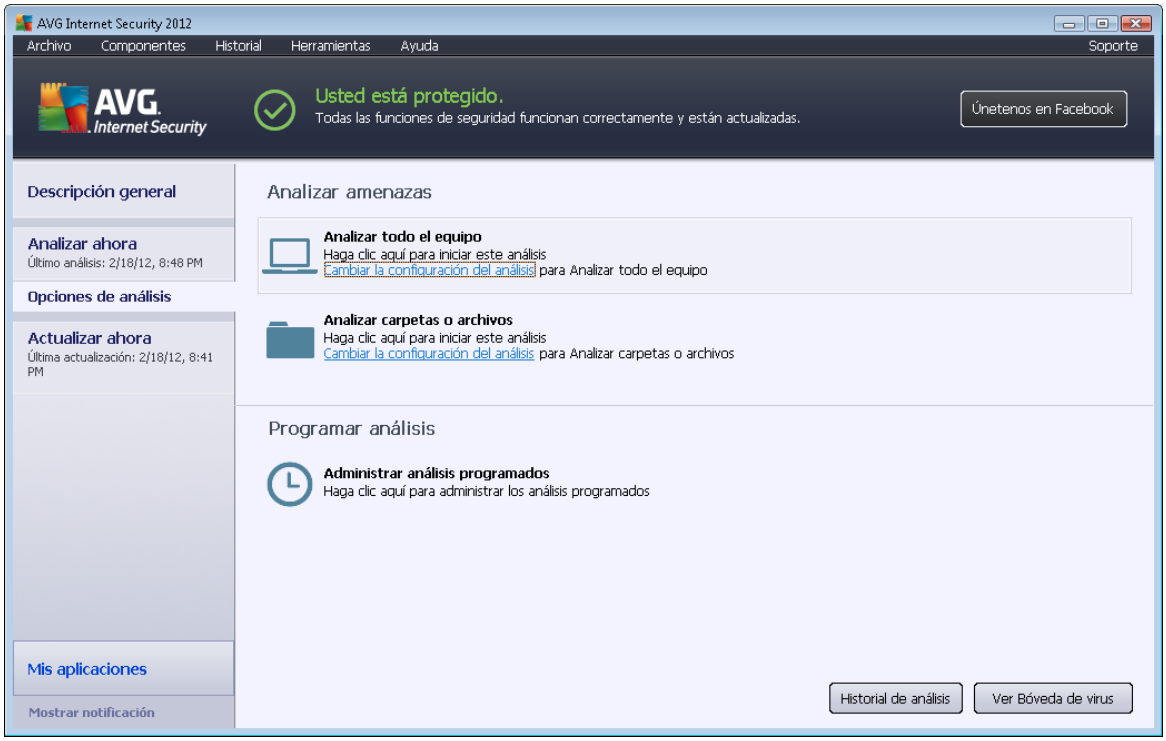
- ***Registrar tráfico entrante desconocido*** *(desactivada de forma predeterminada)*: marque la casilla para guardar en los Registros todos los intentos desconocidos para conectarse a su equipo desde fuera.

- ***Registrar tráfico saliente desconocido*** *(activada de forma predeterminada)*: marque la casilla para guardar en los Registros todos los intentos desconocidos que realice su equipo para conectarse a una ubicación externa.

12. Análisis de AVG

De forma predeterminada, **AVG Internet Security 2012** no realiza ningún análisis, ya que después del inicial, estará perfectamente protegido por los componentes residentes de **AVG Internet Security 2012** que siempre están vigilantes y que no permiten que ningún código malicioso tenga acceso a su equipo. Por supuesto, puede programar un análisis para que se ejecute a intervalos regulares, o ejecutar manualmente un análisis según sus necesidades en cualquier momento.

12.1. Interfaz de análisis



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

- Descripción general de los análisis predefinidos: existen tres tipos de análisis definidos por el proveedor de software para su uso inmediato, ya sea a pedido o a los intervalos programados:
    - Análisis de todo el equipo
    - Analizar carpetas o archivos específicos
- Sección Programar 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 cuadro de 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 Internet Security 2012** 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.

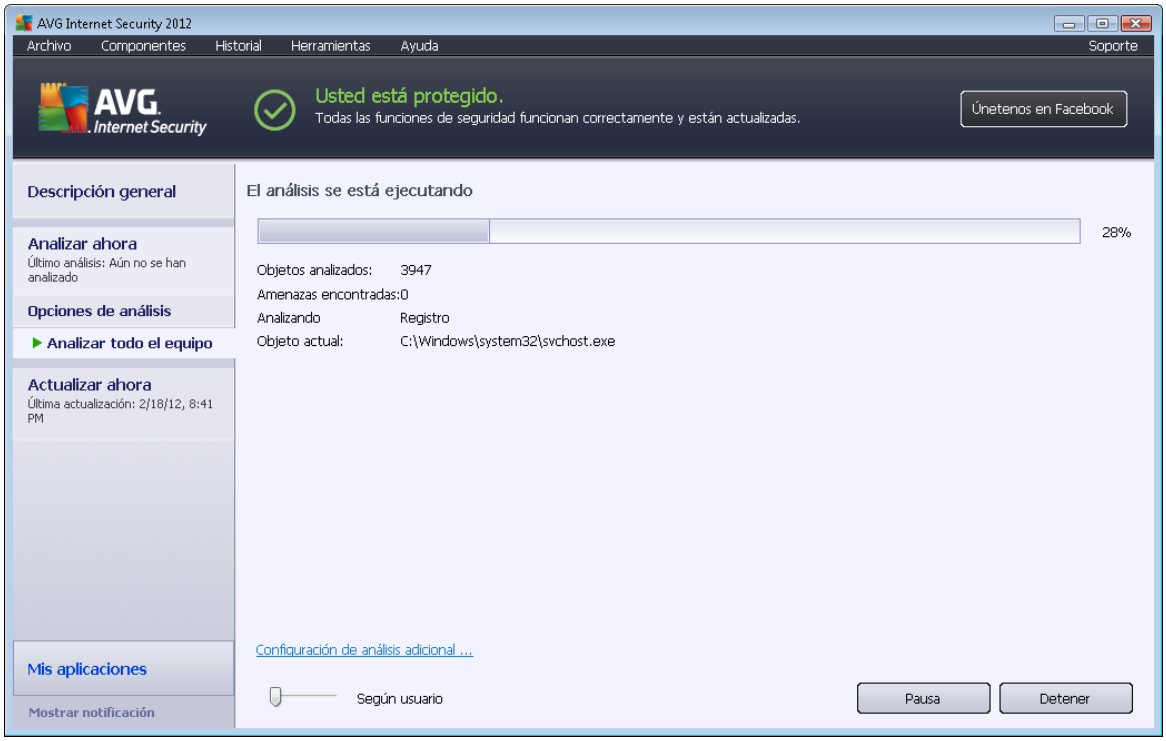
En **AVG Internet Security 2012** encontrará los siguientes tipos de análisis predefinidos por el proveedor del software:

12.2.1. Análisis de todo el equipo

Análisis de 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 enviándola 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.

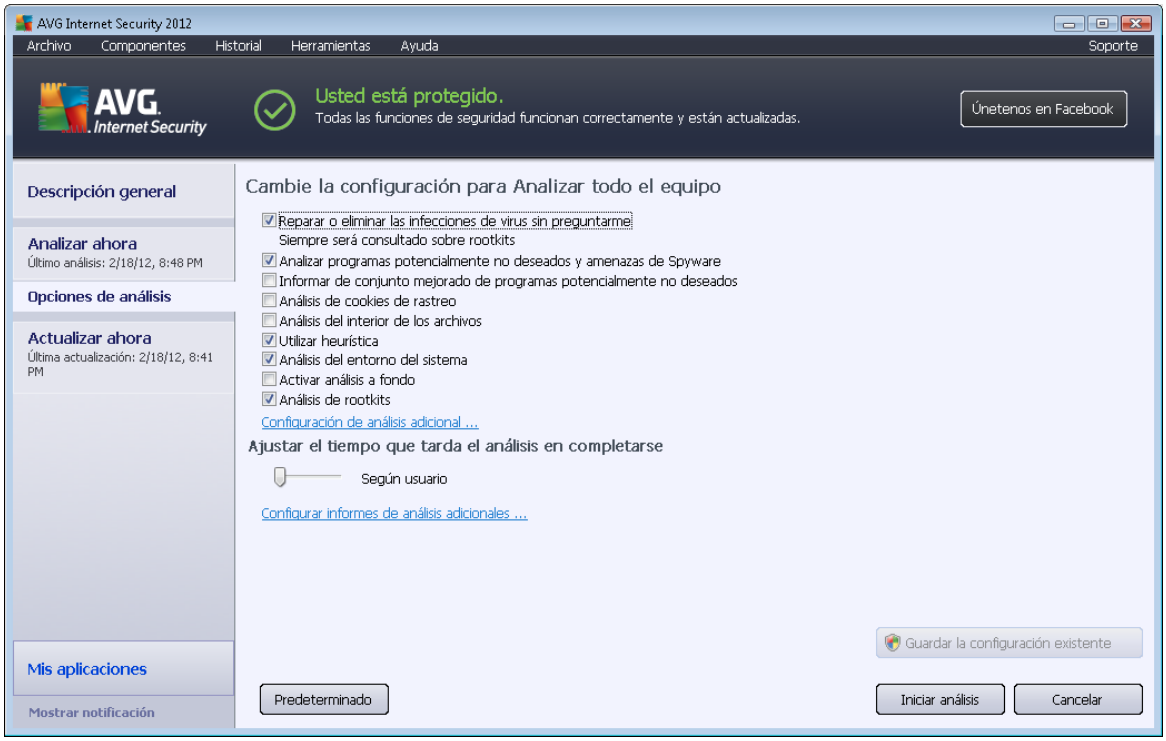
Ejecución del análisis

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



Edición de la configuración de análisis

Tiene la opción de editar la configuración predeterminada predefinida del ***Análisis de todo el equipo***. Presione el vínculo ***Cambiar la configuración del análisis*** para ir al cuadro de diálogo ***Cambie la configuración de análisis para Análisis de todo el equipo*** *(al que se obtiene acceso desde la interfaz de análisis a través del vínculo Cambiar la configuración del análisis para el Análisis de todo el equipo)*. ***Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.***



- ***Parámetros del análisis***: en la lista de parámetros de análisis puede activar o desactivar parámetros según sea necesario:

    - ***Reparar o eliminar las infecciones de virus sin preguntarme*** (*activado de manera predeterminada*): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si hay una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.

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

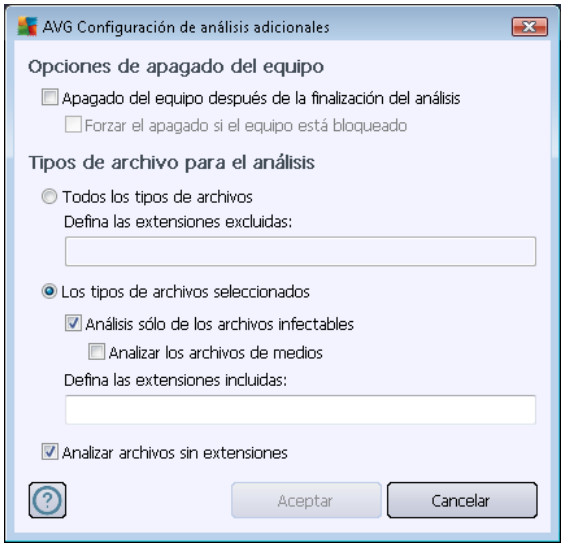
    - ***Informar el conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): seleccione esta opción para detectar un paquete extendido de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que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

    - ***Analizar cookies de rastreo*** (*desactivado de manera predeterminada*): este parámetro del componente Anti-Spyware define que las cookies deben detectarse; (

las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de su carrito de compras electrónico).

