AVG Internet Security 2012

Manual del usuario

Revisión del documento 2012.01 (1.9.2011)

Contenido

1. Introducción

Este manual del usuario proporciona documentación completa sobre **AVG Internet Security 2012**.

AVG Internet Security 2012 proporciona múltiples capas de protección para todas sus actividades en línea, lo que significa que no tiene que preocuparse por el robo de identidad, los virus o visitar sitios peligrosos. Se incluyen la tecnología de nube protectora y la red de protección de la comunidad de AVG, lo que significa que recopilamos la última información sobre amenazas y la compartimos con nuestra comunidad para asegurarnos de que recibe la mejor protección:

- Compre y realice operaciones bancarias en línea con total seguridad gracias a los componentes Firewall, Identity Protection y Anti-Spam de AVG
- Manténgase protegido en las redes sociales gracias a la Protección de redes sociales de AVG
- Navegue y haga búsquedas con confianza con la protección en tiempo real de LinkScanner

2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG Internet Security 2012 se ha diseñado para proteger 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 (x86 y x64, todas las ediciones)

(y probablemente service packs superiores de los sistemas operativos especificados)

***Nota**: el componente Identity Protection (IDP) 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 de hardware mínimos y recomendados

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

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

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

- CPU 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 obtengo 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 está instalando una versión actualizada de **AVG Internet Security 2012**, se recomienda descargar el archivo de instalación desde el sitio web de AVG (http://www.avg.com/). La sección ***Centro de soporte / Descarga*** proporciona información estructurada sobre los archivos de instalación para cada edición de AVG.

Si no está seguro de qué archivos necesita descargar e instalar, puede que desee utilizar el servicio ***Seleccione el producto*** en la parte inferior de la página web. Después de contestar a tres sencillas preguntas, este servicio definirá los archivos exactos que necesita. Pulse el botón ***Continuar*** para que se le redirija a una lista completa de archivos de descarga personalizados para sus necesidades.

¿Qué aspecto tiene el proceso de instalación?

Una vez que haya descargado y guardado el archivo de instalación en el disco duro, podrá iniciar el proceso de instalación. La instalación es una secuencia de cuadros de diálogo simples y fáciles de entender. Cada uno describe brevemente qué se hace en cada paso del proceso de instalación. A continuación se ofrece una explicación detallada de cada ventana de diálogo:

3.1. Bienvenido

El proceso de instalación comienza con el cuadro de diálogo ***Instalador de AVG***:

Seleccione el idioma de instalación

En este cuadro de diálogo puede seleccionar el idioma utilizado para el proceso de instalación. En la esquina derecha del cuadro de diálogo, haga clic en el campo para desplegar el menú de idiomas. Seleccione el idioma deseado, y el proceso de instalación continuará en el idioma que haya elegido.

Atención: de momento, sólo está seleccionando 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. Sin embargo, es posible tener más idiomas instalados para trabajar con AVG Internet Security 2012 en cualquiera de ellos. Deberá confirmar la selección completa de idiomas alternativos en uno de los siguientes cuadros de diálogo de configuración llamado Opciones personalizadas.

Contrato de licencia

El cuadro de diálogo ***Instalador de AVG*** también proporciona el texto completo del contrato de licencia de AVG. Léalo detenidamente. Para confirmar que lo ha leído, comprendido y que lo acepta, pulse el botón ***Acepto***. Si no está de acuerdo con el contrato de licencia, pulse el botón ***Declinar*** y el proceso de instalación finalizará de inmediato.

Política de privacidad de AVG

Aparte del contrato de licencia, este cuadro de diálogo de configuración también le ofrece la opción de conocer más 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 para acceder al sitio web de AVG (http://www.avg.com/), donde puede encontrar la versión completa de los principios de la política de privacidad de AVG Technologies.

Botones de control

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

- ***Acepto***: haga clic para confirmar que ha leído, comprendido y aceptado el contrato de licencia. La instalación continuará, y avanzará hasta el cuadro de diálogo de configuración siguiente.
- ***Declinar***: haga clic para rechazar el contrato de licencia. El proceso de instalación finalizará automáticamente. **AVG Internet Security 2012** no se instalará.

3.2. Active su licencia

En el cuadro de diálogo ***Active su licencia***, se le solicita que introduzca su número de licencia en el campo de texto proporcionado:

Dónde encontrar el número de licencia

Puede encontrar el número de venta en el paquete del CD, dentro de la caja de **AVG Internet Security 2012**. El número de licencia se encontrará en el correo electrónico de confirmación que recibió después de haber comprado **AVG Internet Security 2012** en línea. Debe introducir el número tal como figura. Si cuenta con el formato digital del número de licencia (*en el correo electrónico*), se recomienda usar el método copiar y pegar para insertarlo.

Cómo utilizar el método copiar y pegar

Si utiliza el método ***copiar y pegar*** para especificar su número de licencia de **AVG Internet Security 2012** se asegurará de que el número introducido es el correcto. Realice el siguiente procedimiento:

- Abra el correo electrónico que contiene su número de licencia.
- Haga clic en el botón izquierdo del ratón al principio del número de licencia, mantenga pulsado y arrastre el ratón hasta el final del número, y suelte el botón del ratón. El número aparece seleccionado.
- Pulse y mantenga pulsada la tecla ***Ctrl*** y luego pulse ***C***. Esto copia el número.
- Haga clic en la posición en la que desea pegar el número copiado.

- Pulse y mantenga pulsada la tecla ***Ctrl*** y luego pulse ***V***. Esto pega el número en el lugar seleccionado.

Botones de control

Como en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

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

3.3. Seleccione el tipo de instalación

Tipos de instalación

El cuadro de diálogo ***Seleccione el tipo de instalación*** permite elegir entre dos opciones de instalación: ***Instalación rápida*** e ***Instalación personalizada***.

Para la mayoría de los usuarios, se recomienda elegir la Instalación rápida estándar, que instala **AVG Internet Security 2012** de un modo totalmente automático con la configuración predefinida por el distribuidor del programa. Esta configuración ofrece máxima seguridad con un uso óptimo de los recursos. En el futuro, si fuese necesario modificar la configuración, siempre tendrá la posibilidad de hacerlo directamente desde la aplicación **AVG Internet Security 2012**. Si seleccionó la opción ***Instalación rápida***, pulse el botón ***Siguiente*** para abrir el cuadro de diálogo Instalar AVG Security Toolbar.

La instalación personalizada sólo la deberían realizar usuarios experimentados que tuvieran una buena razón para instalar **AVG Internet Security 2012** con una configuración no estándar, p. ej., para adaptarse a requisitos específicos del sistema. Tras seleccionar esta opción, haga clic en el botón ***Siguiente*** para ir al cuadro de diálogo Opciones personalizadas.

Instalación del gadget de AVG

En la sección del lado derecho del cuadro de diálogo encontrará la casilla de verificación relacionada con el Gadget de AVG (*compatible con Windows Vista/Windows 7*). Si desea instalar este gadget, marque la casilla de verificación correspondiente. A continuación, el Gadget de AVG aparecerá en la barra lateral de Windows para brindarle acceso inmediato a las características más importantes de **AVG Internet Security 2012**; por ejemplo, análisis y actualizaciones.

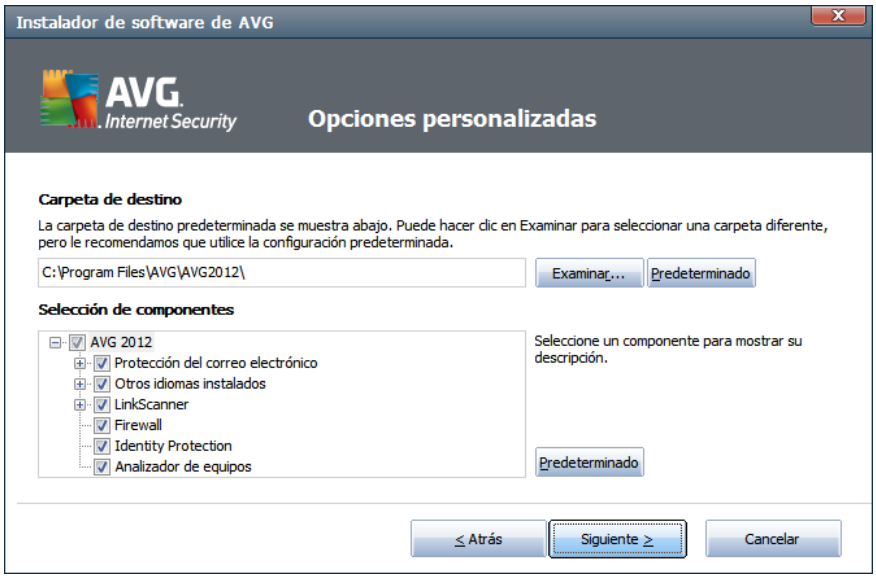
Botones de control

Como en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

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

3.4. Opciones personalizadas

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



Carpeta de destino

En la sección ***Carpeta de destino*** del cuadro de diálogo, debe especificar la ubicación para la instalación de **AVG Internet Security 2012**. De manera predeterminada, **AVG Internet Security 2012** se instalará en la carpeta de archivos de programa ubicada en la unidad C:. Si desea cambiar esta ubicación, utilice el botón ***Examinar*** para mostrar la estructura de la unidad y seleccione la carpeta en cuestión.

Selección de componentes

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

Sin embargo, solamente puede seleccionar componentes incluidos en la edición de AVG que haya adquirido.

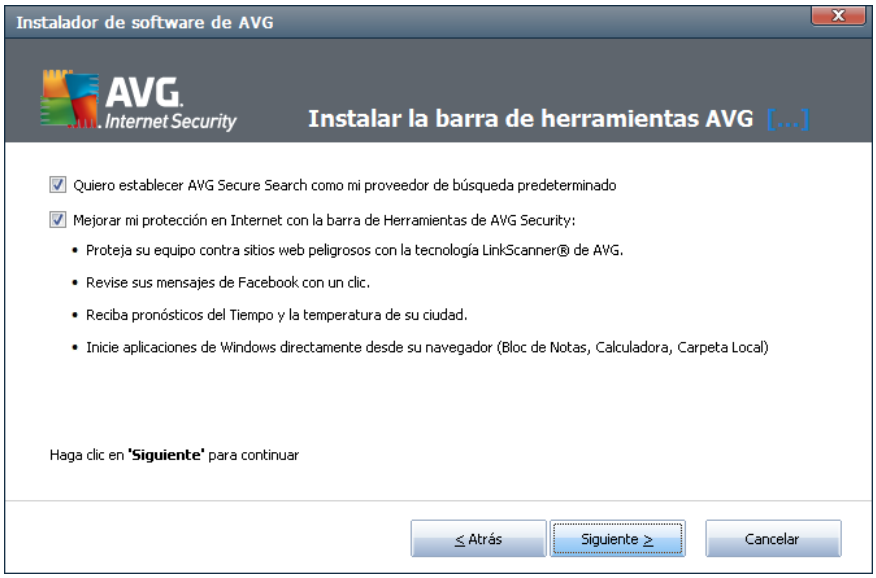
Resalte cualquier elemento de la lista ***Selección de componentes*** y se mostrará una breve descripción del mismo en el lado derecho de esta sección. Para obtener información detallada sobre la funcionalidad de cada componente, consulte el capítulo Información general de los componentes de esta documentación. Para restaurar la configuración predeterminada por el proveedor del software, utilice el botón ***Predeterminado***.

Botones de control

Como en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

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

3.5. Instalar AVG Security Toolbar



En el cuadro de diálogo ***Instalar AVG Security Toolbar***, indique si desea instalar la barra de herramientas 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 amplia protección en línea mientras navega por Internet.

También puede indicar si desea escoger *AVG Secure Search (powered by Google)* como el proveedor de búsqueda predeterminado. Si es así, mantenga la selección de la correspondiente casilla de verificación.

3.6. Progreso de la instalación

El cuadro de diálogo ***Progreso de la instalación*** muestra el avance del proceso de instalación y no requiere ninguna intervención:

Después de finalizar el proceso de instalación, se le redirigirá automáticamente al siguiente cuadro de diálogo.

Botones de control

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

3.7. La instalación se ha realizado correctamente

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

Programa de mejora de productos

En este cuadro de diálogo puede decidir si desea participar en el Programa de mejora de productos (*para obtener más información consulte el capítulo Configuración avanzada de AVG / Programa de mejora de productos*), que recopila información anónima sobre las amenazas detectadas con el objeto de mejorar el nivel de seguridad global de Internet. Si está de acuerdo en participar, mantenga marcada la opción ***Acepto participar en la seguridad web de AVG 2012 y Programa de mejora de productos...*** *(la opción está confirmada de manera predeterminada)*.

Reinicio del equipo

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

Instalación de la licencia Business

Si está utilizando una licencia Business de AVG y ha seleccionado anteriormente que se instale Administración remota *(consulte Opciones personalizadas)*, aparece el cuadro de diálogo La instalación se ha realizado correctamente, con la siguiente interfaz:

Debe especificar los parámetros del Centro de datos de AVG; proporcione la cadena de conexión al Centro de datos de AVG con el formato servidor:puerto. Si esta información no está disponible actualmente, deje en blanco el campo, ya que posteriormente podrá definir la configuración en el cuadro de diálogo Configuración avanzada / Administración remota. Para obtener información detallada sobre la Administración remota de AVG, consulte el manual del usuario de AVG Business Edition que puede descargarse del sitio web de AVG (http://www.avg.com/).

Consulte el capítulo Información general de los componentes de esta documentación. Para restaurar la configuración predeterminada por el proveedor del software, utilice el botón ***Predeterminado***.

Botones de control

En el cuadro de diálogo, están disponibles los siguientes botones de control:

- ***Reiniciar ahora (recomendado)***: es necesario reiniciar para completar el proceso de instalación de **AVG Internet Security 2012**. Se recomienda que reinicie el equipo inmediatamente. Sólo después del reinicio, **AVG Internet Security 2012** estará completamente instalado, y usted estará seguro y protegido.

- ***Reiniciar más tarde***: si por algún motivo no puede reiniciar el equipo ahora, la acción se puede posponer. Sin embargo, se recomienda reiniciar inmediatamente. Sólo después de reiniciar, **AVG Internet Security 2012** puede proteger completamente su equipo.

4. Tras la instalación

4.1. Registro del producto

Cuando haya finalizado la instalación de **AVG Internet Security 2012**, registre el producto en línea en el sitio web de AVG (http://www.avg.com/). Después de registrar el producto, podrá obtener acceso total a su cuenta de usuario de AVG, al boletín de actualizaciones de AVG y a otros servicios que se ofrecen exclusivamente a los usuarios registrados.

La forma más sencilla de registrarse es directamente a través de la interfaz de usuario de **AVG Internet Security 2012**. En el menú principal, seleccione el elemento Ayuda/Registrarse ahora. Se le redirigirá a la página ***Registro*** en el sitio web de AVG (http://www.avg.com/). Siga las instrucciones proporcionadas en dicha página.

4.2. Acceso a la interfaz de usuario

Se puede acceder al cuadro de diálogo principal AVG de varias formas:

- haciendo doble clic en el icono de AVG en la bandeja del sistema
- haciendo doble clic en el icono de AVG en el escritorio
- haciendo doble clic en la línea de estado situada en la sección inferior del gadget de AVG (*si está instalado; compatible con Windows Vista y Windows 7*)
- desde el menú ***Inicio/Programas/AVG 2012/Interfaz del usuario de AVG***

4.3. Análisis del equipo completo

Existe el riesgo potencial de que un virus informático se haya transmitido a su equipo antes de la instalación de **AVG Internet Security 2012**. Por esta razón, le recomendamos ejecutar un Análisis del equipo completo para verificar que no haya infecciones en el equipo.

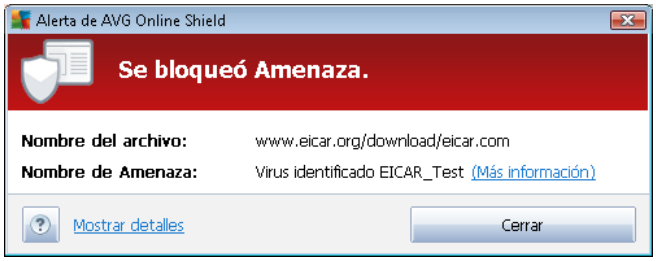
Para ver instrucciones sobre cómo ejecutar un Análisis del equipo completo, consulte el capítulo Análisis de AVG.

4.4. Prueba Eicar

Para confirmar que **AVG Internet Security 2012** se ha instalado correctamente, puede realizar la prueba EICAR.

La prueba EICAR es un método estándar y totalmente seguro empleado para comprobar el funcionamiento de sistemas antivirus. Su distribución es segura, puesto que no es un virus real, y no incluye ningún fragmento de código vírico. La mayoría de los productos reaccionan a la prueba como si fuera un virus (*aunque suelen informar de la misma con un nombre obvio, como "EICAR-AV-Test"*). Puede descargar el virus EICAR en el sitio web de EICAR, www.eicar.com, donde también encontrará toda la información necesaria sobre la prueba EICAR.

Intente descargar el archivo ***eicar.com*** y guárdelo en el disco local. Inmediatamente despues de confirmar la descarga del archivo de prueba, Online Shield (*una parte del componente Link Scanner*) reaccionará con un aviso. Este aviso demuestra que AVG se ha instalado correctamente en el equipo.



En el sitio web http://www.eicar.com también puede descargar la versión comprimida del "virus" EICAR (*p. ej., en forma de eicar_com.zip*). Online Shield le permite descargar este archivo y guardarlo en su disco duro, pero Protección residente (*en el componente Anti-Virus*) detectará el "virus" cuando intente descomprimirlo.

Si AVG no identifica el archivo de la prueba EICAR como un virus, debe comprobar de nuevo la configuración del programa.

4.5. Configuración predeterminada de AVG

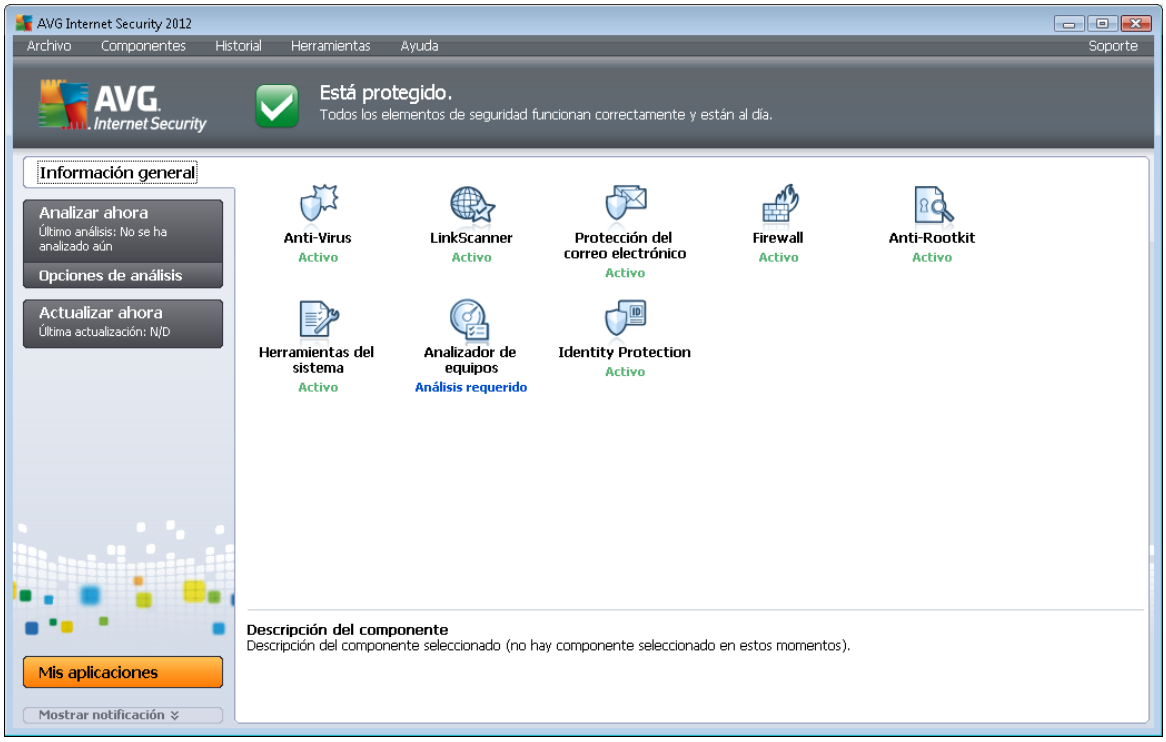
La configuración predeterminada (*es decir, cómo está configurada la aplicación justamente después de la instalación*) de **AVG Internet Security 2012** la realiza el proveedor del software de manera que todos los componentes y funciones ofrezcan un rendimiento óptimo.

A menos que tenga un buen motivo para hacerlo, no modifique la configuración de AVG. Los cambios de configuración debe realizarlos únicamente un usuario experimentado.

Es posible realizar cambios menores en la configuración de los componentes de AVG directamente desde la interfaz de usuario específica de cada componente. Si considera que necesita modificar la configuración de AVG para adaptarla mejor a sus necesidades, vaya a Configuración avanzada de AVG, seleccione el elemento de menú del sistema ***Herramientas/Configuración avanzada*** y edite la configuración de AVG en el cuadro de diálogo Configuración avanzada de AVG que se acaba de abrir.

5. Interfaz de 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 superior del sistema en la ventana)* es la navegación estándar que le permite acceder a todos los componentes, servicios y funciones de **AVG Internet Security 2012** - detalles >>
- ***Información sobre el estado de seguridad*** *(parte superior de la ventana)* le ofrece información sobre el estado actual de su **AVG Internet Security 2012** - detalles >>
- ***Vínculos rápidos*** *(parte izquierda de la ventana)* le permite acceder rápidamente a las tareas más importantes y más utilizadas de **AVG Internet Security 2012** - detalles >>
- ***Mis aplicaciones*** *(sección inferior izquierda de la ventana)* abre información general de las aplicaciones adicionales disponibles para **AVG Internet Security 2012**: LiveKive, Family Safety y PC Tuneup
- ***Información general de los componentes*** *(parte central de la ventana)* ofrece una descripción general de todos los componentes instalados con **AVG Internet Security 2012** - detalles >>
- ***Icono de bandeja del sistema*** *(extremo inferior derecho de la pantalla, en la bandeja del sistema)* indica el estado actual de **AVG Internet Security 2012** - detalles >>
- ***Gadget de AVG*** *(barra lateral de Windows, en 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 utilizado en todas las aplicaciones de Windows. Se encuentra situado horizontalmente en la parte superior de la ventana principal de **AVG Internet Security 2012**. Utilice el menú del sistema para acceder a componentes, características y servicios específicos de AVG.

El menú del sistema se divide en cinco secciones principales:

5.1.1. Archivo

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

5.1.2. Componentes

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

- ***Información general del sistema***: cambia al cuadro de diálogo predeterminado de la interfaz de usuario con la información general de todos los componentes instalados y su estado
- ***Anti-Virus*** detecta virus, spyware, gusanos, troyanos, archivos ejecutables o bibliotecas del sistema no deseados, y le protege del spam malicioso - detalles >>
- ***LinkScanner*** le protege de ataques web mientras navega por Internet - detalles >>
- ***Protección del correo electrónico*** comprueba sus mensajes de correo electrónico en busca de spam y bloquea virus, ataques de suplantación de identidad y otras amenazas - detalles >>
- ***Firewall*** controla toda la comunicación de cada puerto de red, ofrece protección frente a ataques maliciosos y bloquea los intentos de intrusión - detalles >>
- ***Anti-Rootkit*** analiza en busca de rootkits peligrosos ocultos dentro de las aplicaciones, controladores o bibliotecas - detalles >>
- ***Herramientas del sistema*** ofrece un resumen detallado del entorno de AVG e información sobre el sistema operativo - detalles >>
- ***Analizador de equipos*** proporciona información sobre el estado del equipo - detalles >>
- ***Identity Protection*** protege constantemente sus activos digitales contra amenazas nuevas y desconocidas - detalles >>
- ***Security Toolbar*** permite utilizar determinados elementos de la funcionalidad de AVG directamente desde su navegador de Internet - detalles >>
- ***Administración remota*** sólo se muestra en las ediciones AVG Business si durante el proceso de instalación ha especificado que desea instalar este componente

5.1.3. Historial

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

- Detección de Protección residente: abre un cuadro de diálogo con información general de las amenazas detectadas por Protección residente

- Detección de Analizador de correo electrónico: abre un cuadro de diálogo con información general de los archivos adjuntos de correo electrónico detectados como peligrosos por el componente Protección del correo electrónico

- Resultados de Online Shield: abre un cuadro de diálogo con información sobre las amenazas detectadas por el servicio Online Shield del componente LinkScanner

- Almacén de virus: abre la interfaz del espacio de cuarentena (Almacén de virus) donde AVG envía todas las infecciones detectadas que por alguna razón no se pueden reparar automáticamente. Dentro de este espacio de cuarentena, los archivos infectados están aislados y la seguridad del equipo está garantizada, y al mismo tiempo los archivos infectados se almacenan para una posible reparación en el futuro

- Registro del historial de eventos: abre la interfaz del registro del historial con información general de todas las acciones de **AVG Internet Security 2012** registradas

- Firewall: abre la interfaz de configuración del Firewall en la ficha Registros, que contiene información detallada de todas las acciones de este componente

5.1.4. Herramientas

- Analizar equipo: pasa a la interfaz de análisis de AVG e inicia un análisis de todo el equipo.

- Analizar carpeta seleccionada...: pasa a la interfaz de análisis de AVG y permite definir, dentro de la estructura de árbol del equipo, qué archivos y carpetas deben analizarse.

- Analizar archivo... : permite ejecutar un análisis bajo demanda en un solo archivo seleccionado en la estructura de árbol del disco.

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

- ***Actualizar desde directorio...***: ejecuta el proceso de actualización desde los archivos de actualización que se encuentran ubicados en una carpeta específica del disco local. No obstante, esta opción sólo se recomienda en caso de emergencia, es decir, en situaciones en las que no hay conexión a Internet (*por ejemplo, si el equipo está infectado y desconectado de Internet, o bien está conectado a una red que no tiene acceso a Internet, etc.*). En la ventana recién abierta, seleccione la carpeta donde anteriormente se guardó el archivo de actualización e inicie el proceso de actualización.

- Configuración avanzada...: abre el cuadro de diálogo Configuración avanzada de AVG, donde puede editar la configuración de AVG Internet Security 2012. Por lo general, se recomienda mantener la configuración predeterminada de la aplicación definida por el

proveedor del software.

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

5.1.5. Ayuda

- ***Contenido***: abre los archivos de ayuda de AVG
- ***Obtener ayuda en línea***: abre el sitio web de AVG (http://www.avg.com/) en la página del centro de atención al cliente
- ***Web de 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 sobre los virus identificados
- ***Reactivar***: abre el cuadro de diálogo ***Activar AVG*** con los datos que ha introducido en el cuadro de diálogo Personalizar AVG del proceso de instalación. En este cuadro de diálogo puede introducir su número de licencia para reemplazar el número de venta (*el número con el que ha instalado AVG*) o sustituir el número de licencia antiguo (*por ejemplo, cuando actualice a un nuevo producto AVG*).
- ***Registrarse ahora***: conecta con la página de registro del sitio web de AVG (http://www.avg.com/). Introduzca sus datos de registro; solamente los clientes que registran su producto AVG pueden recibir soporte técnico gratuito.

Nota**: si utiliza la versión de prueba de* **AVG Internet Security 2012**, *los últimos dos elementos aparecen como* ***Comprar ahora *y* ***Activar***, *y le permiten adquirir de inmediato la versión completa del programa. Si* **AVG Internet Security 2012** *se ha instalado con un número de venta, se muestran los elementos* ***Registrar*** *y* ***Activar**.*

- ***Acerca de AVG***: abre el cuadro de diálogo ***Información*** con cinco fichas que proporcionan datos sobre el nombre del programa, la versión del programa y de 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 buscar ayuda. El cuadro de diálogo incluye datos básicos sobre su programa AVG instalado (*versión de la base de datos/programa*), datos de licencia y una lista de vínculos rápidos de soporte.

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

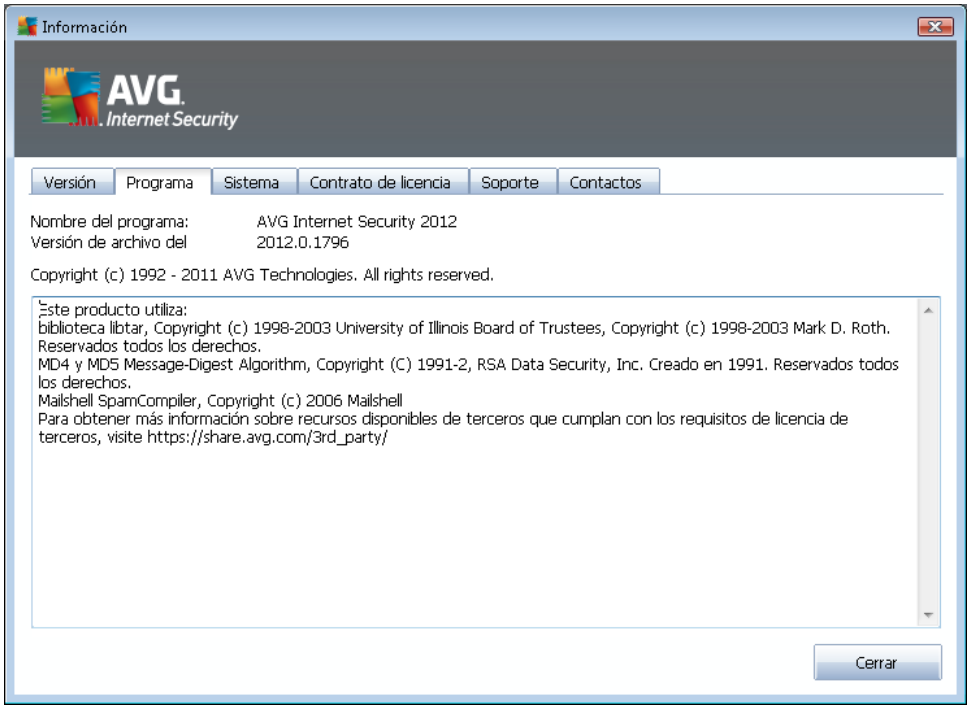
La ficha ***Versión*** está dividida en tres secciones:

- ***Información de soporte***: ofrece información sobre 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.

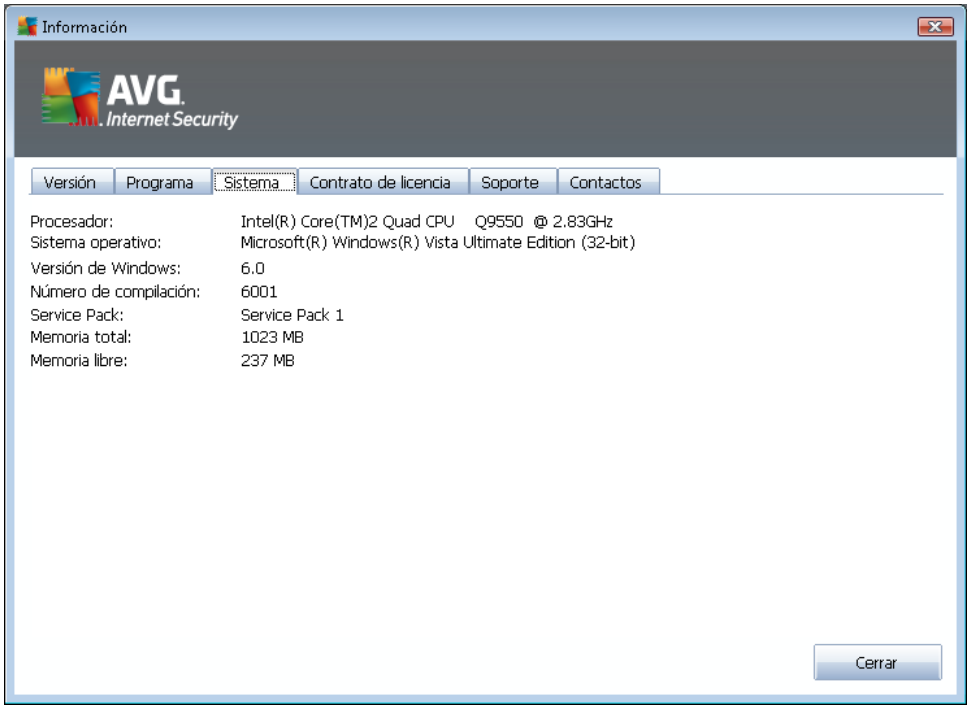
- ***Información del usuario***: ofrece información del usuario registrado y de su empresa.

- ***Detalles de la licencia***: ofrece información de la licencia *(nombre del producto, tipo de licencia, número de licencia, fecha de caducidad y número de puestos*). En esta sección también puede utilizar el vínculo ***Registrar*** para registrar su **AVG Internet Security 2012** en línea; esto le proporciona acceso total al soporte técnico de AVG. Igualmente, utilice el vínculo ***Reactivar*** para abrir en cuadro de diálogo ***Activar AVG***: escriba su número de licencia en el campo respectivo para sustituir su número de venta *(el que utilizó durante la instalación de AVG Internet Security 2012)* o para cambiar su número de licencia actual por otro *(por ejemplo, si actualiza a un producto de AVG superior).*

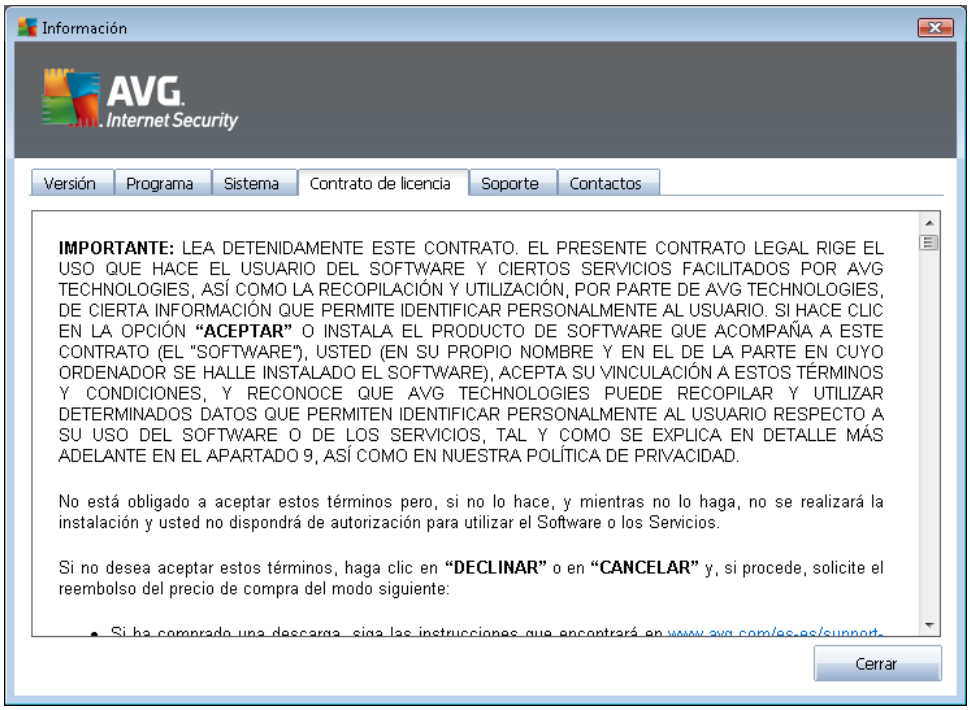
En la ficha ***Programa*** puede encontrar información sobre la versión del archivo de programa de **AVG Internet Security 2012** y del código de terceros empleado en el producto:



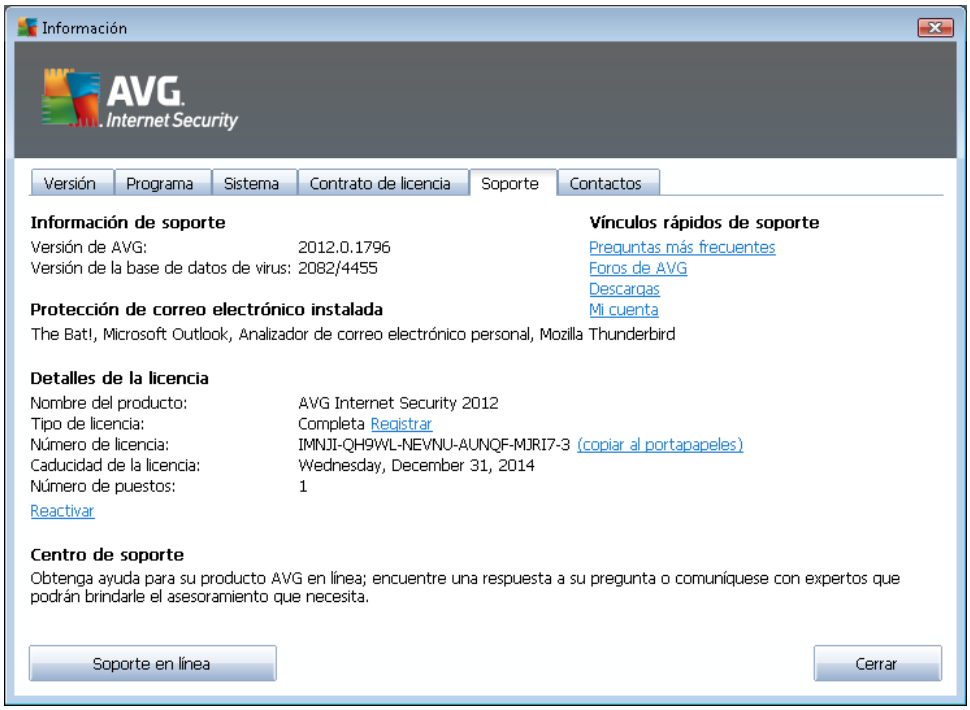
La ficha ***Sistema*** proporciona una lista de parámetros del sistema operativo *(tipo de procesador, sistema operativo y versión, número de compilación, service packs utilizados, tamaño total de memoria y tamaño de memoria libre)*:



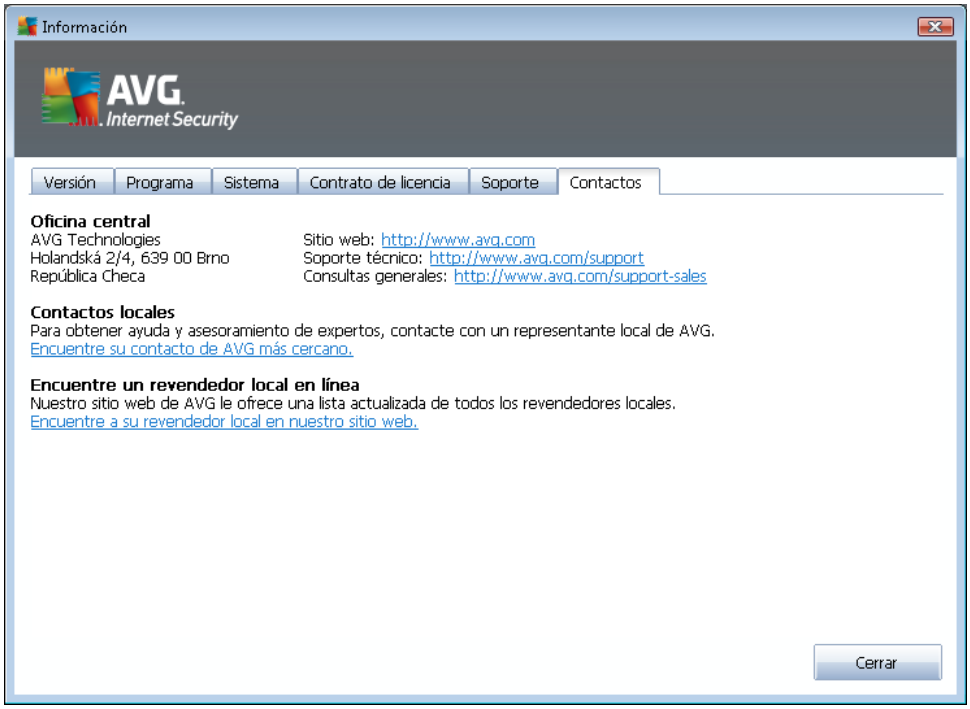
En la ficha ***Contrato de licencia*** puede leer el texto completo del contrato de licencia entre usted y AVG Technologies:



La ficha ***Soporte*** ofrece una lista de las posibilidades para ponerse en contacto con el servicio de atención al cliente. Igualmente, ofrece vínculos al sitio web de AVG (http://www.avg.com/), foros de AVG, preguntas más frecuentes, etc. Además, proporciona información que podría serle útil al contactar con el equipo de atención al cliente:



La ficha ***Contactos*** proporciona una lista de todos los contactos de AVG Technologies, y también los contactos de distribuidores y representantes locales de AVG:



5.2. Información sobre el estado de seguridad

La sección ***Información sobre el estado de seguridad*** se encuentra 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 **AVG Internet Security 2012**. A continuación se describen los iconos que pueden aparecer en esta sección y su significado:

 - El icono verde indica que ***AVG Internet Security 2012 funciona correctamente***. El equipo está totalmente protegido y actualizado, y todos los componentes instalados están funcionando adecuadamente.

 - El icono naranja advierte que ***uno o más componentes no están configurados correctamente***, por lo que se recomienda revisar su configuración o propiedades. No significa que haya un problema crítico en **AVG Internet Security 2012**; quizás simplemente se trate de que decidió desactivar alguno de los componentes de forma intencionada. Sigue estando protegido. Sin embargo, se recomienda revisar la configuración del componente que presenta el problema. En la sección ***Información sobre el estado de seguridad*** encontrará el nombre del componente.

El icono naranja también aparece si, por alguna razón, decidió ignorar el estado de error de

un componente. La opción ***Ignorar el estado de este componente*** está disponible desde el menú contextual (*que se abre cuando se hace clic con el botón secundario*) sobre el icono del componente en cuestión en la información general de los componentes, dentro de la ventana principal de **AVG Internet Security 2012**. Seleccione esta opción para expresar que conoce el estado de error del componente pero que, por alguna razón, desea que **AVG Internet Security 2012** siga así y no quiere que se le advierta mediante el icono en la bandeja del sistema. Es posible que necesite utilizar esta opción en una situación específica, pero se recomienda encarecidamente desactivar la opción ***Ignorar el estado de este componente*** tan pronto como sea posible.

 - El icono rojo indica que ***AVG Internet Security 2012 se encuentra en estado crítico***. Uno o más componentes no funcionan correctamente y **AVG Internet Security 2012** no puede proteger el equipo. Debe corregir de inmediato el problema. Si no es capaz de reparar el problema por sí mismo, contacte con el equipo de soporte técnico de AVG.

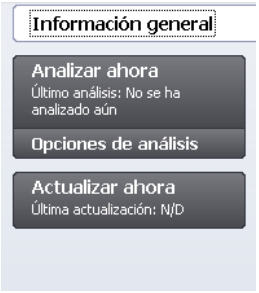
En caso de que AVG Internet Security 2012 no esté configurado para un rendimiento óptimo, aparecerá un botón nuevo llamado Reparar (o bien Reparar todo si el problema concierne a más de un componente) junto a la información del estado de seguridad. Pulse el botón para iniciar un proceso automático de comprobación y configuración del programa. Se trata de una manera sencilla de configurar AVG Internet Security 2012 para un rendimiento óptimo y lograr el máximo nivel de seguridad.

Se recomienda encarecidamente prestar atención a ***Información sobre el estado de seguridad*** y, en caso de que el informe indique algún problema, intentar resolverlo de inmediato. De lo contrario, el equipo se encontrará en riesgo.

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

5.3. Vínculos rápidos

Los ***vínculos rápidos*** están ubicados en el lado izquierdo de la interfaz de usuario de **AVG Internet Security 2012**. Estos vínculos le permiten acceder inmediatamente a las funciones más importantes y más utilizadas de la aplicación, como analizar y actualizar. Los vínculos rápidos son accesibles desde todos los cuadros de diálogo de la interfaz de usuario:



Los ***vínculos rápidos*** se distribuyen gráficamente en tres secciones:

- ***Información general***: utilice este vínculo para cambiar desde cualquier cuadro de diálogo

de AVG abierto a la ventana principal, con una vista general de todos los componentes instalados. *(Consulte los detalles en el capítulo Información general de los componentes)*

- ***Analizar ahora***: de manera predeterminada, este botón proporciona información sobre el último análisis realizado *(p. ej., tipo de análisis y la fecha en que se ejecutó por última vez)* . Haga clic en el comando ***Analizar ahora*** para volver a iniciar el mismo análisis. Si desea iniciar un análisis distinto, haga clic en el vínculo ***Opciones de análisis***. De esta forma, se abrirá la interfaz de análisis de AVG, donde podrá ejecutar y programar análisis o editar sus parámetros. *(Consulte los detalles en el capítulo Análisis de AVG)*

- ***Actualizar ahora***: el vínculo proporciona la fecha y hora de la última actualización. Pulse el botón para ejecutar el proceso de actualización inmediatamente y seguir su curso. *(Consulte los detalles en el capítulo Actualizaciones de AVG)*

Es posible acceder a los ***vínculos rápidos*** desde la interfaz de usuario de AVG en todo momento. Cuando utilice un vínculo rápido para ejecutar un proceso específico, ya sea un análisis o una actualización, la aplicación cambiará a un nuevo cuadro de diálogo, pero los vínculos rápidos seguirán estando disponibles. Además, el proceso que se está ejecutando se representa también gráficamente en la navegación, por lo que dispone de un control total sobre todos los procesos iniciados que estén ejecutándose en **AVG Internet Security 2012** en ese momento.

5.4. Información general de los componentes

Secciones de Información general de los componentes

La sección ***Información general de los componentes*** está ubicada en la parte central de la interfaz de usuario de **AVG Internet Security 2012**. La sección está dividida en dos partes:

- ***Información sobre todos los componentes instalados***, que consiste en paneles gráficos para cada uno de los componentes instalados. Cada panel está etiquetado con su icono de componente y proporciona información sobre si el componente respectivo está activo o inactivo en ese momento.

- ***Descripción del componente***, que está ubicada en la parte inferior de este cuadro de diálogo. La descripción explica brevemente la funcionalidad básica del componente en cuestión. También proporciona información sobre el estado actual del componente seleccionado.

Lista de componentes instalados

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

- ***Anti-Virus*** detecta virus, spyware, gusanos, troyanos, archivos ejecutables o bibliotecas del sistema no deseados, y le protege del spam malicioso - detalles >>

- ***LinkScanner*** le protege de ataques web mientras navega por Internet - detalles >>

- ***Protección del correo electrónico*** comprueba sus mensajes de correo electrónico en busca de spam y bloquea virus, ataques de suplantación de identidad y otras amenazas - detalles >>
- ***Firewall*** controla toda la comunicación de cada puerto de red, ofrece protección frente a ataques maliciosos y bloquea los intentos de intrusión - detalles >>
- ***Anti-Rootkit*** analiza en busca de rootkits peligrosos ocultos dentro de las aplicaciones, controladores o bibliotecas - detalles >>
- ***Herramientas del sistema*** ofrece un resumen detallado del entorno de AVG e información sobre el sistema operativo - detalles >>
- ***Analizador de equipos*** proporciona información sobre el estado del equipo - detalles >>
- ***Identity Protection*** protege constantemente sus activos digitales contra amenazas nuevas y desconocidas - detalles >>
- ***Security Toolbar*** permite utilizar determinados elementos de la funcionalidad de AVG directamente desde su navegador de Internet - detalles >>

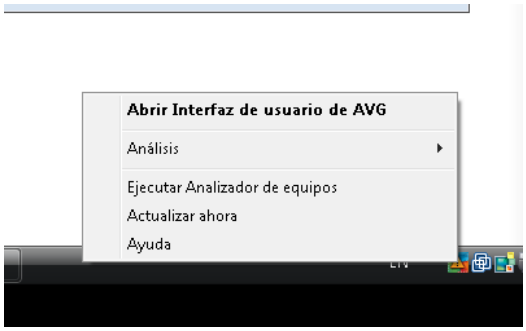
- ***Administración remota*** sólo se muestra en las ediciones AVG Business si durante el proceso de instalación ha especificado que desea instalar este componente

Acciones accesibles

- ***Mueva el ratón sobre el icono*** de cualquier componente para resaltarlo en la información general de los componentes. Simultáneamente aparece una descripción de las funciones básicas del componente en la parte inferior de la interfaz de usuario.
- ***Haga clic en un icono de componente*** para abrir la interfaz propia del componente con una lista de datos estadísticos básicos.
- ***Haga clic con el botón derecho del ratón sobre el icono*** de un componente para expandir un menú contextual:
  - ***Abrir***: haga clic en esta opción para abrir el cuadro de diálogo propio del componente *(es igual que un clic sobre el icono del componente)*.
  - ***Ignorar el estado de este componente***: seleccione esta opción para indicar que conoce el estado de error del componente pero que, por algún motivo, desea que siga así y no quiere que se le advierta mediante el icono en la bandeja del sistema.
  - ***Abrir en Configuración avanzada...***: esta opción sólo está disponible para algunos componentes; es decir, aquellos que proporcionan la posibilidad de configuración avanzada.

5.5. Icono de la bandeja del 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 **AVG Internet Security 2012**. Resulta visible en todo momento en la bandeja del sistema, sin importar si la interfaz de usuario de **AVG Internet Security 2012** está abierta o cerrada:



Apariencia del icono de la bandeja del sistema de AVG

- A todo color sin elementos añadidos, el icono indica que todos los componentes de **AVG Internet Security 2012** están activos y funcionan correctamente. No obstante, el icono también puede presentarse de este modo en una situación en la que uno de los componentes no funciona correctamente, pero el usuario ha decidido ignorar el estado del componente. *(Al haber confirmado la opción de ignorar el estado del componente, expresa que es consciente de su estado de error, pero que por algún motivo quiere mantenerlo así y no desea que se le avise de dicha situación.)*

- El icono con un signo de exclamación indica que un componente *(o incluso más de uno)* se encuentran en estado de error. Preste siempre atención a estas advertencias y trate de resolver el problema de configuración de un componente que no esté configurado adecuadamente. Para poder realizar los cambios en la configuración del componente, haga doble clic en el icono de la bandeja de sistema para abrir la interfaz de usuario de la aplicación. Para obtener información detallada sobre qué componentes se encuentran en estado de error, consulte la sección de información sobre el estado de seguridad.

- El icono de la bandeja de sistema también puede presentarse a todo color con un haz de luz rotatorio y parpadeante. Esta versión gráfica indica que hay un proceso de actualización en ejecución.

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

Información sobre el icono de la bandeja del sistema de AVG

El icono de la bandeja del sistema de AVG informa además de la actividad actual de **AVG Internet Security 2012** y de los posibles cambios de estado en el programa (*por ejemplo, el inicio*

automático de un análisis o actualización programados, un cambio de perfil de Firewall, un cambio de estado de algún componente, la existencia de un estado de error...) mediante una ventana emergente que se abre desde el icono de la bandeja del sistema:

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

El icono de la bandeja del sistema de AVG también puede utilizarse como vínculo rápido para acceder a la interfaz de usuario de **AVG Internet Security 2012**; simplemente haga doble clic en el icono. Al hacer clic con el botón derecho, se abre un pequeño menú contextual con las opciones siguientes:

- ***Abrir Interfaz de usuario de AVG***: haga clic para abrir la interfaz de usuario de **AVG Internet Security 2012**.
- ***Análisis***: haga clic para abrir el menú contextual de los análisis predefinidos (*Analizar todo el equipo*, *Analizar archivos o carpetas específicos*, *Análisis Anti-Rootkit*) y seleccione el análisis requerido para iniciarlo inmediatamente.
- ***Firewall***: haga clic para abrir el menú contextual de las opciones de configuración de Firewall, donde podrá editar los principales parámetros: estado del Firewall (*Habilitar Firewall/Deshabilitar Firewall/Modo de emergencia*), activación/desactivación del modo de juego y perfiles de Firewall.
- ***Ejecutar Analizador de equipos***: haga clic para iniciar el componente Analizador de equipos.
- ***Ejecutando análisis***: este elemento se muestra únicamente en caso de que se esté ejecutando un análisis en el equipo en ese momento. Puede establecer la prioridad de este análisis, detenerlo o pausarlo. Para ello, se tendrá acceso a las siguientes acciones: *Establecer prioridad para todos los análisis, Pausar todos los análisis* o *Detener todos los análisis*.
- ***Actualizar ahora***: inicia una actualización inmediata.
- ***Ayuda***: abre el archivo de ayuda en la página de inicio.

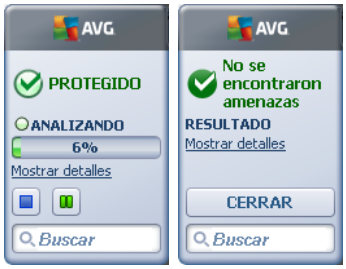
5.6. Gadget de AVG

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

Acceso rápido a análisis y actualización

Si es necesario, el ***gadget de AVG*** le permite iniciar un análisis o una actualización inmediatamente:

- ***Analizar ahora***: haga clic en el vínculo ***Analizar ahora*** para iniciar directamente el análisis del equipo completo. Puede observar el curso del proceso de análisis en la interfaz de usuario alternativa del gadget. La breve descripción estadística proporciona información sobre el número de objetos analizados, las amenazas detectadas y las amenazas reparadas. Durante el análisis, siempre puede poner en pausa o detener el proceso de análisis. Para obtener datos detallados sobre los resultados del análisis, consulte el cuadro de diálogo estándar Información general de los resultados del análisis, que puede abrirse directamente desde el gadget a través de la opción ***Mostrar detalles*** *(los resultados de los análisis correspondientes se enumerarán en Análisis de gadgets de 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 redes sociales

El gadget de AVG también proporciona un vínculo rápido para conectar con las redes sociales principales. Utilice el botón correspondiente para conectar con las comunidades de AVG en Twitter, Facebook o LinkedIn:

- ***Vínculo de Twitter***: abre una nueva interfaz del ***gadget de AVG*** que ofrece una vista de los últimos comentarios de AVG publicados en Twitter. Siga el vínculo ***Ver todas las entradas de Twitter de AVG*** para abrir el navegador de Internet en una nueva ventana; será redirigido directamente al sitio web de Twitter, concretamente a la página dedicada a las noticias referentes a AVG:

- ***Vínculo de Facebook***: abre el navegador de Internet en el sitio web de Facebook, concretamente en la página de la ***comunidad AVG***

- ***LinkedIn***: esta opción sólo está disponible en la instalación de red (*es decir, si se ha instalado AVG utilizando una de las licencias de las ediciones Business de AVG*) y abre el navegador de Internet con el sitio web ***AVG SMB Community*** de la red social LinkedIn

Otras funciones accesibles a través del gadget

- ***Analizador de equipos***: abre la interfaz de usuario en el componente Analizador de equipos

- ***Cuadro de búsqueda***: escriba una palabra clave y obtenga los resultados de la búsqueda inmediatamente en una nueva ventana abierta en su navegador web predeterminado

6. Componentes de AVG

6.1. Anti-Virus

El componente ***Anti-Virus*** es uno de los pilares de **AVG Internet Security 2012** y combina varias de las funciones esenciales de un programa de seguridad:

- Motor de análisis
- Protección residente
- Protección de 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 la actividad relacionada *(apertura/cierre de archivos, etc.)* para detectar virus conocidos. Cualquier virus detectado se bloqueará para que no realice ninguna acción y, a continuación, se limpiará o se pondrá en cuarentena en el Almacén de virus.

La característica esencial de la protección de AVG Internet Security 2012 es que ningún virus conocido puede ejecutarse en el equipo.

Métodos de detección

La mayor parte del software antivirus también utiliza análisis heurístico, mediante el que se analizan los archivos en busca de características típicas de los virus, denominadas firmas de virus. Esto significa que el analizador antivirus tiene capacidad para detectar un virus nuevo y desconocido si éste contiene algunas características típicas de los virus existentes. ***Anti-Virus*** utiliza los métodos de detección siguientes:

- *Análisis*: búsqueda de cadenas de caracteres propias de un virus determinado
- *Análisis heurístico*: emulación dinámica de las instrucciones del objeto analizado en un entorno virtual de equipo
- *Detección genérica*: detección de instrucciones características de un determinado virus o grupo de virus

Dado que una sola tecnología puede tener limitaciones a la hora de detectar o identificar un virus, ***Anti-Virus*** combina diversas tecnologías para garantizar la protección del equipo frente a los virus. **AVG Internet Security 2012** es capaz de analizar y detectar aplicaciones ejecutables o bibliotecas DLL potencialmente no deseadas en el sistema. Estas amenazas se denominan programas potencialmente no deseados *(diversos tipos de spyware, adware etc.)*. Además, **AVG Internet Security 2012** analiza el Registro del sistema para detectar entradas sospechosas, archivos temporales de Internet y cookies, y le permite tratar todos los elementos potencialmente dañinos de la misma forma que cualquier otra infección.

AVG Internet Security 2012 le proporciona protección continua a su equipo.

6.1.2. Protección residente

AVG Internet Security 2012 le proporciona protección continua en la forma denominada protección residente. El componente ***Anti-Virus*** analiza todos los archivos *(con extensiones específicas o sin extensiones)* que se abren, guardan o copian. Protege las áreas de sistema del equipo y los medios extraíbles (*discos flash, etc.*). Cuando se descubre un virus en un archivo al que se está accediendo, detiene la operación que se está ejecutando y no permite que el virus se active. Normalmente, el usuario ni siquiera advierte el proceso, puesto que la protección residente se ejecuta "en segundo plano". Sólo se le notifica cuando se detectan amenazas; al mismo tiempo, ***Anti-Virus*** bloquea la activación de la amenaza y la elimina.

La protección residente se carga en la memoria del equipo durante el inicio del mismo y es vital que se mantenga activada en todo momento.

6.1.3. Protección de Anti-Spyware

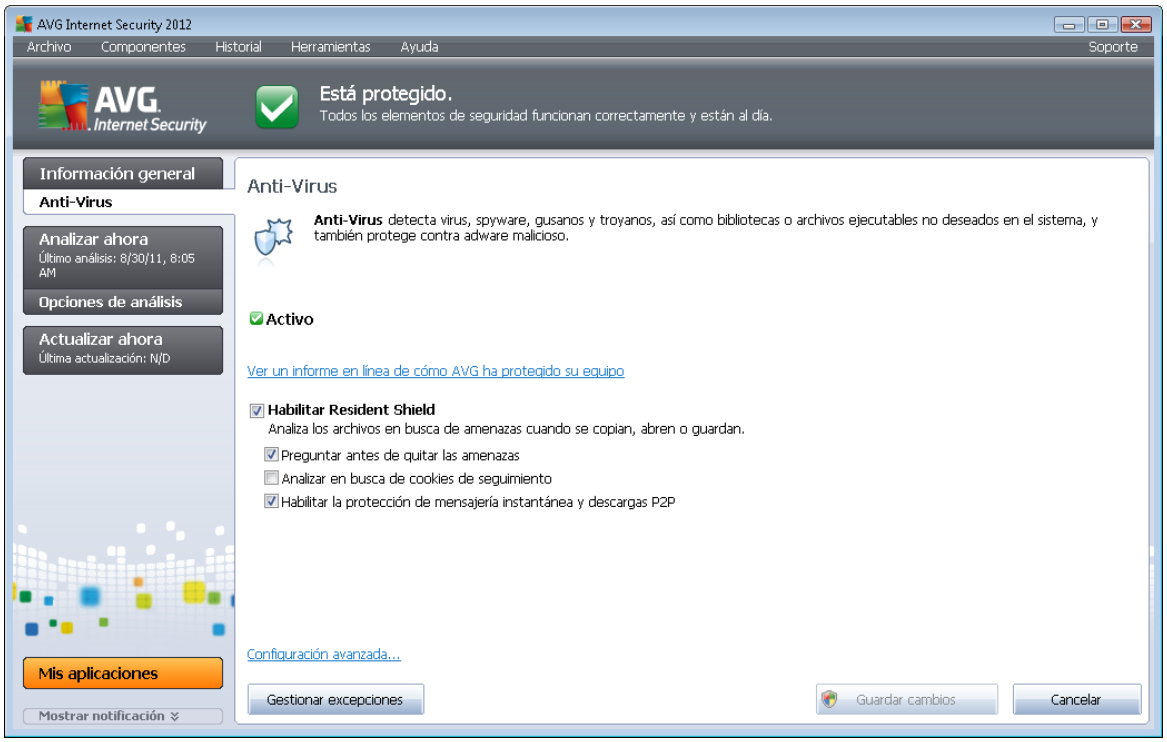
Anti-Spyware consiste en una base de datos de software espía utilizada para identificar tipos conocidos de definiciones de spyware. Los expertos en spyware de AVG trabajan intensamente para identificar y describir los últimos patrones de spyware tan pronto como emergen, y añaden las definiciones a la base de datos. A través del proceso de actualización, se descargan estas nuevas definiciones en el equipo para que esté protegido en todo momento de forma fiable contra los tipos de spyware más recientes. ***Anti-Spyware*** le permite analizar el equipo completamente para detectar software malicioso y software espía. También detecta malware inactivo o en letargo, es decir, el que ha sido descargado, pero que aún no se ha activado.

¿Qué es el spyware?

El spyware se define generalmente como un tipo de malware, es decir, un software que recopila información del equipo de un usuario sin conocimiento ni consentimiento del mismo. Algunas aplicaciones de spyware también se pueden instalar intencionadamente y con frecuencia contienen anuncios, ventanas emergentes o diferentes tipos de software molesto. Actualmente, la fuente de infección más común son los sitios web con contenido potencialmente peligrosso. Otros métodos de transmisión, como el correo electrónico o la transmisión por gusanos y virus, también son frecuentes. La protección más eficaz consiste en utilizar un analizador siempre activo en segundo plano, como ***Anti-Spyware***, que funciona como una protección residente y analiza las aplicaciones en segundo plano mientras se ejecutan.

6.1.4. Interfaz de Anti-Virus

La interfaz del componente ***Anti-Virus*** proporciona información general sobre la funcionalidad del componente, su estado actual *(Activo)* y opciones de configuración básica del componente:



Opciones de configuración

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

- ***Ver un informe en línea de cómo AVG ha protegido su equipo***: el vínculo le redirige a una página específica del sitio web de AVG (http://www.avg.com/). En la página encontrará información estadística detallada de todas las actividades de **AVG Internet Security 2012** realizadas en su equipo durante un periodo de tiempo determinado, y en total.

- ***Habilitar Protección residente***: esta opción le permite activar y desactivar fácilmente la protección residente. Protección residente analiza los archivos al copiarse, abrirse o guardarse. Cuando se detecte un virus o cualquier tipo de amenaza, se le avisará inmediatamente. La función está activada de forma predeterminada, y se recomienda mantenerla así. Con la protección residente activada puede decidir con más detalle cómo deben tratarse las infecciones detectadas:

  - ***Quitar todas las amenazas automáticamente*** / ***Preguntar antes de quitar las amenazas***: seleccione una de estas opciones alternativamente. Esta elección no tiene ningún impacto en el nivel de seguridad y sólo refleja las preferencias del usuario.

- ***Analizar en busca de cookies de seguimiento***: independientemente de las opciones anteriores, puede decidir si desea analizar en busca de cookies de seguimiento. *(Las cookies son fragmentos de texto enviados por un servidor a un navegador y devueltos sin modificar por el navegador cada vez que se accede a ese servidor. Las cookies HTTP se utilizan para autentificar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos.)* En casos específicos puede activar esta opción para conseguir un nivel de seguridad máximo; sin embargo, está desactivada de manera predeterminada.

- ***Habilitar la protección de mensajería instantánea***: marque esta opción si desea verificar que la comunicación por mensajería instantánea (*p. ej., ICQ, MSN Messenger, etc.*) está libre de virus.

- ***Configuración avanzada...***: haga clic en este vínculo para acceder al cuadro de diálogo respectivo de Configuración avanzada de **AVG Internet Security 2012**. Aquí puede editar la configuración del componente en detalle. Sin embargo, debe tener en cuenta que la configuración predeterminada de todos los componentes está pensada para que **AVG Internet Security 2012** proporcione un rendimiento óptimo y la máxima seguridad. A no ser que tenga un motivo de peso para hacerlo, se recomienda mantener la configuración predeterminada.

Botones de control

En el cuadro de diálogo, puede utilizar los siguientes botones de control:

- ***Gestionar excepciones***: abre un nuevo cuadro de diálogo llamado Protección residente - Excepciones. También se puede acceder al cuadro de diálogo desde el menú principal, siguiendo la secuencia Configuración avanzada / Anti-Virus / Protección residente / Excepciones *(consulte el capítulo correspondiente para obtener una descripción detallada)*. En el cuadro de diálogo puede especificar archivos y carpetas que se deben excluir del análisis de la Protección residente. Si no es esencial, se recomienda encarecidamente no excluir ningún elemento. El cuadro de diálogo incluye los siguientes botones de control:

  - *Agregar ruta*: especifique el directorio *o directorios* que serán excluidos del análisis seleccionándolos uno por uno en el árbol de navegación del disco local.

  - *Añadir archivo*: especifique los archivos que serán excluidos del análisis seleccionándolos uno por uno en el árbol de navegación del disco local.

  - *Editar elemento*: le permite editar la ruta de acceso especificada a un archivo o carpeta seleccionados.

  - *Quitar elemento*: le permite eliminar la ruta de acceso al elemento seleccionado de la lista.

- ***Guardar cambios***: guarde todos los cambios realizados sobre la configuración del componente en este cuadro de diálogo y vuelva a la interfaz de usuario principal de **AVG Internet Security 2012** (*información general de los componentes*).

- ***Cancelar***: cancela todos los cambios realizados sobre la configuración del componente en este cuadro de diálogo. Los cambios no se guardarán. Volverá a la interfaz de usuario principal de **AVG Internet Security 2012** (*información general de los componentes*).

6.1.5. Detecciones de Protección residente

¡Amenaza detectada!

Protección residente analiza los archivos al copiarse, abrirse o guardarse. Cuando se detecte un virus o cualquier otro tipo de amenaza, se le notificará inmediatamente mediante el siguiente cuadro de diálogo:

En este cuadro de diálogo de advertencia, encontrará datos sobre el archivo detectado y marcado como infectado (*Nombre del archivo*), el nombre de la infección detectada (*Nombre de la amenaza*) y un vínculo a la Enciclopedia de virus, en la que puede encontrar información detallada sobre la infección detectada, si se conoce (*Más información*).

También debe decidir qué acción realizar en este momento. Hay diversas opciones disponibles. ***Tenga en cuenta que, según las condiciones específicas (de qué tipo es el archivo infectado y dónde se encuentra ubicado), no todas las opciones están siempre disponibles.***

- ***Eliminar amenaza como usuario avanzado***: marque la casilla si sospecha que no tiene derechos suficientes para quitar la amenaza como usuario común. Los usuarios avanzados tienen amplios derechos de acceso y, si la amenaza se encuentra en una determinada carpeta del sistema, tal vez necesite utilizar esta casilla de verificación para quitarla correctamente.

- ***Reparar***: este botón sólo aparece si la infección detectada puede repararse. De ser así, la elimina y devuelve el archivo a su estado original. Si el propio archivo es un virus, utilice esta función para eliminarlo (*es decir, enviarlo al Almacén de virus*)

- ***Mover al Almacén***: el virus se enviará al Almacén de virus

- ***Ir al archivo***: esta opción permite ir a la ubicación exacta donde se encuentra el objeto sospechoso (*abre una ventana nueva del Explorador de Windows*)

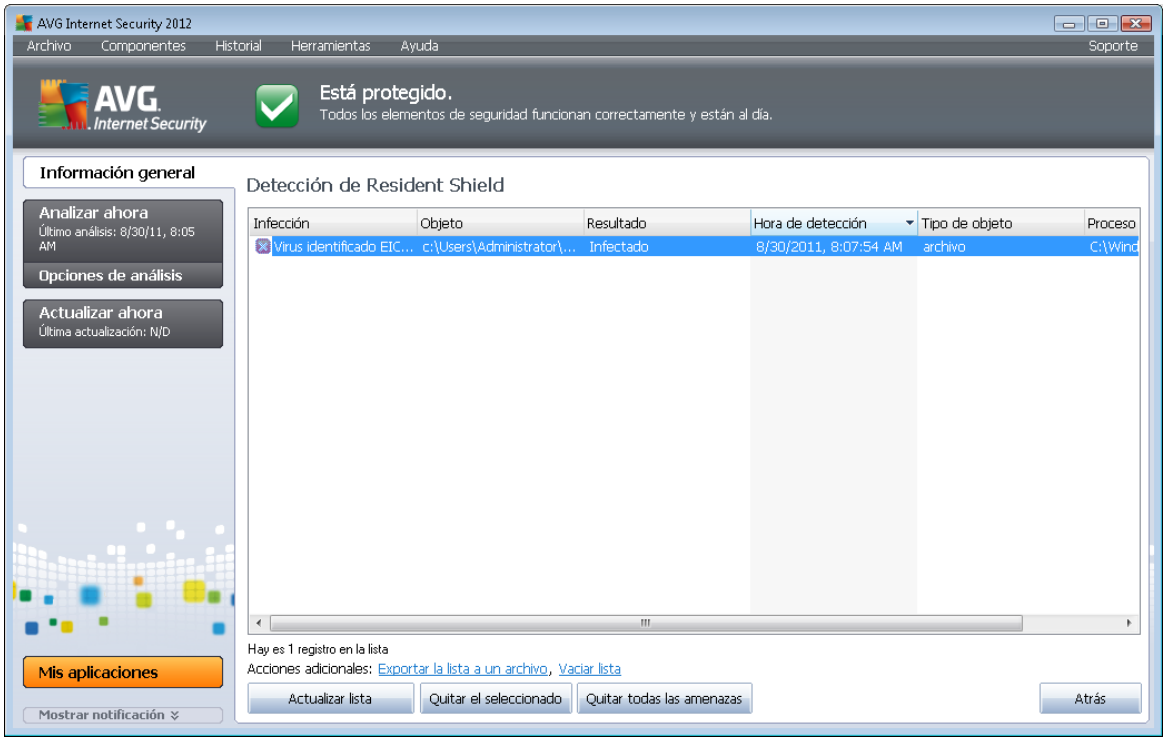
- ***Ignorar***: se recomienda encarecidamente NO USAR esta opción a menos que se tenga un buen motivo para ello.

Nota: *puede suceder que el tamaño del objeto detectado exceda el límite de espacio disponible en el Almacén de virus. Si es así, un mensaje de advertencia aparece informando acerca del problema mientras se intenta mover el objeto infectado al Almacén de virus. No obstante, el tamaño del Almacén de virus puede modificarse. Se define como un porcentaje variable del tamaño real del disco duro. Para aumentar el tamaño del Almacén de virus, vaya al cuadro de diálogo Almacén de virus en Configuración avanzada de AVG y edite la opción "Limitar el tamaño del Almacén de virus".*

En la sección inferior del cuadro de diálogo, encontrará el vínculo ***Mostrar detalles***: haga clic en 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 mismo.

Información general de las detecciones de Protección Residente

La información general completa de todas las amenazas detectadas por Protección residente puede encontrarse en el cuadro de diálogo ***Detección de Protección residente***, al que se puede acceder desde la opción del menú del sistema Historial / Detección de Protección residente:



Detección de Protección residente muestra información general sobre los objetos que detectó Protección residente, que se evaluaron como peligrosos y que se repararon o movieron al Almacén de virus. Para cada objeto detectado, se proporciona la siguiente información:

- ***Infección***: descripción (posiblemente también el nombre) del objeto detectado
- ***Objeto***: ubicación del objeto
- ***Resultado***: acción realizada con el objeto detectado
- ***Hora de detección***: fecha y hora en que se detectó el objeto
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: la acción que se realizó para activar el objeto potencialmente peligroso y así hacer que fuese detectado

En la parte inferior del cuadro de diálogo, bajo la lista, encontrará información sobre el número total de los objetos detectados y enumerados más arriba. Además, puede exportar toda la lista de objetos detectados a un archivo (***Exportar la lista a un archivo***) y eliminar todas las entradas sobre los objetos detectados (***Vaciar lista***). El botón ***Actualizar lista*** actualizará la lista de objetos detectados por ***Protección residente***. El botón ***Atrás*** le devuelve al cuadro de diálogo principal de AVG predeterminado(*información general de los componentes*).

6.2. LinkScanner

LinkScanner protege contra la creciente cantidad de amenazas existentes en la web que se actualizan constantemente. Estas amenazas pueden estar ocultas en cualquier tipo de sitio web, desde gubernamentales y de marcas grandes y reconocidas hasta sitios de empresas pequeñas, y rara vez permanecen en un mismo sitio por más de 24 horas. ***LinkScanner*** protege su equipo analizando las páginas web que se encuentran detrás de todos los vínculos de cualquier página que visite, comprobando que sean seguros en el único momento que importa: cuando se está a punto de hacer clic en ese vínculo.

LinkScanner no ha sido diseñado para la protección de plataformas de servidor.

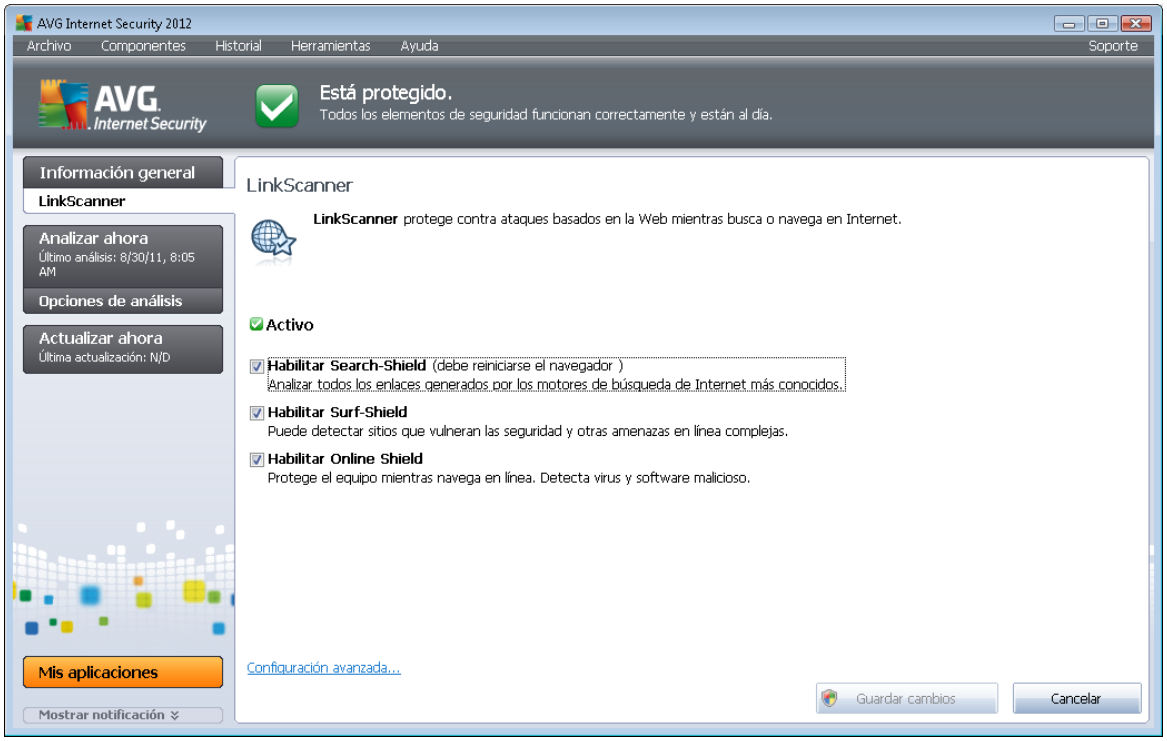
La tecnología ***LinkScanner*** consta de las características principales siguientes:

- Search-Shield contiene una lista de sitios web (direcciones URL) que se sabe que son peligrosos. Al realizar búsquedas en Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask y Seznam, los resultados obtenidos se contrastan con esta lista y se muestran con el icono apropiado *(en el caso de los resultados de búsqueda de Yahoo!, sólo se muestran iconos que indican "sitio web infectado")*.
- Surf-Shield analiza el contenido de los sitios web que visita, independientemente de su dirección. Incluso en el caso de que un sitio web no sea detectado por Search-Shield *(por ejemplo, cuando se crea un nuevo sitio malintencionado o se infecta uno que estaba limpio)*, será detectado y bloqueado por Surf-Shield cuando trate de visitarlo.
- Online Shield funciona como una protección en tiempo real para navegar por Internet. Analiza el contenido de las páginas web visitadas y los posibles archivos incluidos en ellas antes incluso de que aparezcan en el navegador web o se descarguen en el equipo. Online Shield detecta virus y spyware contenidos en la página que está a punto de visitar y detiene al instante la descarga para que no entren amenazas en el equipo.

- ***AVG Accelerator*** permite reproducir vídeo en línea sin interrupciones y facilita las descargas adicionales. Cuando el proceso de aceleración de vídeo esté en curso, se le informará por medio de una ventana emergente en la bandeja del sistema.

6.2.1. Interfaz de LinkScanner

El cuadro de diálogo principal del componente LinkScanner proporciona una breve descripción acerca de la funcionalidad del componente y su estado actual *(Activo)*:



En la parte inferior de cuadro de diálogo podrá encontrar alguna configuración básica del componente:

- ***Habilitar Search-Shield*** (*activada de manera predeterminada*): quite la marca de la casilla sólo si tiene una buena razón para desactivar la funcionalidad Search Shield.

- ***Habilitar Surf-Shield*** (*activada de manera predeterminada*): protección activa (*en tiempo real*) contra sitios que aprovechan las vulnerabilidades de la seguridad y que actúa cuando se accede a tales sitios. Las conexiones a sitios maliciosos conocidos y su contenido que ataca las vulnerabilidades de la seguridad se bloquean en cuanto el usuario accede a ellos mediante el navegador web (*o cualquier otra aplicación que use HTTP*).

- ***Habilitar Online Shield*** (*activada de manera predeterminada*): análisis en tiempo real de

las páginas web que está a punto de visitar en busca de posibles virus o spyware. Si se detectan, la descarga se detiene al instante para que no llegue ninguna amenaza a su equipo.

6.2.2. Detecciones de Search-Shield

Al realizar búsquedas en Internet con ***Search-Shield*** activo, todos los resultados que arrojan los motores de búsqueda más conocidos (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot*) se evalúan en busca de vínculos peligrosos o sospechosos. Comprobando estos vínculos y marcando los que suponen amenaza, LinkScanner le avisa antes de que haga clic en vínculos peligrosos o sospechosos, por lo que le garantiza que solamente visita sitios web seguros.

Mientras se evalúa un vínculo en la página de resultados de búsqueda, junto al mismo verá un signo gráfico informándole de que su verificación está en curso. Al finalizar la evaluación, se mostrará el correspondiente icono informativo:

 La página vinculada es segura (*este icono no se mostrará en los resultados de búsqueda de Yahoo! JP*).

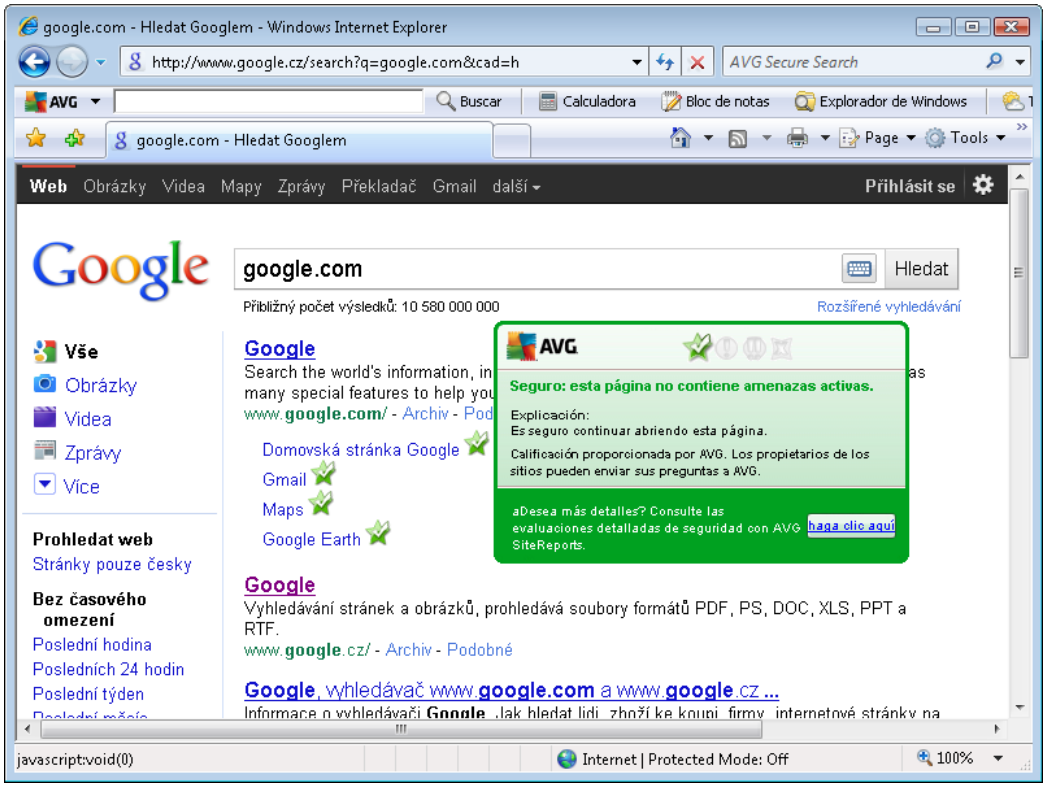
 La página vinculada no contiene amenazas, pero es sospechosa (*dudosa por su origen o propósito, por lo que no se recomienda para compras en línea, etc.*).

 La página vinculada puede ser segura, pero también contener otros vínculos a páginas verdaderamente peligrosas; o bien, sospechosa por su código, aunque no emplea directamente ninguna amenaza en este momento.

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

 No se puede acceder a esta página, por lo que no fue posible analizarla.

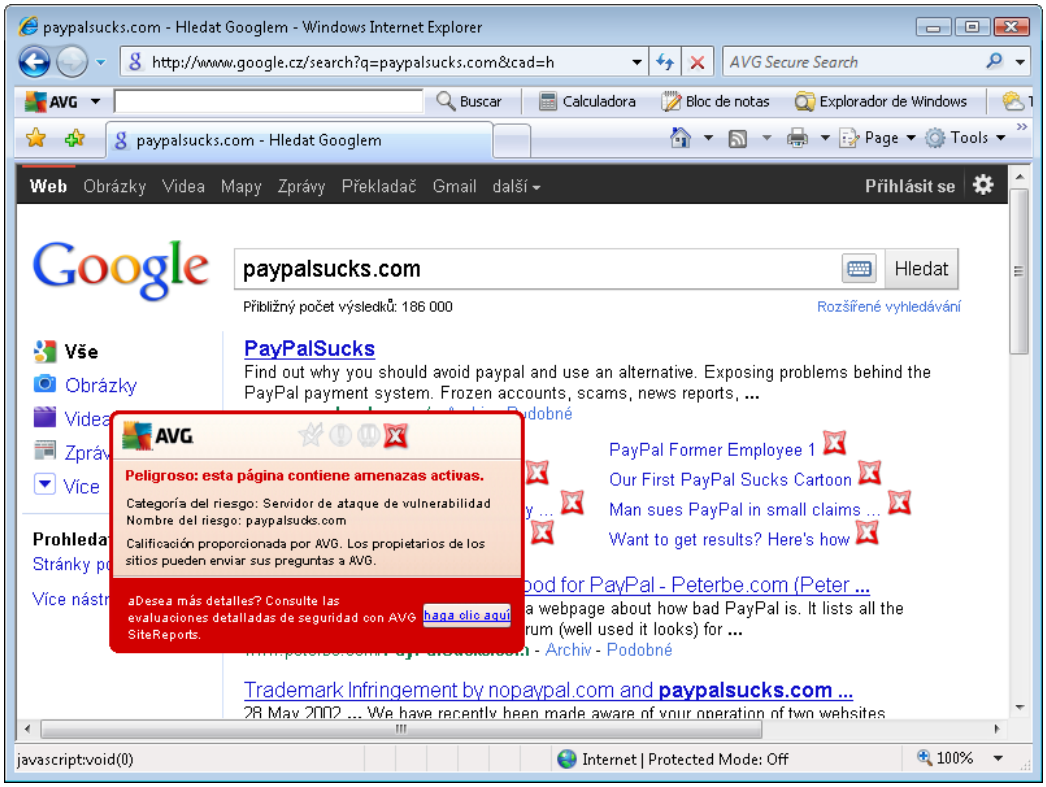
Al desplazar el puntero sobre un icono de calificación concreto, se mostrarán los detalles sobre el vínculo en cuestión. La información incluye detalles adicionales de la amenaza (*si los hubiera*):



6.2.3. Detecciones de Surf-Shield

Esta potente protección bloquea el contenido malicioso de cualquier página web que intente abrir e impide que se descargue en el equipo. Cuando esta característica está habilitada, si hace clic en un vínculo o escribe la URL de un sitio peligroso, impedirá automáticamente que abra la página web, protegiéndole de sufrir una infección involuntaria. Es importante recordar que las páginas web atacadas pueden infectar el equipo simplemente con visitar el sitio afectado, por lo que cuando solicite visitar una página web peligrosa que contenga ataques u otras amenazas serias, LinkScanner no permitirá que el navegador la muestre.

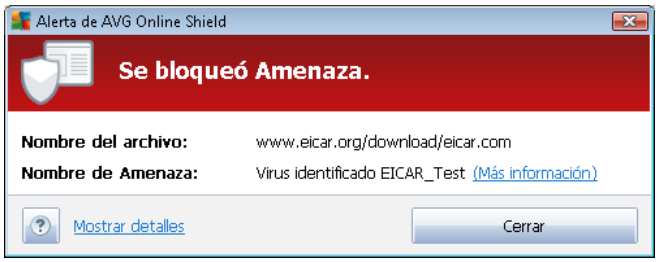
Si se encuentra con un sitio web malicioso, LinkScanner le avisará, en el propio navegador web, con una pantalla similar a la siguiente:



Entrar en este sitio web es sumamente arriesgado, por lo que no se recomienda.