- ***Analizar el interior de los archivos*** (*activado de manera predeterminada*): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos, por ejemplo, ZIP, RAR, etc.
- ***Utilizar método heurístico*** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) 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.
- ***Activar análisis a fondo*** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- ***Analizar en busca de rootkits*** (*activado de manera predeterminada*): el análisis Anti-Rootkit busca en su equipo posibles rootkits, es decir, programas y tecnologías que cubran la actividad de malware en su equipo. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

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



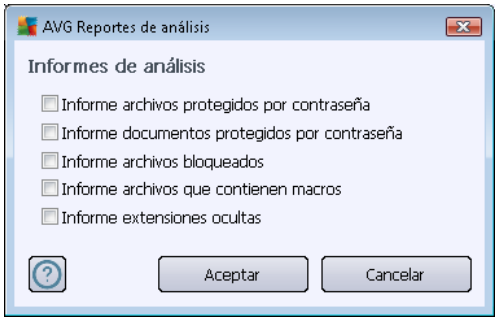
- ***Opciones de apagado del equipo***: decida si el equipo se debe apagar

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

- ***Tipos de archivo para el análisis***: debe decidir si desea analizar:
  - ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;
  - ***Tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.
  - De manera opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

- ***Ajustar el tiempo que tarda el análisis en completarse***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción está establecido en el nivel *según usuario* de empleo automático de recursos. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

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



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

nueva configuración como la predeterminada que se usará para posteriores análisis del equipo completo.

12.2.2. Analizar carpetas o archivos específicos

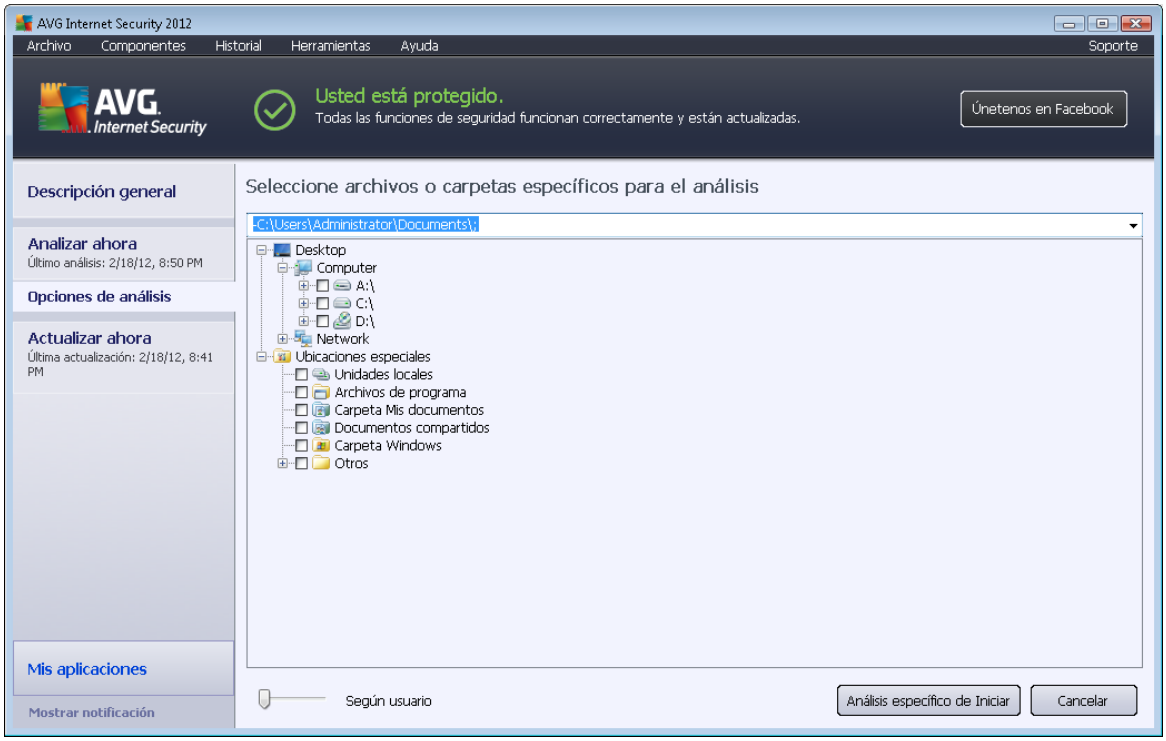
Analizar carpetas o archivos específicos: analiza únicamente las áreas del equipo seleccionadas *(carpetas, discos duros, discos flexibles, CD, etc.)*. El procedimiento de análisis en caso de detección de virus y su tratamiento es el mismo que se realiza con el análisis de todo el equipo: los virus encontrados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

Ejecución del análisis

El ***Análisis de archivos/carpetas*** se puede ejecutar directamente desde la interfaz de análisis haciendo clic en el icono del análisis. Se abre un nuevo cuadro de diálogo denominado ***Seleccione 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 cuadro de diálogo.

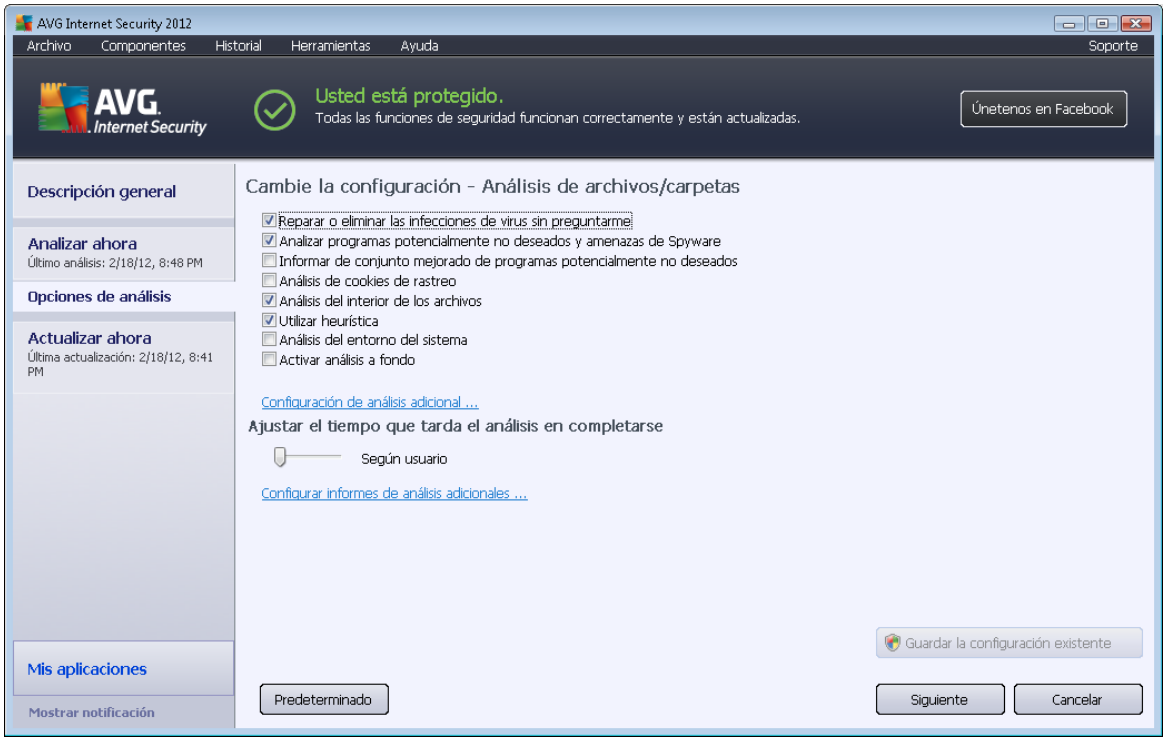
También existe la posibilidad de analizar una carpeta determinada y, a la vez, excluir de este análisis sus subcarpetas; para ello, escriba un signo menos "**-**" delante de la ruta generada automáticamente (*consulte la captura de pantalla*). Para excluir toda la carpeta del análisis utilice el signo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

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



Edición de la configuración de análisis

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



- ***Parámetros del análisis***: en la lista de parámetros de análisis puede activar o desactivar parámetros según sea necesario:
    - ***Reparar o eliminar las infecciones de virus sin preguntarme*** (*activado de manera predeterminada*): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.
    - ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione esta opción para activar el motor Anti-Spyware y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionadamente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
    - ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de forma predeterminada*): seleccione esta opción para detectar un

paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

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

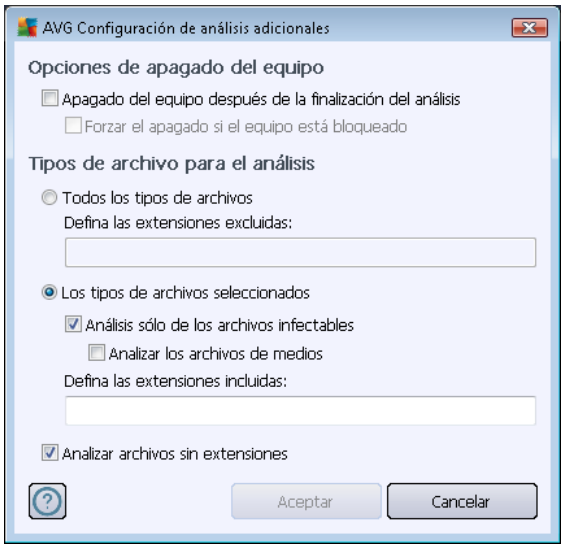
- ***Analizar el interior de los archivos*** (*activado de manera predeterminada*): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos (por ejemplo, ZIP, RAR...)

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

- ***Analizar el entorno del sistema*** (*desactivado de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo.

- ***Activar análisis a fondo*** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

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



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

- ***Tipos de archivo para el análisis***: además debe decidir si desea que se analicen:

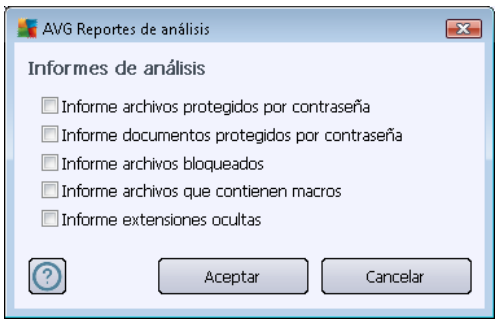
  - ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;

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

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

- ***Prioridad del proceso de análisis***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción está establecido en el nivel *según usuario* de empleo automático de recursos. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

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

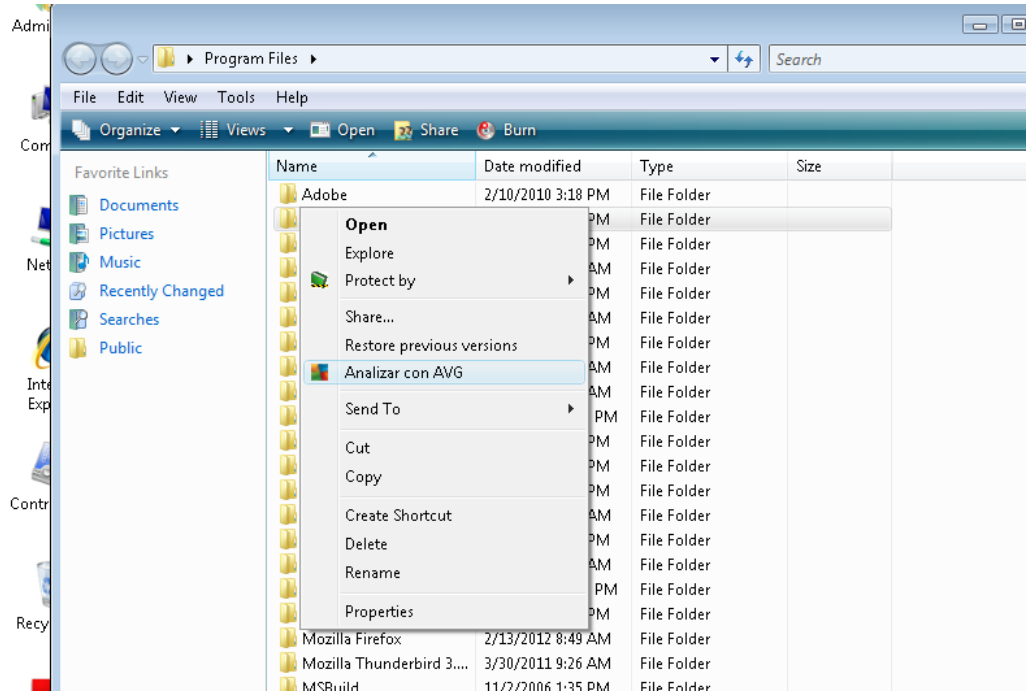


Advertencia: *estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo Análisis de AVG / Programación de análisis / Cómo analizar. Si*

*decide cambiar la configuración predeterminada de **Analizar carpetas o archivos específicos** puede guardar la nueva configuración como la predeterminada que se usará para todos los análisis de archivos/carpetas 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/carpetas).*

12.3. Análisis en el Explorador de Windows

Además de los análisis predefinidos ejecutados para todo el equipo o sus áreas seleccionadas, **AVG Internet Security 2012** 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 analizarlo a pedido. Siga estos pasos:



- Dentro del Explorador de Windows, resalte el archivo *(o carpeta)* que desea comprobar
- Haga clic con el botón secundario del mouse sobre el objeto para abrir el menú contextual.
- Seleccione la opción ***Analizar con AVG*** para que el archivo se analice con **AVG Internet Security 2012**

12.4. Análisis desde línea de comandos

En **AVG Internet Security 2012** existe la opción de realizar el análisis desde la línea de comandos. Puede utilizar esta opción, por ejemplo, en servidores, o bien al crear un script por lotes que se ejecutará automáticamente una vez reiniciado el equipo. Desde la línea de comandos, puede ejecutar el análisis con la mayoría de los parámetros ofrecidos en la interfaz gráfica de usuario de AVG.

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

- ***avgscanx*** para SO de 32 bits
- ***avgscana*** 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*** .. al utilizar varios parámetros, estos deben alinearse en una fila y separarse mediante un espacio y un signo de barra
- si un parámetro requiere que se proporcione un valor específico (p. ej., el parámetro ***/scan*** requiere información sobre qué áreas seleccionadas del equipo se deben analizar, por lo que debe proporcionar una ruta de acceso exacta hasta la sección seleccionada), los valores se separan mediante punto y coma, por ejemplo: ***avgscanx /scan=C:\;D:***

Parámetros del análisis

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

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

Análisis desde CMD iniciado desde la interfaz gráfica

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

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

12.4.1. Parámetros del análisis desde CMD

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

- ***/SCAN*** Analizar carpetas o archivos específicos /SCAN=ruta de acceso; ruta de acceso *(por ejemplo /SCAN=C:\;D:\)*
- ***/COMP*** Análisis de 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
- ***/LOG*** Generar un archivo de los resultados del análisis
- ***/MACROW*** Informar de macros
- ***/PWDW*** Informar de archivos protegidos por contraseña
- ***/ARCBOMBSW*** Informar de bombas de archivo *(archivos comprimidos reiteradas veces)*
- ***/IGNLOCKED*** Omitir archivos bloqueados
- ***/REPORT*** Informar en archivo /nombre de archivo/
- ***/REPAPPEND*** Anexar al archivo de reporte
- ***/REPOK*** Informar de archivos no infectados como correctos
- ***/NOBREAK*** No permitir la anulación mediante CTRL+BREAK
- ***/BOOT*** Activar la comprobación de MBR/BOOT
- ***/PROC*** Analizar los procesos activos
- ***/PUP*** Informar de Programas potencialmente no deseados

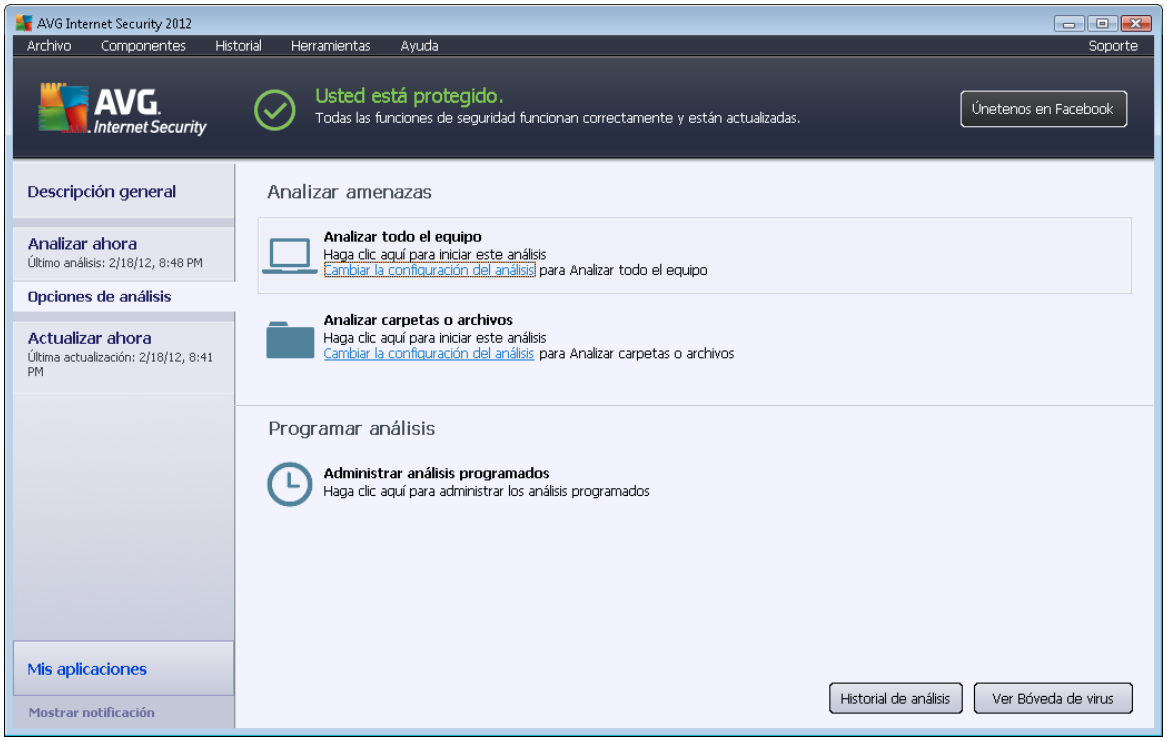
- ***/PUPEXT*** Informar de conjunto mejorado de Programas potencialmente no deseados
- ***/REG*** Analizar el registro
- ***/COO*** Analizar cookies
- ***/?*** Mostrar ayuda sobre este tema
- ***/HELP*** Mostrar ayuda sobre este tema
- ***/PRIORITY*** *Establecer prioridad de análisis /Baja, Automática, 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)*
- ***/HIDDEN*** Informar de archivos con extensión oculta
- ***/INFECTABLEONLY*** Analizar los archivos con extensiones infectables
- ***/THOROUGHSCAN*** Activar el análisis a fondo
- ***/CLOUDCHECK*** Verificar falsos positivos
- ***/ARCBOMBSW*** Informar de archivos recomprimidos

12.5. Programación de análisis

Con **AVG Internet Security 2012** 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.

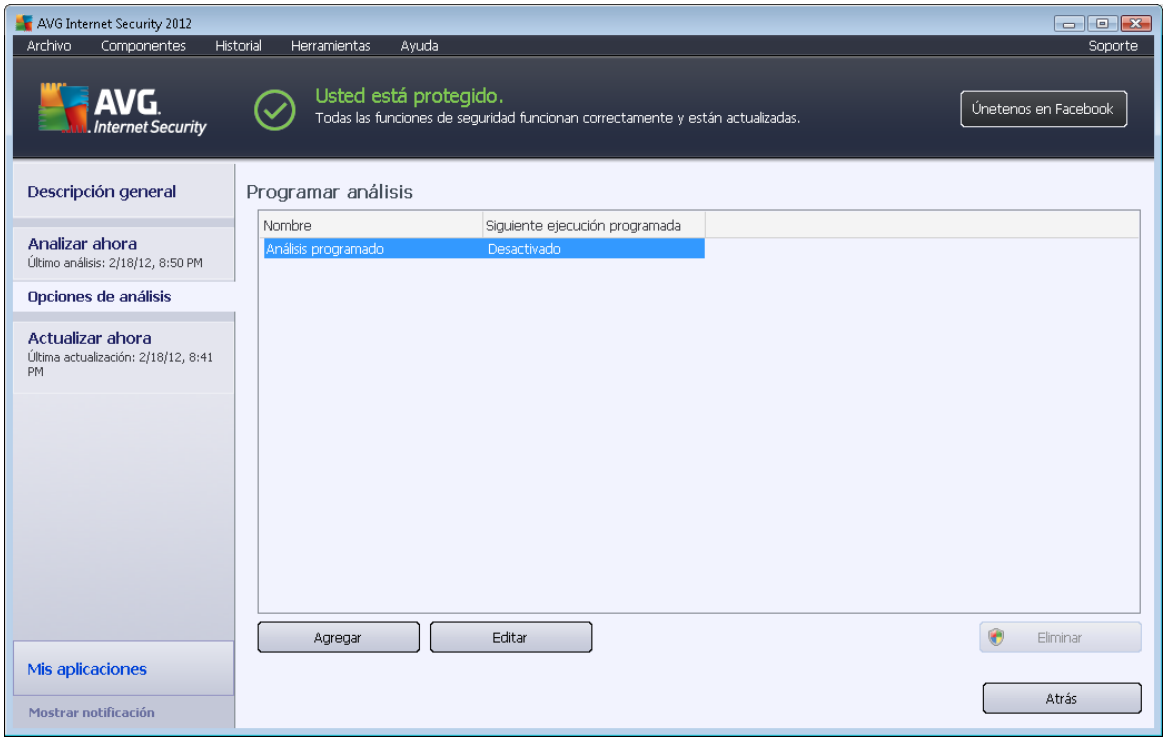
Se debe ejecutar el Análisis de todo el equipo periódicamente, al menos una vez a la semana. Sin embargo, si es posible, ejecute el análisis de todo su equipo diariamente, como está establecido en la configuración predeterminada de programación del análisis. Si el equipo siempre está encendido, se pueden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