6.2.4. Detecciones de Online Shield

Online Shield analiza el contenido de las páginas web visitadas y los posibles archivos incluidos en ellas antes incluso de que aparezcan en el navegador web o se descarguen en el equipo. Si se detecta un virus, se le notificará inmediatamente mediante el siguiente cuadro de diálogo:

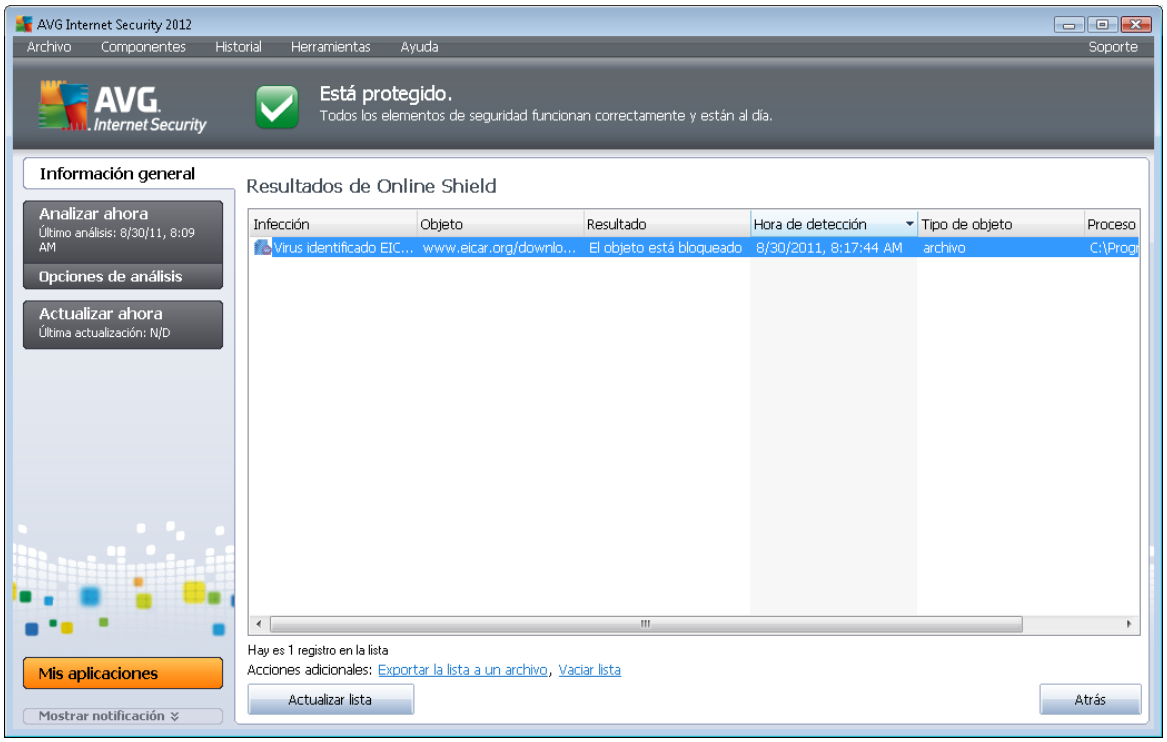


En este cuadro de diálogo de advertencia, encontrará datos sobre el archivo detectado y marcado como infectado (*Nombre del archivo*), el nombre de la infección detectada (*Nombre de la amenaza*) y un vínculo a la Enciclopedia de virus, en la que puede encontrar información detallada sobre la infección detectada (*si se conoce*). El cuadro de diálogo contiene los siguientes botones:

- ***Mostrar detalles***: haga clic en el botón ***Mostrar detalles*** para abrir una nueva ventana emergente con información detallada sobre el proceso que se estaba ejecutando cuando se detectó la infección y la identificación del proceso.

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

La página web sospechosa no se abrirá y se registrará la detección de la amenaza en la lista de ***Resultados de Online Shield***: se puede acceder a esta información general de amenazas detectadas a través del menú del sistema Historial / Resultados de Online Shield.



Para cada objeto detectado, se proporciona la siguiente información:

- ***Infección***: descripción (*posiblemente también el nombre*) del objeto detectado
- ***Objeto***: origen del objeto (*página web*)
- ***Resultado***: acción realizada con el objeto detectado
- ***Hora de detección***: fecha y hora en que se detectó y bloqueó el objeto
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: la acción que se realizó para activar el objeto potencialmente peligroso y así hacer que fuese detectado

En la parte inferior del cuadro de diálogo, bajo la lista, encontrará información sobre el número total de los objetos detectados y enumerados más arriba. Además, puede exportar toda la lista de objetos detectados a un archivo (***Exportar la lista a un archivo***) y eliminar todas las entradas sobre los objetos detectados (***Vaciar lista***).

Botones de control

- ***Actualizar lista***: actualiza la lista de resultados detectados por ***Online Shield***
- ***Atrás***: le devuelve al cuadro de diálogo principal de AVG predeterminado *(información general de los componentes)*

6.3. Protección del correo electrónico

Uno de los focos más habituales de virus y troyanos es el correo electrónico. El phishing y el spam aumentan el nivel de riesgo del correo electrónico. Las cuentas gratuitas de correo electrónico tienen mayor probabilidad de recibir correos electrónicos maliciosos (*ya que no suelen emplear tecnología anti-spam*) y su uso entre los usuarios domésticos está muy extendido. Asimismo, los usuarios domésticos, al navegar por sitios desconocidos y facilitar sus datos personales en formularios en línea (*tales como su dirección de correo electrónico*), aumentan su exposición a los ataques por correo electrónico. Las empresas generalmente utilizan cuentas corporativas de correo electrónico y emplean mecanismos como filtros anti-spam para reducir el riesgo.

El componente ***Protección del correo electrónico*** es responsable de analizar cada mensaje de correo electrónico, enviado o recibido; cuando se detecta un virus en un correo, se mueve al Almacén de virus inmediatamente. Este componente también puede filtrar ciertos tipos de adjuntos de correo electrónico y añadir un texto de certificación a los mensajes que no contengan infecciones. ***Protección del correo electrónico*** consta de dos funciones principales:

- Analizador de correo electrónico
- Anti-Spam

6.3.1. Analizador de correo electrónico

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

Durante la instalación de AVG, se crean servidores automáticos para el control del correo electrónico: uno para comprobar los correos entrantes y otro para los salientes. Con estos dos servidores, los correos electrónicos se comprueban automáticamente en los puertos 110 y 25 (*los puertos estándar para enviar/recibir correo electrónico*).

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

- ***Correo entrante:*** al recibir un mensaje desde el servidor, el componente ***Analizador de correo electrónico*** comprueba si contiene virus, elimina los datos adjuntos infectados y añade una certificación. Cuando se detectan virus, se ponen inmediatamente en cuarentena en el Almacén de virus. A continuación, el mensaje se transfiere al cliente de correo electrónico.

- ***Correo saliente:*** el mensaje se envía desde el cliente de correo electrónico hasta el Analizador de correo electrónico; éste comprueba si el mensaje y sus datos adjuntos contienen virus y, a continuación, envía el mensaje al servidor SMTP (*de manera predeterminada, el análisis del correo electrónico saliente está deshabilitado, pero se puede configurar manualmente*).

El Analizador de correo electrónico no ha sido diseñado para plataformas de servidor.

6.3.2. Anti-Spam

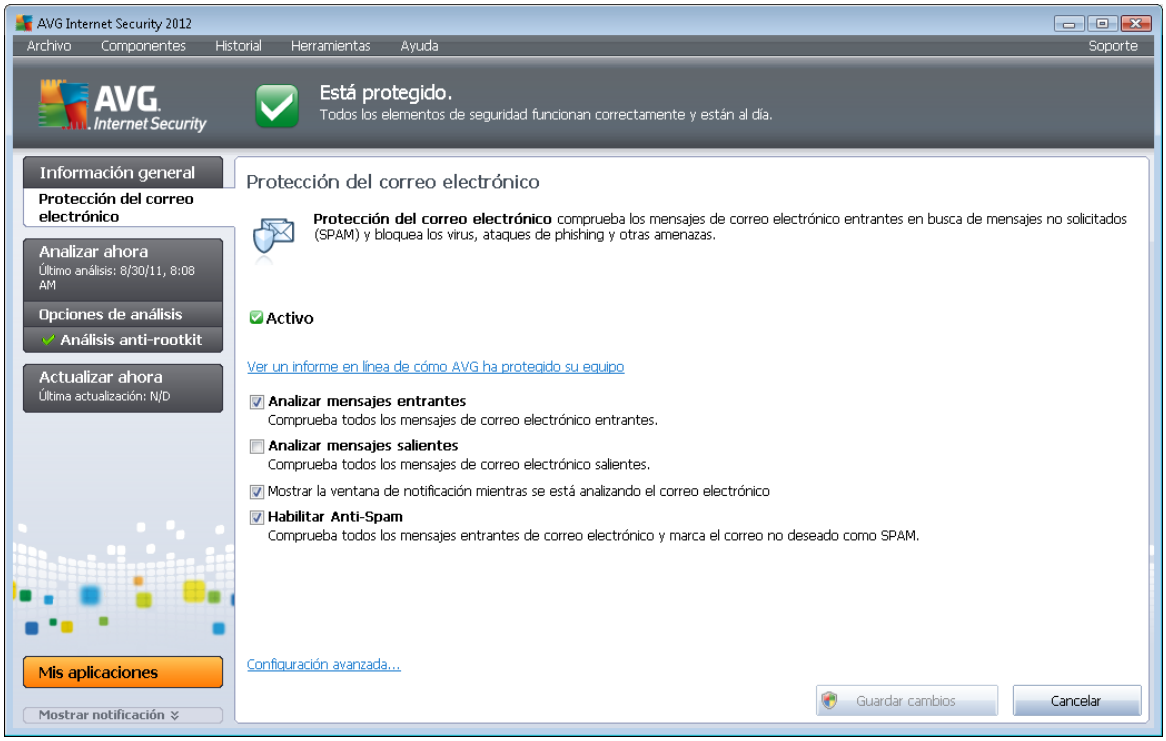
¿Cómo funciona Anti-Spam?

Anti-Spam comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como spam. ***Anti-Spam*** puede modificar el asunto del correo electrónico (*que se ha identificado como spam*) añadiendo una cadena especial de texto. De esta manera puede filtrar fácilmente los mensajes en el cliente de correo electrónico. El componente ***Anti-Spam*** utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado. ***Anti-Spam*** emplea una base de datos constantemente actualizada para detectar el spam. También es posible utilizar servidores RBL (*bases de datos públicas de direcciones de correo electrónico de "spammers conocidos"*) y agregar manualmente direcciones de correo electrónico a la Lista blanca (*nunca se marcan como spam*) y a la Lista negra (*siempre se marcan como spam*).

¿Qué es el spam?

El spam se refiere al correo electrónico no solicitado, generalmente anunciando un producto o servicio, que se envía masiva y simultáneamente a un gran número de direcciones de correo electrónico, llenando los buzones de los destinatarios. El spam no hace referencia al correo comercial legítimo al que los consumidores dan su consentimiento. El spam no solamente es molesto, sino que también suele ser fuente de estafas, virus o contenidos ofensivos.

6.3.3. Interfaz de Protección del correo electrónico



En el cuadro de diálogo ***Protección del correo electrónico*** puede encontrar un breve texto que describe la funcionalidad del componente e información sobre su estado actual *(Activo).* Utilice el vínculo ***Ver un informe en línea de cómo AVG ha protegido su equipo*** para ver estadísticas detalladas de las actividades y detecciones de **AVG Internet Security 2012** en una página dedicada del sitio web de AVG (http://www.avg.com/).

Configuración básica de Protección del correo electrónico

En el cuadro de diálogo ***Protección del correo electrónico*** puede editar algunas funciones elementales de la funcionalidad del componente:

- ***Analizar mensajes entrantes*** *(activada de manera predeterminada)*: marque la opción para especificar que los correos entregados en su cuenta deben ser analizados en busca de virus.
- ***Analizar mensajes salientes*** *(desactivada de manera predeterminada)*: marque la opción para especificar que los correos enviados desde su cuenta deben ser analizados en busca de virus.
- ***Mostrar la ventana de notificación mientras se está analizando el correo electrónico*** *(activada de manera predeterminada)*: marque la opción para confirmar que desea ser informado a través del cuadro de diálogo de notificación mostrado sobre el icono de AVG en la bandeja del sistema durante el análisis del correo electrónico.

- ***Habilitar Anti-Spam*** *(activada de manera predeterminada)*: marque la opción para especificar si desea que se filtre su correo entrante en busca de correo no deseado.

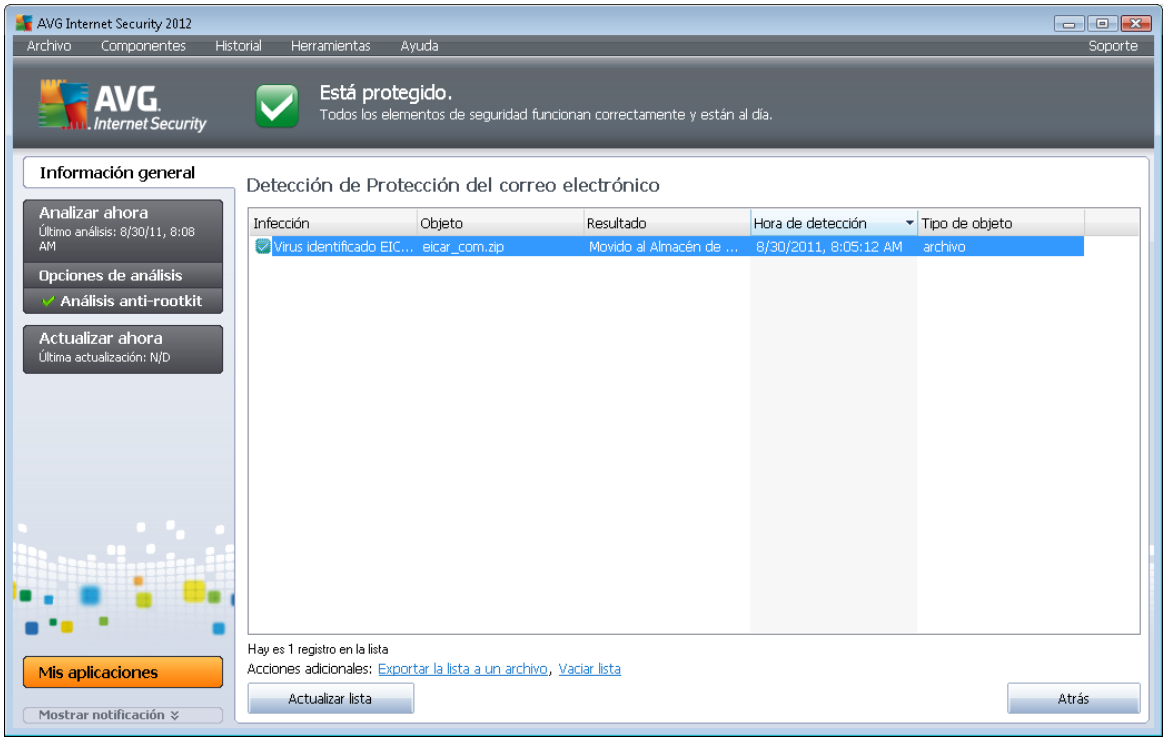
El proveedor del software ha configurado todos los componentes de AVG para ofrecer un rendimiento óptimo. A menos que tenga un buen motivo para hacerlo, no modifique la configuración de AVG. Cualquier cambio de configuración debe realizarlo únicamente un usuario experimentado. Si necesita cambiar la 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 acaba de abrir.

Botones de control

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

- ***Guardar cambios***: pulse este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo
- ***Cancelar***: pulse este botón para regresar al cuadro de diálogo principal de AVG (*información general de los componentes*)

6.3.4. Detecciones de Protección del correo electrónico



En el cuadro de diálogo ***Detección de Analizador de correo electrónico*** (*accessible a través de la opción de menú del sistema Historial / Detección de Analizador de correo electrónico*) 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 (posiblemente también el nombre) del objeto detectado
- ***Objeto***: ubicación del objeto
- ***Resultado***: acción realizada con el objeto detectado
- ***Hora 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, bajo la lista, encontrará información sobre el número total de los objetos detectados y enumerados más arriba. Además, puede exportar toda la lista de objetos detectados a un archivo (***Exportar la lista a un archivo***) y eliminar todas las entradas sobre los objetos detectados (***Vaciar lista***).

Botones de control

Los botones de control disponibles en la interfaz de ***Detección de Analizador de correo electrónico*** son los siguientes:

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

6.4. Firewall

Un ***firewall*** o cortafuegos es un sistema que impone una política de control de acceso entre dos o más redes bloqueando o permitiendo el tráfico. El ***firewall*** contiene un conjunto de reglas que protegen la red interna frente a los ataques externos *(generalmente a través de Internet* y controla todas las comunicaciones en todos los puertos de red. La comunicación se evalúa en función de las reglas definidas y, a continuación, se permite o se prohíbe. Si el ***firewall*** reconoce un intento de intrusión, lo “bloquea” y no permite que el intruso acceda al equipo.

El ***firewall*** está configurado para autorizar o denegar la comunicación interna y externa (en ambos sentidos, de entrada y de salida) a través de los puertos definidos y para las aplicaciones de software definidas. Por ejemplo, se puede configurar para que permita únicamente el flujo de datos web en el interior y el exterior con Microsoft Explorer. En tal caso, cualquier intento de trasmitir datos web con otro navegador será bloqueado.

El ***firewall*** impide el envío de sus datos de identificación personal desde el equipo sin su permiso. Controla asimismo el intercambio de datos realizado entre el equipo y otros equipos por Internet o a través de la red local. En una organización, el ***firewall*** también protege al equipo individual de ataques iniciados por usuarios internos en otros equipos de la red.

Los equipos que no están protegidos por un firewall son un objetivo fácil para los hackers y ladrones de datos.

Recomendación: *generalmente no se recomienda utilizar más de un firewall en un equipo*

individual. Si instala más de un firewall, no mejorará la seguridad del equipo. Es más probable que se produzcan conflictos entre las dos aplicaciones. Por este motivo, se recomienda utilizar solamente un firewall en el equipo y desactivar el resto, ya que así se eliminará el riesgo de posibles conflictos y problemas relacionados con este hecho.

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. Según las reglas definidas, el ***Firewall*** evalúa las aplicaciones que se están ejecutando en su equipo *(y quieren conectarse con la red local o Internet)* o las aplicaciones que intentan conectarse con el equipo desde el exterior. Para cada una de estas aplicaciones, el ***Firewall*** permite o impide la comunicación en los puertos de red. De manera 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.

AVG Firewall no está destinado a plataformas de servidor.

AVG Firewall puede:

- Permitir o bloquear automáticamente los intentos de comunicación de aplicaciones conocidas o pedirle su confirmación
- Utilizar perfiles completos con reglas predefinidas según cada necesidad
- Cambiar de perfil automáticamente al conectarse con varias redes o usar varios adaptadores de red

6.4.2. Perfiles de Firewall

El Firewall permite definir reglas de seguridad específicas dependiendo si el equipo se encuentra en un dominio, es un equipo independiente o incluso un portátil. Cada una de estas opciones requiere un nivel diferente de protección y los niveles están cubiertos por los perfiles respectivos. En resumen, un perfil de Firewall es una configuración específica del componente Firewall, pudiendo utilizarse diversas configuraciones predefinidas.

Perfiles disponibles

- ***Permitir todas***: un perfil de Firewall del sistema preconfigurado por el fabricante y que está siempre presente. Cuando se activa este perfil, se permiten todas las comunicaciones de la red y no se aplican reglas de directivas de seguridad, como si la protección del Firewall estuviese desactivada (es decir, se permiten todas las aplicaciones, pero los paquetes se siguen comprobando; para deshabilitar por completo cualquier filtrado, se debe deshabilitar el Firewall). Este perfil de sistema no se puede duplicar o eliminar y su configuración no se puede modificar.
- ***Bloquear todas***: un perfil de Firewall del sistema preconfigurado por el fabricante y que está siempre presente. Cuando este perfil está activado, toda la comunicación de red queda bloqueada, y el equipo no es accesible desde redes externas ni se puede comunicar con el exterior. No es posible duplicar ni eliminar este perfil del sistema, ni tampoco puede

modificarse su configuración.

- ***Perfiles personalizados***: los perfiles personalizados le permiten beneficiarse del cambio automático de perfil, que puede ser especialmente útil si se conecta a diferentes redes frecuentemente *(p. ej., con un portátil).* Los perfiles personalizados se generan automáticamente después de la instalación de **AVG Internet Security 2012** y cubren cualquier necesidad individual de las reglas de directivas del Firewall. Están disponibles los siguientes perfiles personalizados:

    - ***Directamente conectado a Internet***: adecuado para equipos domésticos de sobremesa comunes o portátiles conectados directamente a Internet, sin ninguna protección extra. Esta opción también se recomienda cuando conecta su portátil a varias redes desconocidas y probablemente no seguras (*p. ej., un cibercafé, la habitación de un hotel, etc.*). Las reglas más estrictas de las directivas del Firewall de este perfil garantizan que tales equipos tienen una protección adecuada.

    - ***Equipo dentro del dominio***: adecuado para equipos de una red local, normalmente centros escolares o trabajo. Se supone que la red está administrada de forma profesional y protegida por medidas adicionales, por lo que el nivel de seguridad puede ser inferior al de los casos mencionados anteriormente, lo que permitiría el acceso a carpetas compartidas, unidades de disco, etc.

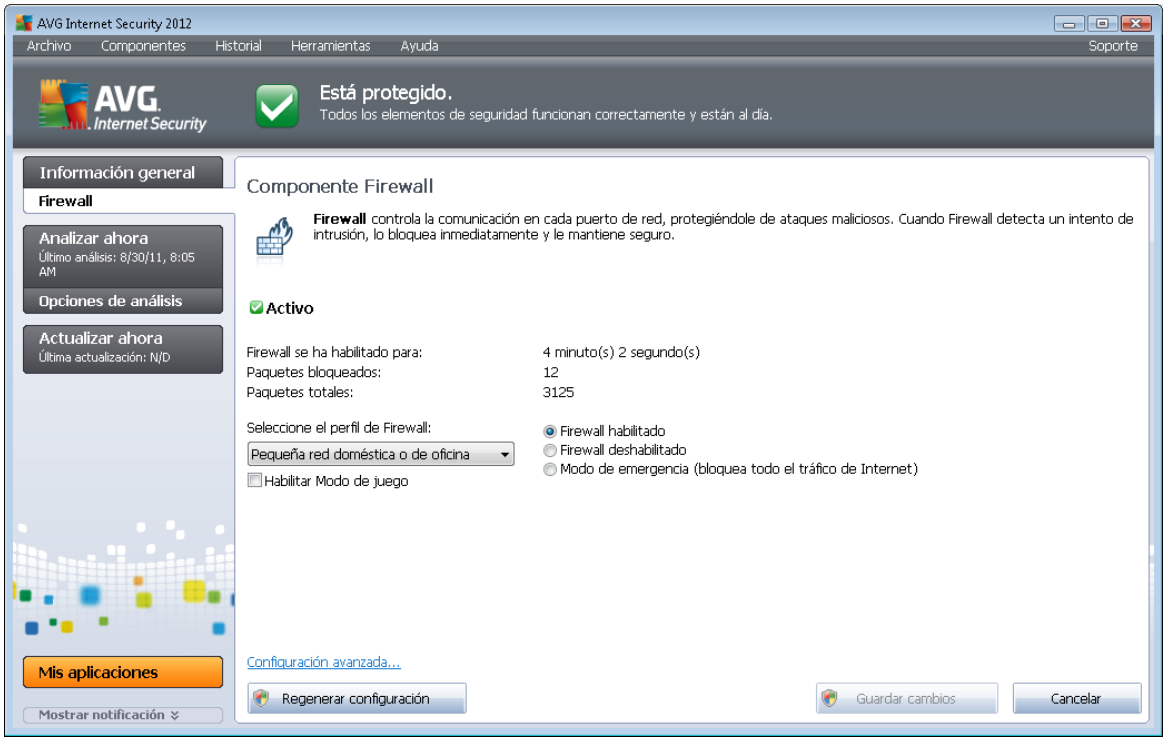
    - ***Pequeña red doméstica o de oficina***: adecuado para los equipos de una red pequeña, normalmente en casa o en un pequeño negocio. Habitualmente, este tipo de red no tiene un administrador "central" y consta sólo de varios equipos conectados entre sí que a menudo comparten una impresora, escáner o dispositivo similar, lo cual se debe reflejar en las reglas del Firewall.

Cambio de perfil

La característica de cambio de perfil permite que el Firewall cambie automáticamente al perfil definido al utilizar un adaptador de red determinado o cuando se conecta a cierto tipo de red. Si aún no se ha asignado ningún perfil a un área de red, entonces, cuando se realice la próxima conexión con esa área, el Firewall mostrará un cuadro de diálogo para preguntarle si desea asignarle un perfil. Puede asignar perfiles a todas las áreas o interfaces de red local y especificar más parámetros en el cuadro de diálogo Perfiles de adaptadores y áreas, donde también puede deshabilitar la característica si no desea utilizarla (*para cualquier clase de conexión se usará el perfil predeterminado*).

Por lo general, los usuarios que tienen un portátil y utilizan varios tipos de conexión encontrarán útil esta característica. Si tiene un equipo de escritorio y solamente usa un tipo de conexión (*por ejemplo, conexión por cable a Internet*), no necesita preocuparse del cambio de perfil, ya que lo más probable es que nunca lo utilice.

6.4.3. Interfaz de Firewall



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

- ***Firewall ha estado habilitado***: tiempo transcurrido desde la última vez que se inició el Firewall
- ***Paquetes bloqueados***: número de paquetes bloqueados con respecto al total de paquetes comprobados
- ***Paquetes totales***: número de todos los paquetes comprobados 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 sobre cada perfil y su uso recomendado, consulte el capítulo Perfiles de Firewall*)
- ***Habilitar Modo juego***: marque esta opción para asegurarse de que al ejecutar aplicaciones a pantalla completa (*juegos, presentaciones, películas, etc.*) el Firewall no mostrará cuadros de diálogo preguntando si se desea permitir o bloquear la comunicación de las aplicaciones desconocidas. En caso de que una aplicación desconocida intente comunicarse por la red en ese momento, el Firewall permitirá o bloqueará automáticamente

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

- Adicionalmente, en esta sección de configuración básica, puede seleccionar tres opciones alternativas para definir el estado actual del componente Firewall:

    - ***Firewall habilitado*** *(activada de manera predeterminada)*: seleccione esta opción para permitir la comunicación con aquellas aplicaciones que se han definido como "permitidas" en el conjunto de reglas definidas en el perfil de Firewall seleccionado.

    - ***Firewall deshabilitado***: con esta opción se desactiva por completo el Firewall y se permite todo el tráfico de red sin comprobación

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

Nota: *el proveedor del software ha configurado todos los componentes de AVG Internet Security 2012 para ofrecer un rendimiento óptimo. A menos que tenga un buen motivo para hacerlo, no modifique la configuración de AVG. Cualquier cambio de configuración debe realizarlo únicamente un usuario experimentado. Si necesita cambiar la configuración del Firewall, seleccione el elemento del menú del sistema* ***Herramientas/Configuración de Firewall*** *y edite la configuración de Firewall en el cuadro de diálogo Configuración de Firewall que se acaba de abrir.*

Botones de control

- ***Regenerar configuración***: pulse este botón para sobrescribir la configuración actual de Firewall y restaurar la configuración predeterminada basada en la detección automática

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

- ***Cancelar***: pulse este botón para regresar al cuadro de diálogo principal de AVG (*información general de los componentes*).

6.5. Anti-Rootkit

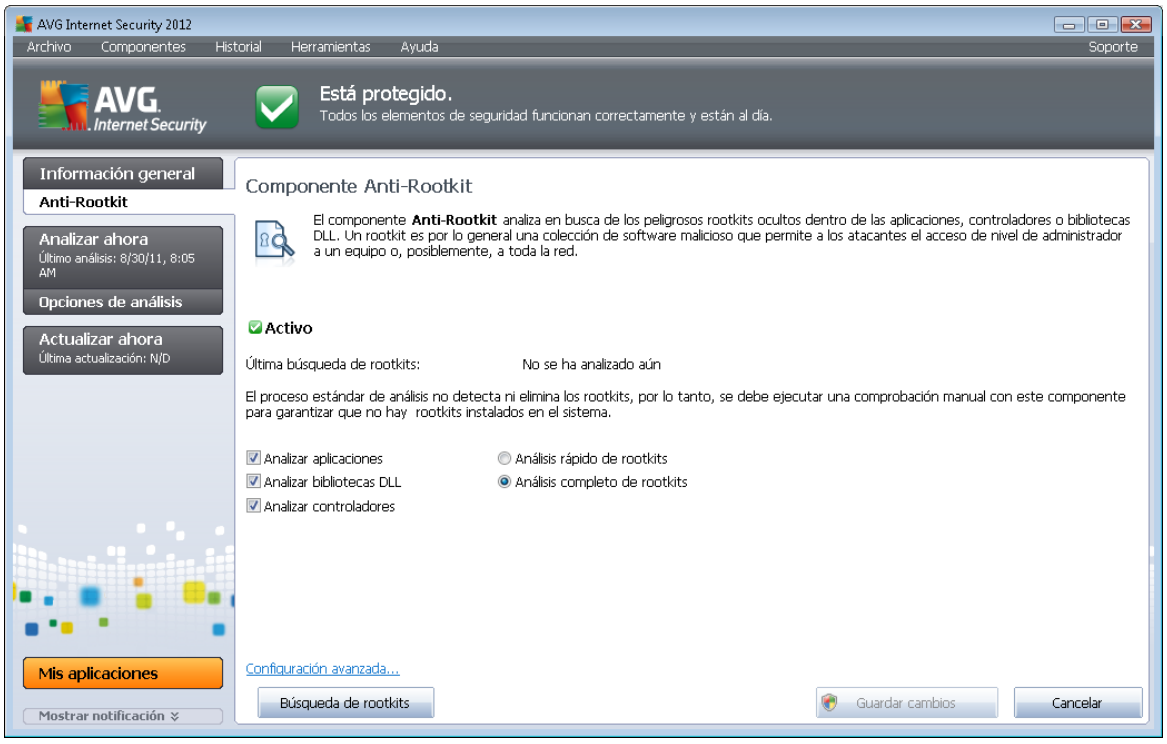
Anti-Rootkit es una herramienta especializada que detecta y elimina eficazmente los rootkits peligrosos, es decir, programas y tecnologías que pueden enmascarar la presencia de software malicioso en el equipo. ***Anti-Rootkit*** es capaz de detectar rootkits basándose en un conjunto predefinido de reglas. Tenga en cuenta que se detectan todos los rootkits (*no sólo los infectados*). Cuando ***Anti-Rootkit*** encuentra un rootkit, no significa necesariamente que esté infectado. Algunas veces, los rootkits se utilizan como controladores o forman parte de aplicaciones correctas.

¿Qué es un rootkit?

Un rootkit es un programa diseñado para asumir el control de un equipo sin autorización de los

propietarios y los administradores legítimos del sistema. El acceso al hardware normalmente no es necesario, ya que el rootkit está diseñado para tomar el control del sistema operativo que se ejecuta en el hardware. Generalmente, 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 se presentan en forma de troyanos, engañando a los usuarios para hacerles creer que es seguro ejecutarlos en sus sistemas. Las técnicas que se utilizan para conseguir este propósito incluyen 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 sobre su estado actual *(Activo)* y también muestra información sobre la última vez que se inició el análisis ***Anti-Rootkit*** (***última búsqueda de rootkits***). El cuadro de diálogo ***Anti-Rootkit*** también proporciona el vínculo Herramientas/Configuración avanzada. Este vínculo conduce al entorno de configuración avanzada del componente ***Anti-Rootkit***.

El proveedor del software ha configurado todos los componentes de AVG para ofrecer un rendimiento óptimo. A menos que tenga un buen motivo para hacerlo, no modifique la configuración de AVG. Cualquier cambio de configuración debe realizarlo únicamente un usuario experimentado.

Configuración básica de Anti-Rootkit

En la parte inferior del cuadro de diálogo puede configurar algunas funciones elementales del análisis de presencia de rootkits. En primer lugar, marque las casillas de verificación

correspondientes para especificar los objetos que deben analizarse:

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

Además, 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 (*normalmente c:\Windows*).
- ***Análisis completo de rootkits***: analiza todos los procesos en ejecución, los controladores cargados y la carpeta del sistema (*normalmente c:\Windows*), además de todas las unidades de disco locales (*incluida la unidad de almacenamiento extraíble, pero no las unidades de CD y disquete*).

Botones de control

- ***Búsqueda de rootkits***: dado que el análisis de rootkits no es una parte implícita en el Análisis del equipo completo, puede ejecutar el análisis de rootkits directamente desde la interfaz de ***Anti-Rootkit*** por medio de este botón.
- ***Guardar cambios***: pulse este botón para guardar todos los cambios realizados en esta interfaz y volver al cuadro de diálogo principal de AVG (*información general de los componentes*).
- ***Cancelar***: pulse este botón para volver al cuadro de diálogo principal de AVG (*información general de los componentes*) sin guardar los cambios realizados.

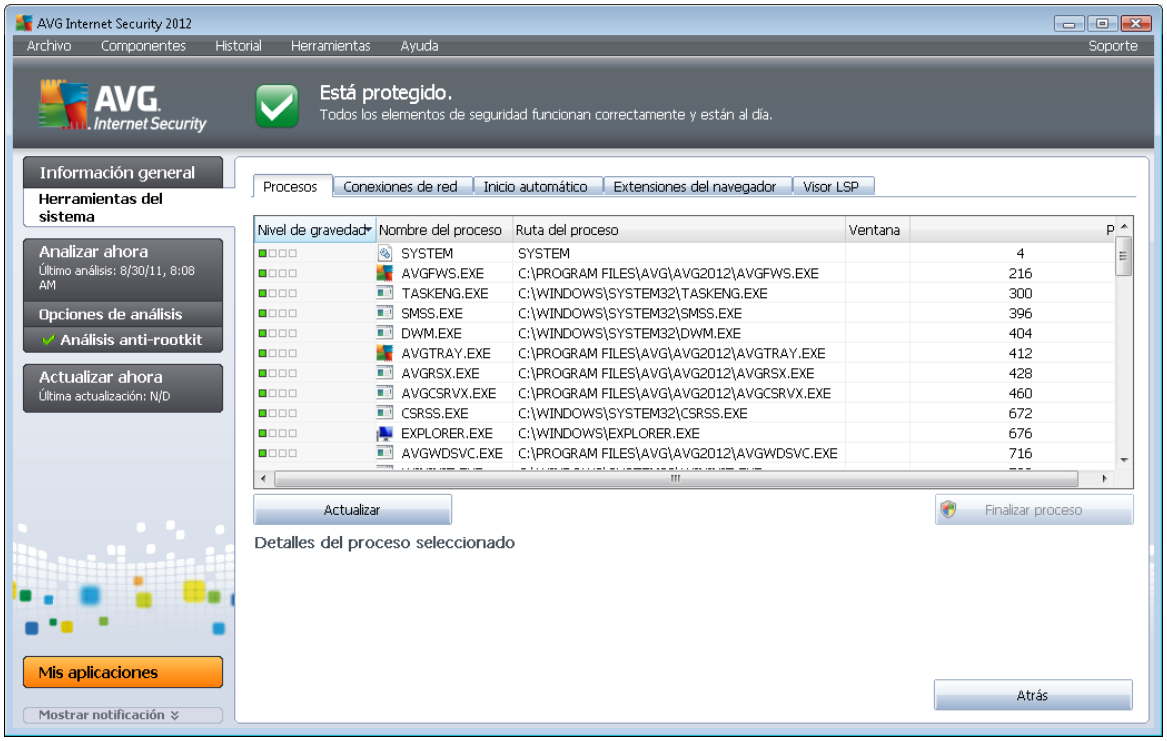
6.6. Herramientas del sistema

Herramientas del sistema se refiere a las herramientas que ofrecen un resumen detallado del entorno de **AVG Internet Security 2012** y el sistema operativo. El componente muestra información general sobre:

- Procesos: lista de los procesos (*es decir, aplicaciones en ejecución*) que están activos actualmente en el equipo
- Conexiones de red: lista de las conexiones actualmente activas
- Inicio automático: lista de todas las aplicaciones que se ejecutan en el inicio del sistema Windows
- Extensiones del navegador: lista de complementos (*es decir, aplicaciones*) que están instalados en el navegador de Internet
- Visor LSP: lista de proveedores de servicios por capas (*LSP*)

También es posible editar resúmenes específicos de información, pero se recomienda que sólo lo hagan usuarios expertos.

6.6.1. Procesos



El cuadro de diálogo ***Procesos*** muestra una lista de los procesos (*es decir, aplicaciones en ejecución*) que están activos actualmente en el equipo. La lista se divide en varias columnas:

- ***Nivel de gravedad***: identificación gráfica de la gravedad de cada proceso en una escala de cuatro niveles que van desde el menos importante (■□□□) al nivel crítico (■■■■)
- ***Nombre del proceso***: nombre del proceso en ejecución
- ***Ruta del proceso***: la ruta física del proceso en ejecución
- ***Ventana***: si corresponde, indica el nombre de la ventana de la aplicación
- ***PID***: es el número de identificación del proceso, un identificador único de proceso interno de Windows

Botones de control

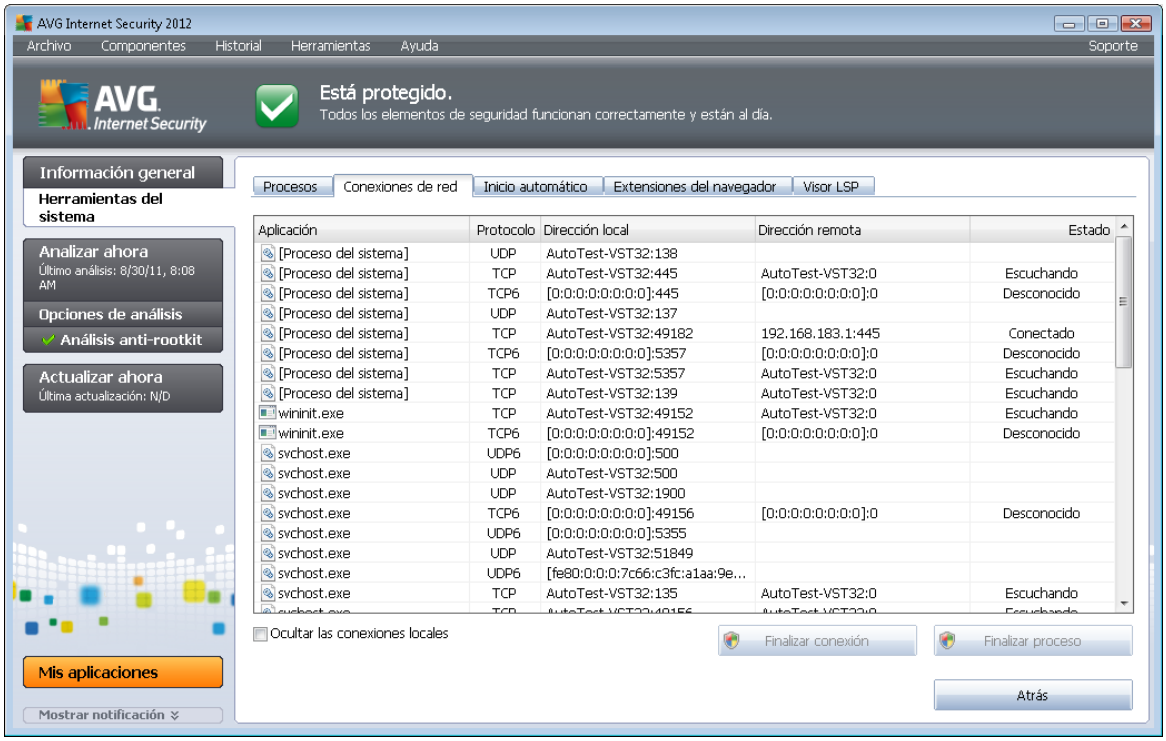
Los botones de control disponibles en la ficha ***Procesos*** son los siguientes:

- ***Actualizar***: actualiza la lista de procesos según el estado actual

- ***Finalizar proceso***: puede seleccionar una o más aplicaciones de la lista y finalizarlas pulsando este botón. ***Se aconseja no finalizar ninguna aplicación a menos que se esté absolutamente seguro de que representa una amenaza real.***

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

6.6.2. Conexiones de red



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

- ***Aplicación***: nombre de la aplicación relacionada con la conexión (*excepto en Windows 2000, donde esta información no está disponible*)

- ***Protocolo***: muestra el tipo de protocolo de transmisión utilizado para la conexión:

  - TCP: protocolo utilizado en combinación con el protocolo de Internet (IP) para transmitir información a través de Internet

  - UDP: alternativa al protocolo TCP

- ***Dirección local***: dirección IP del equipo local y número de puerto utilizado

- ***Dirección remota***: dirección IP del equipo remoto y número de puerto al que está conectado. Siempre que sea posible, también buscará el nombre de host del equipo remoto.

- ***Estado***: indica el estado actual más probable (*conectado, el servidor debe cerrarse, escuchar, cierre activo finalizado, cierre pasivo, cierre activo*)

Para enumerar solamente las conexiones externas, seleccione la casilla de verificación ***Ocultar las conexiones locales*** en la sección inferior del cuadro de diálogo que aparece debajo de la lista.