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



Programar análisis

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



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

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

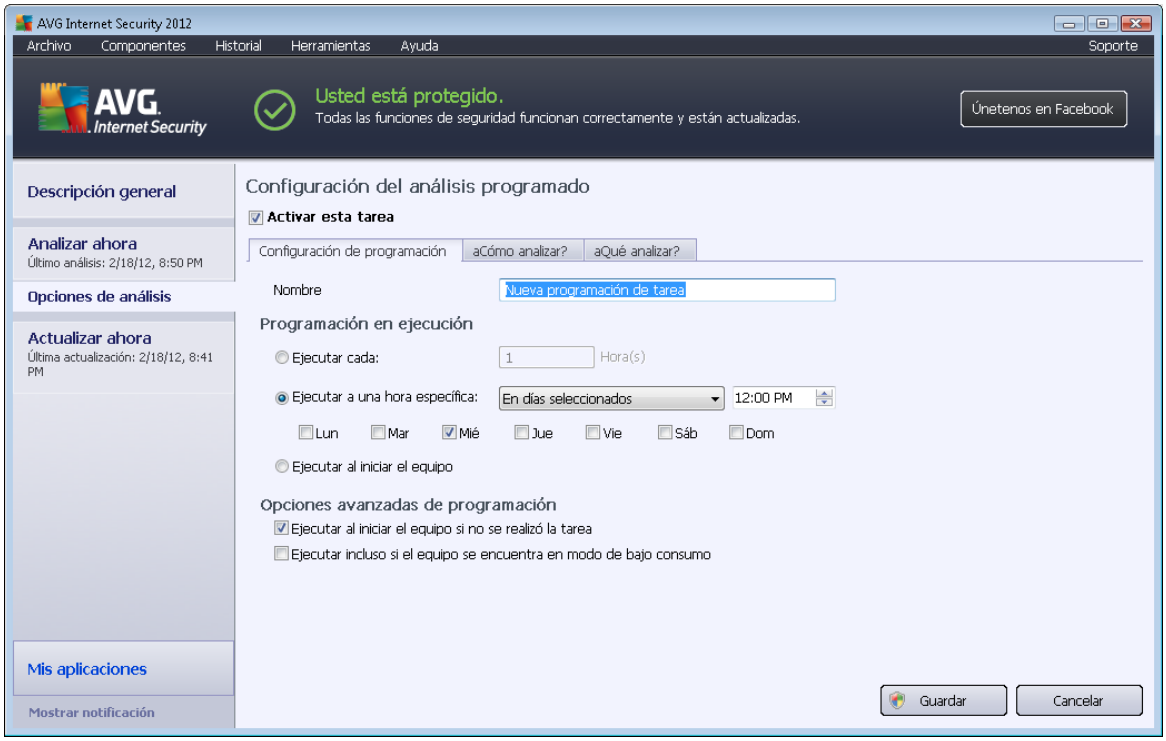
- ***Editar la programación de análisis***: este botón sólo se puede emplear si ha seleccionado previamente un análisis existente en la lista de análisis programados. En ese caso, el botón aparece como activo y puede hacer clic en él para ir al cuadro de diálogo ***Configuración del análisis programado***,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

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

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

12.5.1. Configuración de programación

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



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

A continuación, dé un nombre al análisis que está a punto de crear y programar. Escriba el nombre en el campo de texto que está junto al 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 comprueba. 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 cuadro de diálogo puede definir con mayor detalle los siguientes parámetros del análisis:

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

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

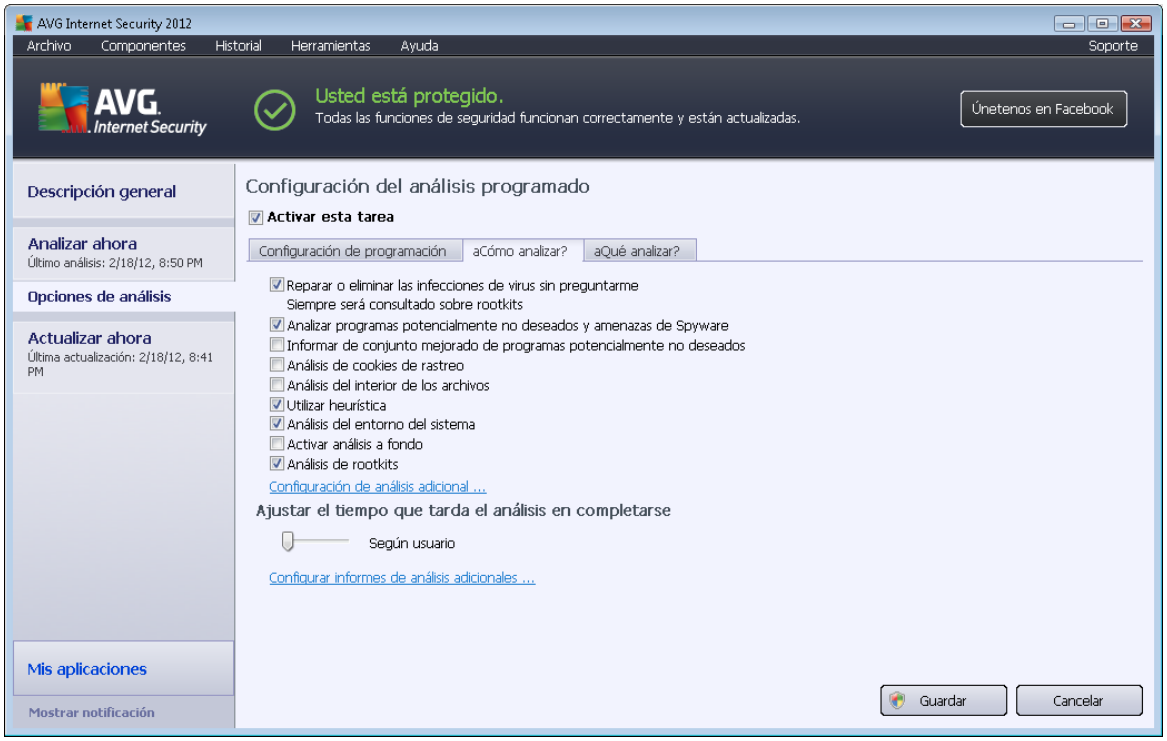
Botones de control del cuadro de diálogo Configuración del análisis programado.

Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo ***Configuración del análisis programado*** *(Configuración de programación, ¿Cómo analizar? y ¿Qué analizar?)*, y 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 cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después de haber especificado todos los requisitos.

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

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 o 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 las infecciones de virus sin preguntarme*** (*activada de forma predeterminada*): si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible una reparación. Si no se puede reparar

automáticamente el archivo infectado o decide desactivar esta opción, cada vez que se detecte un virus, se le avisará y tendrá que decidir qué hacer con la infección detectada. El método recomendado consiste en eliminar el archivo infectado a la Bóveda de virus.

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

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

- ***Analizar cookies de rastreo*** (*desactivado de forma predeterminada*): este parámetro del componente Anti-Spyware define que las 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 el contenido de sus carritos de compra electrónicos*).

- ***Analizar el interior de los archivos*** (*desactivado de forma 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*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.

- ***Analizar el entorno del sistema*** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.

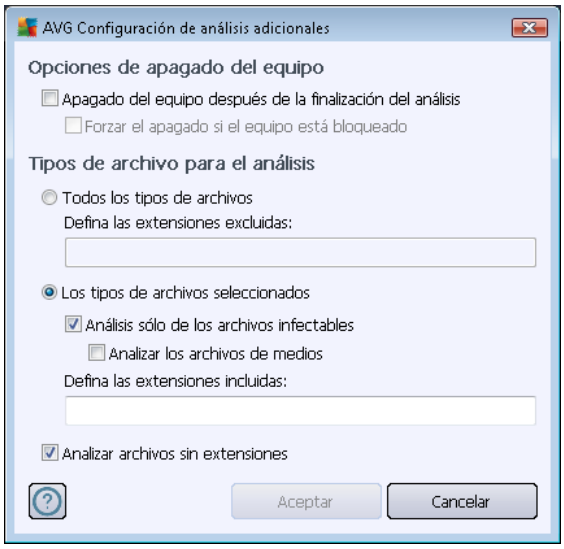
- ***Activar análisis a fondo*** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

- ***Analizar en busca de rootkits*** (*activado de forma predeterminada*): Anti-Rootkit busca en su equipo posibles rootkits, es decir, programas y tecnologías que cubran la actividad de malware en su equipo. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

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

- ***Configuración de análisis adicional***: el vínculo abre un nuevo cuadro de diálogo

Configuración de análisis adicional, donde puede especificar los siguientes parámetros:



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

- ***Tipos de archivo para el análisis***: debe decidir si desea analizar:

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

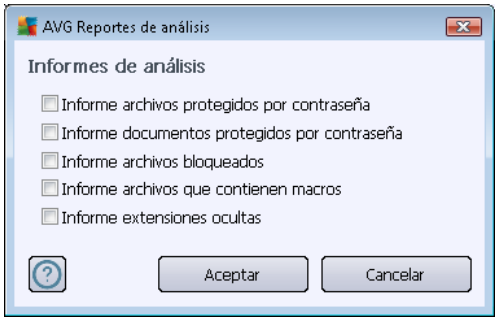
  - ***Tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos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

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

- ***Ajustar el tiempo que tarda el análisis en completarse***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción está establecido en el nivel *según usuario* de empleo automático de recursos. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que*

trabajar en el equipo pero no importa cuánto dure el análisis) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

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



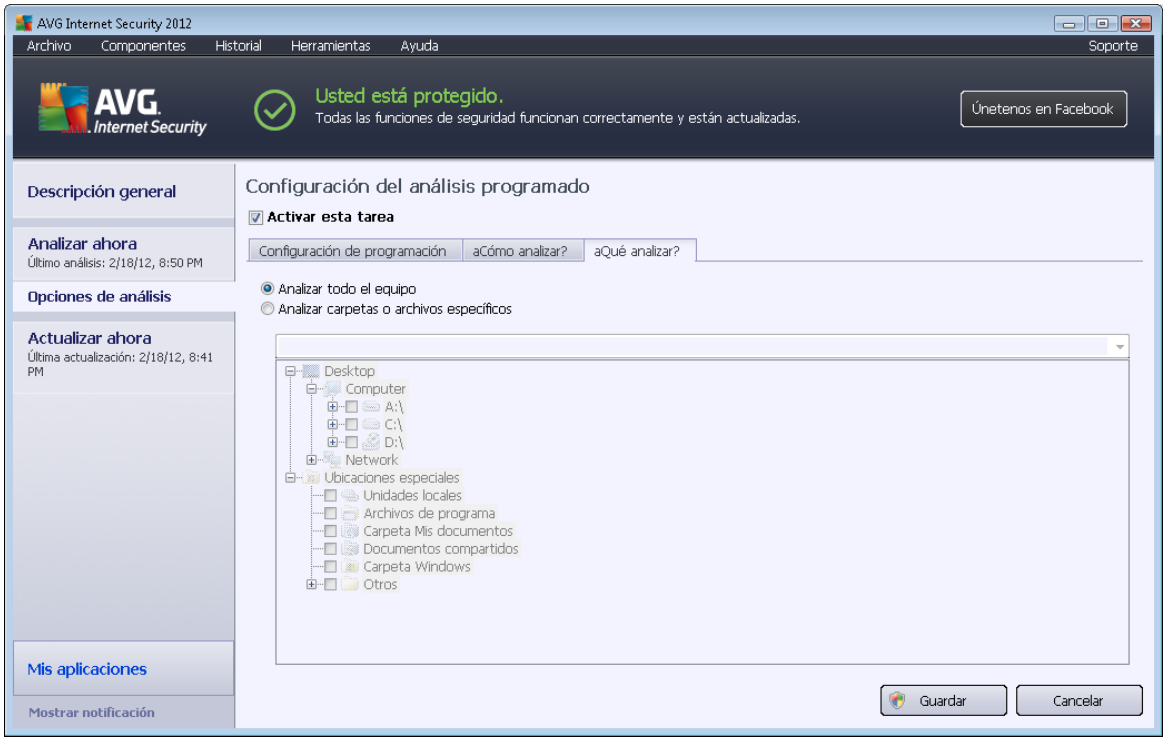
Botones de control

Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo ***Configuración del análisis programado*** (*Configuración de programación, ¿Cómo analizar? y ¿Qué analizar?*), y 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 cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después de haber especificado todos los requisitos.

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

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/carpetas.

Si selecciona analizar archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activará la estructura de árbol visualizada y podrá especificar las carpetas que se analizarán (*expanda los elementos haciendo clic en el nodo "más" hasta que encuentre la carpeta que desea analizar*). Puede seleccionar varias carpetas marcando las casillas respectivas. Las carpetas seleccionadas aparecerán en el campo de texto en la parte superior del cuadro de diálogo, y el menú desplegable mantendrá el historial de sus análisis seleccionados para uso posterior. De manera alternativa, puede introducir manualmente la ruta de acceso completa a la carpeta deseada (*si introduce varias rutas de acceso, es necesario separarlas con punto y coma, sin espacios*).

En la estructura de árbol también puede ver una rama denominada ***Ubicaciones especiales***. A continuación encontrará una lista de ubicaciones que se analizarán si se marca la casilla de verificación correspondiente:

- ***Unidades locales***: todas las unidades de disco duro de su equipo
- ***Archivos de programa***
  - C:\Program Files\
  - *en la versión de 64 bits* C:\Program Files (x86)
- ***Carpeta Mis documentos***

- *para Windows XP:* C:\Documents and Settings\Default User\My Documents\
- *para Windows Vista/7*: C:\Users\user\Documents\

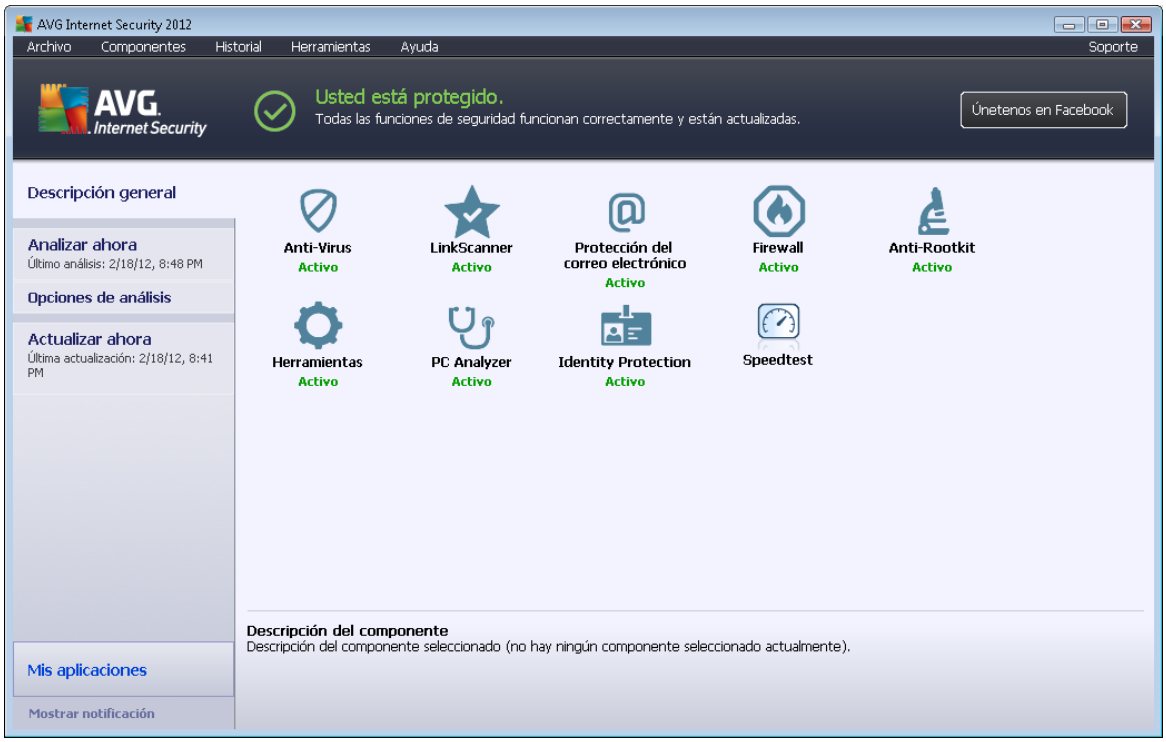
- ***Documentos compartidos***
  - *para Windows XP*: C:\Documents and Settings\All Users\Documents\
  - *para Windows Vista/7*: C:\Users\Public\Documents\
- ***Carpeta de Windows***: C:\Windows\
- ***Otros***
  - *Unidad del sistema*: el disco duro en el cual está instalado el sistema operativo (normalmente C:)
  - *Carpeta del sistema*: C:\Windows\System32\
  - *Carpeta de archivos temporales*: C:\Documents and Settings\User\Local\ (*Windows XP*); o C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Archivos temporales de Internet*: C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); o C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Botones de control

Los mismos dos botones de control están disponibles en las tres pestañas del cuadro de diálogo ***Configuración del análisis programado*** *(Configuración de programación, Cómo analizar y Qué analizar)*:

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

12.6. Descripción general de los resultados del análisis



El diálogo ***Descripción general de los resultados del análisis*** está disponible desde la interfaz de análisis de 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 indica que durante el análisis no se detectó ninguna infección

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

  - el icono rojo indica que durante el análisis se detectó una infección y que no se pudo eliminar

  Cada icono puede ser sólido o cortado a la mitad: los iconos sólidos representan un análisis que se completó y finalizó adecuadamente; el icono cortado a la mitad significa que el análisis se canceló o se interrumpió.

  Nota: *para obtener información detallada sobre cada análisis, consulte el diálogo Resultados del análisis disponible a través del botón Ver detalles (en la parte inferior de este diálogo).*

- ***Hora de inicio***: fecha y hora en que se inició el análisis

- ***Hora de finalización***: fecha y hora en que finalizó el análisis
- ***Objetos analizados***: número de objetos que se verificaron durante el análisis
- ***Infecciones***: número de infecciones de virus detectadas/eliminadas
- ***Spyware***: número de spyware detectados/eliminados
- ***Advertencias***: número de objetos sospechosos detectados
- ***Rootkits***: número de rootkits detectados
- ***Información de registros del análisis***: información relacionada con el curso y el resultado del análisis (normalmente sobre su finalización o interrupción)

Botones de control

Los botones de control para el diálogo ***Descripción general de los resultados del análisis*** son:

- ***Ver detalles***: presione este botón para pasar al cuadro de diálogo Resultados del análisis para ver la información detallada sobre el análisis seleccionado
- ***Eliminar resultado***: presione este botón para eliminar el elemento seleccionado de la descripción general de resultados
- ***Atrás***: regresa al diálogo predeterminado de la interfaz de análisis de AVG

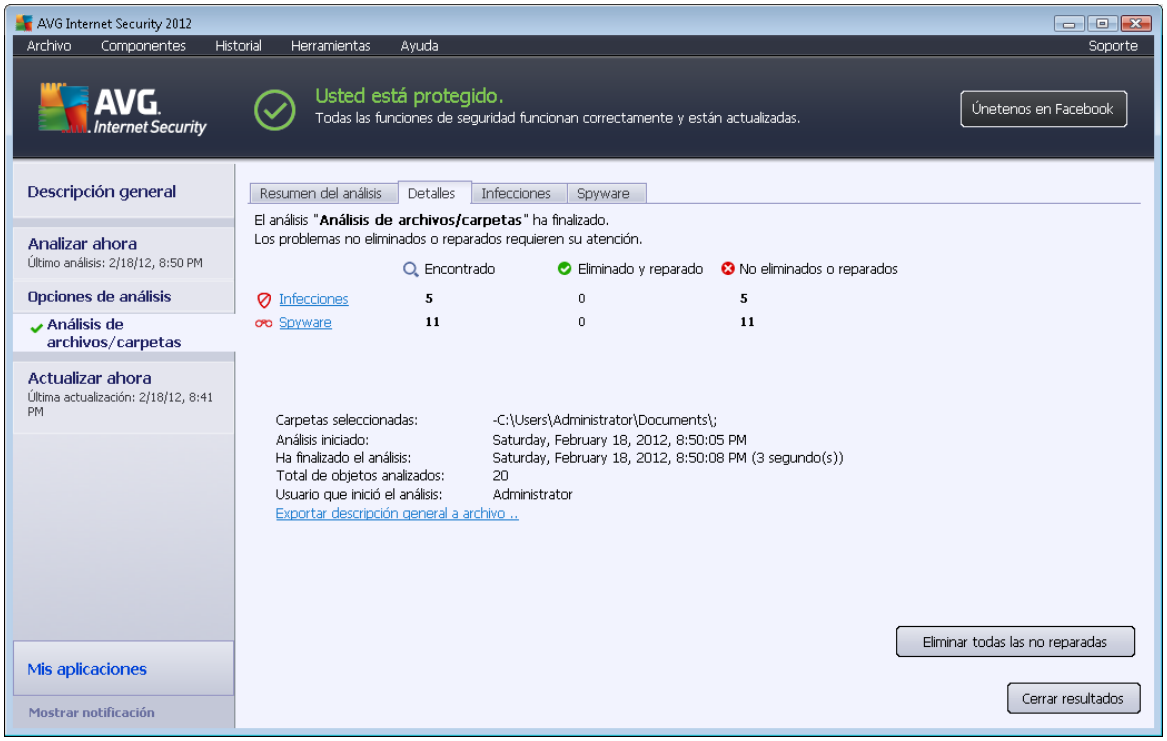
12.7. Detalles de los resultados del análisis

Si en el cuadro de diálogo Descripción general de los resultados del análisis está seleccionado un análisis específico, puede hacer clic en el botón ***Ver detalles*** para cambiar al cuadro de diálogo ***Resultados del análisis***, que proporciona datos detallados sobre el curso y resultado del análisis seleccionado. El cuadro de diálogo está dividido en varias pestañas:

- Descripción general de los resultados: esta pestaña se visualiza en todo momento y proporciona los datos estadísticos que describen el progreso del análisis.
- Infecciones: esta pestaña se visualiza sólo si durante el análisis se detectó una infección de virus.
- Spyware: esta pestaña se visualiza sólo si durante el análisis se detectó un spyware.
- Advertencias: esta pestaña se muestra si, por ejemplo, se detectaron cookies durante el análisis.
- 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. También se mostrará información

sobre objetos que no pudieron analizarse *(por ejemplo, archivos protegidos por contraseña)* .