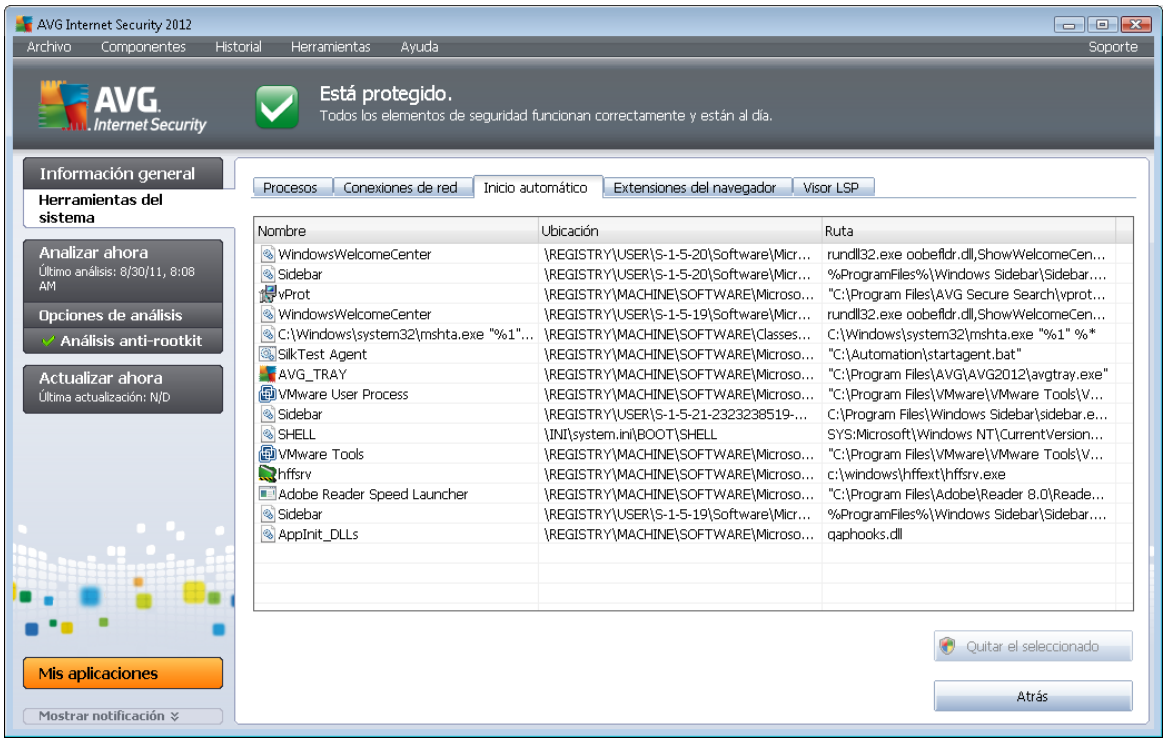
Botones de control

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

- ***Finalizar conexión***: cierra una o varias conexiones seleccionadas en la lista
- ***Finalizar proceso***: cierra una o varias aplicaciones relacionadas con las conexiones seleccionadas en la lista
- ***Atrás***: le devuelve al cuadro de diálogo principal de AVG predeterminado (información general de los componentes).

Tenga en cuenta que a veces sólo es posible finalizar aplicaciones que actualmente se encuentran conectadas. Se aconseja no finalizar ninguna conexión a menos que se esté absolutamente seguro de que representa una amenaza real.

6.6.3. Inicio automático



El cuadro de diálogo ***Inicio automático*** muestra una lista de todas las aplicaciones que se ejecutan en el inicio del sistema Windows. Muy a menudo, varias aplicaciones de malware se agregan

automáticamente a la entrada de inicio del Registro.

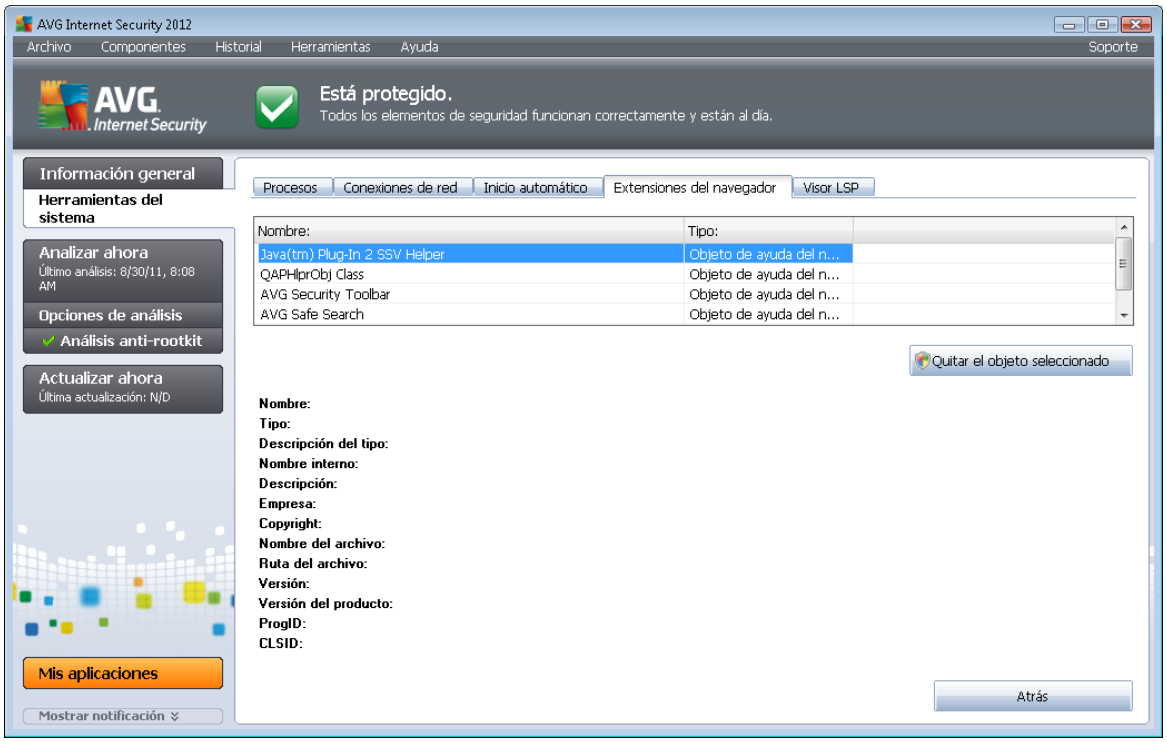
Botones de control

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

- ***Quitar el seleccionado***: pulse el botón para quitar una o más de las entradas seleccionadas.
- ***Atrás***: le devuelve al cuadro de diálogo principal de AVG predeterminado (*información general de los componentes).*

Se aconseja no eliminar ninguna aplicación de la lista a menos que se esté absolutamente seguro de que representa una amenaza real.

6.6.4. Extensiones del navegador



El cuadro de diálogo ***Extensiones del navegador*** contiene una lista de complementos (*es decir, aplicaciones*) que están instalados en el navegador de Internet. Esta lista puede contener aplicaciones de complemento normales, así como programas potencialmente de malware. Haga clic en un objeto de la lista para obtener información detallada sobre el complemento seleccionado, que se mostrará en la sección inferior del cuadro de diálogo.

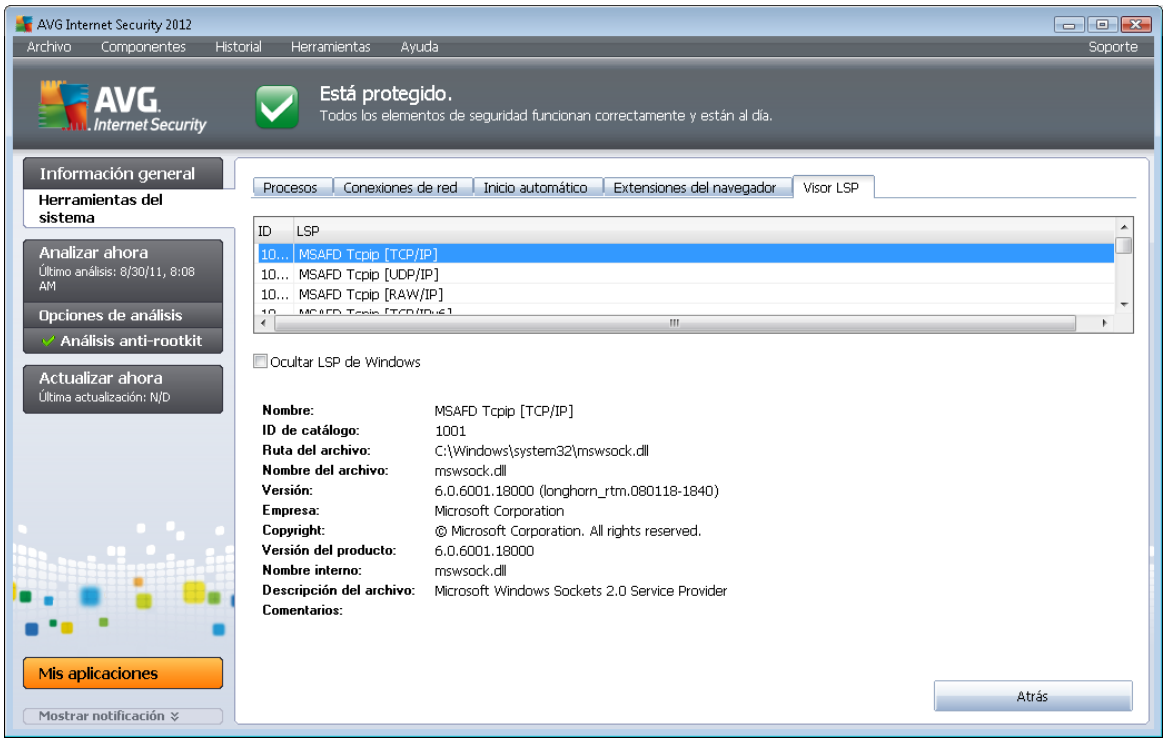
Botones de control

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

- ***Quitar el objeto seleccionado***: elimina el complemento que aparece resaltado en la lista. ***Se aconseja no eliminar ningún complemento de la lista a menos que se esté absolutamente seguro de que representa una amenaza real.***

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

6.6.5. Visor LSP



El cuadro de diálogo ***Visor LSP*** muestra una lista de proveedores de servicios por capas (LSP).

Un ***proveedor de servicios por capas*** (LSP) es un controlador del sistema vinculado a los servicios de red del sistema operativo Windows. Tiene acceso a todos los datos que entran y salen del equipo y puede, además, modificar dichos datos. Algunos LSP son necesarios para que Windows pueda conectarle a otros equipos y a Internet. Sin embargo, algunas aplicaciones de malware también pueden instalarse en forma de LSP y, por lo tanto, tener acceso a todos los datos que transmita su equipo. Por ello, esta revisión puede ayudarle a comprobar todas las posibles amenazas de LSP.

En algunas circunstancias, también es posible reparar LSP rotos (*por ejemplo, cuando el archivo se ha eliminado pero las entradas del Registro permanecen intactas*). Cuando se descubre un LSP reparable, se muestra un nuevo botón para solucionar el problema.

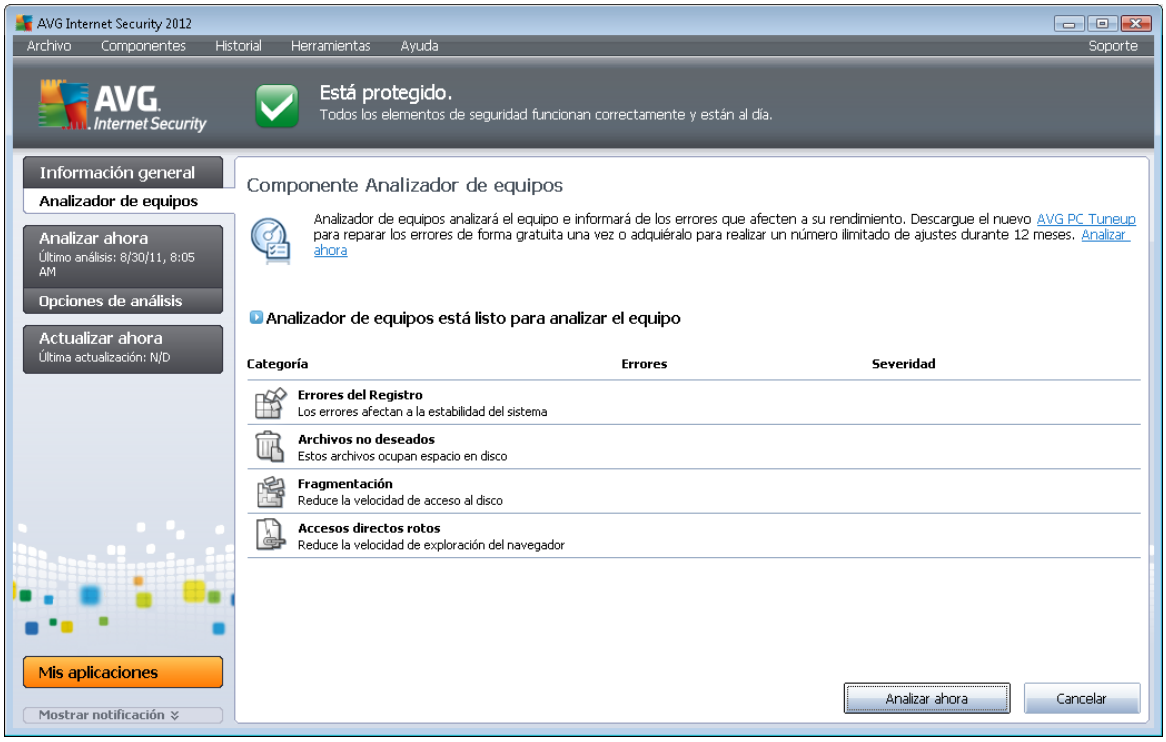
Botones de control

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

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

6.7. Analizador de equipos

El componente ***Analizador de equipos*** puede analizar el equipo en busca de problemas del sistema y brindarle una información clara sobre qué podría estar afectando a su rendimiento general. En la interfaz de usuario del componente se muestra una tabla dividida en cuatro líneas, una por cada categoría, con errores del Registro, archivos no deseados, fragmentación y accesos directos rotos:

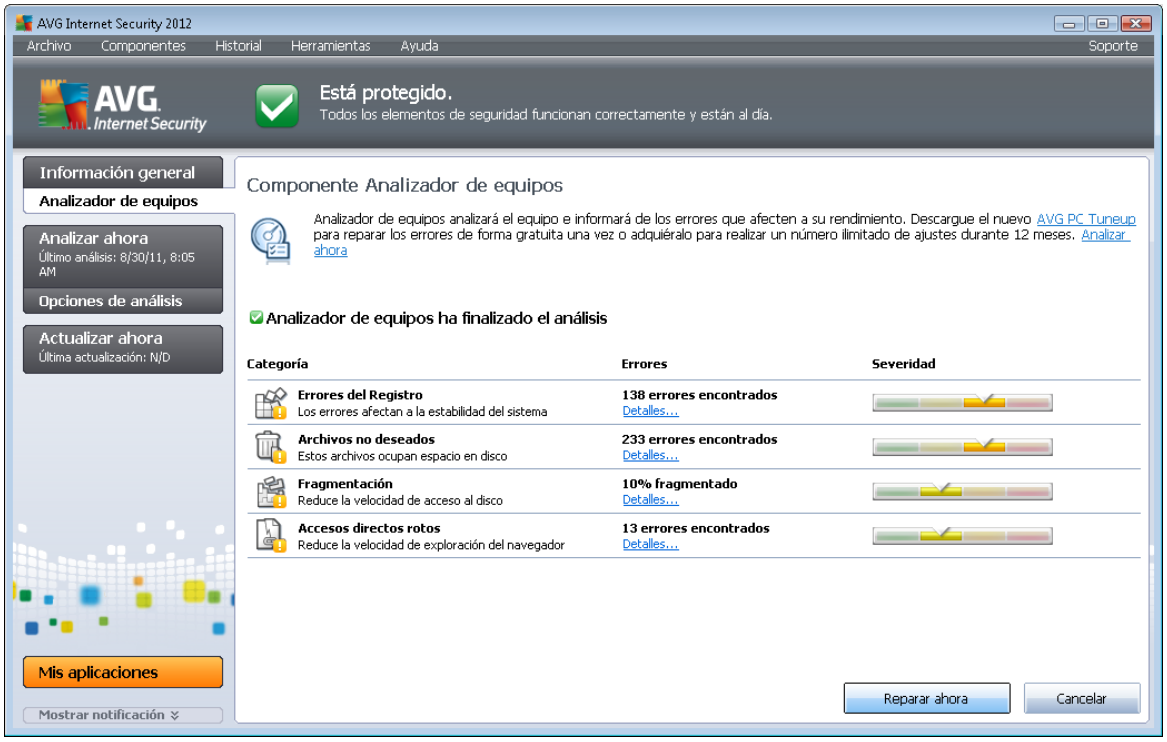


- ***Errores del Registro*** le dará la cantidad de errores que hay en el Registro de Windows. Dado que para corregir el Registro se requieren conocimientos bastante avanzados, no es recomendable intentar solucionar los errores por uno mismo.
- ***Archivos no deseados*** le indicará la cantidad de archivos de los que podría prescindir sin problemas. Por lo general, se trata de distintos tipos de archivos temporales y archivos que se encuentran en la Papelera de reciclaje.
- ***Fragmentación*** calculará el porcentaje del disco duro que se encuentra fragmentado; es decir, que ha estado en uso por mucho tiempo y en el que, por ello, la mayoría de los archivos se encuentran dispersos por diferentes partes. Para corregirlo, puede utilizar

alguna herramienta de desfragmentación.

- ***Accesos directos rotos*** le informará sobre accesos directos que han dejado de funcionar, que conducen a ubicaciones no existentes, etc.

Para iniciar el análisis del sistema, pulse el botón ***Analizar ahora***. A continuación, podrá observar el avance del análisis y sus resultados directamente en el gráfico:



La vista general de resultados muestra la cantidad de problemas del sistema detectados (***Errores***), divididos según las diferentes categorías analizadas. Los resultados del análisis también se presentarán gráficamente sobre un eje en la columna ***Gravedad***.

Botones de control

- ***Analizar ahora*** (*aparece antes de que comience el análisis*): pulse este botón para iniciar inmediatamente el análisis del equipo
- ***Reparar ahora*** (*aparece una vez que ha finalizado el análisis*): pulse este botón para dirigirse al sitio web de AVG (http://www.avg.com/) en la página donde podrá ver información actualizada y detallada sobre el componente ***Analizador de equipos***
- ***Cancelar***: pulse este botón para detener el análisis o para regresar al cuadro de diálogo principal de AVG (*información general de los componentes*) una vez finalizado el análisis

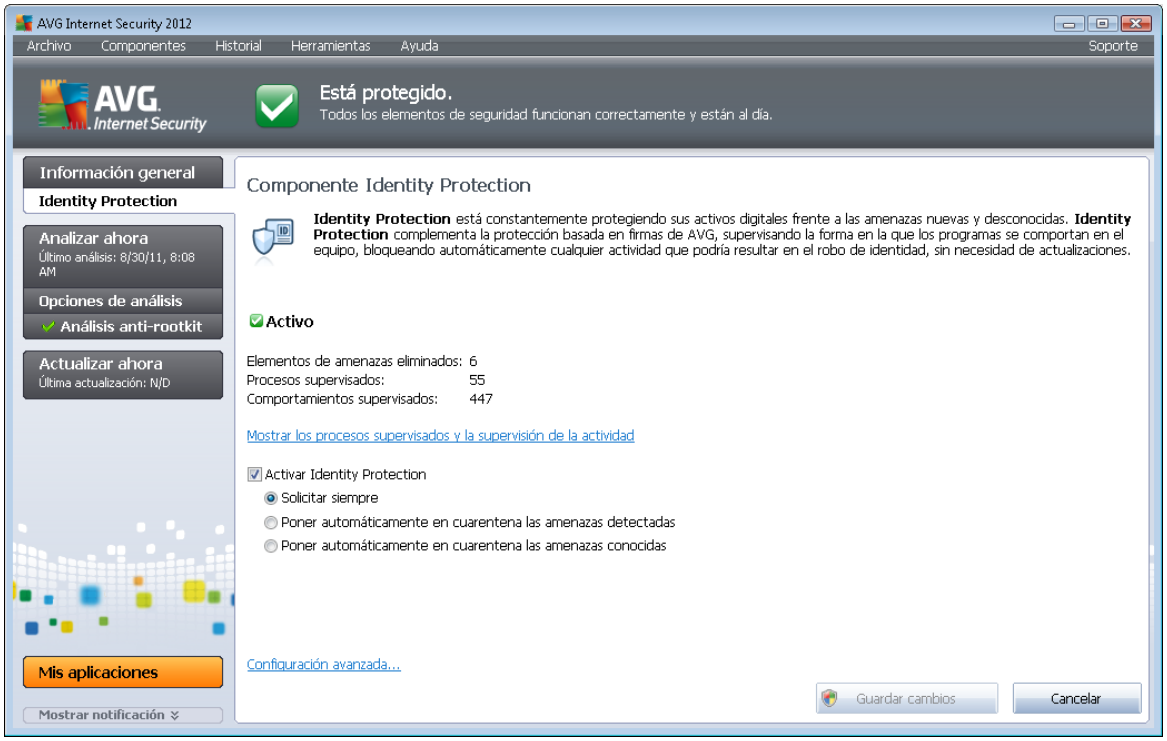
6.8. Identity Protection

Identity Protection es un componente anti-malware que le protege frente a todo tipo de software malicioso (*spyware, robots, robo de identidad, etc.*) utilizando tecnologías de comportamiento y ofreciendo protección ante los ataques de día cero de virus nuevos. ***Identity Protection*** se centra en impedir que los ladrones de identidad roben sus contraseñas, datos bancarios, números de tarjeta de crédito y otros activos digitales personales desde todo tipo de software malicioso (*malware*) que ataque a su equipo. Se asegura de que todos los programas que se ejecutan en el equipo funcionan correctamente. ***Identity Protection*** detecta y bloquea constantemente los comportamientos sospechosos y protege el equipo frente a todo el malware nuevo.

Identity Protection protege a su equipo en tiempo real contra amenazas nuevas e incluso desconocidas. Monitoriza todos los procesos *(incluidos los ocultos)* y más de 285 patrones de comportamiento diferentes, y puede determinar si está ocurriendo algo malicioso en su sistema. De esta forma puede revelar amenazas que aún no han sido descritas en la base de datos de virus. Siempre que un fragmento desconocido de código entra en un equipo, se vigila y controla inmediatamente para buscar comportamientos maliciosos. Si se determina que el archivo es malicioso, ***Identity Protection*** moverá el código al Almacén de virus y deshará cualquier cambio que se haya hecho en el sistema *(inserción de código, cambios en el Registro, apertura de puertos, etc.)*. No es necesario iniciar un análisis para estar protegido. La tecnología es muy proactiva, raramente necesita ser actualizada y siempre está en guardia.

Identity Protection es una protección adicional de Anti-Virus. Recomendamos encarecidamente que instale ambos componentes para tener una protección completa de su equipo.

6.8.1. Interfaz de Identity Protection



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

- ***Elementos de amenazas eliminados***: indica el número de aplicaciones detectadas como malware que se han quitado
- ***Procesos supervisados***: número de aplicaciones en ejecución que está supervisando IDP
- ***Comportamientos supervisados***: número de acciones específicas que se están ejecutando en las aplicaciones supervisadas

A continuación encontrará el vínculo Mostrar los procesos supervisados y la supervisión de la actividad, que le lleva a la interfaz de usuario del componente Herramientas del sistema, donde encontrará una vista detallada de todos los procesos supervisados.

Configuración básica de Identity Protection

En la parte inferior del cuadro de diálogo puede editar algunas características elementales de la funcionalidad del componente:

- ***Activar Identity Protection***: (*activada de manera predeterminada*): marque esta casilla para activar el componente IDP y abrir más opciones de edición.

  En algunos casos, ***Identity Protection*** puede indicar que algunos archivos legítimos son sospechosos o peligrosos. Dado que ***Identity Protection*** detecta las amenazas en función de su comportamiento, esto suele ocurrir cuando un programa intenta supervisar pulsaciones de teclas o instalar otros programas, o cuando se instala un nuevo controlador en el equipo. Por este motivo, seleccione una de las siguientes opciones especificando el comportamiento de ***Identity Protection*** en caso de detectar alguna actividad sospechosa:

  - ***Solicitar siempre***: si una aplicación se detecta como malware, se le preguntará si debe bloquearse (*esta opción está activada de manera predeterminada y se recomienda no modificarla a menos que tenga un buen motivo para ello*)
  - ***Poner automáticamente en cuarentena las amenazas detectadas***: todas las aplicaciones detectadas como malware se bloquearán automáticamente
  - ***Poner automáticamente en cuarentena las amenazas conocidas***: solamente se bloquearán las aplicaciones detectadas con total certeza como malware

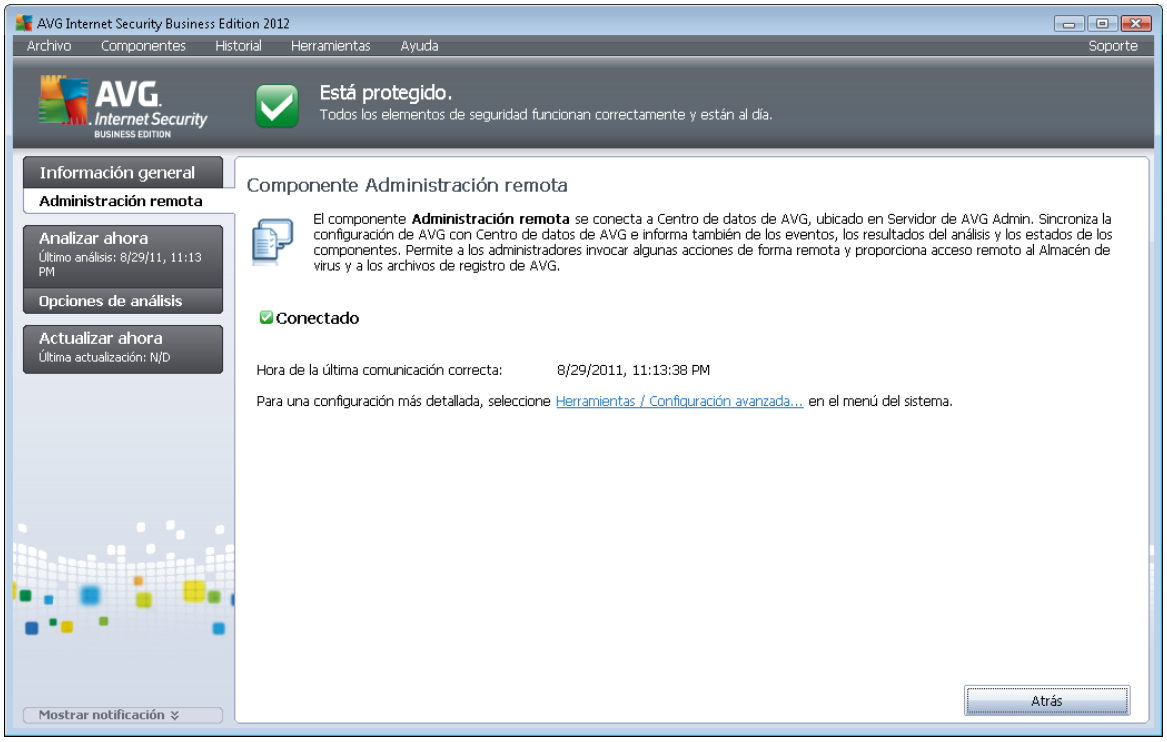
Botones de control

Los botones de control disponibles en la interfaz de ***Identity Protection*** son los siguientes:

- ***Guardar cambios***: pulse este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo
- ***Cancelar***: pulse el botón para volver al cuadro de diálogo principal de AVG

predeterminado (*información general de los componentes*)

6.9. Administración remota



El componente ***Administración remota*** sólo aparecerá en la interfaz de usuario de **AVG Internet Security 2012** si ha instalado la versión Business Edition del producto *(para obtener información sobre la licencia utilizada en la instalación, consulte la ficha Versión del cuadro de diálogo Información, que puede abrirse mediante el elemento de menú del sistema Soporte)*. En el cuadro de diálogo ***Componente Administración remota*** puede obtener información sobre si el componente está activo y conectado al servidor. Toda la configuración del componente ***Administración remota*** debe hacerse dentro de ***Configuración avanzada / Administración remota***.

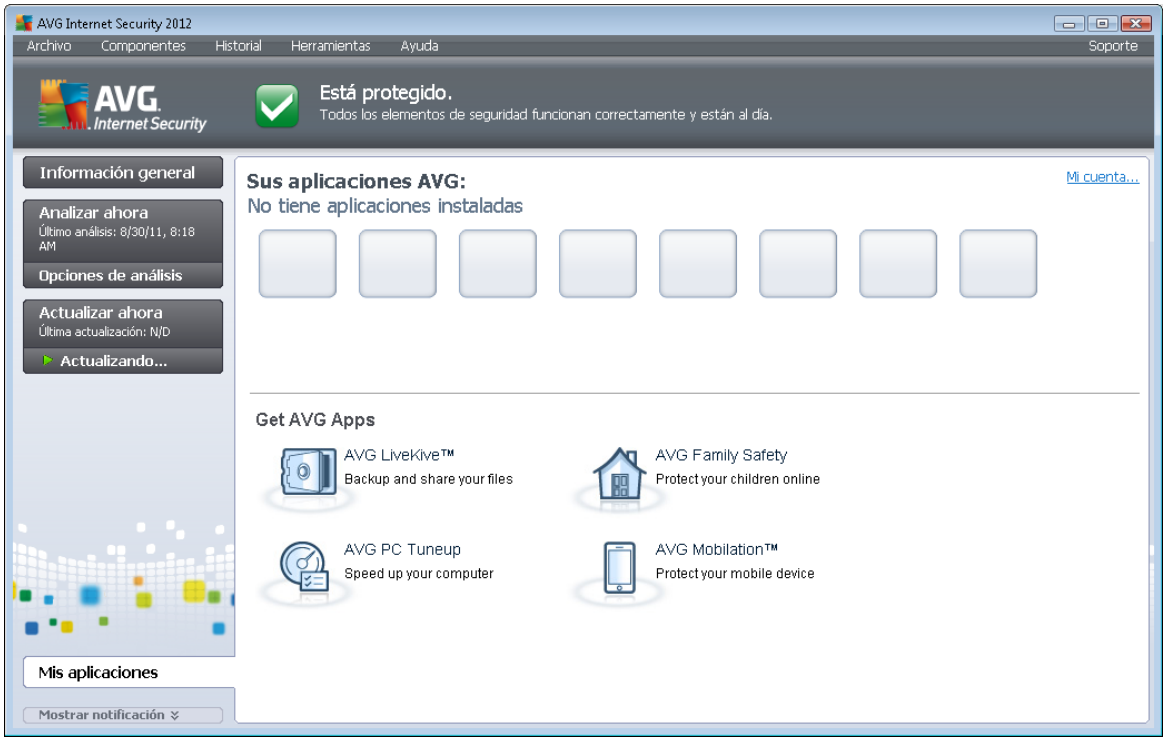
Para ver una descripción detallada de las opciones y funciones del componente dentro del sistema de Administración remota de AVG, consulte la documentación específica dedicada exclusivamente a este tema. Se puede descargar esta documentación del sitio web de AVG (http://www.avg.com/)), en la sección ***Centro de soporte / Descarga / Documentación***.

Botones de control

- ***Atrás***: pulse este botón para regresar al cuadro de diálogo principal de AVG (*información general de los componentes*).

7. Mis aplicaciones

Cada una de las siguientes tres aplicaciones, LiveKive, Family Safety y PC Tuneup, se encuentra disponible como producto de AVG independiente y como parte opcional de la instalación de **AVG Internet Security 2012**. En el cuadro de diálogo ***Sus aplicaciones AVG*** *(accesible directamente a través del botón Mis aplicaciones del cuadro de diálogo principal de AVG)* puede ver información general de las aplicaciones ya instaladas y las que están listas para instalarse de manera opcional:



7.1. LiveKive

LiveKive está diseñado para hacer copias de seguridad en línea de sus datos en servidores seguros. ***LiveKive*** hace copias de seguridad de forma automática de todos los archivos, fotos y música en un lugar seguro, permitiendo compartirlos con su familia y amigos así como acceder a ellos desde cualquier dispositivo habilitado para la web, incluyendo dispositivos iPhone y Android. Las características de ***LiveKive*** incluyen:

- Medida de seguridad en caso de que el equipo o disco duro se dañen
- Acceso a sus datos mediante cualquier dispositivo conectado a Internet
- Organización sencilla
- Capacidad de compartir los datos con cualquier persona que usted autorice

Para obtener más información, visite la página web dedicada de AVG, desde donde también podrá descargar el componente de forma inmediata. Para hacerlo, puede utilizar el vínculo LiveKive en el cuadro de diálogo Mis aplicaciones.

7.2. Family Safety

Family Safety contribuye a proteger a los menores ante sitios web, contenidos multimedia y búsquedas en línea inapropiados, proporcionando informes de su actividad en línea. Puede definir un nivel de protección adecuado para cada uno de sus hijos y supervisarlos de forma individual por medio de inicios de sesión independientes.

Para obtener más información, visite la página web dedicada de AVG, desde donde también podrá descargar el componente de forma inmediata. Para hacerlo, puede utilizar el vínculo Family Safety en el cuadro de diálogo Mis aplicaciones.

7.3. PC Tuneup

La aplicación ***PC Tuneup*** es una herramienta avanzada que permite realizar un análisis detallado del sistema y conocer cómo pueden mejorarse la velocidad y el rendimiento general del equipo. Entre las características de ***PC Tuneup*** se incluyen:

- Limpiador de disco: elimina archivos no deseados que ralentizan el equipo.
- Desfragmentador de disco: desfragmenta los discos y optimiza la colocación de los archivos del sistema.
- Limpiador del Registro: repara los errores del Registro para aumentar la estabilidad del equipo.
- Desfragmentador del Registro: compacta el Registro eliminando espacios que ocupan memoria.
- Doctor del disco: localiza sectores erróneos, clústeres perdidos y errores de directorio, y los repara.
- Optimizador de Internet: optimiza la configuración de Internet en función de la conexión disponible.
- Borrador de rastros: elimina el historial de uso del equipo y de Internet.
- Liberador de disco: borra el espacio libre de los discos para impedir la recuperación de datos confidenciales.
- Destructor de archivos : borra los archivos seleccionados en un disco o memoria USB de forma imposible de recuperar.
- Recuperación de archivos: recupera los archivos eliminados por accidente de discos, memorias USB o cámaras.
- Buscador de archivos duplicados: ayuda a encontrar y eliminar archivos duplicados que ocupan espacio en disco.
- Administrador de servicios: desactiva los servicios innecesarios que ralentizan el equipo.
- Administrador de inicio: permite al usuario administrar los programas que se inician

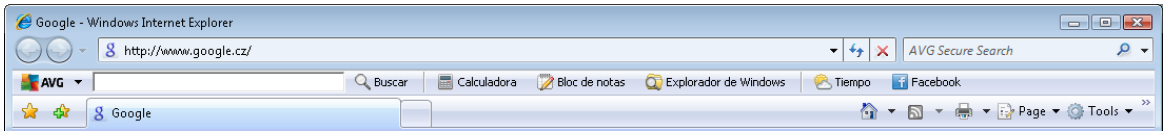
automáticamente al arrancar Windows.

- Administrador de desinstalación: desinstala completamente el software que ya no necesita.
- Administrador de cambios: permite al usuario controlar cientos de configuraciones ocultas de Windows.
- Administrador de tareas: muestra todos los procesos en ejecución, servicios y archivos bloqueados.
- Explorador de disco: muestra los archivos que ocupan más tamaño en el equipo.
- Información del sistema: ofrece información detallada sobre el hardware y software instalado.

Para obtener más información, visite la página web dedicada de AVG, desde donde también podrá descargar el componente de forma inmediata. Para hacerlo, puede utilizar el vínculo de PC Tuneup en el cuadro de diálogo Mis aplicaciones.

8. AVG Security Toolbar

AVG Security Toolbar es una herramienta que coopera estrechamente con el componente LinkScanner y proporciona la máxima seguridad mientras se navega por Internet. Al instalar **AVG Internet Security 2012**, la instalación de ***AVG Security Toolbar*** es opcional; durante el proceso de instalación se le invita a decidir si desea instalar el componente. ***AVG Security Toolbar*** está disponible directamente en su navegador de Internet. De momento, los navegadores de Internet compatibles son Internet Explorer (*versión 6.0 y superior*) y/o Mozilla Firefox (*versión 3.0 y superior*). Los demás navegadores no son compatibles *(si utiliza otro navegador, como Avant Browser, se puede producir un comportamiento inesperado)*.



La barra de herramientas ***AVG Security Toolbar*** contiene los siguientes elementos:

- ***Logotipo de AVG*** en el menú desplegable:
  - ***Utilizar AVG Secure Search***: le permite buscar directamente desde ***AVG Security Toolbar*** utilizando el motor de ***AVG Secure Search***. Todos los resultados de las búsquedas son verificados continuamente por el servicio Search-Shield, para que se sienta totalmente seguro en línea.
  - ***Nivel actual de amenaza***: abre la página web del laboratorio de virus con un esquema gráfico del nivel de amenaza actual en Internet.
  - ***Laboratorios de amenazas de AVG***: abre la página ***Site Reports*** en la web de AVG (http://www.avg.com/), donde puede buscar amenazas específicas por nombre y obtener información detallada sobre cada una de ellas.
  - ***Ayuda de la barra de herramientas***: abre la ayuda en línea, que cubre toda la funcionalidad de ***AVG Security Toolbar***.
  - ***Enviar comentarios del producto***: abre una página web con un formulario que puede rellenar para comentarnos su experiencia con la ***AVG Security Toolbar***.
  - ***Acerca de...***: abre una nueva ventana con información sobre la versión de la barra de herramientas ***AVG Security Toolbar*** instalada.
- ***Campo de búsqueda***: busque en Internet con ***AVG Security Toolbar*** para estar completamente seguro y cómodo, ya que todos los resultados de la búsqueda son cien por cien seguros. Escriba la palabra o frase en el campo de búsqueda, y pulse el botón ***Buscar*** *(o Intro)*. Todos los resultados de la búsqueda son comprobados continuamente por el servicio Search-Shield *(en el componente LinkScanner)*.
- Botones de acceso directo para acceder rápidamente a estas aplicaciones: ***Calculadora***, ***Bloc de notas***, ***Windows Explorer***
- ***Tiempo***: el botón abre un nuevo cuadro de diálogo que proporciona información sobre el

tiempo actual en su localidad, así como las previsiones para los próximos dos días. Esta información se actualiza regularmente, cada 3-6 horas. En el cuadro de diálogo, puede cambiar la ubicación deseada manualmente y decidir si desea ver la información sobre temperatura en grados Celsius o Fahrenheit.

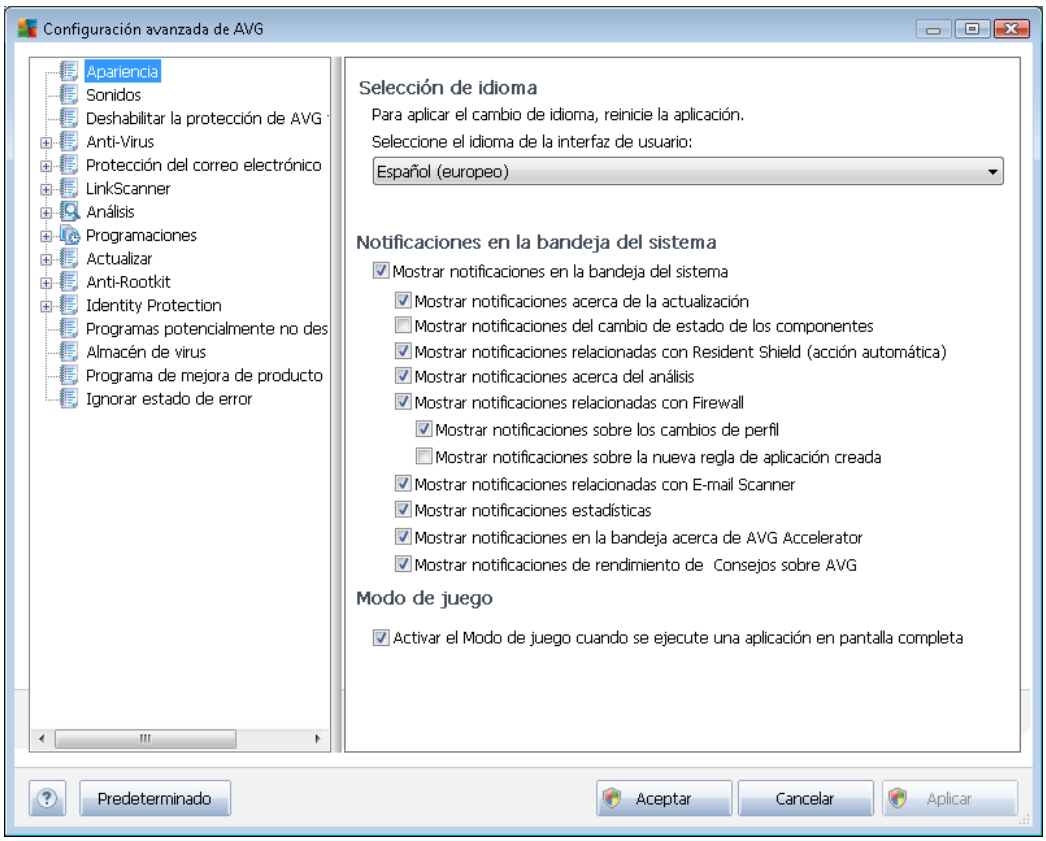
- ***Facebook***: este botón le permite conectarse a la red social Facebook directamente desde ***AVG Security Toolbar***.

9. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG Internet Security 2012** se abre en una nueva ventana denominada ***Configuración avanzada de AVG***. Dicha ventana está dividida en dos secciones: la parte izquierda ofrece navegación en forma de árbol a las opciones de configuración del programa. Seleccione el componente cuya configuración desea modificar (*o una parte concreta*) para abrir el cuadro de diálogo de edición en la sección derecha de la ventana.

9.1. Apariencia

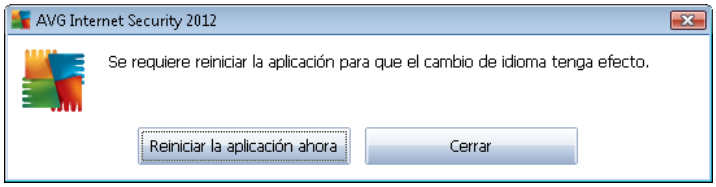
El primer elemento del árbol de navegación, ***Apariencia***, hace referencia a la configuración general de la interfaz de usuario de **AVG Internet Security 2012** y proporciona algunas funciones elementales del comportamiento de la aplicación:



Selección de idioma

En la sección ***Selección de idioma*** puede elegir el idioma deseado en el menú desplegable. El idioma seleccionado se utilizará en toda la interfaz de usuario de **AVG Internet Security 2012**. El menú desplegable sólo contiene aquellos idiomas que el usuario ha seleccionado para que se instalen durante el proceso de instalación (*consulte el capítulo Opciones personalizadas*), además del inglés (*que se instala de forma predeterminada*). Para que se efectúe el cambio de **AVG Internet Security 2012** a otro idioma, debe reiniciar la aplicación. Realice el siguiente procedimiento:

- En el menú desplegable, seleccione el idioma deseado de la aplicación
- Confirme su selección pulsando el botón ***Aplicar*** *(esquina inferior derecha del cuadro de diálogo)*
- Pulse el botón ***Aceptar*** para confirmar
- Aparece un nuevo cuadro de diálogo que le informa de que debe reiniciar **AVG Internet Security 2012**
- Pulse el botón ***Reiniciar la aplicación ahora*** para confirmar el reinicio del programa y espere un segundo hasta que el cambio de idioma tenga efecto:



Notificaciones en la bandeja del sistema

En esta sección puede suprimir la visualización de notificaciones en la bandeja del sistema sobre el estado de la aplicación **AVG Internet Security 2012**. De manera predeterminada, se permite que se muestren las notificaciones del sistema. Se recomienda encarecidamente mantener esta configuración. Las notificaciones del sistema informan, por ejemplo, sobre el inicio de procesos de análisis o actualización, o sobre el cambio de estado de un componente de **AVG Internet Security 2012**. Se recomienda prestar atención a estas notificaciones.