12.7.1. Pestaña Descripción general de los resultados



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

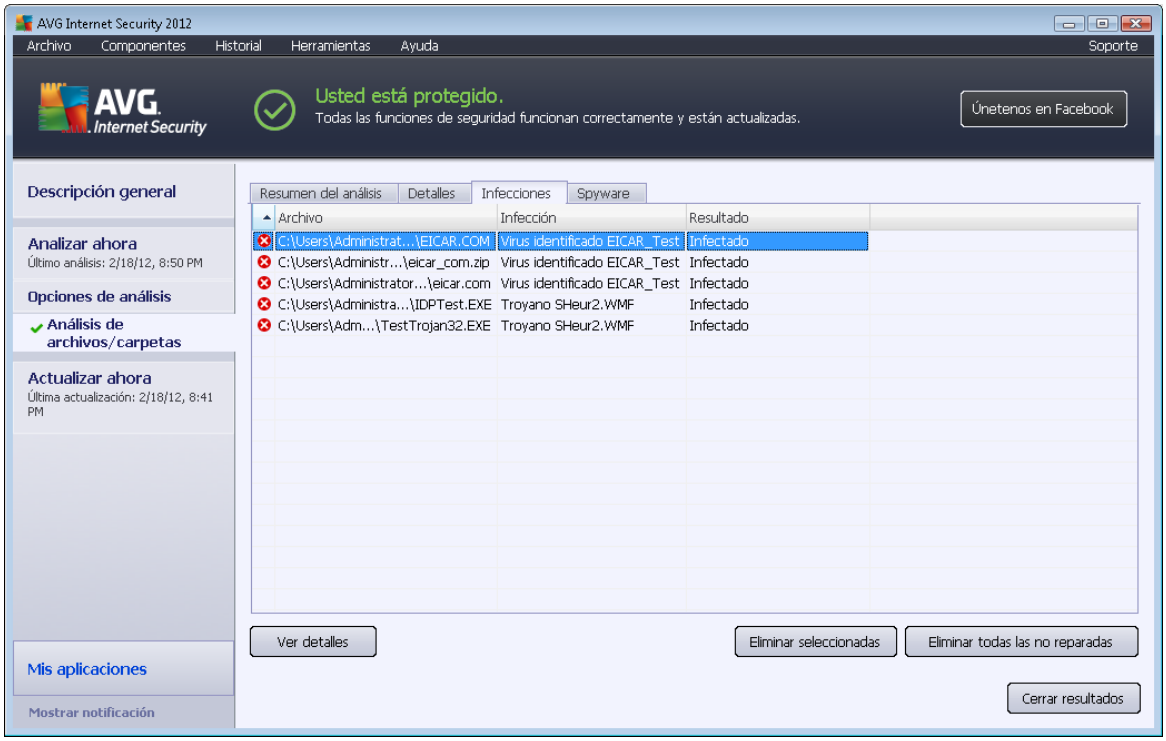
- Infecciones de virus/spyware detectadas
- Infecciones de virus/spyware eliminadas
- El número de infecciones de virus/spyware que no se han podido eliminar ni reparar

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

Botones de control

En este cuadro de diálogo, sólo 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 cuadro de 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.
  - ***Transferido 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*

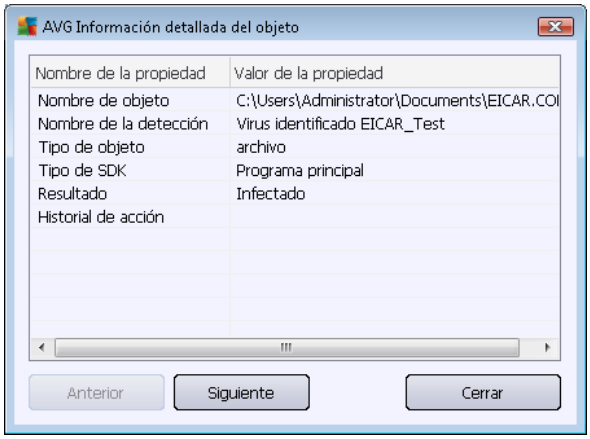
diálogo Excepciones PPND de la configuración avanzada)

- ***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 (*puede que, por ejemplo, contenga macros*); la información es sólo una advertencia
- ***Es necesario reiniciar para finalizar la acción***: 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 cuadro de diálogo:

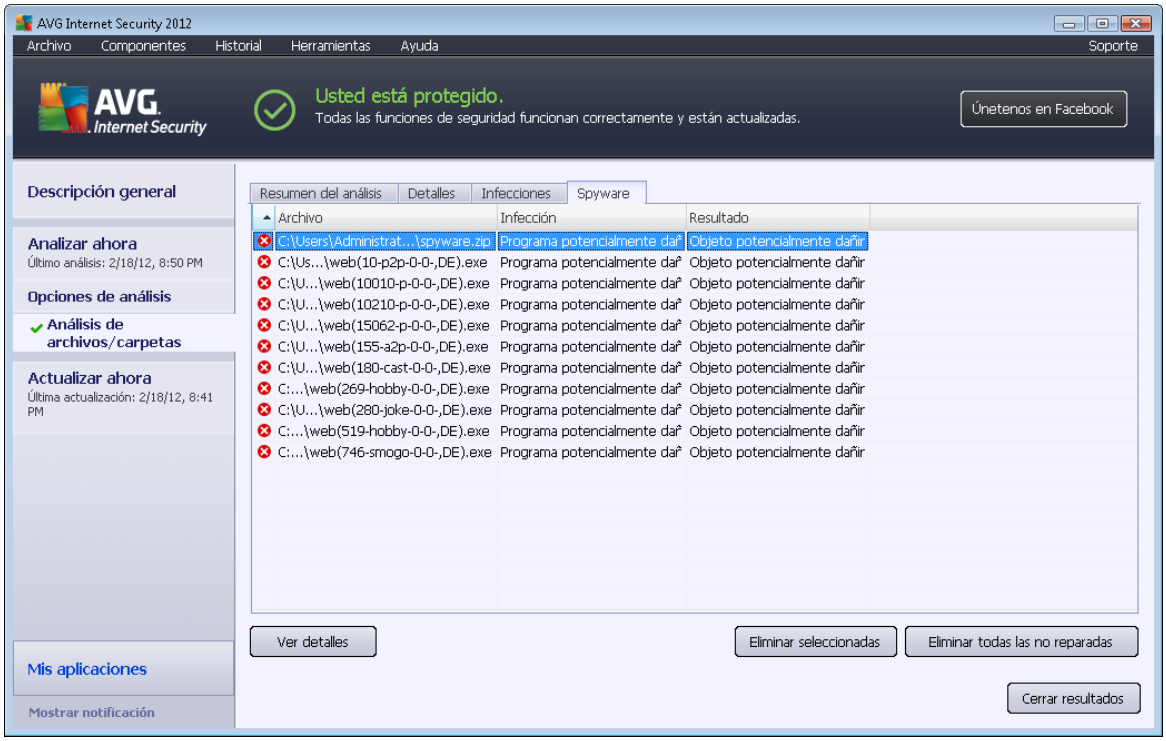
- ***Ver detalles***: el botón abre una nueva ventana del cuadro de diálogo denominada ***Información detallada del objeto***:



  En este cuadro de diálogo puede encontrar información detallada sobre el objeto infeccioso detectado (*por ejemplo, el nombre y la ubicación del objeto infectado, el tipo de objeto, el tipo de SDK, el resultado de la detección y el historial de acciones relativas al objeto detectado*). Mediante los botones ***Anterior***/***Siguiente*** puede ver información sobre hallazgos concretos. Utilice el botón ***Cerrar*** para cerrar este cuadro de diálogo.

- ***Eliminar seleccionadas***: utilice este botón para mover el hallazgo seleccionado a la Bóveda de virus
- ***Eliminar todas las no reparadas***: este botón elimina todos los hallazgos que no se pueden reparar ni mover a la Bóveda de virus
- ***Cerrar resultados***: cierra la descripción general de información detallada y permite volver al cuadro de diálogo Descripción general de los resultados del análisis.

12.7.3. Pestaña Spyware



La pestaña ***Spyware*** sólo se visualiza en el cuadro de 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 PUP***: el hallazgo se ha evaluado como una excepción y se ha agregado a la lista de excepciones de PUP *(configurada en el cuadro de diálogo Excepciones de programas potencialmente no deseados de la configuración*

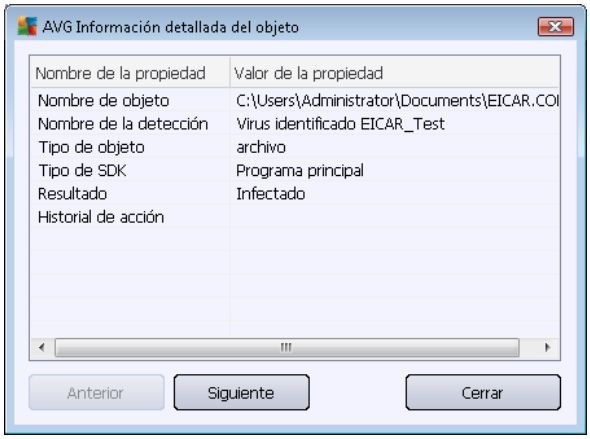
avanzada)

- ***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.
- ***Es necesario reiniciar para finalizar la acción***: 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 cuadro de diálogo:

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



  En este cuadro de diálogo puede encontrar información detallada sobre el objeto infeccioso detectado (*por ejemplo, el nombre y la ubicación del objeto infectado, el tipo de objeto, el tipo de SDK, el resultado de la detección y el historial de acciones relativas al objeto detectado*). Mediante los botones ***Anterior***/***Siguiente*** puede ver información sobre hallazgos concretos. Utilice el botón ***Cerrar*** para salir de este cuadro de diálogo.

- ***Eliminar seleccionadas***: utilice este botón para mover el hallazgo seleccionado a la Bóveda de virus
- ***Eliminar todas las no reparadas***: este botón elimina todos los hallazgos que no se pueden reparar ni mover a la Bóveda de virus
- ***Cerrar resultados***: cierra la descripción general de información detallada y permite volver al cuadro de 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 por contraseñas, etc. Estos archivos no presentan ninguna amenaza directa a su equipo o a su seguridad. La información acerca de estos archivos es útil generalmente en caso de que se detecte adware o spyware en el equipo. Si en los resultados del análisis sólo aparecen advertencias detectadas por **AVG Internet Security 2012**, no se requiere ninguna acción.

Esta es una breve descripción de los ejemplos más comunes de tales objetos:

- ***Archivos ocultos***: de manera predeterminada, los archivos ocultos no son visibles en Windows, y algunos virus y otras amenazas pueden intentar evitar su detección almacenando sus archivos con este atributo. Si **AVG Internet Security 2012** informa acerca de un archivo oculto que sospecha que es malicioso, puede moverlo a la Bóveda de virus.
- ***Cookies***: las cookies son archivos de texto sin formato que utilizan los sitios Web para almacenar información específica del usuario, que posteriormente se utiliza para cargar el diseño personalizado del sitio Web, rellenar previamente el nombre de usuario, etc.
- ***Claves de registro sospechosas***: algunos malware almacenan su información en el registro de Windows, con el fin de asegurarse de que se cargan al iniciar el equipo o para prolongar su efecto en el sistema operativo.

12.7.5. Pestaña Rootkits

La pestaña ***Rootkits*** muestra la información sobre rootkits detectados durante el análisis anti-rootkit incluido en el Análisis de todo el equipo.

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

La estructura de esta pestaña es básicamente la misma que la de la pestaña Infecciones o la pestaña Spyware.

12.7.6. Pestaña Información

La pestaña ***Información*** contiene datos sobre los "hallazgos" que no se pueden clasificar como infecciones, spyware, etc. No se pueden etiquetar positivamente como peligrosos pero, sin embargo, merecen su atención. El análisis de **AVG Internet Security 2012** puede detectar archivos que quizás no están infectados pero que son sospechosos. Estos archivos se notifican como Advertencia o como Información.

La ***Información*** de severidad se puede notificar por uno de los siguientes motivos:

- ***Tiempo de ejecución comprimido***: el archivo fue comprimido con uno de los empaquetadores de tiempo de ejecución menos comunes, algo que puede indicar un intento de evitar el análisis de dicho archivo. No obstante, no todos los reportes de dicho archivo indican la existencia de un virus.