Sin embargo, si por algún motivo decide que no quiere ser informado de esta forma, o que sólo desea ver ciertas notificaciones *(relacionadas con un componente específico de AVG Internet Security 2012)*, puede definir y especificar sus preferencias seleccionando o dejando en blanco las siguientes opciones:

- ***Mostrar notificaciones en la bandeja del sistema*** *(activado de manera predeterminada)*: se muestran todas las notificaciones por defecto. Desactive este elemento para deshabilitar completamente la visualización de todas las notificaciones. Cuando está activo, puede seleccionar las notificaciones específicas que deben mostrarse:
  - ***Mostrar notificaciones acerca de la actualización*** *(activado de manera predeterminada)*: decida si se debe mostrar la información relacionada con el inicio, progreso y finalización del proceso de actualización de **AVG Internet Security 2012** .
  - ***Mostrar notificaciones del cambio de estado de los componentes*** *(desactivado de manera predeterminada)*: decida si desea que se muestre información relacionada con la actividad o inactividad del componente o sus problemas relacionados. Cuando se notifica un estado de fallo del componente, esta opción realiza la misma función informativa que el icono de la bandeja del sistema y avisa de problemas en cualquier componente de **AVG Internet Security 2012**.

- ***Mostrar notificaciones relacionadas con Protección residente (acción automática)*** *(activado de manera predeterminada)*: decida si la información relacionada con los procesos de guardado, copia y apertura se deben mostrar o suprimir (*esta configuración sólo muestra si la opción Reparación automática de Protección residente está activada*).

- ***Mostrar notificaciones acerca del análisis*** *(activado de manera predeterminada)*: decida si se debe mostrar información cuando se inicie automáticamente un análisis programado, su progreso y los resultados.

- ***Mostrar notificaciones relacionadas con Firewall*** *(activado de manera predeterminada)*: decida si la información relacionada con estados y procesos del Firewall, como los avisos de activación/desactivación de componentes, posible bloqueo del tráfico etc. debe mostrarse. Este elemento proporciona otras dos opciones de selección más específicas *(para obtener una explicación más detallada de cada una de ellas, consulte el capítulo Firewall de este documento)*:

  - ***Mostrar notificaciones sobre los cambios de perfil*** *(activado de manera predeterminada)*: le notifica sobre cambios automáticos de los perfiles del Firewall.

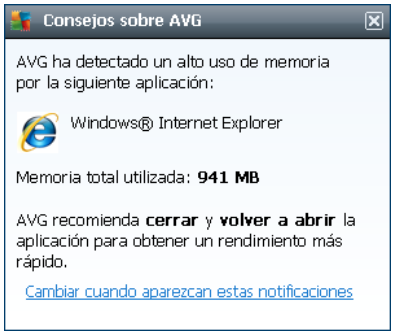
  - ***Mostrar notificaciones sobre la nueva regla de aplicación creada*** *(desactivado de manera predeterminada)*: le notifica sobre la creación automática del reglas del Firewall para nuevas aplicaciones basadas en una lista segura.

- ***Mostrar notificaciones relacionadas con Analizador de correo electrónico*** *(activado de manera predeterminada)*: decida si se debe mostrar información tras el análisis de todos los mensajes de correo electrónico entrantes y salientes.

- ***Mostrar notificaciones estadísticas*** *(activado de manera predeterminada)*: mantenga el elemento marcado para permitir que la notificación periódica de revisión estadística se muestre en la bandeja del sistema.

- ***Mostrar notificaciones en la bandeja acerca de AVG Accelerator*** *(activado de manera predeterminada)*: decida si desea que se muestre información sobre las actividades de ***AVG Accelerator***. El servicio ***AVG Accelerator*** permite reproducir vídeo en línea sin interrupciones y facilita las descargas adicionales.

- ***Mostrar notificaciones de rendimiento de AVG Advisor*** *(activado de manera 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 utilice más cantidad de memoria de la recomendada. En esta situación, el rendimiento de su equipo se puede reducir de forma significativa, y se recomienda reiniciar el navegador para agilizar los procesos. Deje activado el elemento ***Mostrar notificaciones de rendimiento de AVG Advisor*** si desea que se le informe al respecto.

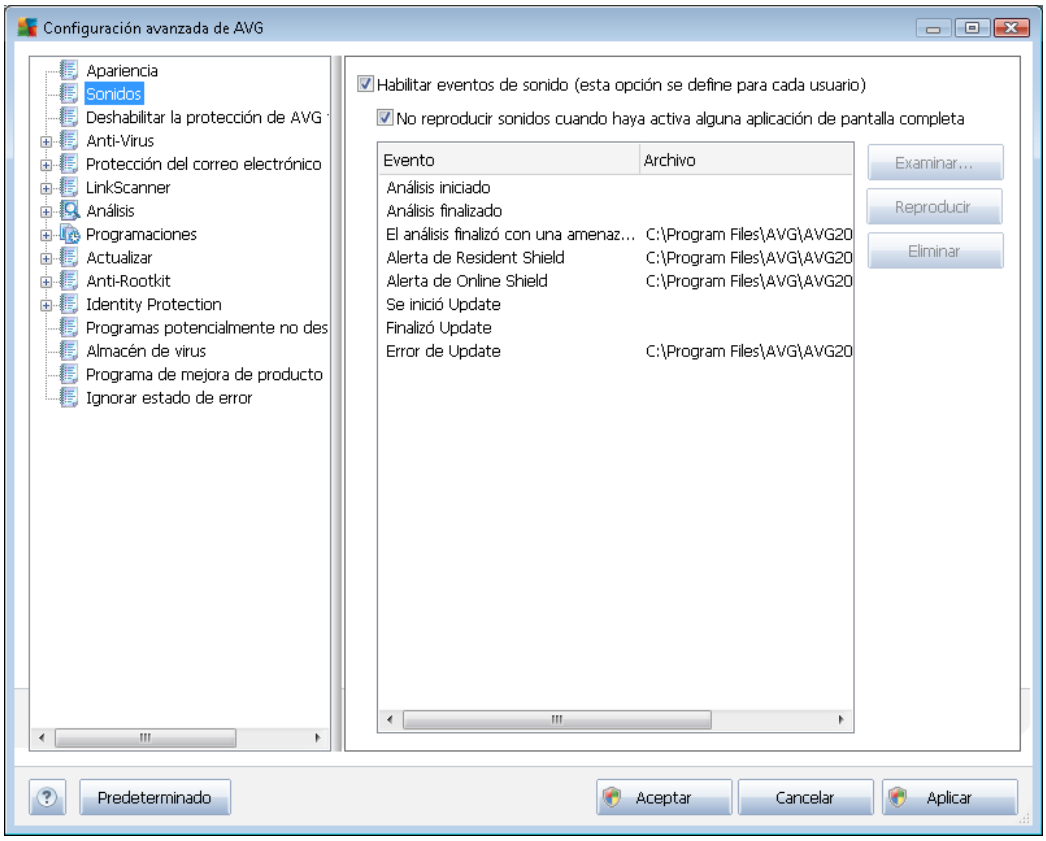


Modo de juego

Esta función de AVG está diseñada para aplicaciones de pantalla completa en las que los globos de información de AVG (*mostrados, por ejemplo, al iniciarse un análisis programado*) pueden resultar molestos (*minimizando la aplicación o dañando sus gráficos*). Para evitar esta situación, mantenga marcada la casilla de verificación correspondiente a la opción ***Activar el modo de juego cuando se ejecute una aplicación en pantalla completa*** (*configuración predeterminada*).

9.2. Sonidos

En el cuadro de diálogo ***Sonidos*** puede especificar si desea recibir información sobre acciones específicas de **AVG Internet Security 2012** mediante una notificación sonora:



La configuración solamente es válida para la cuenta de usuario actual. Es decir, cada usuario del equipo tiene su propia configuración de sonido. Si desea permitir las notificaciones de sonido, mantenga la opción ***Habilitar eventos de sonido*** marcada (*la opción está activada de forma predeterminada*) para activar la lista de todas las acciones relevantes. Además, podría desear marcar la opción ***No reproducir sonidos cuando haya activa alguna aplicación de pantalla completa*** para suprimir las notificaciones sonoras en las situaciones en las que podrían resultar molestas *(consulte también la sección Modo de juego en el capítulo Configuración avanzada/ Apariencia de este documento)*.

Botones de control

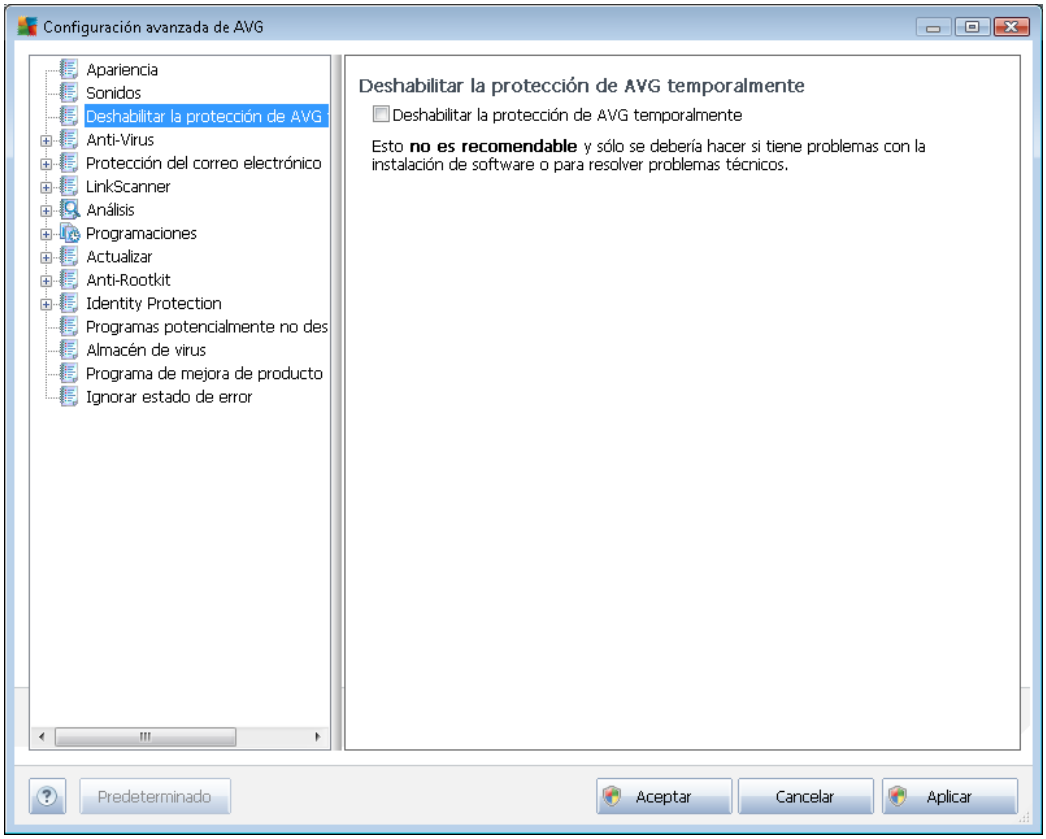
- ***Examinar***: tras seleccionar el evento seleccionado de la lista, utilice el botón ***Examinar*** para buscar en el disco duro el sonido que desea asignar a este evento. *(Tenga en cuenta que sólo se admiten archivos de sonido *.wav en este momento.)*
- ***Reproducir***: para escuchar el sonido seleccionado, resalte el elemento de la lista y pulse el botón ***Reproducir***.

- ***Eliminar***: utilice el botón ***Eliminar*** para quitar el sonido asignado a un evento específico.

9.3. Deshabilitar la protección de AVG temporalmente

En el cuadro de diálogo ***Deshabilitar la protección de AVG temporalmente*** tiene la opción de deshabilitar toda la protección otorgada por **AVG Internet Security 2012**.

Recuerde que no debe utilizar esta opción a menos que sea absolutamente necesario.



En la mayoría de los casos, ***no será necesario*** deshabilitar **AVG Internet Security 2012** antes de instalar un nuevo software o controladores, ni siquiera si el instalador o asistente del software sugiere que primero se cierren programas y aplicaciones para asegurarse de que no ocurrirán interrupciones no deseadas durante el proceso de instalación. Si llegase a tener algún problema durante la instalación, intente desactivar la protección residente (*Habilitar Protección residente*) primero. Si tiene que deshabilitar **AVG Internet Security 2012** temporalmente, vuelva a habilitarlo tan pronto como termine. Si está conectado a Internet o a una red durante el tiempo en que el software antivirus se encuentra desactivado, el equipo está expuesto a sufrir ataques.

Cómo desactivar la protección de AVG

- Marque la casilla de verificación ***Deshabilitar la protección de AVG temporalmente*** y confirme su elección con el botón ***Aplicar***

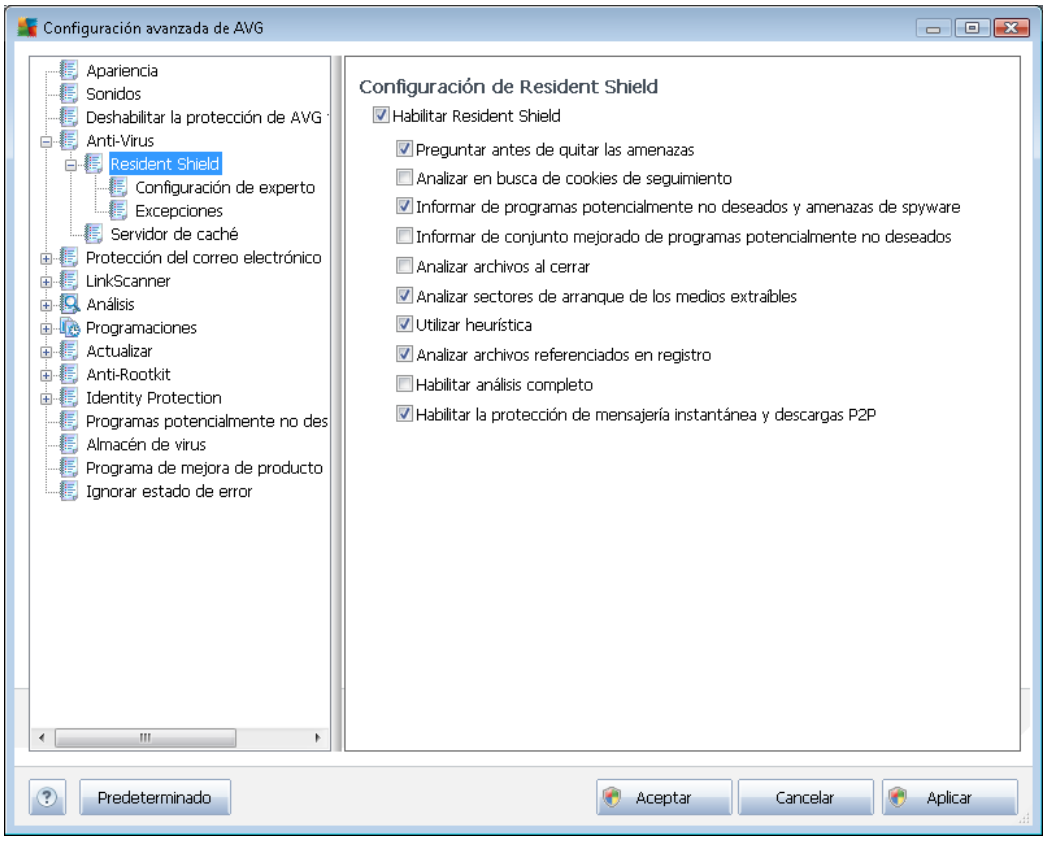
- En el cuadro de diálogo recién abierto ***Deshabilitar protección de AVG temporalmente***, especifique durante cuánto tiempo desea deshabilitar **AVG Internet Security 2012**. De manera predeterminada, la protección se desactivará durante 10 minutos, que debería ser suficiente para realizar cualquier tarea común como instalar nuevo software, etc. Tenga en cuenta que el plazo inicial que posiblemente se puede establecer es de 15 minutos y que, por motivos de seguridad, no puede ser reemplazado por un valor personalizado. Tras el periodo de tiempo especificado, todos los componentes desactivados se activarán de nuevo automáticamente.

9.4. Anti-Virus

Escriba aquí el texto del tema.

9.4.1. Protección residente

Protección residente realiza una protección instantánea de archivos y carpetas contra virus, spyware y demás software malicioso.



En el cuadro de diálogo ***Configuración de Protección residente*** puede activar o desactivar la protección residente completamente marcando o dejando en blanco el elemento ***Habilitar Protección residente*** (*esta opción está activada de manera predeterminada*). Además puede seleccionar las características de la protección residente que deben activarse:

- ***Analizar en busca de cookies de seguimiento*** (*desactivado manera predeterminada*): este parámetro define que deben detectarse las cookies durante el análisis. (*Las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos.*)

- ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de manera predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada manera predeterminada*): marque esta opción para detectar un paquete

extendido de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

- ***Analizar archivos al cerrar*** (*desactivada de manera predeterminada*): realizar un análisis al cerrar asegura que AVG analizará objetos activos (p. ej., aplicaciones, documentos...) en el momento de abrirse y también cuando se cierren; esta característica protege el equipo contra algunos tipos sofisticados de virus.

- ***Analizar sectores de arranque de los medios extraíbles*** (*activada de manera predeterminada*)

- ***Utilizar heurística*** (*activada de manera predeterminada*): se utilizará el análisis heurístico para detectar virus (*emulación dinámica de las instrucciones del objeto analizado en un entorno de equipo virtual*).

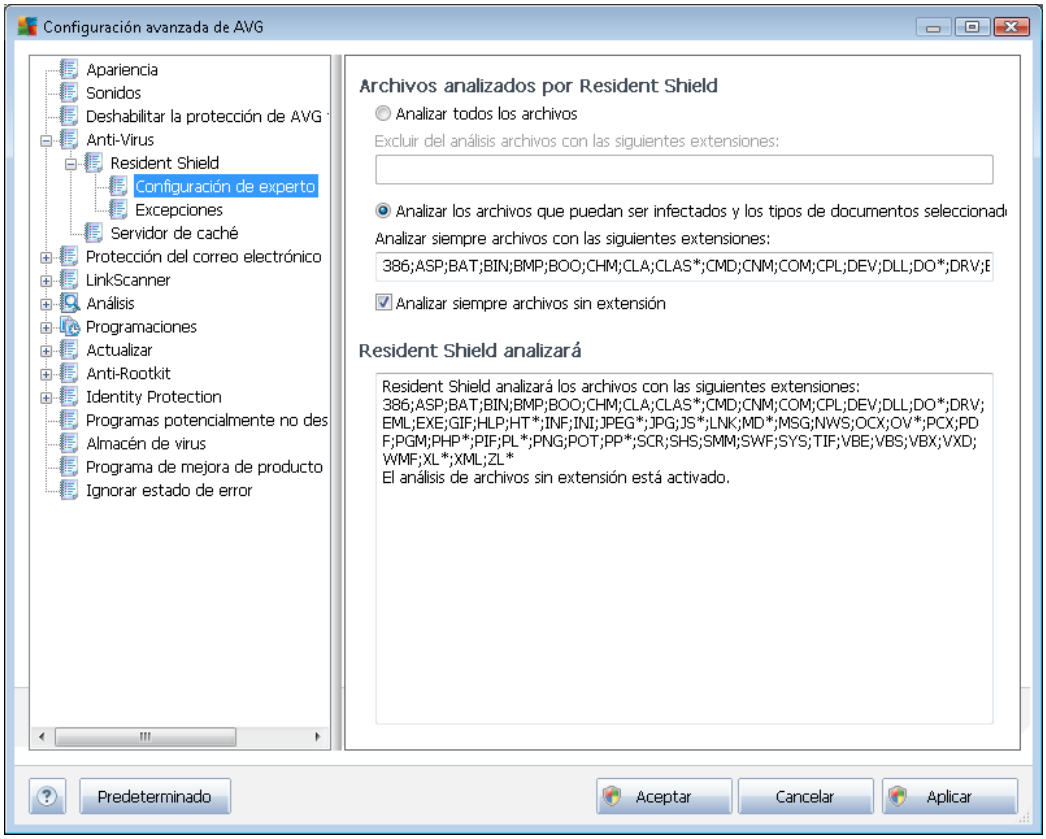
- ***Quitar todas las amenazas automáticamente*** (*desactivada de manera predeterminada*): cualquier infección detectada se reparará automáticamente si hay una cura disponible, y todas las infecciones que no puedan repararse se quitarán.

- ***Analizar archivos referenciados en 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 en el siguiente inicio del equipo.

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en situaciones específicas (*en un estado de emergencia extrema*) puede marcar esta opción para activar los algoritmos más completos que comprobarán minuciosamente todos los objetos que puedan constituir una amenaza. Recuerde, sin embargo, que este método tiene una duración considerable.

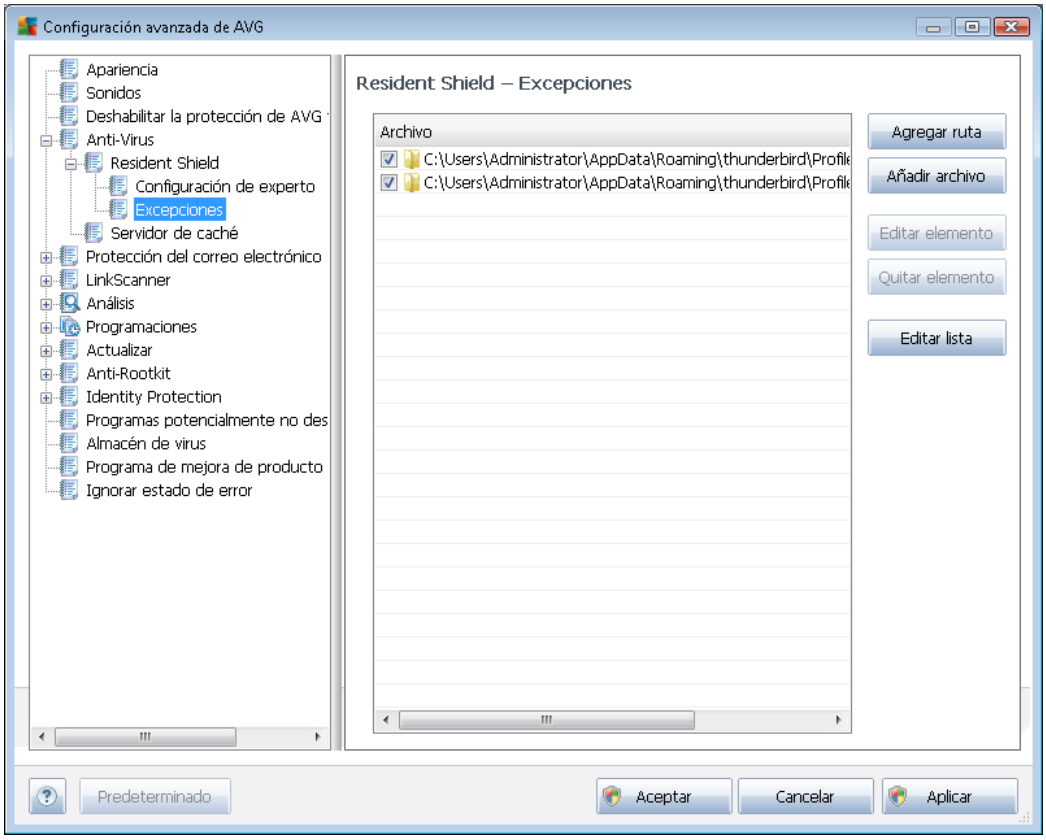
- ***Habilitar la protección de mensajería instantánea y descargas P2P*** (*activado de manera predeterminada*): marque este elemento si desea comprobar que las comunicaciones de mensajería instantánea (*p. ej., ICQ, MSN Messenger, etc.*) y descargas P2P están libres de virus.

En el cuadro de diálogo ***Archivos analizados por Protección residente*** se pueden configurar los archivos a analizar (*por extensiones específicas*):



Marque la casilla de verificación respectiva para decidir si desea ***Analizar todos los archivos*** o ***Analizar los archivos que puedan ser infectados y los tipos de documentos seleccionados*** solamente. Si decide marcar la última opción, podrá especificar una lista de las extensiones que definen los archivos que se deben excluir del análisis, y también una lista de las extensiones que definen los archivos que se deben analizar en todas las circunstancias.

En la sección inferior denominada ***Protección residente analizará*** se resume la configuración actual y se muestra una vista detallada de lo que ***Protección residente*** analizará realmente.



El cuadro de diálogo ***Protección residente - Excepciones*** ofrece la posibilidad de definir archivos y/o carpetas que deberán ser excluidos del análisis de ***Protección residente***.

Si no es esencial, se recomienda encarecidamente no excluir ningún elemento.

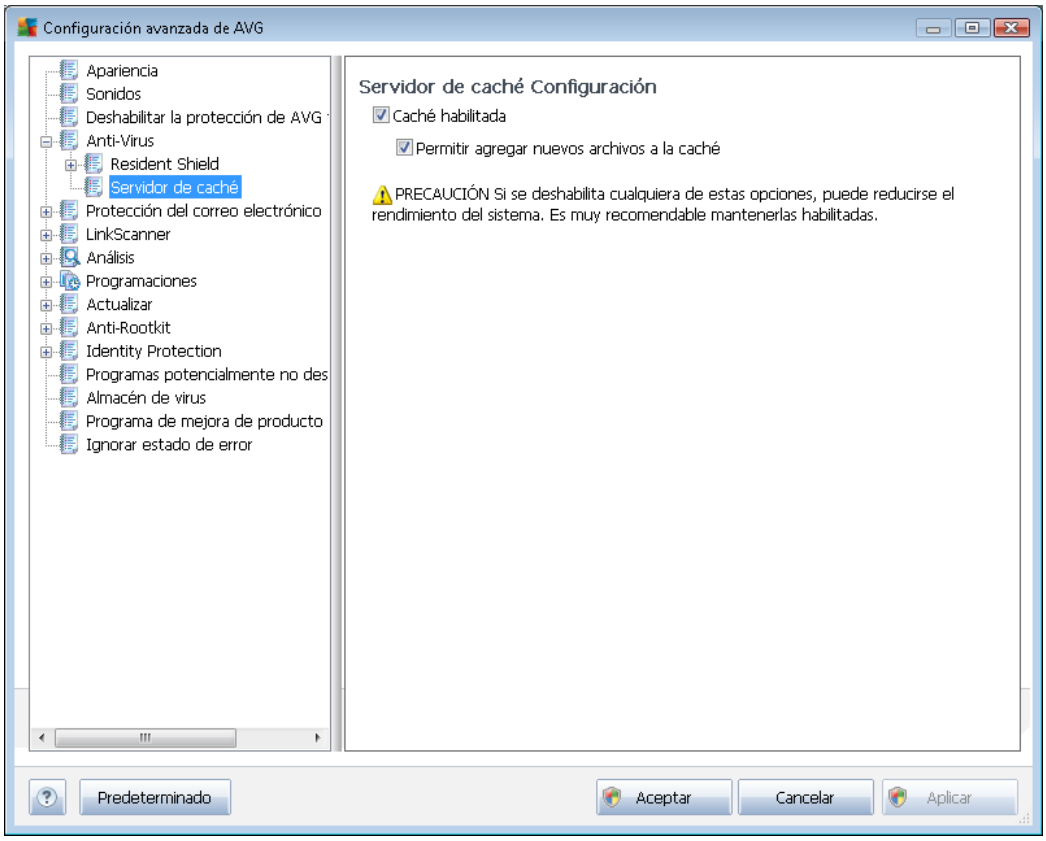
Botones de control

El cuadro de diálogo incluye los siguientes botones de control:

- ***Agregar ruta***: especifique los directorios a excluir del análisis seleccionándolos uno por uno en el árbol de navegación del disco local
- ***Agregar archivo***: especifique los archivos a excluir del análisis seleccionándolos uno por uno en el árbol de navegación del disco local
- ***Editar elemento***: permite editar la ruta especificada de un archivo o una carpeta seleccionados
- ***Quitar elemento***: le permite eliminar de la lista la ruta de un elemento seleccionado
- ***Editar lista***: le permite editar la lista completa de excepciones definidas en un nuevo cuadro de diálogo que funciona como un editor de texto estándar

9.4.2. Servidor de caché

El cuadro de diálogo ***Configuración del servidor de caché*** se refiere al proceso del servidor de caché destinado a agilizar todos los tipos de análisis de **AVG Internet Security 2012**:



El servidor de caché recopila y mantiene información de archivos fiables (*un archivo se considera fiable si está firmado con firma digital de una fuente de confianza*). Estos archivos se consideran automáticamente como seguros y no necesitan volver a analizarse; por tanto, se excluyen del análisis.

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

- ***Caché habilitada*** (*activada de forma predeterminada*): deje en blanco esta casilla de verificación para desactivar ***Servidor de caché*** y vaciar la memoria caché. Tenga en cuenta que la velocidad del análisis y el rendimiento general del equipo pueden disminuir, dado que se analizará primero cada archivo que esté en uso para comprobar si tiene virus y spyware.

- ***Permitir agregar nuevos archivos a la caché*** (*activada de forma predeterminada*): deje en blanco esta casilla de verificación para no añadir más archivos a la memoria caché. Los archivos que ya se encuentren en la memoria caché se conservarán y se utilizarán hasta que se desactive por completo el uso de la memoria caché o hasta que se produzca la siguiente actualización de la base de datos de virus.

A no ser que tenga un buen motivo para desactivar el servidor de caché, recomendamos que

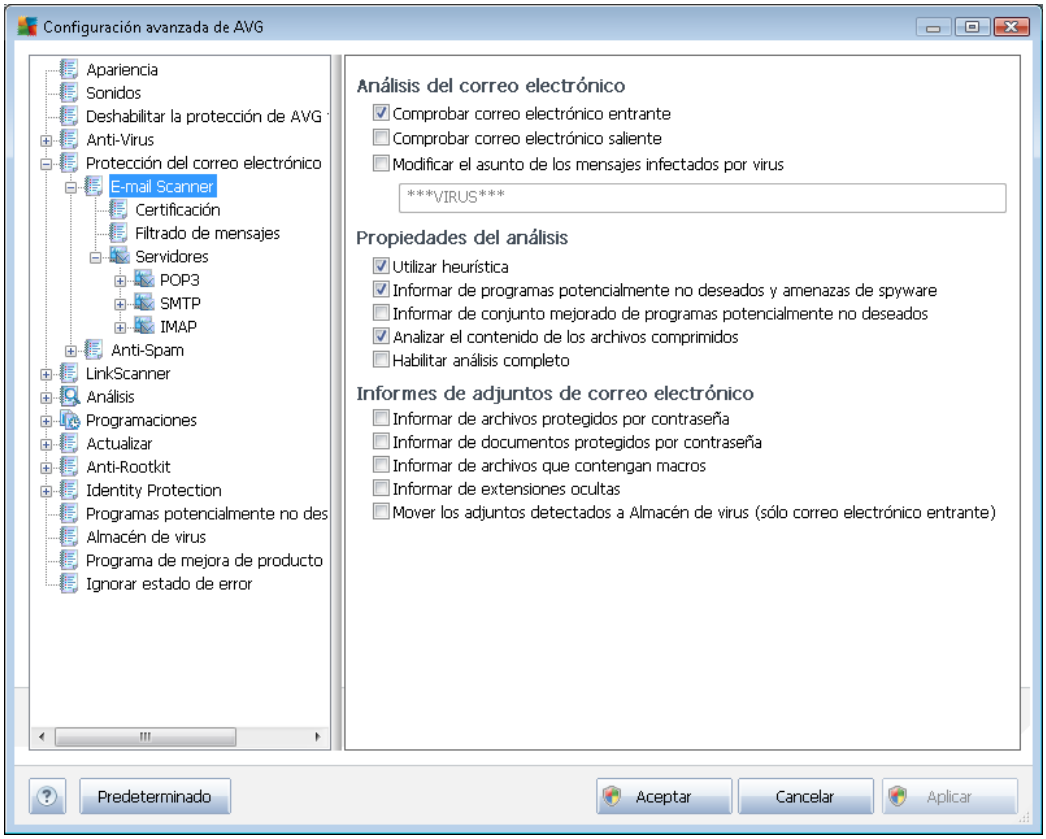
mantenga la configuración predeterminada y deje la opción activada. Si no lo hace, es posible que sufra una reducción importante de la velocidad y el rendimiento del sistema.

9.5. Protección del correo electrónico

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

9.5.1. Analizador de correo electrónico

El cuadro de diálogo ***Analizador de correo electrónico*** se divide en tres secciones:



Análisis del correo electrónico

En esta sección, puede definir los siguientes aspectos básicos para los mensajes de correo electrónico entrantes y/o salientes:

- ***Comprobar correo electrónico entrante*** (*activada de manera predeterminada*): marque esta opción para activar o desactivar el análisis de todos los mensajes entregados en su cliente de correo electrónico
- ***Comprobar correo electrónico saliente*** (*desactivada de manera predeterminada*): marque esta opción para activar o desactivar el análisis de todos los mensajes de correo electrónico enviados desde su cuenta

- ***Modificar el asunto de los mensajes infectados por virus*** (*desactivada de manera predeterminada*): si desea recibir avisos al detectar mensajes de correo electrónico infecciosos, marque esta opción e introduzca el texto que desee en el campo de texto. Este texto se añadirá al campo "Asunto" de cada mensaje de correo electrónico infectado para que resulte más fácil identificarlo y filtrarlo. El valor predeterminado es ***VIRUS***, el cual recomendamos mantener.

Propiedades del análisis

En esta sección, puede especificar de qué manera se analizarán los mensajes de correo electrónico:

- ***Utilizar heurística*** (*activada de manera predeterminada*): marque esta casilla de verificación para usar el método de detección heurístico al analizar mensajes de correo electrónico. Cuando esta opción está activada, los adjuntos de correo electrónico se filtran no sólo según su extensión, sino que también se tiene en cuenta el contenido real del adjunto. El proceso de filtrado se puede configurar en el cuadro de diálogo Filtrado de mensajes.

- ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de manera predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

- ***Analizar el contenido de los archivos comprimidos*** (*activada de manera predeterminada*): marque esta opción para que se analice el contenido de los archivos comprimidos adjuntados a mensajes de correo electrónico.

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*por ejemplo, si sospecha que su equipo ha sido infectado por un virus o es víctima de un ataque de vulnerabilidad*), puede marcar esta opción para activar los algoritmos de análisis más profundos, que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

Informes de adjuntos de correo electrónico

En esta sección, puede establecer informes adicionales acerca de archivos potencialmente peligrosos o sospechosos. Tenga en cuenta que no se mostrará ningún aviso, tan sólo se añadirá un texto de certificación al final del mensaje, y todos los informes de ese tipo se enumerarán en el

cuadro de diálogo Detección de Analizador de correo electrónico:

- ***Informar de archivos protegidos por contraseña***: archivos comprimidos (*ZIP, RAR, etc.*) que están protegidos por contraseña y que no se pueden analizar en busca de virus. Marque esta opción para que el programa informe de estos archivos como posiblemente peligrosos.

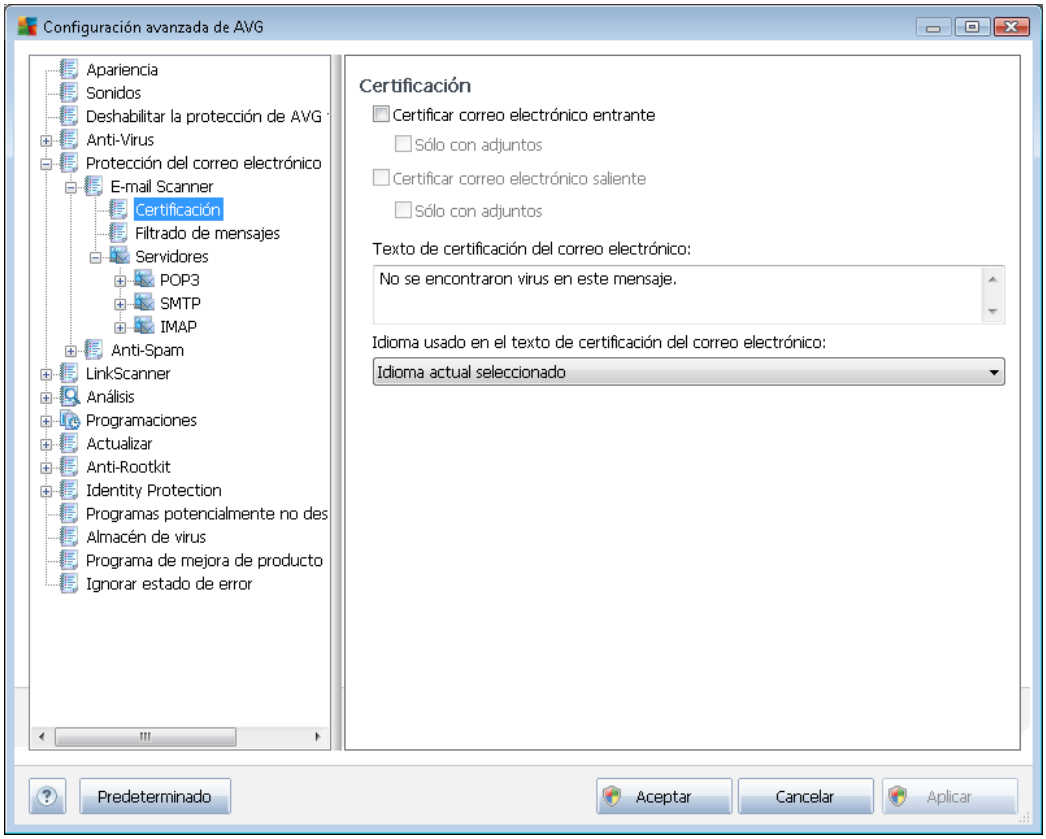
- ***Informar de documentos protegidos por contraseña***: documentos que están protegidos por contraseña y que no se pueden analizar en busca de virus. Marque esta opción para que el programa informe de estos documentos como posiblemente peligrosos.

- ***Informar de archivos que contengan macros***: una macro es una secuencia predefinida de pasos que tiene como objetivo facilitar ciertas tareas para el usuario (*las macros de MS Word son muy conocidas*). Dada su naturaleza, una macro puede contener instrucciones posiblemente peligrosas y quizás desee marcar esta casilla de verificación para asegurarse de que el programa informe de los archivos con macros como sospechosos.

- ***Informar de extensiones ocultas***: una extensión oculta puede hacer que un archivo ejecutable sospechoso "algo.txt.exe" se muestre como un inofensivo archivo de texto sin formato "algo.txt". Marque esta casilla de verificación para que el programa informe de este tipo de archivos como posiblemente peligroso.

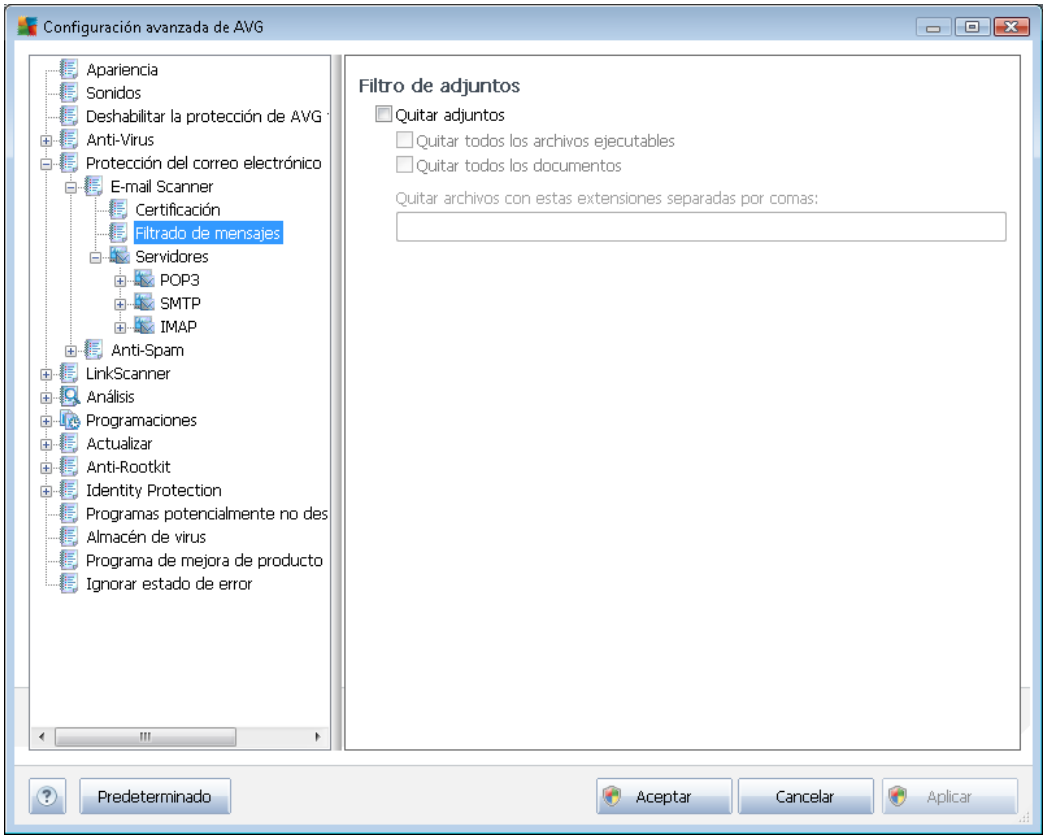
- ***Mover los adjuntos detectados a Almacén de virus***: indique si desea recibir notificaciones por correo electrónico sobre archivos comprimidos protegidos por contraseña, documentos protegidos por contraseña, archivos que contengan macros y/o archivos con extensión oculta detectados como datos adjuntos del mensaje de correo electrónico analizado. Si durante el análisis se identifica un mensaje de este tipo, indique si el objeto infeccioso detectado se debe mover al Almacén de virus.

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



De forma predeterminada, el texto de la certificación consiste en información básica que indica *No se encontraron virus en este mensaje.* Sin embargo, esta información se puede ampliar o cambiar según sus necesidades: escriba el texto deseado para la certificación en el campo de texto ***Texto de certificación del correo electrónico***. En la sección ***Idioma usado en el texto de certificación del correo electrónico*** puede definir en qué idioma se debe mostrar la parte de la certificación generada automáticamente (*No se encontraron virus en este mensaje*).

Nota: *tenga en cuenta que sólo el texto predeterminado se mostrará en el idioma establecido y que su texto personalizado no se traducirá automáticamente.*



En el cuadro de diálogo ***Filtro de adjuntos***, puede configurar parámetros que se utilizarán para analizar los adjuntos a los mensajes de correo electrónico. De manera predeterminada, la opción ***Quitar adjuntos*** se encuentra desactivada. Si decide activarla, todos los adjuntos a los mensajes de correo electrónico que se consideren infecciosos o potencialmente peligrosos se quitarán de manera automática. Si desea definir qué tipos específicos de adjuntos se deberían quitar, seleccione la opción que corresponda:

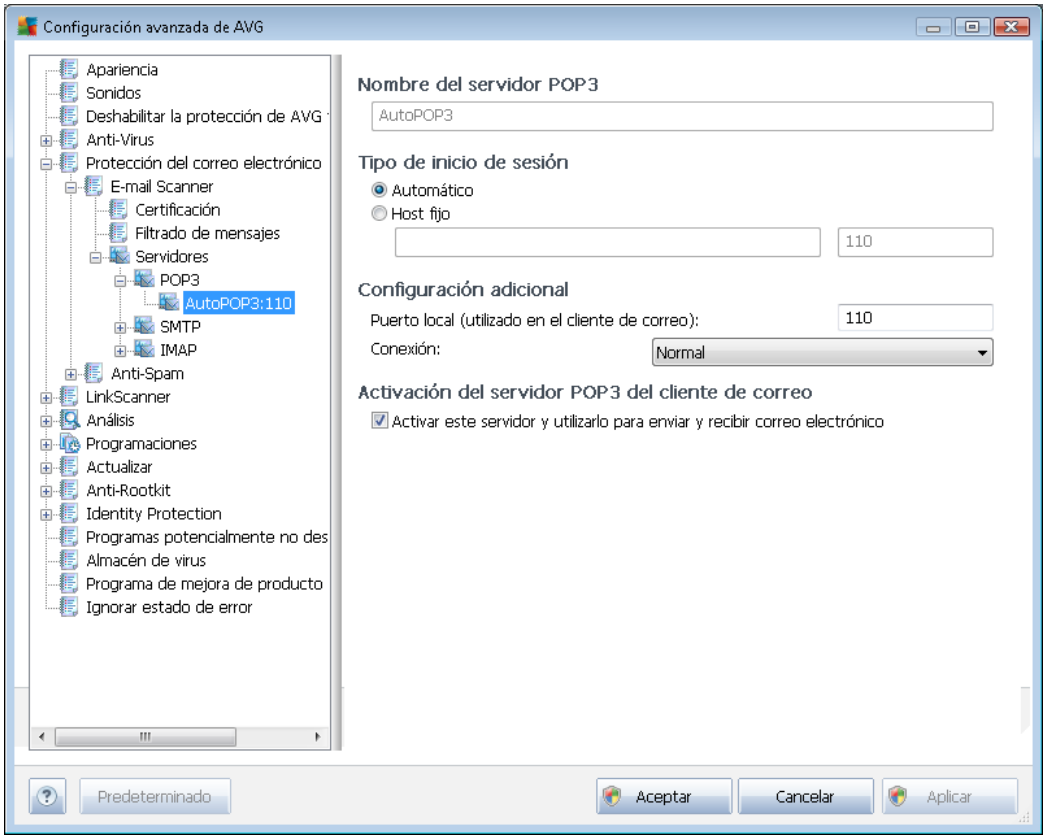
- ***Quitar todos los archivos ejecutables***: se eliminarán todos los archivos *.exe.
- ***Quitar todos los documentos***: se eliminarán todos los archivos *.doc, *.docx, *.xls, *.xlsx.
- ***Quitar archivos con estas extensiones separadas por comas***: se eliminarán todos los archivos con las extensiones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

En la sección ***Servidores*** puede editar los parámetros de los servidores del Analizador de correo electrónico:

- Servidor POP3
- Servidor SMTP

- Servidor IMAP

Igualmente, también puede definir un nuevo servidor para correo electrónico entrante o saliente por medio del botón ***Agregar nuevo servidor***.



En este cuadro de diálogo (*que se abre mediante **Servidores / POP3***), puede configurar un nuevo servidor para el Analizador de correo electrónico empleando el protocolo POP3 para el correo electrónico entrante:

- ***Nombre de servidor POP3***: en este campo, puede especificar el nombre de servidores recientemente añadidos (*para añadir un servidor POP3, haga clic con el botón secundario del ratón sobre el elemento POP3 del menú de navegación izquierdo*). Para el servidor "AutoPOP3" creado automáticamente, este campo está desactivado.

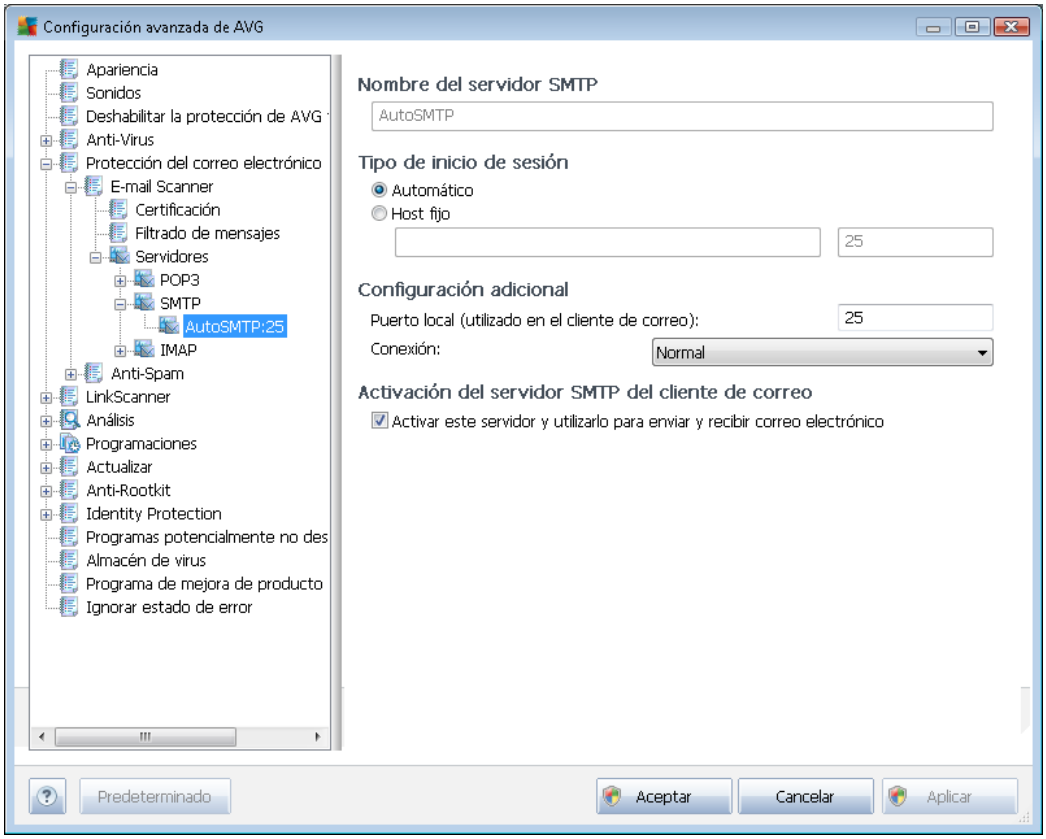
- ***Tipo de inicio de sesión***: define el método para determinar el servidor utilizado para el correo electrónico entrante:

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

    - ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. El nombre empleado para iniciar sesión permanece igual. Por ejemplo, puede usar un nombre de dominio

(*como pop.acme.com*) o una dirección IP (*como 123.45.67.89*). Si el servidor de correo electrónico emplea un puerto no estándar, puede especificar este puerto después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, pop.acme.com:8200*). El puerto estándar para las comunicaciones POP3 es el 110.

- ***Configuración adicional***: permite especificar parámetros más detallados:
  - ***Puerto local***: especifica el puerto en que debería esperarse la comunicación de la aplicación de correo electrónico. Luego, debe indicar en la aplicación de correo electrónico este puerto como el puerto para la comunicación POP3.
  - ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos se envían cifrados sin riesgo de que otra persona pueda rastrearlos o supervisarlos. Esta característica también está disponible únicamente si el servidor de correo electrónico de destino la admite.
- ***Activación del servidor POP3 del cliente de correo***: marque o deje en blanco este elemento para activar o desactivar el servidor POP3 especificado



En este cuadro de diálogo (*que se abre a través de **Servidores / SMTP***), puede configurar un nuevo servidor de Analizador de correo electrónico utilizando el protocolo SMTP para el correo electrónico

saliente:

- ***Nombre de servidor SMTP***: en este campo, puede especificar el nombre de servidores recientemente añadidos (*para añadir un servidor SMTP, haga clic con el botón secundario del ratón sobre el elemento SMTP del menú de navegación izquierdo*). Para el servidor "AutoSMTP" creado automáticamente, este campo se encuentra desactivado.

- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo que se usará para el correo electrónico saliente:

    - ***Automático***: el inicio de sesión se efectuará automáticamente en función de la configuración del cliente de correo electrónico

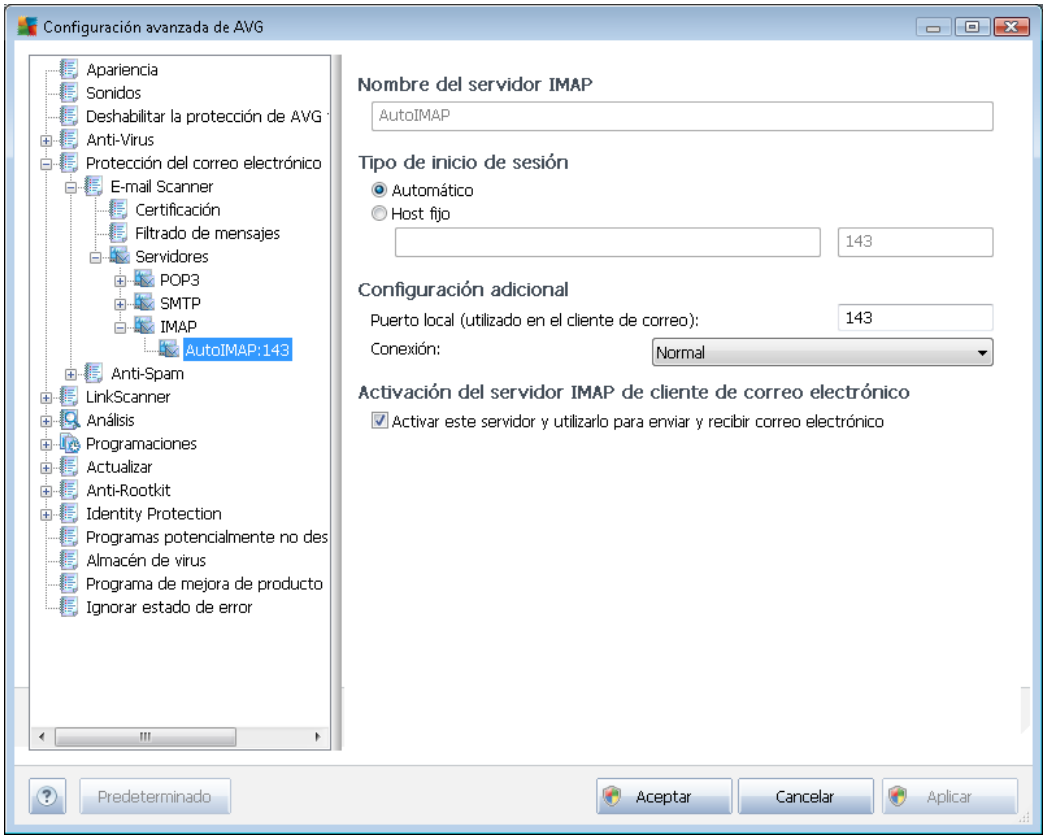
    - ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. Como nombre puede usar un nombre de dominio (*por ejemplo, smtp.acme.com*) o una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo electrónico emplea un puerto no estándar, puede especificar este puerto después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, smtp.acme.com:8200*). El puerto estándar para la comunicación SMTP es el 25.

- ***Configuración adicional***: permite especificar parámetros más detallados:

    - ***Puerto local***: especifica el puerto en que debería esperarse la comunicación de la aplicación de correo electrónico. A continuación, debe establecer este puerto como puerto para la comunicación SMTP en la aplicación de correo.

    - ***Conexión***: en este menú desplegable, puede especificar el tipo de conexión a utilizar (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos se envían cifrados sin riesgo de que otra persona pueda rastrearlos o supervisarlos. Esta característica sólo está disponible si el servidor de correo de destino la admite.

- ***Activación del servidor SMTP del cliente de correo***: marque o deje en blanco esta casilla para activar o desactivar el servidor SMTP indicado anteriormente



En este cuadro de diálogo (que se abre a través de ***Servidores / IMAP***), puede configurar un nuevo servidor de Analizador de correo electrónico utilizando el protocolo IMAP para el correo saliente:

- ***Nombre de servidor IMAP***: en este campo, puede especificar el nombre de los servidores agregados recientemente (*para agregar un servidor IMAP, haga clic con el botón secundario del ratón 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 que se usará para el correo electrónico saliente:

    - ***Automático***: el inicio de sesión se efectuará automáticamente en función de la configuración del cliente de correo electrónico

    - ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. Como nombre puede usar un nombre de dominio (*por ejemplo, smtp.acme.com*) o una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo electrónico emplea un puerto no estándar, puede especificar este puerto después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, imap.acme.com:8200*). El puerto estándar para la comunicación IMAP es el 143.

- ***Configuración adicional***: permite especificar parámetros más detallados:

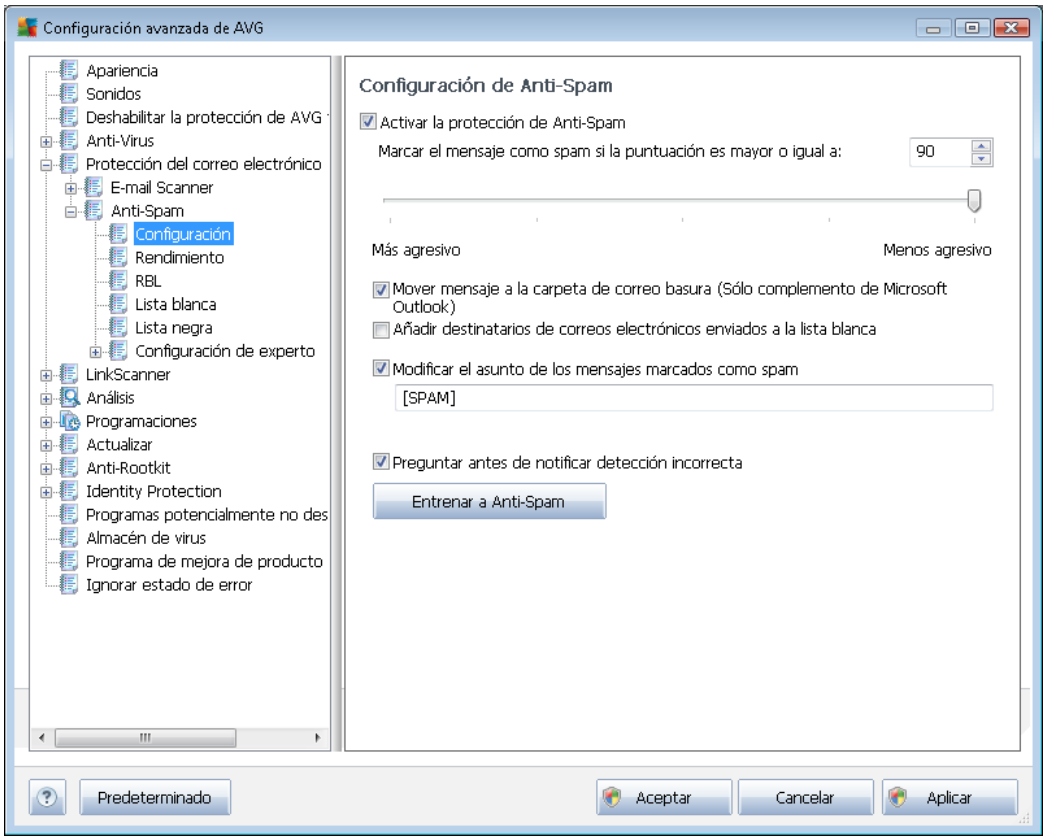
- ***Puerto local***: especifica el puerto en que debería esperarse la comunicación de la aplicación de correo electrónico. A continuación, debe establecer este puerto como puerto para la comunicación IMAP en la aplicación de correo.

- ***Conexión***: en este menú desplegable, puede especificar el tipo de conexión a utilizar (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos se envían cifrados sin riesgo de que otra persona pueda rastrearlos o supervisarlos. Esta característica sólo está disponible si el servidor de correo de destino la admite.

- ***Activación del servidor IMAP del cliente de correo***: marque o deje en blanco esta casilla para activar o desactivar el servidor IMAP indicado anteriormente

9.5.2. Anti-Spam

Escriba aquí el texto del tema.



En el cuadro de diálogo ***Configuración de Anti-Spam*** puede marcar o quitar la marca de la casilla ***Activar la protección Anti-Spam*** para permitir o impedir el análisis anti-spam de la comunicación por correo electrónico. De manera predeterminada, esta opción está activada y, como es habitual, se recomienda mantener esta configuración a menos que se tenga un buen motivo para modificarla.

A continuación, también puede seleccionar valores de puntuación más o menos agresivos. El filtro ***Anti-Spam*** asigna una puntuación a cada mensaje (*es decir, el grado de similitud del contenido del mensaje con el spam*) en función de diversas técnicas de análisis dinámico. Puede ajustar la configuración de ***Marcar el mensaje como spam si la puntuación es mayor o igual a***

introduciendo un valor o moviendo el control deslizante hacia la izquierda o hacia la derecha (*el intervalo del valor está limitado entre 50 y 90*).

En general se recomienda definir un umbral comprendido entre 50 y 90 o, si no se está seguro, en 90. A continuación se ofrece un resumen del umbral de puntuación:

- ***Valor 80-90***: los mensajes de correo electrónico con alta probabilidad de ser spam se filtrarán. También pueden filtrarse erróneamente algunos mensajes que no son spam.
- ***Valor 60-79***: considerada como una configuración bastante agresiva. Los mensajes que posiblemente puedan ser spam se filtrarán. Es probable que también se retengan mensajes que no son spam.
- ***Valor 50-59***: configuración muy agresiva. Es probable que los mensajes de correo electrónico que no son spam se identifiquen como mensajes de spam auténticos. Este intervalo no se recomienda para uso normal.

En el cuadro de diálogo ***Configuración de Anti-Spam*** puede definir cómo se deben tratar los mensajes de correo electrónico de spam:

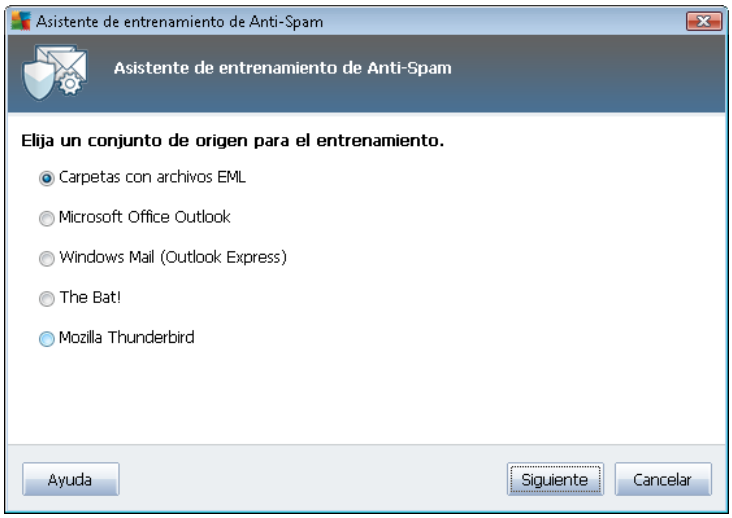
- ***Mover mensaje a la carpeta de correo basura***: marque esta casilla de verificación para indicar que todos los mensajes de spam detectados deben moverse automáticamente a la carpeta de correo basura específica de su cliente de correo electrónico;
- ***Añadir destinatarios de correos electrónicos enviados a la lista blanca***: marque esta casilla de verificación para confirmar que todos los destinatarios de los correos electrónicos enviados son de confianza y que todos los mensajes procedentes de sus cuentas se pueden entregar;
- ***Modificar el asunto de los mensajes marcados como spam***: marque esta casilla de verificación si desea que todos los mensajes detectados como spam se marquen con una palabra o un carácter concreto en el campo de asunto del correo electrónico; el texto deseado se puede escribir el campo de texto activo.
- ***Preguntar antes de notificar detección incorrecta***: siempre que durante el proceso de instalación haya aceptado participar en el Programa de mejora de productos. En tal caso, aceptó informar a AVG de las amenazas detectadas. La notificación se procesa automáticamente. No obstante, puede marcar esta casilla de verificación para confirmar que desea ser consultado antes de informar a AVG sobre spam detectado con el fin de asegurarse de que el mensaje debe clasificarse realmente como spam.

Botones de control

El botón ***Entrenar a Anti-Spam*** abre el Asistente de entrenamiento de Anti-Spam descrito en detalle en el siguiente capítulo.

El primer cuadro de diálogo del ***Asistente de entrenamiento de Anti-Spam*** le pide que seleccione el origen de los mensajes de correo electrónico que desea utilizar para el entrenamiento. Normalmente deseará utilizar correos electrónicos marcados incorrectamente como spam o

mensajes de spam que no han sido reconocidos.



Puede elegir entre las siguientes opciones:

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

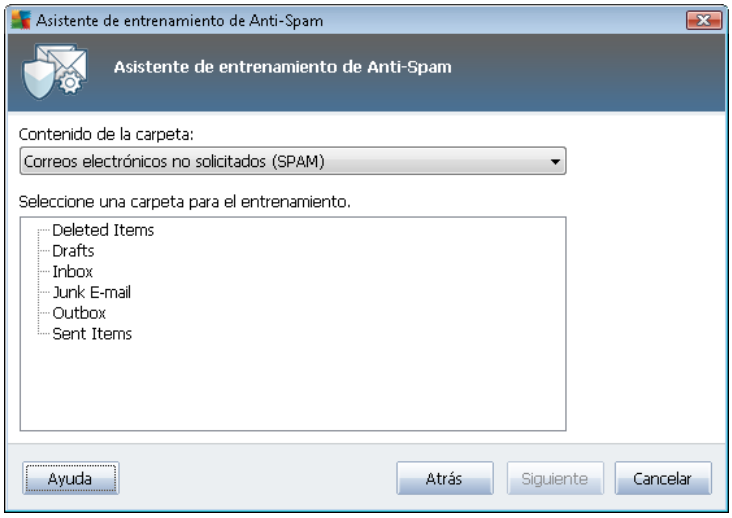
- ***Carpeta con archivos EML***: si utiliza cualquier otro programa de correo electrónico, deberá guardar previamente los mensajes en una carpeta determinada (*en formato .eml*) o asegurarse de que conoce la ubicación de las carpetas de mensajes de su cliente de correo electrónico. A continuación, seleccione ***Carpeta con archivos EML***, que le permite localizar la carpeta deseada en el siguiente paso

Para que el proceso de entrenamiento sea más rápido y fácil, se recomienda ordenar de antemano los correos electrónicos en las carpetas, de manera que la carpeta que utilice para el entrenamiento contenga solamente los mensajes de entrenamiento (deseados o no deseados). No obstante, esto no es necesario, ya que posteriormente podrá filtrar los correos electrónicos.

Seleccione la opción adecuada y haga clic en ***Siguiente*** para continuar con el asistente.

El cuadro de diálogo mostrado en este paso depende de su selección previa.

Carpetas con archivos EML



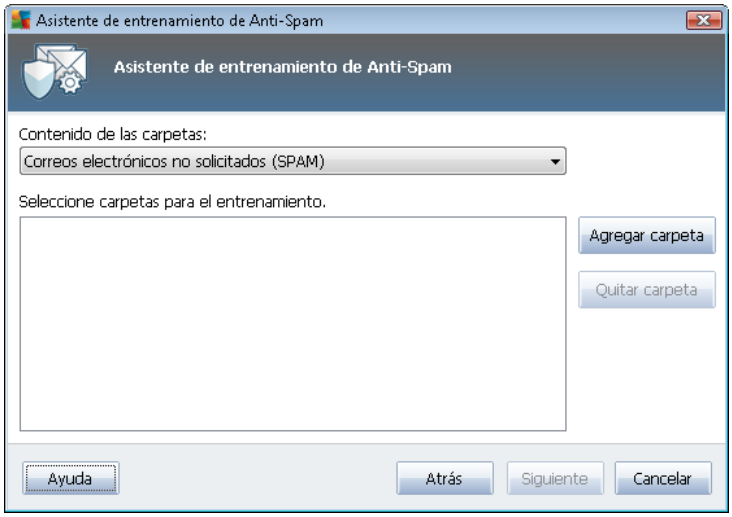
En este cuadro de diálogo, seleccione la carpeta con los mensajes que desea utilizar para el entrenamiento. Pulse el botón ***Agregar carpeta*** para localizar la carpeta con los archivos .eml (*mensajes de correo electrónico guardados*). A continuación, la carpeta seleccionada aparecerá en el cuadro de diálogo.

En el menú desplegable ***Contenido de las carpetas***, defina una de las dos opciones: si la carpeta seleccionada contiene mensajes deseados (*HAM*) o no deseados (*SPAM*). Tenga en cuenta que podrá filtrar los mensajes en el paso siguiente, por lo que no es necesario que la carpeta contenga solamente los correos electrónicos para el entrenamiento. También puede quitar de la lista carpetas que no desee seleccionándolas y haciendo clic en el botón ***Quitar carpeta***.

Cuando haya finalizado, haga clic en ***Siguiente*** y pase a Opciones de filtrado de mensajes.

Cliente de correo electrónico específico

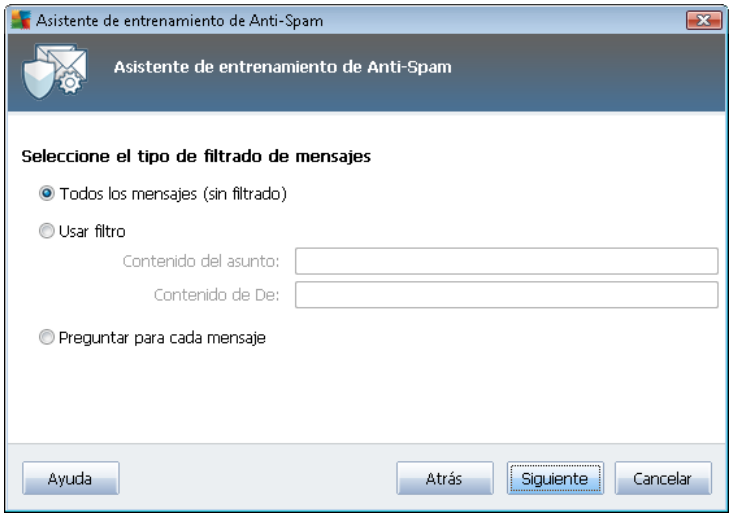
Cuando haya confirmado una de las opciones, aparecerá un nuevo cuadro de diálogo.



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

En el menú desplegable ***Contenido de las carpetas***, defina una de las dos opciones: si la carpeta seleccionada contiene mensajes deseados (*HAM*) o no deseados (*SPAM*). Tenga en cuenta que podrá filtrar los mensajes en el paso siguiente, por lo que no es necesario que la carpeta contenga solamente los correos electrónicos para el entrenamiento. En la sección principal del cuadro de diálogo aparece un árbol de navegación del cliente de correo electrónico seleccionado. Localice en el árbol la carpeta deseada y resáltela con el ratón.

Cuando haya finalizado, haga clic en ***Siguiente*** y pase a Opciones de filtrado de mensajes.



En este cuadro de diálogo puede definir el filtrado de los mensajes de correo electrónico.

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

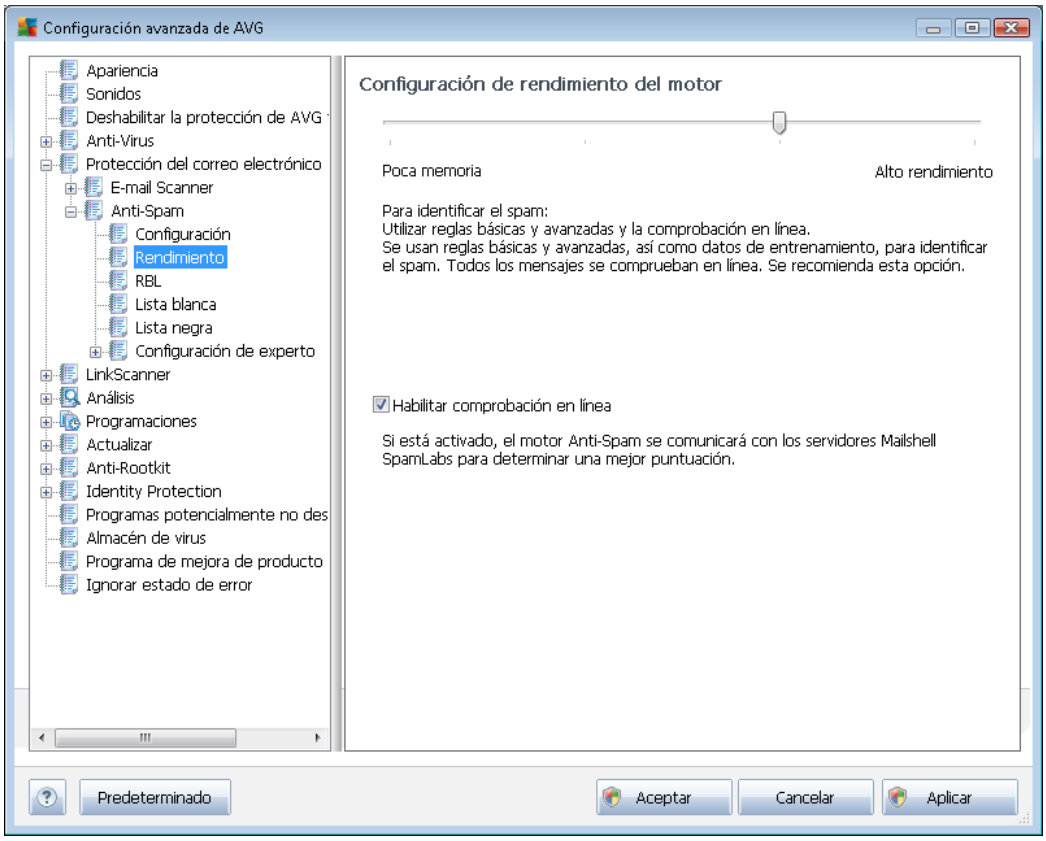
- ***Usar filtro***: si prefiere un filtrado más avanzado, seleccione la opción ***Usar filtro***. Puede escribir una palabra (*nombre*), parte de una palabra o una frase para buscar en el asunto del correo electrónico y/o el campo del remitente. Todos los mensajes que coincidan exactamente con los criterios introducidos se utilizarán para el entrenamiento sin necesidad de seguir interviniendo. Si rellena los dos campos de texto, también se usarán las direcciones que coincidan solamente con una de las condiciones.

- ***Preguntar para cada mensaje***: si tiene dudas acerca de los mensajes que contiene la carpeta y desea que el asistente le pregunte sobre cada mensaje *(para que pueda indicar si desea utilizarlo para el entrenamiento o no)*, seleccione la opción ***Preguntar para cada mensaje***.

Cuando haya seleccionado la opción apropiada, haga clic en ***Siguiente***. El siguiente cuadro de diálogo es meramente informativo y le indica que el asistente está preparado para procesar los mensajes. Para comenzar el entrenamiento, vuelva a hacer clic en el botón ***Siguiente***. El

entrenamiento se iniciará según las condiciones seleccionadas con anterioridad.

El cuadro de diálogo ***Configuración de rendimiento del motor*** (*al que se accede mediante el elemento* ***Rendimiento*** *del panel de navegación izquierdo*) ofrece la configuración de rendimiento del componente ***Anti-Spam***:



Mueva el control deslizante hacia la izquierda o la derecha para cambiar el nivel de rendimiento del análisis entre los modos ***Poca memoria*** / ***Alto rendimiento***.

- ***Poca memoria***: durante el proceso de análisis para identificar el spam, no se utilizará ninguna regla. Sólo se emplearán datos de entrenamiento para la identificación. Este modo no se recomienda para uso común, a menos que el equipo cuente con escasos recursos de hardware.

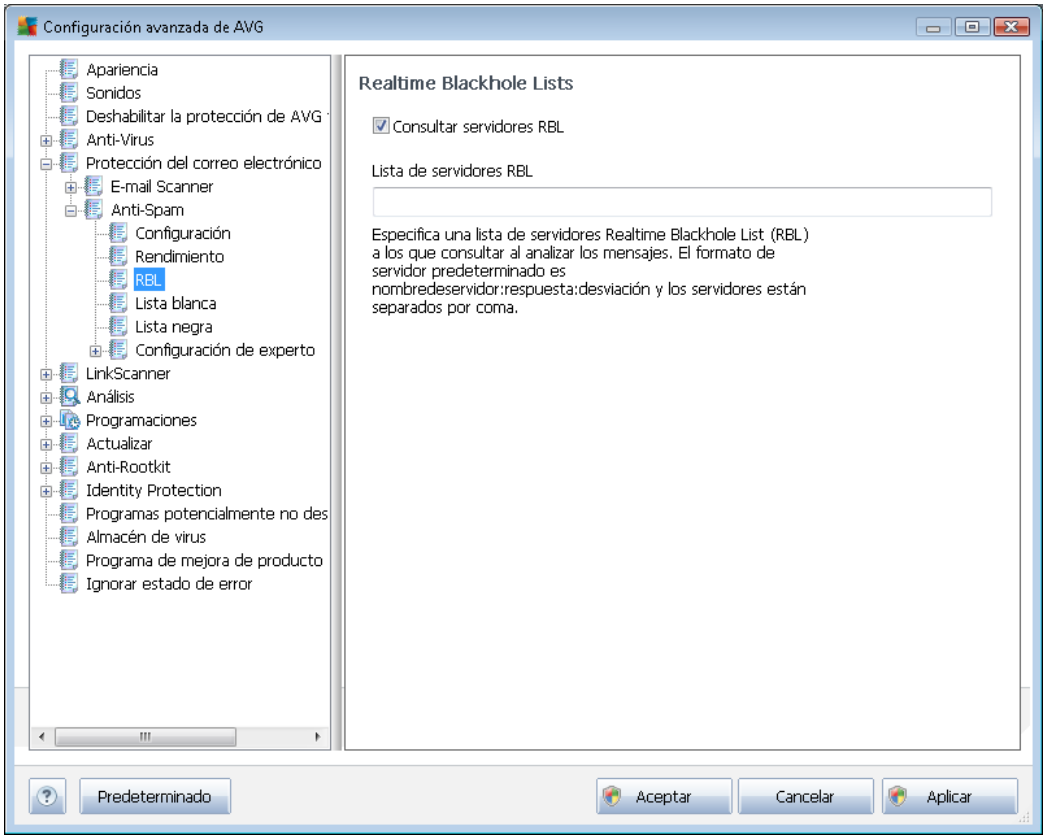
- ***Alto rendimiento***: este modo consumirá una gran cantidad de memoria. Durante el proceso de análisis realizado para detectar spam, se emplearán las siguientes características: reglas y caché de base de datos de spam, reglas básicas y avanzadas, direcciones IP de remitentes que envían spam y bases de datos de remitentes que envían spam.

El elemento ***Habilitar comprobación en línea*** está activado de manera predeterminada. En consecuencia, se obtiene una detección más precisa del spam gracias a la comunicación con los servidores Mailshell; es decir, los datos analizados se compararán con el contenido de la base de

datos de Mailshell en línea.

En términos generales, se recomienda mantener la configuración predeterminada y cambiarla únicamente si existe algún motivo que en verdad justifique hacerlo. Cualquier cambio en la configuración sólo debe ser realizado por usuarios expertos.

El elemento ***RBL*** abre un cuadro de diálogo de edición llamado ***Realtime Blackhole Lists*** donde puede activar o desactivar la función ***Consultar servidores RBL***:

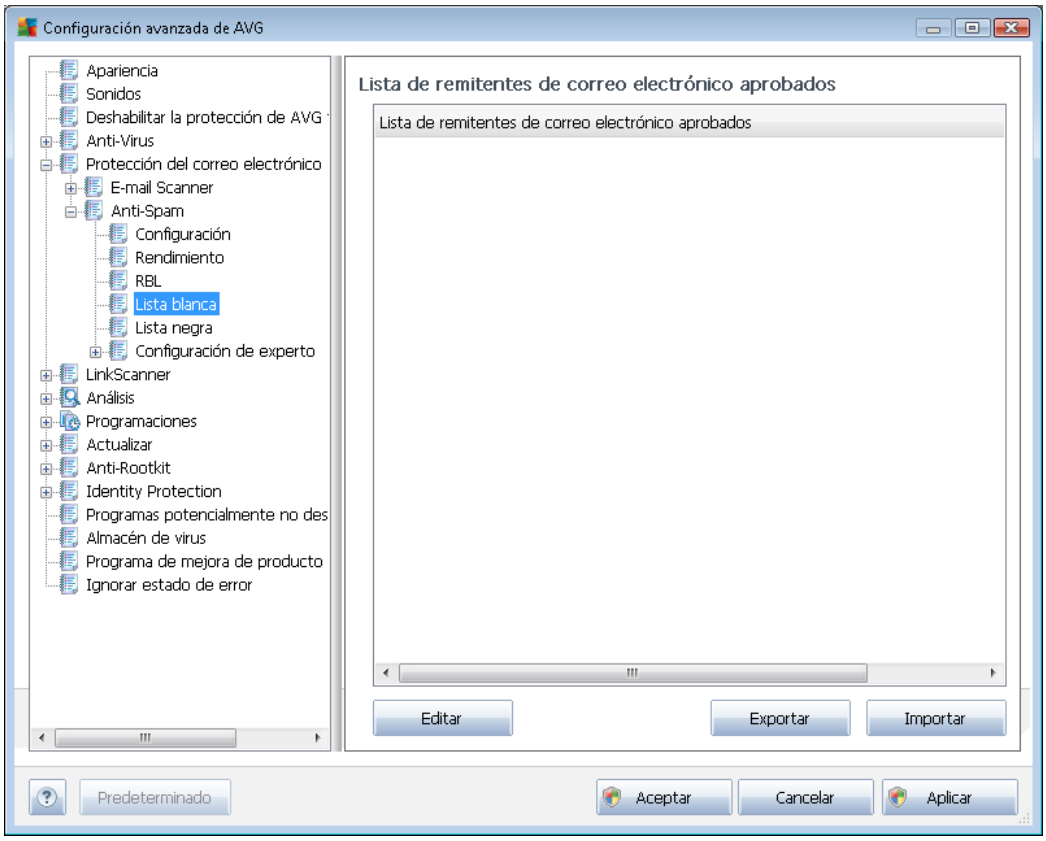


Un servidor RBL (*Realtime Blackhole List*) es un servidor DNS con una extensa base de datos de remitentes que se sabe suelen enviar correo no deseado (spam). Cuando esta característica está activada, todos los mensajes de correo electrónico se verifican comparándolos con la base de datos del servidor RBL y se marcan como spam si coinciden con alguna de las entradas de la base de datos. Las bases de datos de los servidores RBL contienen las últimas huellas dactilares de spam, actualizadas al minuto, lo que proporciona una detección del spam sumamente precisa y eficiente. Esta característica es útil en especial para aquellos usuarios que reciben grandes cantidades de spam que el motor Anti-Spam normalmente no detecta.

La ***Lista de servidores RBL*** le permite definir ubicaciones específicas de los servidores RBL (*tenga en cuenta que el hecho de habilitar esta característica puede hacer que el proceso de recepción de correos electrónicos se vuelva más lento en algunos sistemas y configuraciones, dado que se debe verificar cada mensaje según la base de datos de servidores RBL).*

No se envía ningún dato personal al servidor.

El elemento ***Lista blanca*** abre un cuadro de diálogo llamado ***Lista de remitentes de correo electrónico aprobados*** con una lista global de direcciones de correo electrónico y nombres de dominio de remitentes que nunca se marcarán como spam.



En la interfaz de edición puede compilar una lista de remitentes de los que tiene la seguridad que nunca le enviarán mensajes no deseados (spam). Del mismo modo, puede compilar una lista de nombres de dominio completos (*por ejemplo, avg.com*), que sabe que no generan mensajes de spam. Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo.

Botones de control

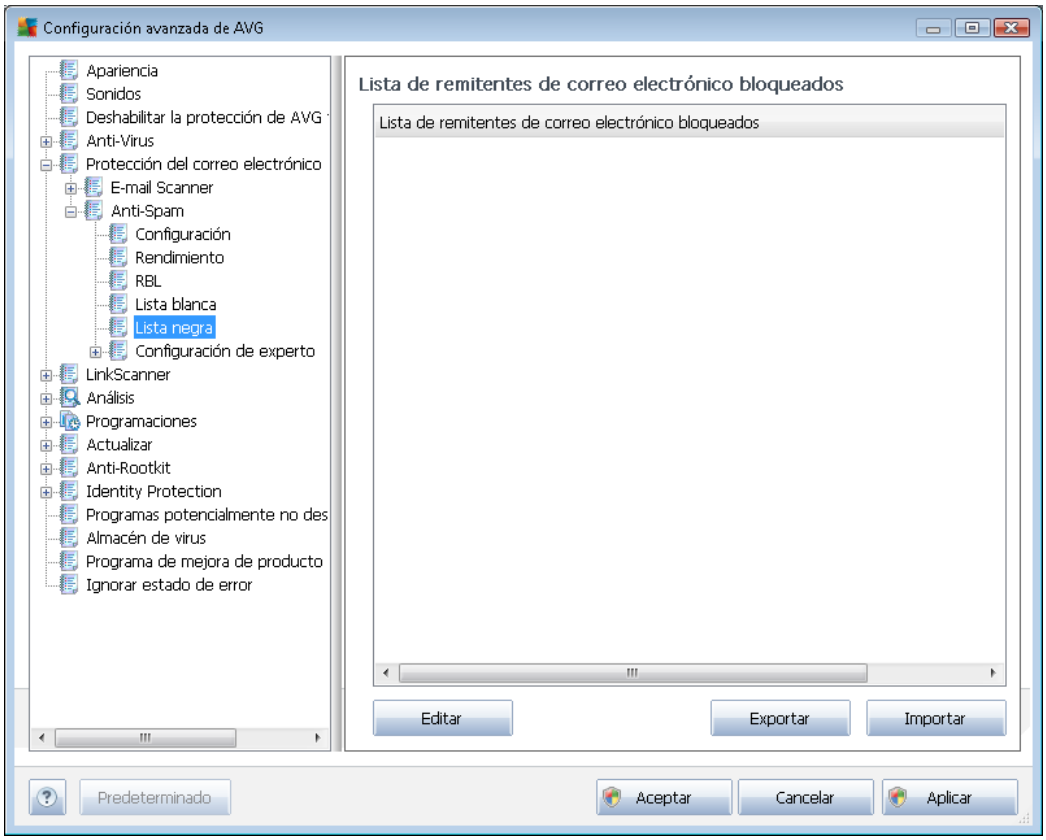
Los botones de control disponibles son los siguientes:

- ***Editar***: pulse este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (también puede *copiar y pegar*). Inserte un elemento (*remitente, nombre de dominio*) por línea.