- ***Tiempo de ejecución comprimido recursivo***: parecido al anterior, pero menos frecuente en software común. Estos archivos son sospechosos y se debería tener en cuenta la posibilidad de eliminarlos o someterlos a un análisis.

- ***Archivo o documento protegido por contraseña***: **AVG Internet Security 2012** no puede analizar los archivos protegidos por contraseña (*ni cualquier otro programa anti-malware en general*).

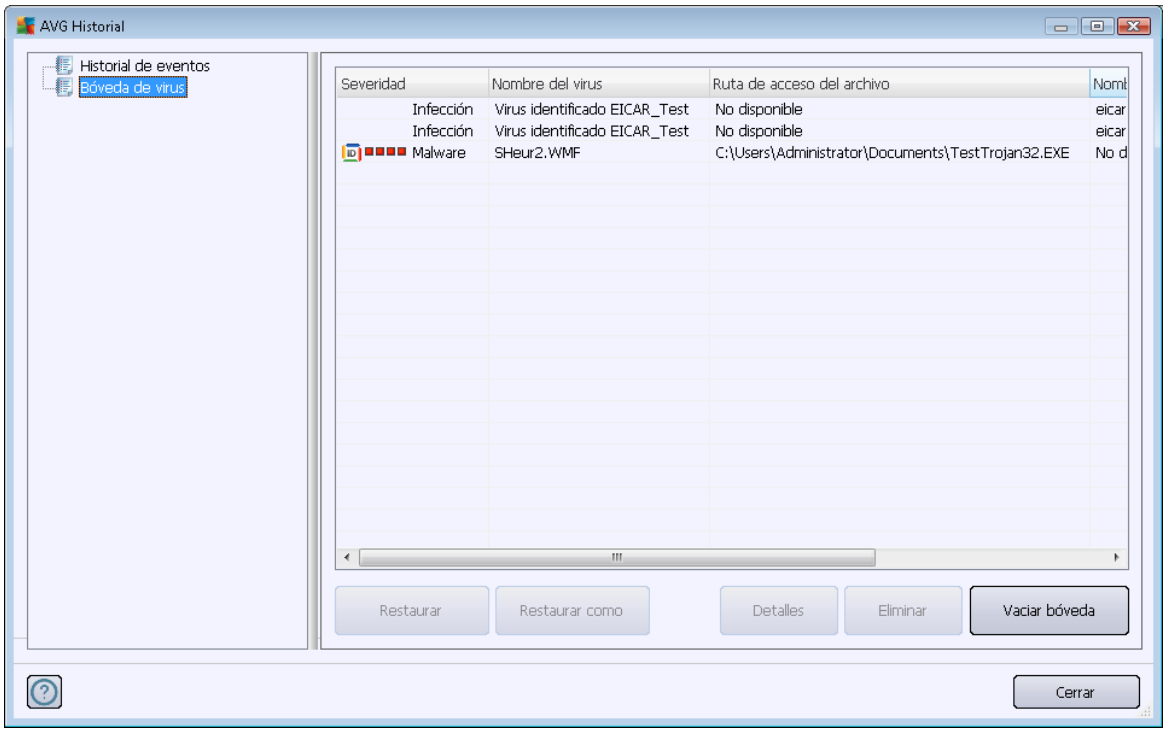
- ***Documento con macros***: el documento notificado contiene macros, que pueden ser maliciosos.

- ***Extensión oculta***: los archivos con la extensión oculta pueden aparentar que son, por ejemplo, imágenes, pero en realidad son archivos ejecutables (*por ejemplo, imagen.jpg.exe*). La segunda extensión no es visible en Windows de forma predeterminada, y **AVG Internet Security 2012** reporta estos archivos para prevenir que se abran accidentalmente.

- ***Ruta de acceso del archivo incorrecta***: si algún archivo importante del sistema se ejecuta desde otra ruta de acceso que no sea la predeterminada (*por ejemplo, si winlogon.exe se ejecuta desde otra carpeta que no sea Windows*), **AVG Internet Security 2012** notifica esta discrepancia. En algunos casos, los virus utilizan nombres de procesos estándar del sistema para hacer que su presencia sea menos aparente en el sistema.

- ***Archivo bloqueado***: el archivo notificado está bloqueado, por lo que **AVG Internet Security 2012** no puede analizarlo. Esto suele significar que el sistema utiliza un archivo constantemente (*por ejemplo, un archivo swap*).

12.8. Bóveda de virus



La ***Bóveda de virus*** es un entorno seguro para administrar los objetos sospechosos o infectados que se han detectado durante los análisis de AVG. Una vez que se detecta un objeto infectado durante el análisis, y AVG no puede repararlo de inmediato, se le pide que decida qué hacer con el objeto sospechoso. La solución recomendada es mover el objeto a la ***Bóveda de virus*** para tratarlo allí. El objetivo principal de la ***Bóveda de virus*** es conservar cualquier archivo eliminado durante un cierto periodo de tiempo, para que pueda asegurarse de que ya no necesita el archivo en la ubicación original. Si la ausencia de un archivo provoca problemas, puede enviar dicho archivo a análisis, o bien restaurarlo a su ubicación original.

La interfaz de la ***Bóveda de virus*** se abre en una ventana aparte y ofrece una descripción general de información sobre los objetos infectados en cuarentena:

- ***Severidad***: si decidió instalar el componente Identity Protection en **AVG Internet Security 2012**, en esta sección se ofrecerá una identificación gráfica de la severidad de los hallazgos en una escala de cuatro niveles que van desde inobjetable (□□□□) hasta muy peligroso (■■■■), y la información del tipo de infección (*basada en el nivel de infección; todos los objetos enumerados pueden estar infectados o potencialmente infectados*)
- ***Nombre del virus***: especifica el nombre de la infección detectada conforme a la Enciclopedia de virus *(en línea).*
- ***Ruta al archivo***: ruta completa de la ubicación original del archivo infeccioso detectado.
- ***Nombre del objeto original***: todos los objetos detectados listados en la tabla se han etiquetado con el nombre estándar dado por AVG durante el proceso de análisis. Si el

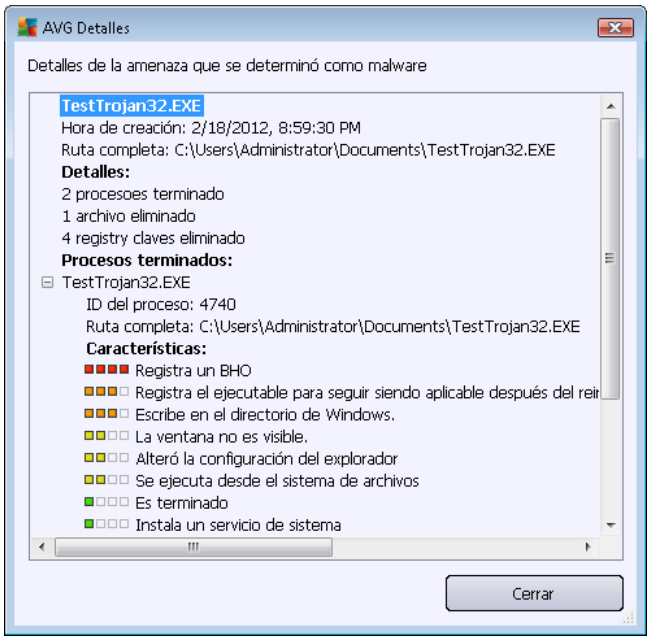
objeto tenía un nombre original específico que es conocido (*por ejemplo el nombre de un dato adjunto de correo electrónico que no responde al contenido real del dato adjunto*), se proporcionará en esta columna.

- ***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***: mueve el archivo infectado a una carpeta seleccionada.
- ***Detalles***: este botón sólo se aplica a las amenazas detectadas por Identity Protection. Al hacer clic, aparece una descripción general de los detalles de la amenaza (*archivos o procesos que se han visto afectados, características del proceso, etc.*). Observe que para los elementos que no hayan sido detectados por IDP, este botón aparece en gris y está inactivo!



- ***Eliminar***: elimina el archivo infectado de la ***Bóveda de virus*** de forma total e irreversible.
- ***Vaciar la Bóveda de virus***: elimina todo el contenido de la ***Bóveda de virus*** permanentemente. Al eliminar los archivos de la ***Bóveda de virus***, estos archivos se borran del disco de forma irreversible (*no se transfieren a la Papelera de reciclaje*).

13. Actualizaciones de AVG

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.

Teniendo en cuenta la cantidad de nuevas amenazas para su equipo que surgen cada día y la velocidad a la que se propagan, es absolutamente esencial actualizar su **AVG Internet Security 2012** de manera periódica. La mejor solución consiste en mantener la configuración predeterminada del programa donde está configurada la actualización automática. Tenga en cuenta que si la base de datos de virus de su **AVG Internet Security 2012** no está actualizada, el programa no podrá detectar las amenazas más recientes.

Es fundamental actualizar el programa AVG periódicamente. Las actualizaciones de definiciones de virus esenciales deben ser diarias si es posible. Las actualizaciones del programa menos urgentes pueden efectuarse semanalmente.

13.1. Ejecución de actualizaciones

Con el fin de proporcionar la máxima seguridad disponible, **AVG Internet Security 2012** está programado de forma predeterminada para buscar nuevas actualizaciones cada cuatro horas. Como las actualizaciones de AVG no se publican de acuerdo con ninguna programación fija, sino en respuesta a la cantidad y severidad de nuevas amenazas, esta comprobación es muy importante para tener la seguridad de que su base de datos de virus de AVG se mantenga actualizada en todo momento.

Si desea reducir el número de ejecuciones de actualizaciones, puede configurar sus propios parámetros de ejecución de actualizaciones. No obstante, se recomienda estrictamente ejecutar la actualización al menos una vez al día. La configuración se puede editar en la sección Configuración avanzada/Programaciones, en concreto en los siguientes cuadros de diálogo:

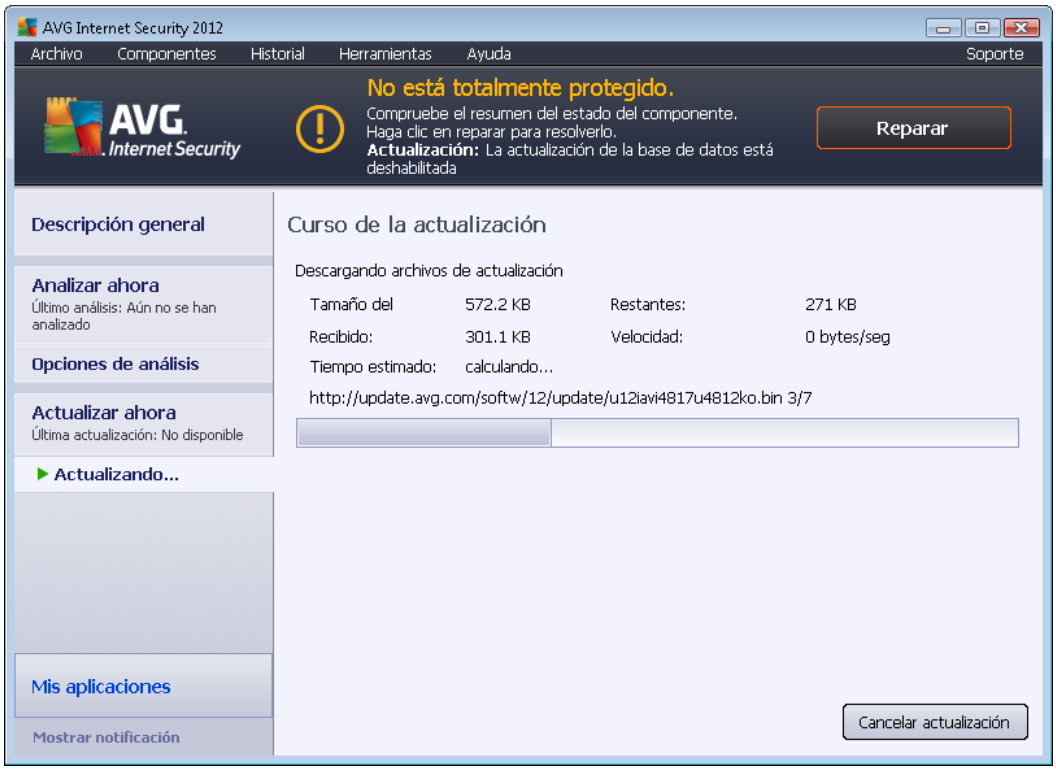
- Programación de actualización de las definiciones
- Programación de actualización del programa
- Programación de actualización de Anti-Spam

En caso de que desee comprobar la existencia de nuevos archivos de actualización inmediatamente, utilice el vínculo rápido Actualizar ahora de la interfaz del usuario principal. Este vínculo está disponible en todo momento desde cualquier cuadro de diálogo de la interfaz del usuario.

13.2. Curso de la actualización

Una vez que se inicia la actualización, AVG comprobará primero si hay nuevos archivos de actualización disponibles. Si es así, **AVG Internet Security 2012** iniciará la descarga y ejecutará el proceso de actualización por sí mismo. Durante el proceso de actualización, se le enviará a la interfaz de ***actualización***, en donde puede ver una representación gráfica del progreso del proceso,

así como una descripción general de los parámetros estadísticos relevantes (*tamaño del archivo actualizado, datos recibidos, velocidad de descarga, tiempo transcurrido, etc.)*:



***Nota**: antes de cada ejecución de la actualización del programa AVG, se crea un punto de restauración del sistema. Si el proceso de actualización falla y el 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 del menú de Windows: Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema. ¡Recomendado sólo para usuarios avanzados!*

13.3. Niveles de actualización

AVG Internet Security 2012 permite seleccionar dos niveles de actualización:

- ***Actualización de definiciones*** contiene los cambios necesarios para una protección antivirus, anti-spam y anti-malware confiable. Por lo general, no incluye cambios del código y sólo actualiza la base de datos de definiciones. Esta actualización se debe aplicar tan pronto como esté disponible.
- ***Actualización del programa*** contiene diferentes modificaciones, arreglos y mejoras del programa.

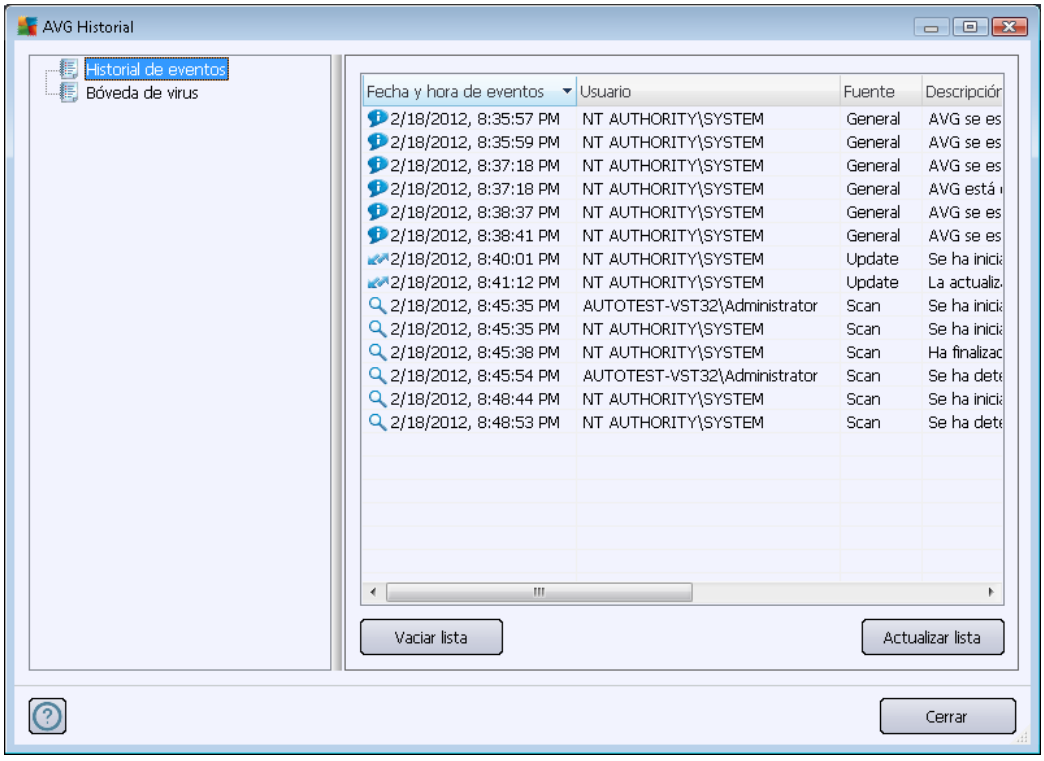
Al programar una actualización, es posible definir parámetros específicos para ambos niveles de actualización:

- Programación de actualización de las definiciones

- Programación de actualización del programa

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

14. Historial de eventos



Se puede obtener acceso al cuadro de diálogo ***Historial*** 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 **AVG Internet Security 2012**. ***Historial*** registra los tipos de eventos siguientes:

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

Para cada evento, se muestra la información siguiente:

- ***Fecha y hora de eventos*** da la fecha y hora exactos en que ocurrió el evento
- ***Usuario*** indica el nombre del usuario que había iniciado sesión en el momento en que se produjo el evento
- ***Fuente*** ofrece información sobre el componente de origen u otra parte del sistema AVG que desencadenó el evento

- ***Descripción del evento*** da un breve resumen del evento

Botones de control

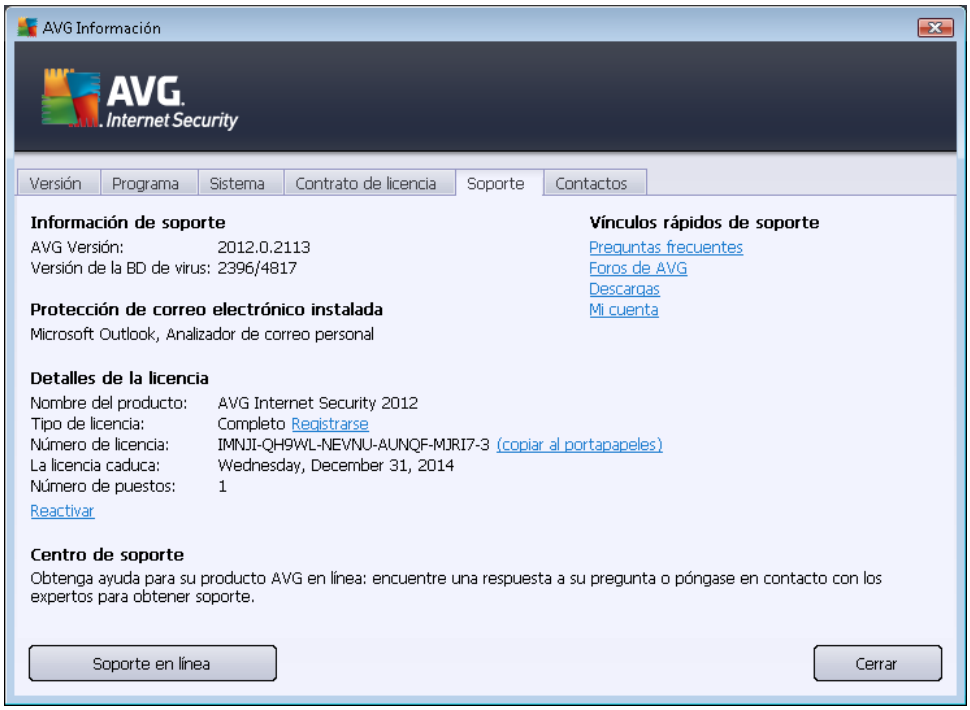
- ***Vaciar lista***: presione este botón para eliminar todas las entradas de la lista de eventos
- ***Actualizar lista***: presione este botón para actualizar todas las entradas de la lista de eventos

15. Preguntas frecuentes y soporte técnico

Si tiene algún problema técnico o referente a la compra de la aplicación **AVG Internet Security 2012**, existen varios modos de buscar ayuda. Elija una de las opciones siguientes:

- ***Obtener soporte***: directamente desde la aplicación AVG, puede obtener acceso a una página dedicada de soporte al cliente en el sitio Web de AVG.(http://www.avg.com/) Seleccione el elemento del menú principal ***Ayuda / Obtener soporte*** para acceder al sitio Web de AVG con las opciones de soporte disponibles. Para continuar, siga las instrucciones de la página Web.

- ***Soporte (vínculo del menú principal)***: el menú de la aplicación AVG (*en la parte superior de la interfaz del usuario principal*) incluye el vínculo ***Soporte***, que abre un cuadro de diálogo nuevo con todos los tipos de información que puede necesitar cuando intente encontrar ayuda. El cuadro de diálogo incluye datos básicos sobre el programa AVG instalado (*versión del programa o la base de datos*), detalles de la licencia y una lista de vínculos de soporte rápidos:



- ***Resolución de problemas en el archivo de ayuda***: hay disponible una sección ***Resolución de problemas*** directamente en el archivo de ayuda de **AVG Internet Security 2012** *(para abrir el archivo de ayuda, presione la tecla F1 en cualquier cuadro de diálogo en la aplicación)*. Esta sección proporciona una lista de las situaciones que se producen con más frecuencia cuando un usuario desea obtener ayuda profesional sobre una cuestión técnica. Seleccione la situación que mejor describa su problema y haga clic en ella para abrir instrucciones detalladas que le permitan solucionarlo.

- ***Centro de soporte del sitio Web de AVG***: como alternativa, puede buscar la solución a su problema en el sitio Web de AVG (http://www.avg.com/). En la sección ***Centro de soporte*** encontrará una descripción general estructurada de grupos temáticos referentes

tanto a cuestiones técnicas como a la compra.

- ***Preguntas frecuentes***: en el sitio Web de AVG (http://www.avg.com/) también encontrará una sección independiente y minuciosamente estructurada de preguntas frecuentes. Se puede obtener acceso a esta sección por medio de la opción de menú ***Centro de soporte / Preguntas frecuentes***. Una vez más, todas las preguntas están divididas de forma bien organizada en las categorías de ventas, técnicas y sobre virus.

- ***Acerca de virus y amenazas***: un capítulo específico del sitio Web de AVG (http://www.avg.com/) está dedicado a los problemas de virus *(se accede a la página Web desde el menú principal mediante la opción Ayuda / Acerca de virus y amenazas)*. En el menú, seleccione ***Centro de soporte / Acerca de virus y amenazas*** para tener acceso a una página que proporciona una descripción general estructurada de información relacionada con amenazas en línea. También encontrará instrucciones sobre cómo eliminar virus y spyware y cómo mantenerse protegido.

- ***Foro de discusión***: también puede utilizar el foro de discusión de usuarios de AVG en http://forums.avg.com.