- ***Exportar***: si por algún motivo decide exportar los registros, puede hacerlo pulsando este botón. Todos los registros se guardarán en un archivo de texto sin formato.

- ***Importar***: si ya tiene preparado un archivo de texto de direcciones de correo electrónico/ nombres de dominio, puede importarlo seleccionando este botón. El contenido del archivo debe tener únicamente un elemento (*dirección, nombre de dominio*) por línea.

El elemento ***Lista negra*** abre un cuadro de diálogo con una lista global de direcciones de correo electrónico y nombres de dominio de remitentes bloqueados cuyos mensajes siempre se marcarán como spam.



Puede compilar una lista de remitentes de los que espera recibir mensajes no deseados (*spam*) en la interfaz de edición. Del mismo modo, puede compilar una lista de nombres de dominio completos (*por ejemplo, empresadespam.com*) de los que espera o recibe mensajes de spam. Todo el correo electrónico procedente de las direcciones o de los dominios enumerados se identificará como spam. Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo.

Botones de control

Los botones de control disponibles son los siguientes:

- ***Editar***: pulse este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (también puede *copiar y pegar*). Inserte un elemento (*remitente, nombre de dominio*) por línea.
- ***Exportar***: si por algún motivo decide exportar los registros, puede hacerlo pulsando este botón. Todos los registros se guardarán en un archivo de texto sin formato.
- ***Importar***: si ya tiene preparado un archivo de texto de direcciones de correo electrónico/ nombres de dominio, puede importarlo seleccionando este botón.

La rama Configuración avanzada contiene numerosas opciones de configuración para el componente Anti-Spam. Estas configuraciones están dirigidas sólo a usuarios expertos, normalmente, administradores de red que necesitan configurar la protección anti-spam con gran detalle para optimizar la seguridad de sus servidores de correo electrónico. Por este motivo, no hay ayuda adicional disponible para cada cuadro de diálogo, pero sí se incluye una breve descripción de cada opción directamente en la interfaz de usuario.

Recomendamos encarecidamente no hacer modificaciones en ninguna de las opciones a menos que se esté completamente familiarizado con la configuración avanzada de Spamcatcher (MailShell Inc.). Cualquier cambio que no sea apropiado puede resultar en un mal rendimiento o en un funcionamiento incorrecto del componente.

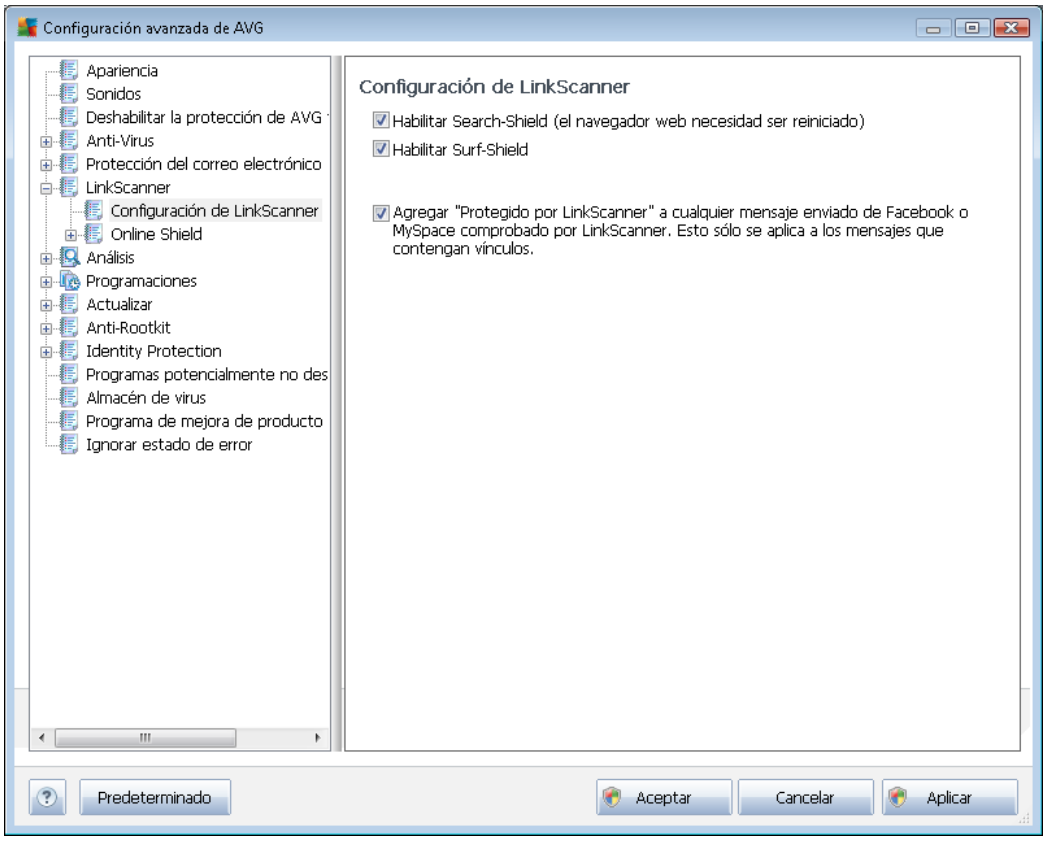
Si aún cree que necesita modificar la configuración de Anti-Spam en el nivel más avanzado, siga las instrucciones proporcionadas directamente en la interfaz de usuario. En cada cuadro de diálogo encontrará una única característica específica que podrá editar y cuya descripción siempre se incluye en el propio cuadro:

- ***Caché***: huella dactilar, reputación del dominio, LegitRepute
- ***Entrenamiento***: máximo de palabras, umbral de autoentrenamiento, relevancia
- ***Filtrado***: lista de idiomas, lista de países, direcciones IP aprobadas, direcciones IP bloqueadas, países bloqueados, conjuntos de caracteres bloqueados, suplantación de remitentes
- ***RBL***: servidores RBL, múltiples coincidencias, umbral, tiempo de espera, máximo de direcciones IP
- ***Conexión a Internet***: tiempo de espera, servidor proxy, autenticación de proxy

9.6. LinkScanner

9.6.1. Configuración de LinkScanner

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

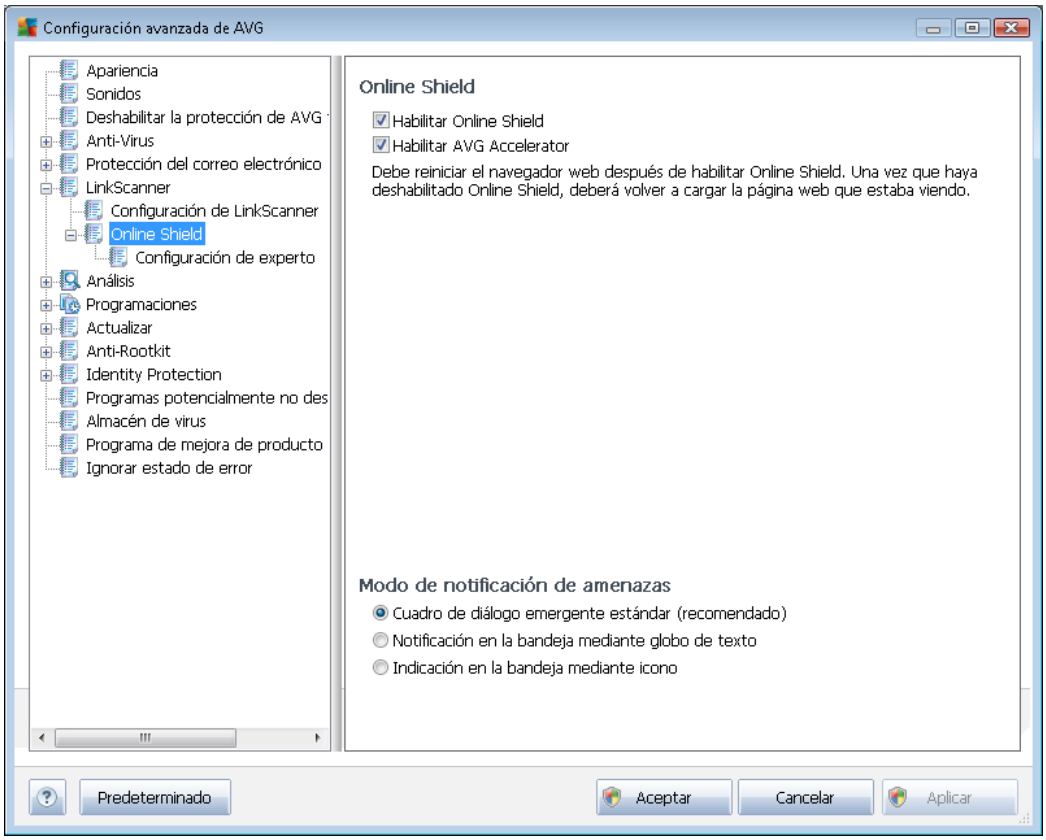


- ***Habilitar Search-Shield*** (*habilitado de manera predeterminada*): iconos de notificación sobre búsquedas realizadas con Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg y SlashDot que indican que se ha comprobado de antemano el contenido de los sitios encontrados por el motor de búsqueda.

- ***Habilitar Surf-Shield*** (*habilitado de manera predeterminada*): protección activa (*en tiempo real*) contra sitios que aprovechan las vulnerabilidades de la seguridad y que actúa cuando se accede a tales sitios. Las conexiones a sitios maliciosos conocidos y su contenido que ataca las vulnerabilidades de la seguridad se bloquean en cuanto el usuario accede a ellos mediante el navegador web (*o cualquier otra aplicación que use HTTP*).

- ***Agregar "Protegido por LinkScanner"...*** (*activado de manera predeterminada*): marque este elemento para confirmar que desea agregar el aviso que certifica que se ha comprobado con LinkScanner a todos los mensajes con hipervínculos activos que se envíen desde las redes sociales Facebook y MySpace.

9.6.2. Online Shield



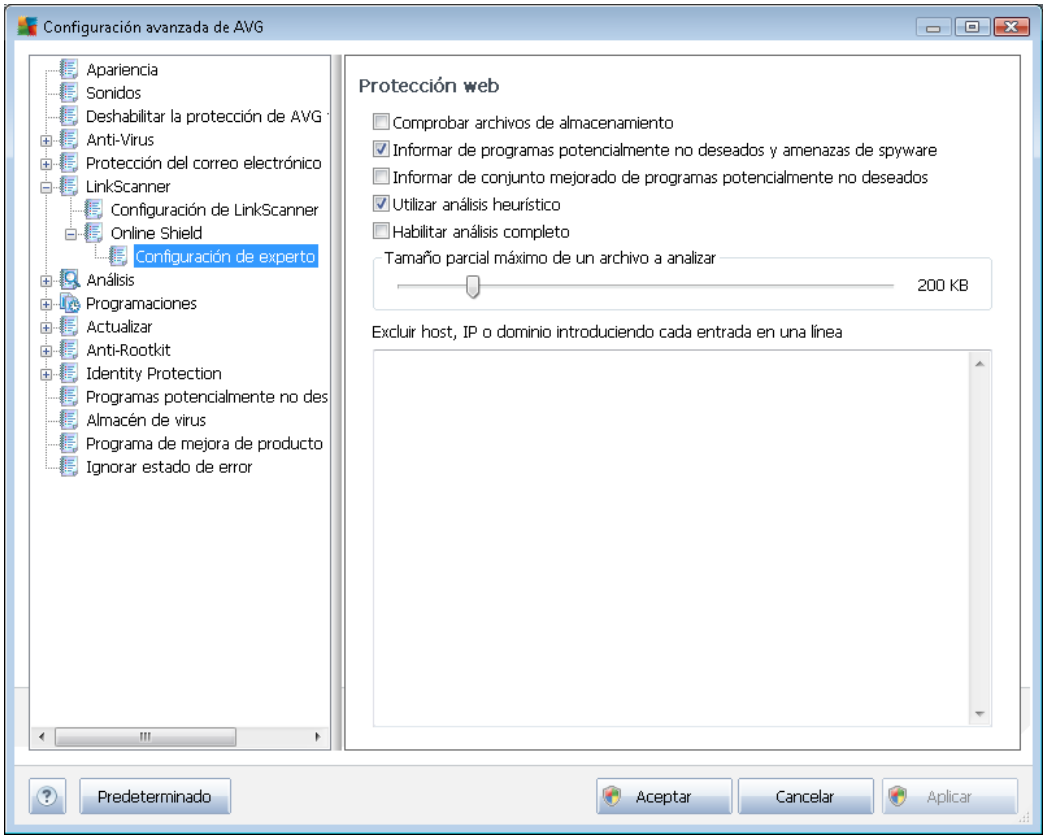
El cuadro de diálogo ***Online Shield*** ofrece las siguientes opciones:

- ***Habilitar Online Shield*** *(activado de manera predeterminada)*: activa o desactiva todo el servicio ***Online Shield***. Para continuar con la configuración avanzada de ***Online Shield***, vaya al siguiente cuadro de diálogo, denominado Protección web.

- ***Habilitar AVG Accelerator*** *(activado de manera predeterminada):* activa o desactiva el servicio ***AVG Accelerator*** que permite reproducir vídeo en línea sin interrupciones y facilita las descargas adicionales.

Modo de notificación de amenazas

En la sección inferior del cuadro de diálogo, seleccione la forma en que desea que se le informe acerca de las posibles amenazas detectadas: por medio de un cuadro de diálogo emergente estándar, de un globo de texto en la bandeja del sistema o de un icono informativo en dicha bandeja.



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

- ***Habilitar protección web***: esta opción confirma que ***Online Shield*** llevará a cabo el análisis del contenido de las páginas web. Si está opción está activada (*valor predeterminado*), es posible activar o desactivar también los siguientes elementos:
    - ***Comprobar archivos comprimidos*** (*desactivada de forma predeterminada*): al marcar esta opción se analiza el contenido de los archivos comprimidos que posiblemente se incluyan en las páginas web que se muestren.
    - ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de forma predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.
    - ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de forma predeterminada*): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas perfectamente correctos y que no causan daño alguno cuando se adquieren directamente del fabricante, pero que

pueden utilizarse, más adelante, para fines maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

- ***Utilizar análisis heurístico*** (*activada de forma predeterminada*): al marcar esta opción, se analiza el contenido de la página que se va a mostrar utilizando el método de análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en el entorno de un equipo virtual*).

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*si sospecha que su equipo ha sido infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

- ***Tamaño parcial máximo de un archivo a analizar***: si la página mostrada incluye archivos, también es posible analizar su contenido incluso antes de que sean descargados en el equipo. Sin embargo, el análisis de archivos grandes lleva bastante tiempo y se puede ralentizar la descarga de la página web de forma significativa. Mediante el control deslizante se puede especificar el tamaño máximo de un archivo que se vaya a analizar con ***Online Shield***. Incluso si el archivo descargado es mayor de lo especificado y, por tanto, no se analizará con Online Shield, se estará todavía protegido: en caso de que el archivo esté infectado, ***Protección residente*** lo detectará inmediatamente.

- ***Excluir host, IP o dominio***: en el campo de texto se puede escribir el nombre exacto de un servidor (*host, dirección IP, dirección IP con máscara o URL*) o un dominio que no deba ser analizado por ***Online Shield***. Por tanto, sólo se deben excluir hosts de los que se tenga la absoluta certeza de que nunca proporcionarán contenido web peligroso.

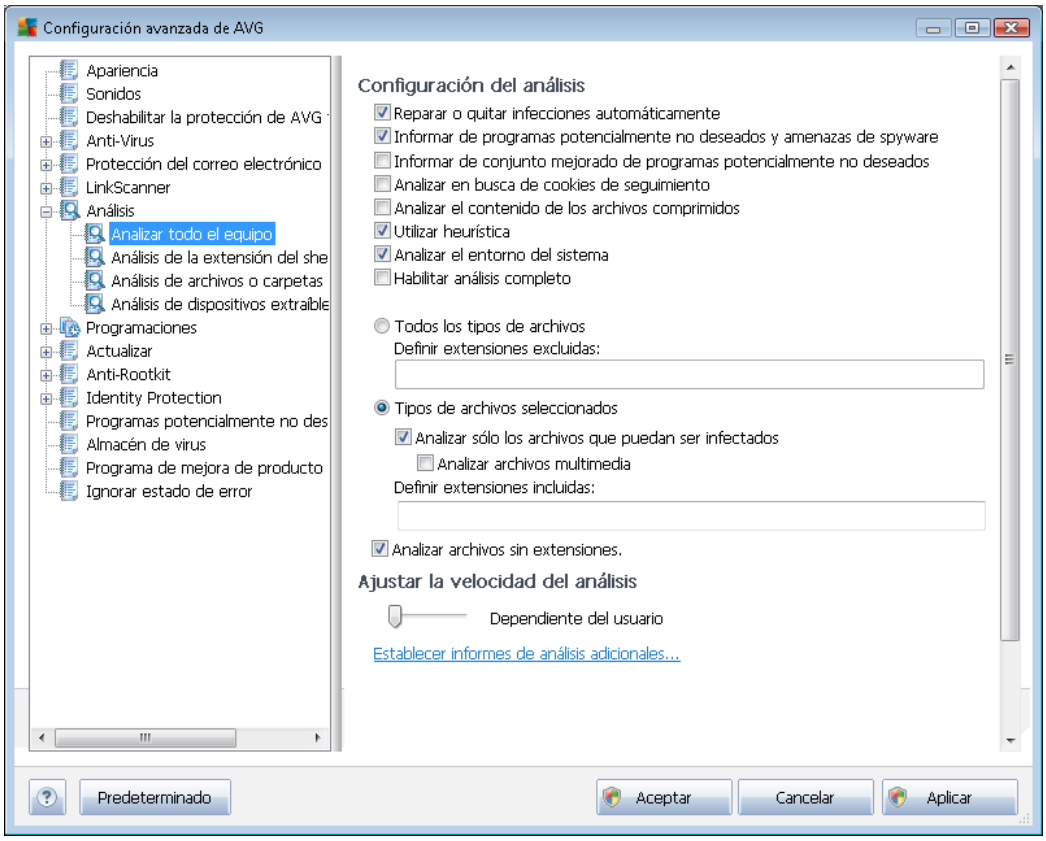
9.7. Análisis

La configuración avanzada del análisis se divide en cuatro categorías que se refieren a tipos de análisis específicos tal y como los definió el proveedor del software:

- ***Análisis del equipo completo***: análisis predefinido estándar de todo el equipo
- ***Análisis de la extensión del shell***: análisis específico de un objeto seleccionado directamente en el entorno del Explorador de Windows
- ***Análisis de archivos o carpetas específicos***: análisis predefinido estándar de áreas seleccionadas del equipo
- ***Análisis de dispositivos extraíbles***: análisis específico de los dispositivos extraíbles conectados al equipo

9.7.1. Análisis del equipo completo

La opción ***Análisis del equipo completo*** le permite editar los parámetros de uno de los análisis predefinidos por el distribuidor del software, Análisis del equipo completo:



Configuración del análisis

La sección ***Configuración del análisis*** contiene una lista de los parámetros de análisis que pueden activarse o desactivarse de manera opcional:

- ***Reparar o quitar infecciones automáticamente*** (*activada de manera predeterminada*): si durante el análisis se identifica algún virus, éste se puede reparar automáticamente en caso de que haya alguna cura disponible. Si el archivo infectado no puede repararse automáticamente, el objeto infectado se moverá al Almacén de virus.
- ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de manera predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.
- ***Informar de conjunto mejorado de programas potencialmente no deseados*** (

desactivada de manera predeterminada): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

- ***Analizar en busca de cookies de seguimiento*** (*desactivado de manera predeterminada*): este parámetro del componente Anti-Spyware indica que las cookies deben detectarse (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos*).

- ***Analizar el contenido de los archivos comprimidos*** (*desactivado de forma predeterminada*): este parámetro establece que el análisis debe comprobar todos los archivos que se encuentren dentro de archivos comprimidos, tales como ZIP, RAR, etc.

- ***Utilizar heurística*** (*activada de manera predeterminada*): el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos utilizados para detectar virus durante el análisis;

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

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*si sospecha que su equipo ha sido infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

Además, debe definir si desea que se analicen:

- ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis proporcionando una lista con las extensiones de archivo, separadas por comas (*una vez guardado el archivo, cada coma se convierte en punto y coma*), que deben quedar excluidas del análisis;

- ***Tipos de archivos seleccionados***: puede especificar que desea analizar solamente los archivos que puedan estar infectados (*no se analizarán los archivos que no se pueden infectar, por ejemplo, algunos archivos de texto sin formato u otro tipo de archivos no ejecutables*), incluyendo archivos multimedia (*archivos de vídeo y audio - si deja esta casilla en blanco, se reducirá aún más el tiempo del análisis, ya que estos archivos suelen ser grandes y no es demasiado probable que estén infectados por un virus*). Del mismo modo, puede especificar las extensiones de los archivos que se analizarán siempre.

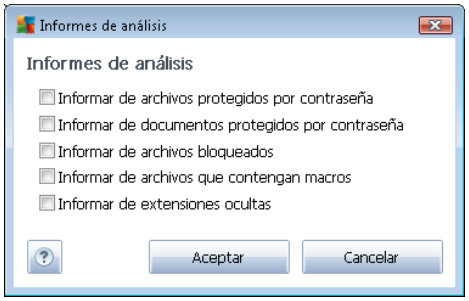
- Opcionalmente, puede indicar que desea ***Analizar archivos sin extensiones***: esta opción está activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

Ajustar la velocidad del análisis

En la sección ***Ajustar la velocidad del análisis*** puede especificar la rapidez con que desea que se ejecute el análisis, según el uso de los recursos del sistema. De manera predeterminada, el valor de esta opción se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos del sistema. Si desea que el análisis se ejecute más rápido, llevará menos tiempo pero se incrementará significativamente el consumo de los recursos del sistema durante el análisis, y el resto de las actividades del equipo se volverán más lentas (*esta opción puede utilizarse cuando el equipo está encendido pero no hay nadie trabajando en él*). En cambio, puede reducir el consumo de los recursos del sistema aumentando la duración del análisis.

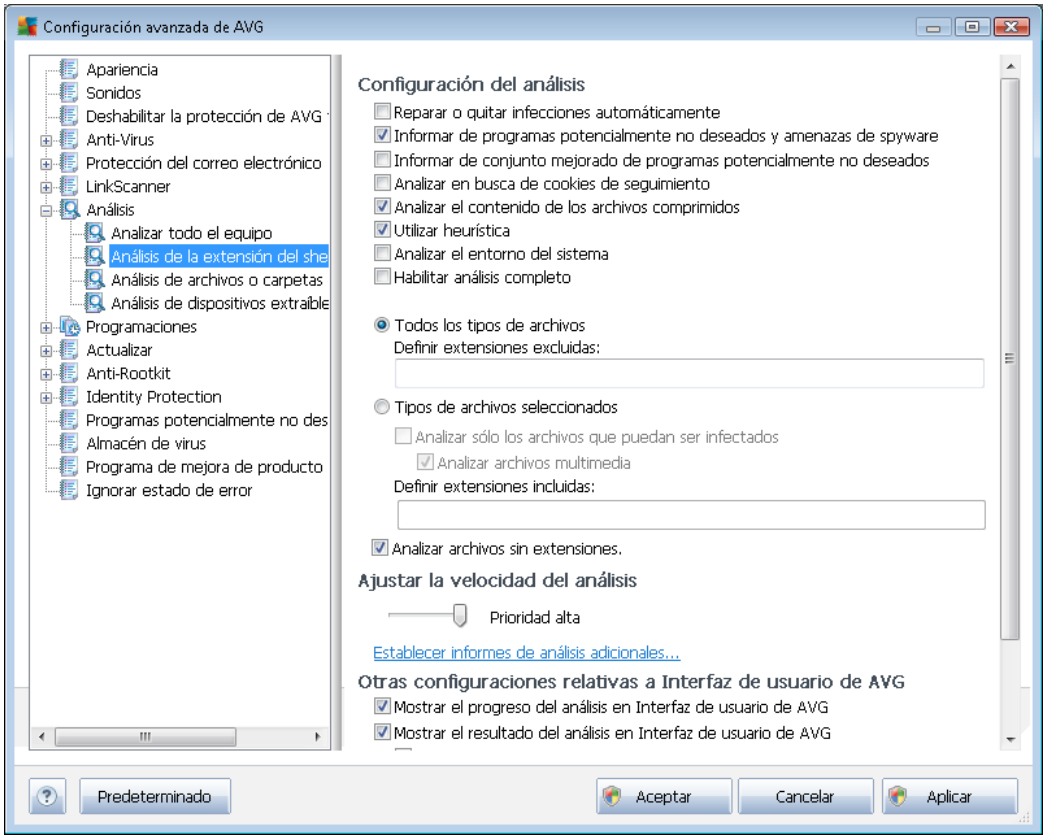
Establecer informes de análisis adicionales...

Haga clic en el vínculo ***Establecer informes de análisis adicionales...*** para abrir una nueva ventana de cuadro de diálogo independiente llamada ***Informes de análisis*** en la que puede marcar diferentes elementos para definir qué resultados del análisis deben incluirse en el informe:



9.7.2. Análisis de la extensión del shell

De manera similar al elemento anterior, Análisis del equipo completo, este elemento llamado ***Análisis de la extensión del shell*** también ofrece varias opciones para editar el análisis predefinido por el proveedor del software. Esta vez la configuración se relaciona con el análisis de objetos específicos iniciado directamente desde el entorno del Explorador de Windows (*extensión del shell*). Consulte el capítulo Análisis en el Explorador de Windows:



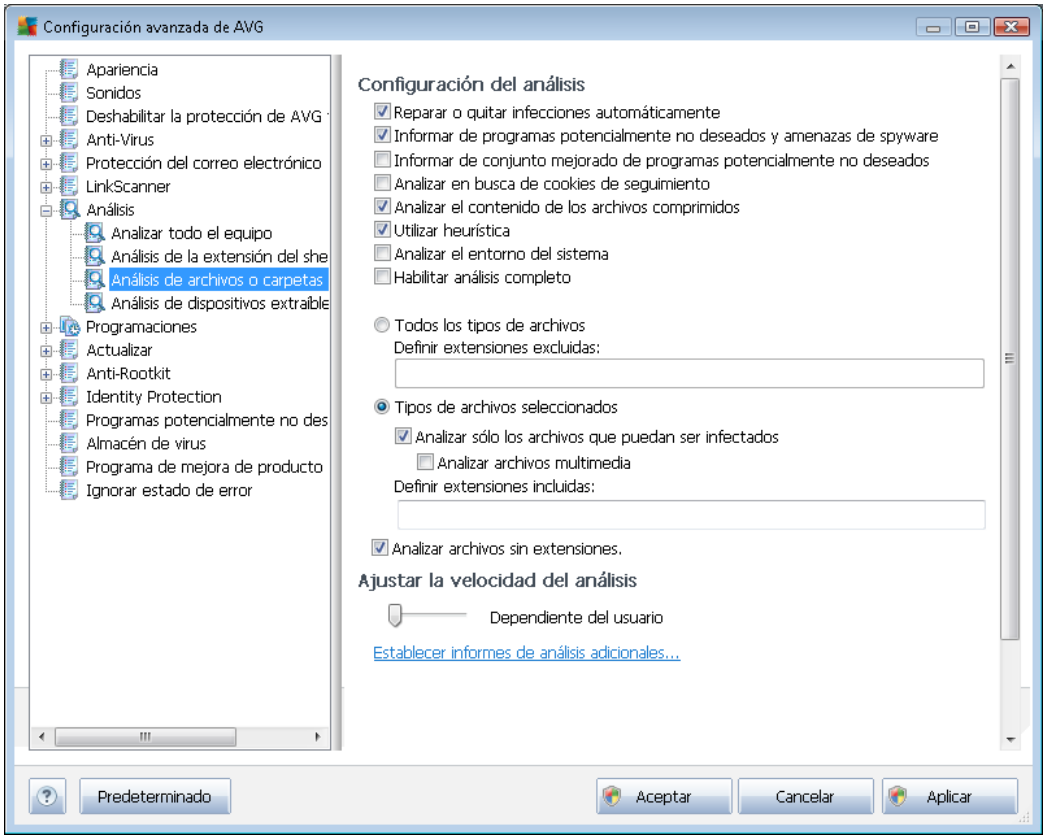
La lista de parámetros es idéntica a la que incluye el Análisis del equipo completo. Sin embargo, la configuración predeterminada es distinta (*por ejemplo, el Análisis del equipo completo no comprueba los archivos comprimidos de manera predeterminada, pero sí que analiza el entorno del sistema, mientras que con el Análisis de la extensión del shell es justo al revés*).

Nota: *para ver una descripción de parámetros específicos, consulte el capítulo Configuración avanzada de AVG / Análisis / Análisis del equipo completo.*

Comparado con el cuadro de diálogo Análisis del equipo completo, el cuadro de diálogo ***Análisis de la extensión del shell*** incluye también la sección llamada ***Otras configuraciones relativas a Interfaz de usuario de AVG***, donde puede especificar si desea acceder al progreso y a los resultados del análisis desde la interfaz de usuario de AVG. Del mismo modo, también puede definir que los resultados del análisis se muestren únicamente en caso de que se detecte una infección durante el análisis.

9.7.3. Análisis de archivos o carpetas específicos

La interfaz de edición de ***Analizar archivos o carpetas específicos*** es idéntica al cuadro de diálogo de edición de Análisis del equipo completo. Todas las opciones de configuración son iguales. No obstante, la configuración predeterminada es más estricta en el caso de Análisis del equipo completo:

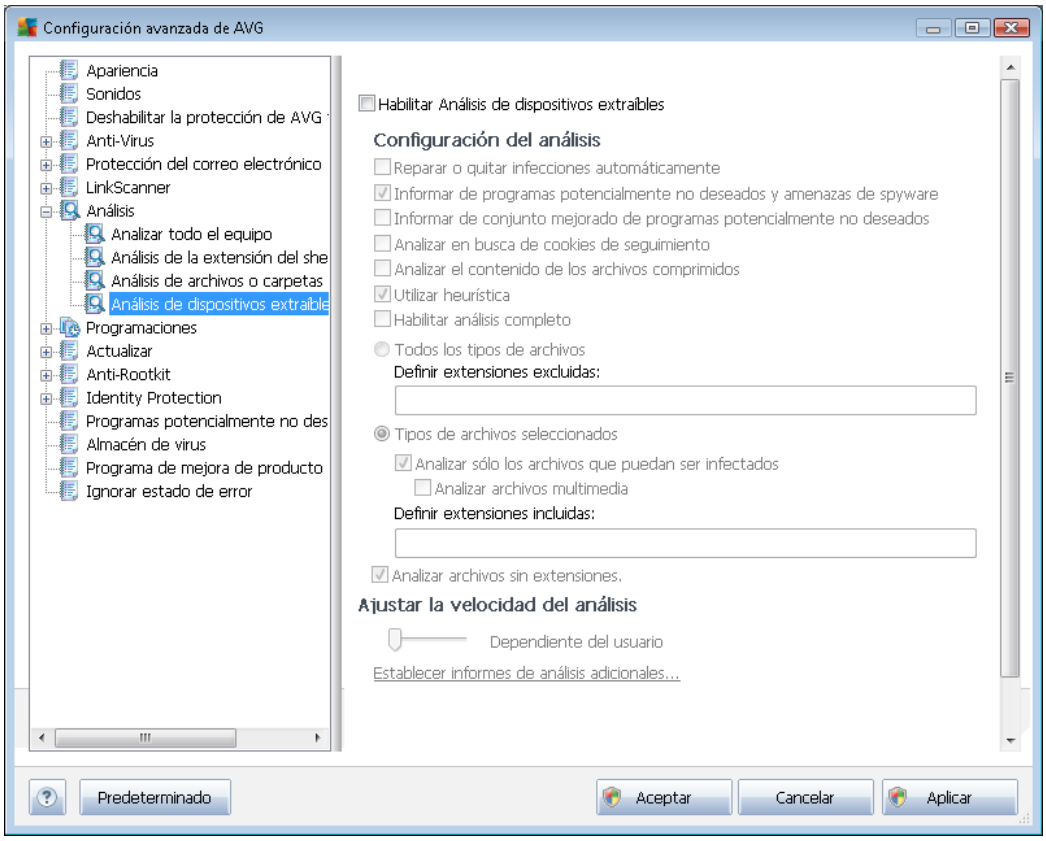


Todos los parámetros definidos en este cuadro de diálogo de configuración se aplican únicamente a las áreas seleccionadas para ser analizadas mediante la opción Analizar archivos o carpetas específicos.

Nota: *para ver una descripción de parámetros específicos, consulte el capítulo Configuración avanzada de AVG / Análisis / Análisis del equipo completo.*

9.7.4. Análisis de dispositivos extraíbles

La interfaz de edición de ***Análisis de dispositivos extraíbles*** es también muy similar al cuadro de diálogo de edición de Análisis del equipo completo:



El ***Análisis de dispositivos extraíbles*** se inicia automáticamente al conectar un dispositivo extraíble al equipo. De manera predeterminada, este tipo de análisis se encuentra desactivado. Sin embargo, es crucial analizar los dispositivos extraíbles para ver si presentan posibles amenazas, dado que constituyen una importante fuente de infección. Para habilitar este análisis y que pueda iniciarse automáticamente cuando sea necesario, marque la opción ***Habilitar análisis de dispositivos extraíbles***.

Nota: *para ver una descripción de parámetros específicos, consulte el capítulo Configuración avanzada de AVG / Análisis / Análisis del equipo completo.*

9.8. Programaciones

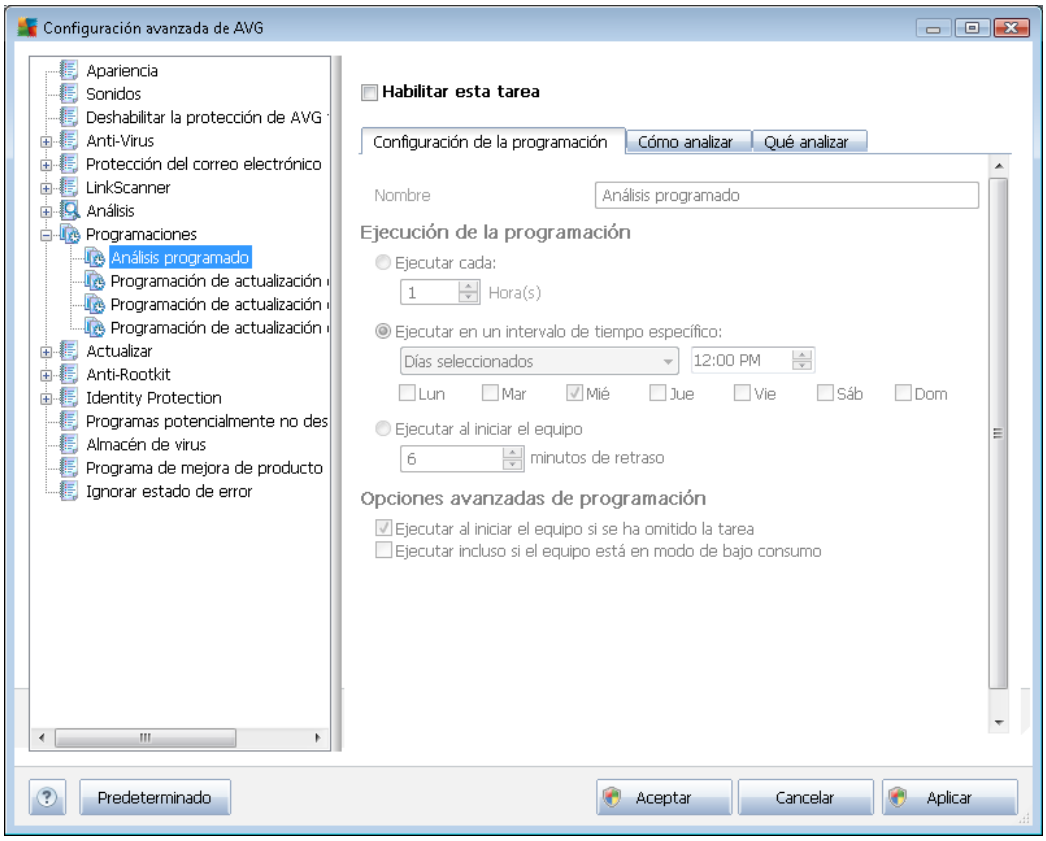
En la sección ***Programaciones*** puede editar la configuración predeterminada de:

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

- Programación de actualización de Anti-Spam

9.8.1. Análisis programado

Es posible editar los parámetros del análisis programado (*o configurar una nueva programación*) en tres fichas. En cada ficha puede desactivar el elemento ***Habilitar esta tarea*** simplemente para desactivar temporalmente el análisis programado, y marcarlo para volver a activarlo cuando sea necesario:



A continuación, en el campo de texto ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) figura el nombre asignado por el proveedor del programa a esta programación. Para programaciones agregadas recientemente (*puede agregar una nueva programación haciendo clic con el botón secundario del ratón sobre el elemento* ***Análisis programado*** *en el árbol de navegación izquierdo*), puede especificar el nombre que desee y, en este caso, el campo de texto se abrirá para que pueda editarlo. Trate de usar siempre nombres breves, descriptivos y adecuados para los análisis con el objeto de facilitar su reconocimiento posterior.

Ejemplo: *no resulta apropiado llamar al análisis con el nombre de "Análisis nuevo" o "Mi análisis" puesto que estos nombres no hacen referencia a lo que realmente se comprueba en el análisis. En cambio, un ejemplo de un buen nombre descriptivo podría ser "Análisis de las áreas del sistema", etc. Del mismo modo, no es necesario especificar en el nombre del análisis si se trata de un análisis de todo el equipo o sólo de ciertos archivos o carpetas: los análisis creados por el usuario siempre serán una versión concreta del análisis de archivos o carpetas específicos.*

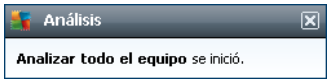
En este cuadro de diálogo puede definir aún más los parámetros siguientes del análisis:

Ejecución de la programación

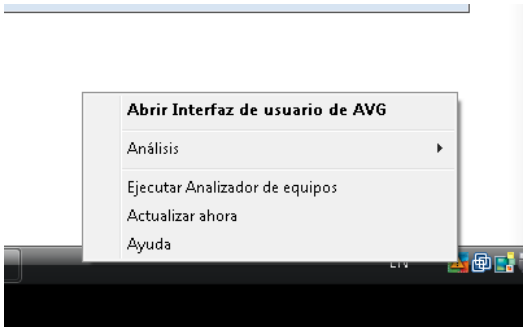
En esta sección puede especificar los intervalos de tiempo para el inicio del análisis que acaba de programar. Los intervalos pueden definirse por la ejecución repetida del análisis tras un cierto período de tiempo (***Ejecutar cada...***), indicando una fecha y hora exactas (***Ejecutar en un intervalo de tiempo específico...***) o posiblemente definiendo un evento al que debe asociarse la ejecución del análisis (***Basada en acciones: Al iniciar el equipo***).

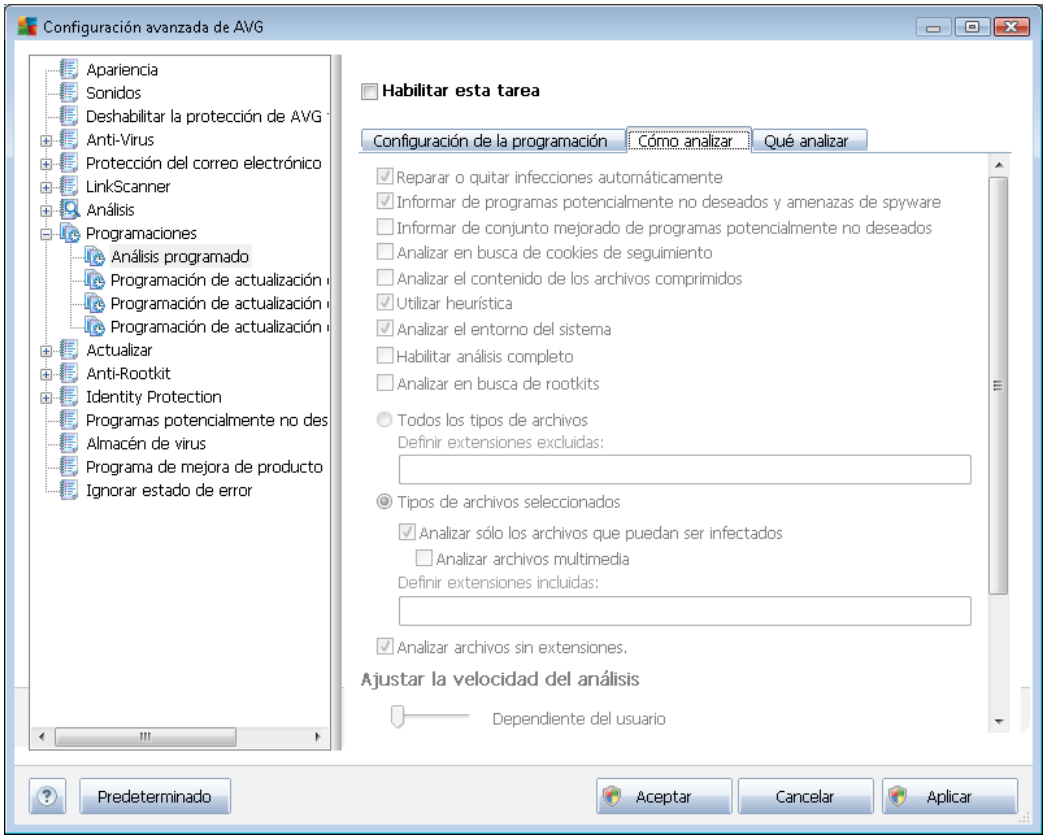
Opciones avanzadas de programación

Esta sección permite definir bajo qué condiciones deberá iniciarse o no el análisis si el equipo está en modo de bajo consumo o apagado completamente. Cuando se inicie el análisis programado en el momento especificado, se informará de este hecho mediante una ventana emergente que se abrirá sobre el icono de AVG en la bandeja del sistema:



Aparecerá un nuevo icono de AVG en la bandeja del sistema (*a todo color con una luz intermitente*) que le informa de que se está ejecutando un análisis programado. Haga clic con el botón secundario sobre el icono de AVG del análisis que se está ejecutando para abrir un menú contextual en el que puede poner en pausa el análisis en curso e incluso detenerlo por completo, pudiendo también cambiar su prioridad:





En la ficha ***Cómo analizar*** encontrará una lista de parámetros de análisis que pueden activarse o desactivarse de manera opcional. De manera predeterminada, la mayoría de los parámetros están activados y las funciones se aplicarán durante el análisis. ***A menos que tenga un buen motivo para modificarla, se recomienda mantener la configuración predefinida***:

- ***Reparar o quitar infecciones automáticamente*** *(activada de manera predeterminada):* si durante el análisis se identifica algún virus, éste se puede reparar automáticamente en caso de que haya alguna cura disponible. Si el archivo infectado no puede repararse automáticamente, el objeto infectado se moverá al Almacén de virus.

- ***Informar de programas potencialmente no deseados y amenazas de spyware*** *(activada de manera predeterminada):* marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción

está desactivada de manera predeterminada.

- ***Analizar en busca de cookies de seguimiento*** (*desactivado de manera predeterminada*): este parámetro del componente Anti-Spyware indica que deben detectarse cookies durante el análisis (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos*)

- ***Analizar el contenido de los archivos comprimidos*** (*desactivado de manera predeterminada*): este parámetro indica que se deben analizar todos los archivos, incluso si se encuentran dentro de archivos comprimidos, por ejemplo, ZIP, RAR...

- ***Utilizar heurística***(*activado de manera predeterminada*): el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos utilizados para detectar virus durante el análisis;

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

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*si sospecha que su equipo ha sido infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

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

Además, debe definir si desea que se analicen:

- ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis proporcionando una lista con las extensiones de archivo, separadas por comas (*una vez guardado el archivo, cada coma se convierte en punto y coma*), que deben quedar excluidas del análisis;

- ***Tipos de archivos seleccionados***: puede especificar que desea analizar solamente los archivos que puedan estar infectados (*no se analizarán los archivos que no se pueden infectar, por ejemplo, algunos archivos de texto sin formato u otro tipo de archivos no ejecutables*), incluyendo archivos multimedia (*archivos de vídeo y audio - si deja esta casilla en blanco, se reducirá aún más el tiempo del análisis, ya que estos archivos suelen ser grandes y no es demasiado probable que estén infectados por un virus*). Del mismo modo, puede especificar las extensiones de los archivos que se analizarán siempre.

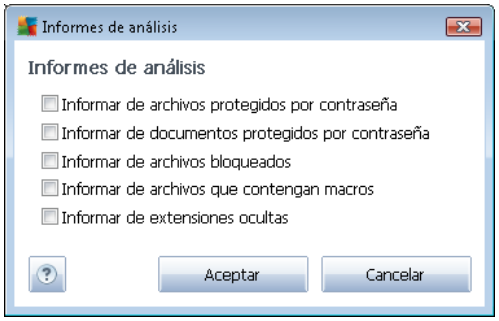
- Opcionalmente, puede indicar que desea ***Analizar archivos sin extensiones***: esta opción está activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

Ajustar la velocidad del análisis

En la sección ***Ajustar la velocidad del análisis*** puede especificar la rapidez con que desea que se ejecute el análisis, según el uso de los recursos del sistema. De manera predeterminada, el valor de esta opción se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos del sistema. Si desea que el análisis se ejecute más rápido, llevará menos tiempo pero se incrementará significativamente el consumo de los recursos del sistema durante el análisis, y el resto de las actividades del equipo se volverán más lentas (*esta opción puede utilizarse cuando el equipo está encendido pero no hay nadie trabajando en él*). En cambio, puede reducir el consumo de los recursos del sistema aumentando la duración del análisis.

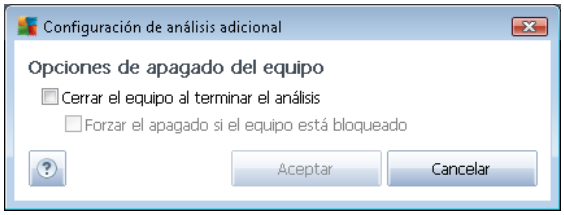
Establecer informes de análisis adicionales

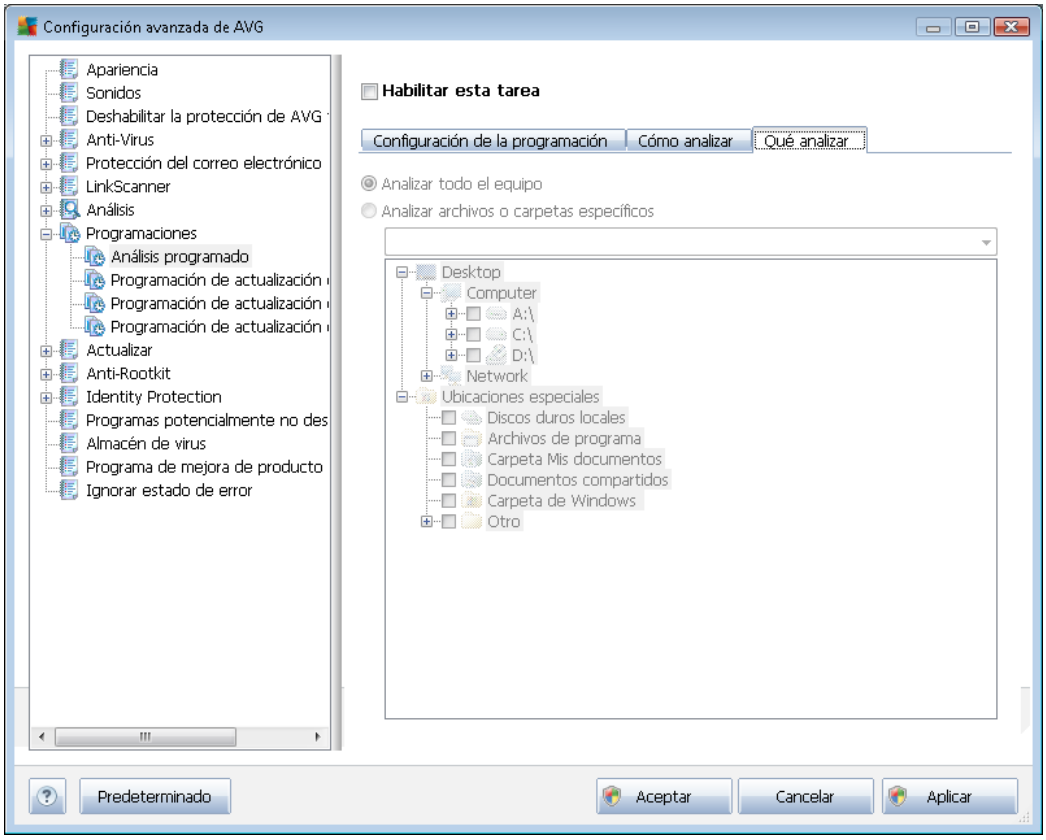
Haga clic en el vínculo ***Establecer informes de análisis adicionales...*** para abrir una nueva ventana de cuadro de diálogo independiente llamada ***Informes de análisis*** en la que puede marcar diferentes elementos para definir qué resultados del análisis deben incluirse en el informe:



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 apagará automáticamente cuando termine el proceso de análisis en ejecución. Una vez confirmada esta opción (***Cerrar el equipo al terminar el análisis***), se activa una nueva opción que permite apagar el equipo aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

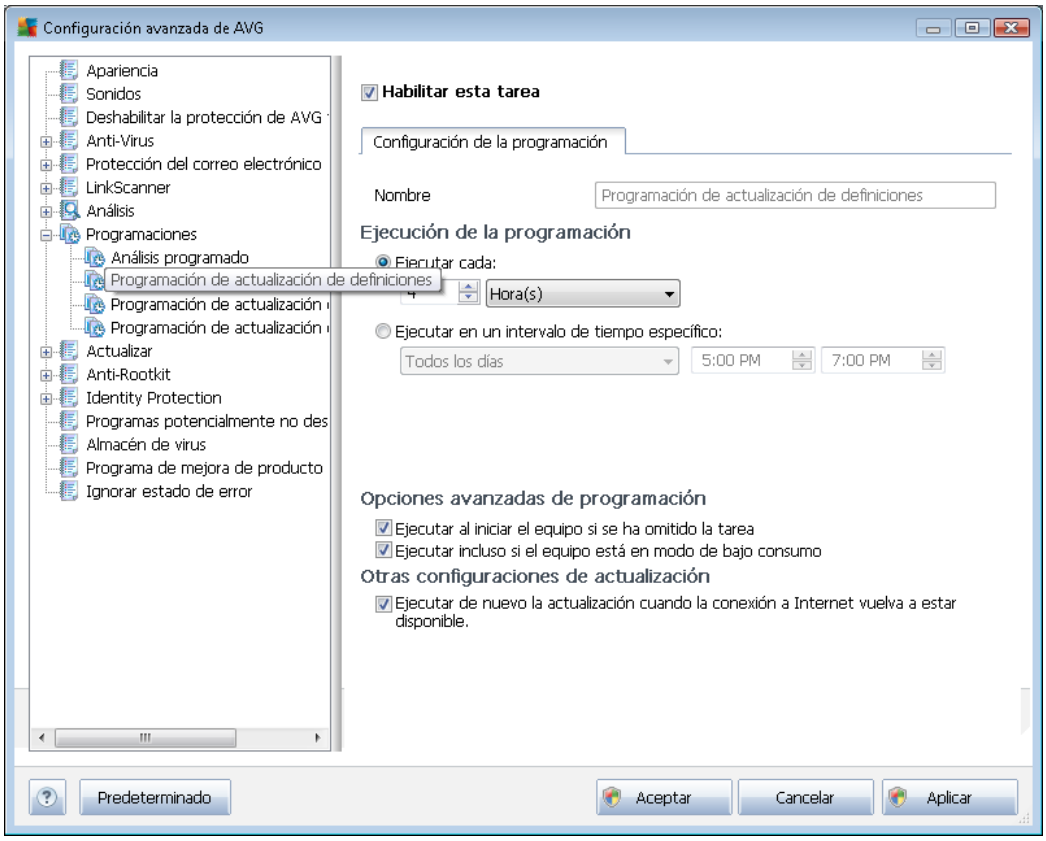




En la ficha ***Qué analizar*** se puede definir si se desea programar el análisis del equipo completo o el análisis de archivos o carpetas específicos. En caso de que se seleccione el análisis de archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activa la estructura de árbol mostrada, pudiéndose especificar las carpetas a analizar.

9.8.2. Programación de actualización de definiciones

Si es ***realmente necesario***, puede quitar la marca de la opción ***Habilitar esta tarea*** para desactivar temporalmente la actualización programada de las definiciones, y activarla de nuevo más tarde:



En este cuadro de diálogo se pueden configurar algunos parámetros detallados de la programación de actualización de definiciones. En el campo de texto llamado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) figura el nombre asignado por el proveedor del programa a esta programación.

Ejecución de la programación

En esta sección, especifique los intervalos de tiempo en los que se ejecutará la actualización de definiciones recién programada. Los intervalos se pueden definir mediante el inicio repetido de la actualización tras un período de tiempo (***Ejecutar cada...***) o indicando una fecha y hora exactas (***Ejecutar en un intervalo...***).

Opciones avanzadas de programación

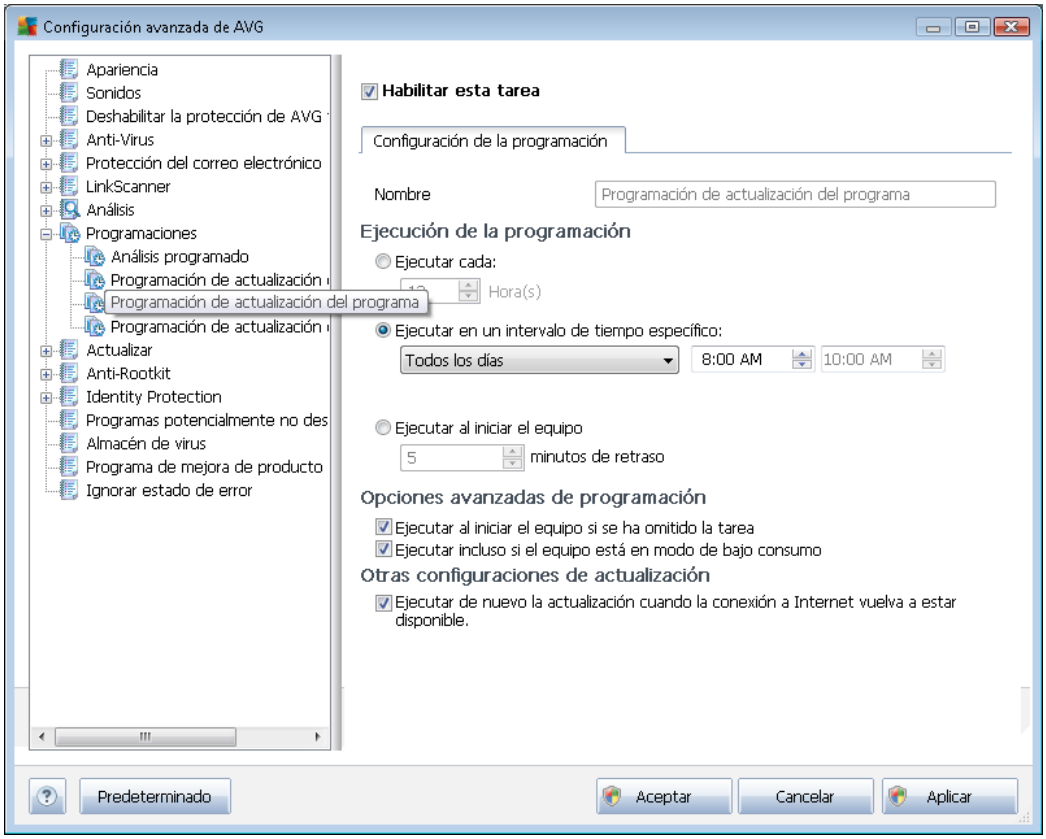
Esta sección le permite definir bajo qué condiciones deberá iniciarse o no la actualización de definiciones si el equipo está en modo de bajo consumo o apagado completamente.

Otras configuraciones de actualización

Finalmente, marque la opción ***Ejecutar de nuevo la actualización cuando la conexión a Internet vuelva a estar disponible*** para asegurarse de que si la conexión a Internet se interrumpe y falla el proceso de actualización, se iniciará automáticamente de nuevo cuando la conexión de Internet se restablezca. Cuando la actualización programada se inicie a la hora especificada, se le informará de este hecho por medio de una ventana emergente que se abrirá encima del icono de AVG en la bandeja del sistema (*siempre que haya mantenido la configuración predeterminada en el cuadro de diálogo Configuración avanzada/Apariencia*).

9.8.3. Programación de actualización del programa

Si ***realmente fuese necesario***, puede dejar en blanco el elemento ***Habilitar esta tarea*** para desactivar temporalmente la actualización programada y activarla de nuevo más adelante:



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

Ejecución de la programación

En esta sección, especifique los intervalos de tiempo en los que se ejecutará la actualización del programa recién programada. Los intervalos se pueden definir mediante el inicio repetido de la

actualización tras un período de tiempo (***Ejecutar cada...***), indicando una fecha y hora exactas (***Ejecutar en un intervalo...***) o posiblemente definiendo un evento al que debe asociarse el inicio de la actualización (***Basada en acciones: Al iniciar el equipo***).

Opciones avanzadas de programación

Esta sección permite definir bajo qué condiciones deberá iniciarse o no la actualización del programa si el equipo está en modo de bajo consumo o apagado completamente.

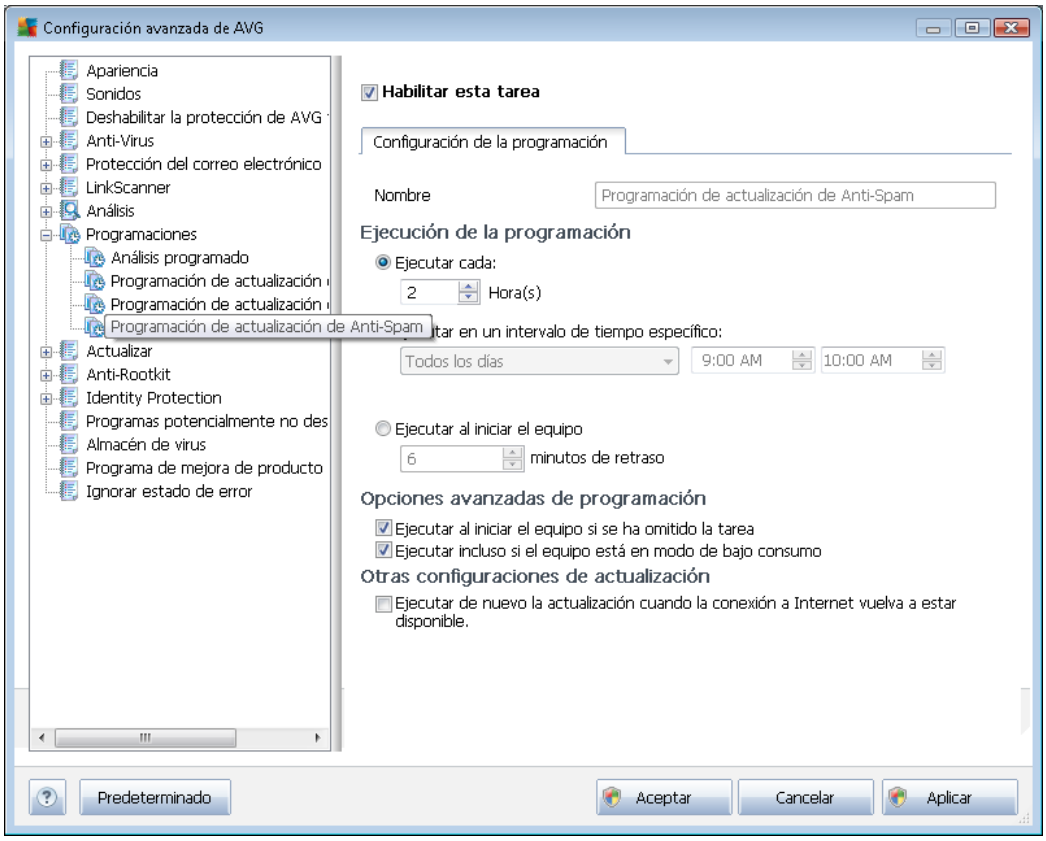
Otras configuraciones de actualización

Marque la opción ***Ejecutar de nuevo la actualización cuando la conexión a Internet vuelva a estar disponible*** para asegurarse de que si la conexión a Internet se interrumpe y falla el proceso de actualización, se iniciará automáticamente de nuevo cuando la conexión de Internet se restablezca. Cuando la actualización programada se inicie a la hora especificada, se le informará de este hecho por medio de una ventana emergente que se abrirá encima del icono de la bandeja del sistema de AVG (*siempre que haya mantenido la configuración predeterminada del cuadro de diálogo Configuración avanzada/Apariencia*).

Nota: *si llegase a coincidir el momento de una actualización programada del programa y un análisis programado, el proceso de actualización tiene prioridad y, por lo tanto, se interrumpirá el análisis.*

9.8.4. Programación de actualización de Anti-Spam

Si es realmente necesario, puede quitar la marca de la opción ***Habilitar esta tarea*** para desactivar temporalmente la actualización de Anti-Spam programada y activarla de nuevo más tarde:



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

Ejecución de la programación

Aquí, especifique los intervalos de tiempo en los que se ejecutará la actualización de Anti-Spam recién programada. Los intervalos se pueden definir mediante el inicio repetido de la actualización de Anti-Spam tras cierto periodo de tiempo (***Ejecutar cada...***), indicando una fecha y hora exactas (***Ejecutar en un intervalo de tiempo específico...***) o posiblemente definiendo el evento con el que debería asociarse la ejecución del análisis (***Basada en acciones: Ejecutar al iniciar el equipo***).

Opciones avanzadas de programación

Esta sección le permite definir bajo qué condiciones deberá iniciarse o no la actualización de Anti-Spam si el equipo está en modo de bajo consumo o apagado completamente.

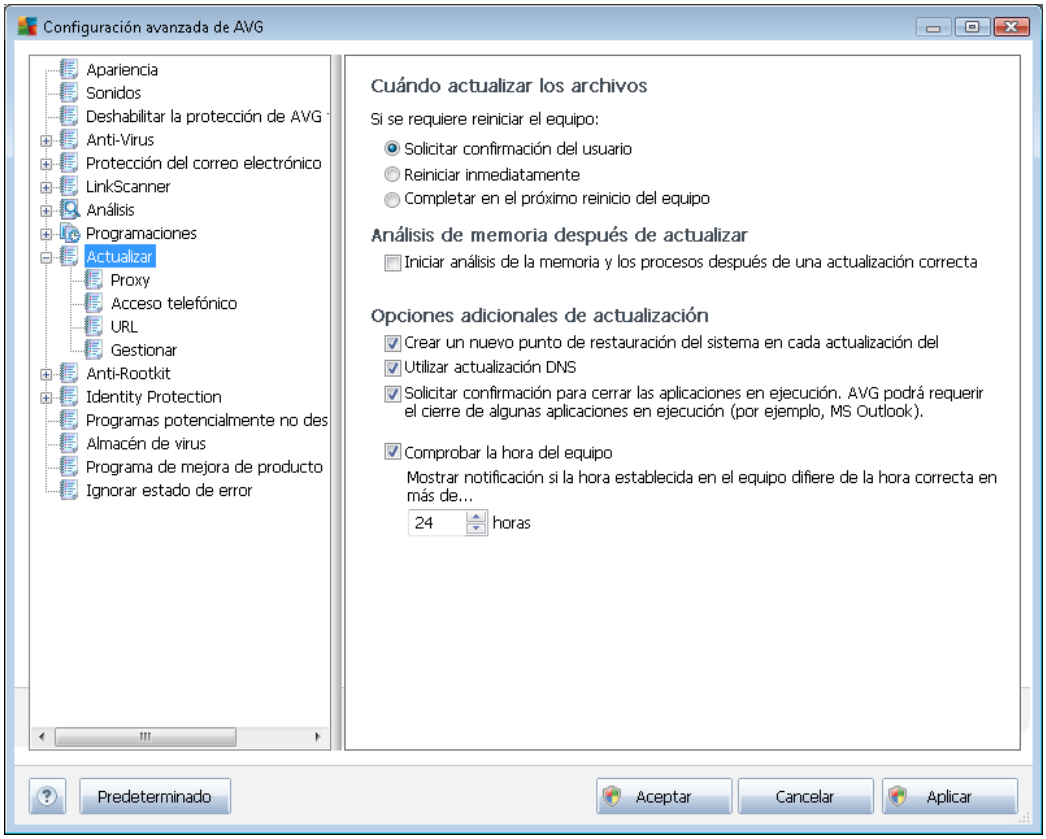
Otras configuraciones de actualización

Marque la opción ***Ejecutar de nuevo la actualización cuando la conexión a Internet vuelva a estar disponible*** para asegurarse de que si la conexión a Internet se interrumpe y falla el proceso de actualización de Anti-Spam, se iniciará automáticamente de nuevo cuando la conexión de Internet se restablezca.

Cuando el análisis programado se inicie a la hora especificada, se le informará de este hecho por medio de una ventana emergente que se abrirá encima del icono de la bandeja del sistema de AVG (*siempre que haya mantenido la configuración predeterminada del cuadro de diálogo Configuración avanzada/Apariencia*).

9.9. Actualizar

El elemento de navegación ***Actualizar*** abre un nuevo cuadro de diálogo en el que se pueden especificar los parámetros generales de la actualización de AVG:



Cuándo actualizar los archivos

En esta sección se puede seleccionar entre tres opciones alternativas que se utilizarán en caso de que el proceso de actualización requiera reiniciar el equipo. Es posible programar la finalización de

la actualización para el siguiente reinicio del equipo, o bien reiniciar inmediatamente:

- ***Solicitar confirmación del usuario*** *(activado de manera predeterminada)*: se le pedirá autorizar el reinicio del equipo necesario para finalizar el proceso de actualización
- ***Reiniciar inmediatamente***: el equipo se reiniciará automáticamente una vez haya terminado el proceso de actualización, y no será necesaria su autorización
- ***Completar en el próximo reinicio del equipo***: la finalización del proceso de actualización se pospondrá hasta el siguiente reinicio del equipo. Tenga en cuenta que esta opción sólo se recomienda si se tiene la certeza de que el equipo se reinicia regularmente, al menos una vez al día.

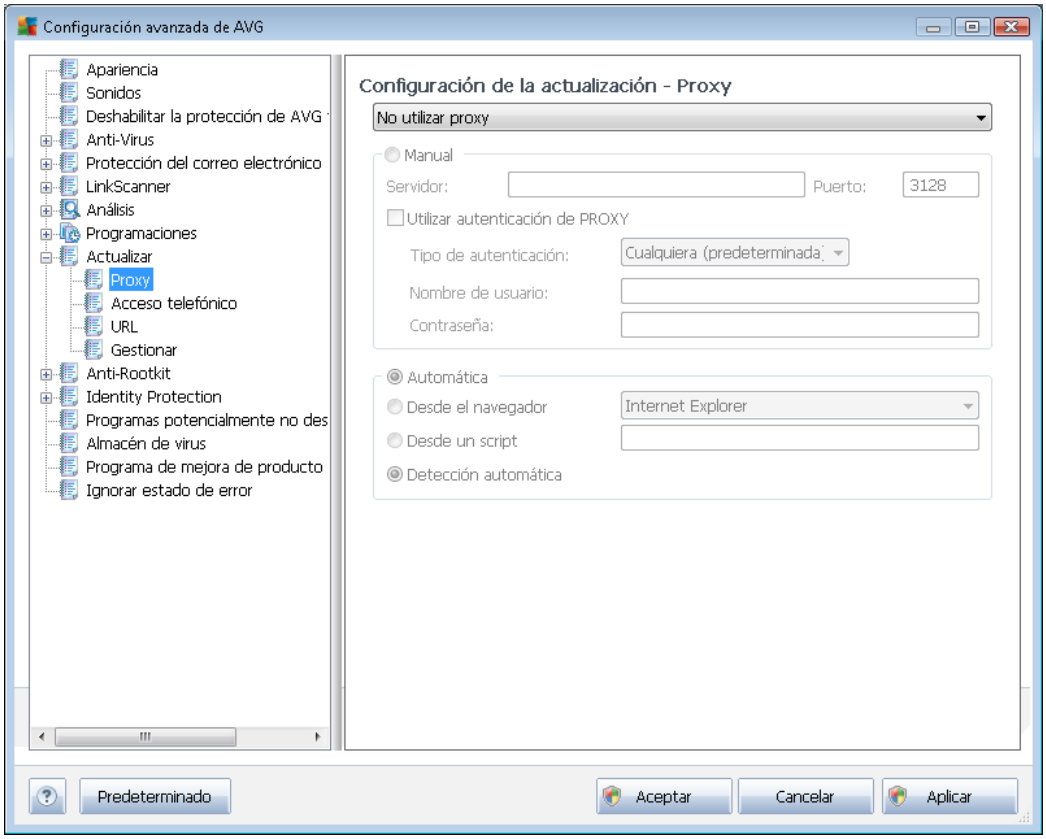
Análisis de memoria después de actualizar

Marque esta casilla de verificación para definir que desea iniciar un nuevo análisis de la memoria tras cada actualización completada correctamente. La última actualización descargada podría contener nuevas definiciones de virus, que se aplicarían en el análisis inmediatamente.

Opciones adicionales de actualización

- ***Crear un nuevo punto de restauración del sistema en cada actualización del programa***: antes de iniciar cada actualización del programa AVG, se creará un punto de restauración del sistema. En caso de que falle el proceso de actualización y se bloquee el sistema operativo, este último siempre se podrá restaurar a la configuración original desde este punto. A esta opción se puede acceder a través de Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema, pero se recomienda que sólo realicen cambios los usuarios experimentados. Mantenga marcada esta casilla de verificación si desea utilizar esta funcionalidad.
- ***Utilizar actualización DNS*** (*activado de forma predeterminada*): si se marca este elemento, cuando se inicia la actualización, **AVG Internet Security 2012** busca información acerca de la versión más reciente de la base de datos de virus y del programa en el servidor DNS. Luego sólo se descargará y se aplicará el número mínimo de archivos indispensables. De esta forma se minimiza la cantidad total de datos descargados y se agiliza el proceso de actualización.
- ***Solicitar confirmación para cerrar las aplicaciones en ejecución*** (*activado de forma predeterminada*): le permitirá asegurarse de que no se cerrará ninguna aplicación en ejecución sin autorización del usuario en caso de que fuese necesario para finalizar el proceso de actualización.
- ***Comprobar la hora del equipo***: marque esta opción para indicar que desea recibir notificación visual en caso de que la hora del equipo difiera de la hora correcta en un número de horas especificado.

9.9.1. Proxy



El servidor proxy es un servidor independiente o un servicio que se ejecuta un equipo y que garantiza una conexión más segura a Internet. Según las reglas de red especificadas, puede acceder a Internet directamente o a través del servidor proxy. También es posible permitir ambas posibilidades al mismo tiempo. Por tanto, en el primer elemento del cuadro de diálogo ***Configuración de la actualización - Proxy***, debe seleccionar en el cuadro combinado si desea:

- ***Utilizar proxy***
- ***No utilizar proxy***: configuración predeterminada
- ***Intentar la conexión mediante proxy y, si falla, conectar directamente***

Si selecciona cualquiera de las opciones en que se utiliza servidor proxy, deberá especificar ciertos datos adicionales. Puede establecer la configuración del servidor de forma manual o automática.

Configuración manual

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

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

- ***Puerto***: especifique el número de puerto que permite el acceso a Internet (*de manera predeterminada, este número está fijado en 3128, pero se puede establecer en otro diferente. Si no está seguro, póngase en contacto con el administrador de la red*)

El servidor proxy también puede tener configuradas reglas específicas para cada usuario. Si el servidor proxy está configurado de esta manera, marque la opción ***Utilizar autenticación de PROXY*** para verificar que el nombre de usuario y la contraseña son válidos para la conexión a Internet a través del servidor proxy.

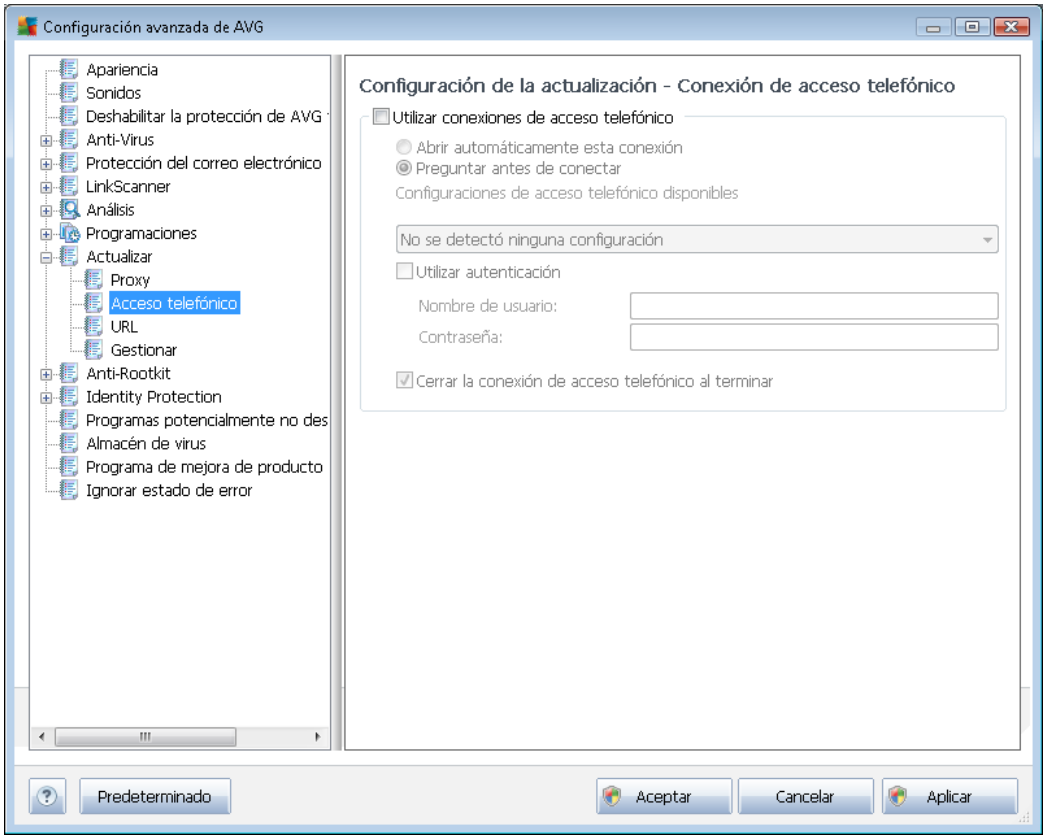
Configuración automática

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

- ***Desde el navegador***: la configuración se obtendrá del navegador de Internet predeterminado
- ***Desde un script***: la configuración se obtendrá de un script descargado con una función que devuelva la dirección del proxy
- ***Detección automática***: la configuración se detectará de manera automática directamente desde el servidor proxy

9.9.2. Acceso telefónico

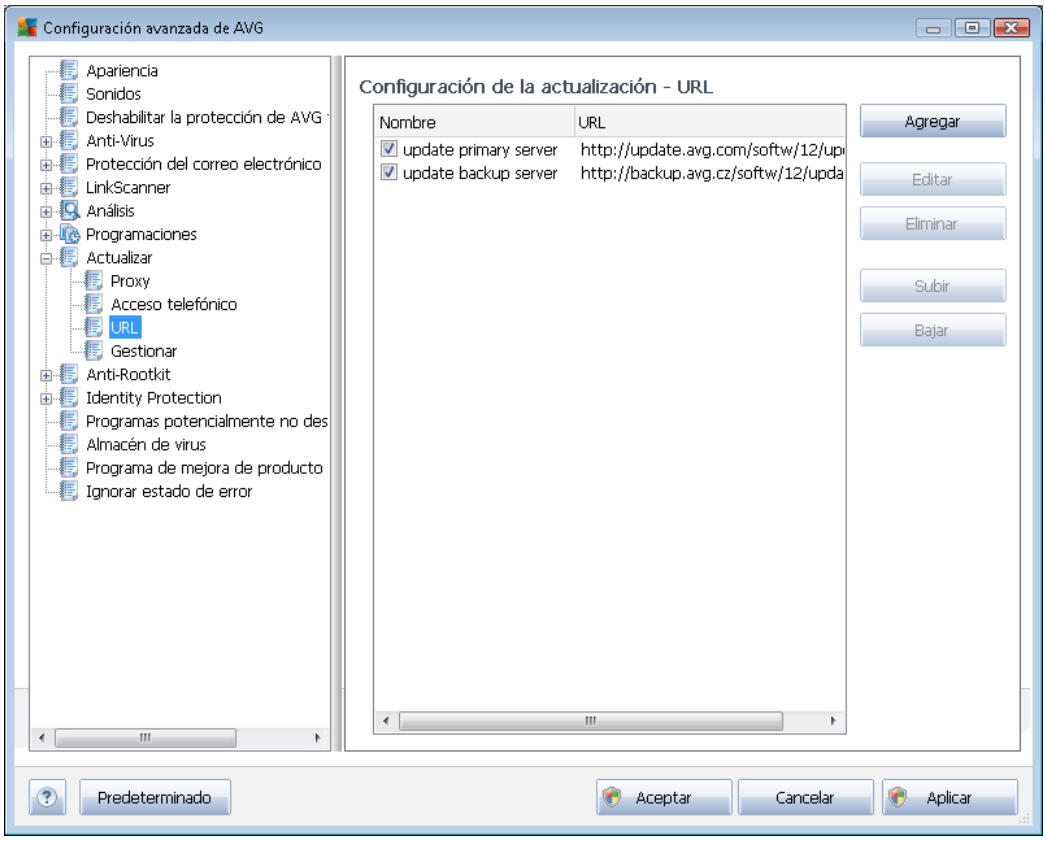
Todos los parámetros definidos opcionalmente en el cuadro de diálogo ***Configuración de la actualización - Conexión de acceso telefónico*** hacen referencia a la conexión de acceso telefónico a Internet. Los campos del cuadro de diálogo están inactivos hasta que se selecciona la opción ***Utilizar conexiones de acceso telefónico*** que los activa:



Indique si desea conectarse a Internet automáticamente (***Abrir automáticamente esta conexión***) o si prefiere confirmar manualmente cada conexión (***Preguntar antes de conectar***). En caso de conexión automática, también es necesario indicar si la conexión debe cerrarse al finalizar la actualización (***Cerrar la conexión de acceso telefónico al terminar***).

9.9.3. URL

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



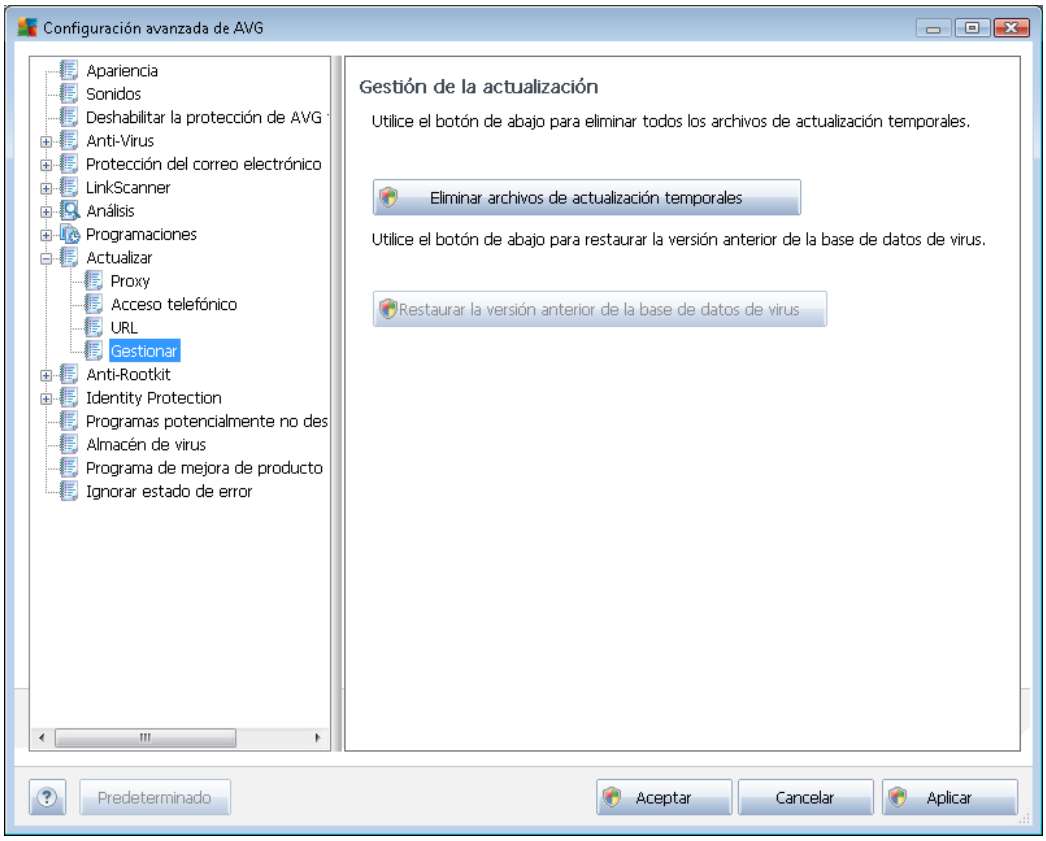
Botones de control

Puede modificar la lista y sus elementos empleando los siguientes botones de control:

- ***Agregar***: abre un cuadro de diálogo donde puede especificar una nueva URL para añadir a la lista
- ***Editar***: abre un cuadro de diálogo donde puede editar los parámetros de la URL seleccionada
- ***Eliminar***: elimina de la lista la URL seleccionada
- ***Subir***: mueve la URL seleccionada una posición hacia arriba en la lista
- ***Bajar***: mueve la URL seleccionada una posición hacia abajo en la lista

9.9.4. Gestionar

El cuadro de diálogo ***Gestión de la actualización*** ofrece dos opciones accesibles a través de dos botones:

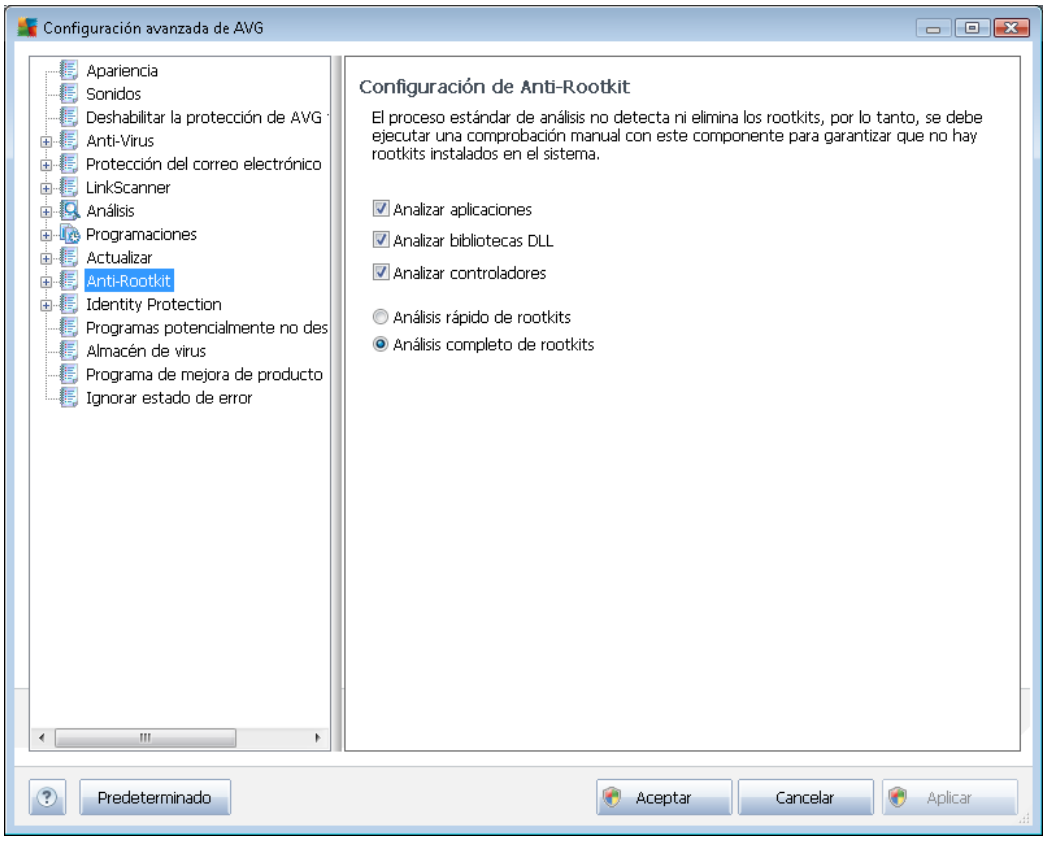


- ***Eliminar archivos de actualización temporales***: pulse este botón para quitar todos los archivos de actualización redundantes del disco duro (*de manera predeterminada, permanecen almacenados allí durante 30 días*)

- ***Restaurar la versión anterior de la base de datos de virus***: pulse este botón para eliminar la última versión de la base de datos de virus del disco duro y para recuperar la versión guardada anteriormente (*la nueva versión de la base de datos de virus formará parte de la actualización siguiente*).

9.10. Anti-Rootkit

En el cuadro de diálogo ***Configuración de Anti-Rootkit*** puede editar la configuración del componente Anti-Rootkit:



Todas las funciones del componente Anti-Rootkitque contiene este cuadro de diálogo también están disponibles para edición directamente desde la interfaz del componente Anti-Rootkit.

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

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

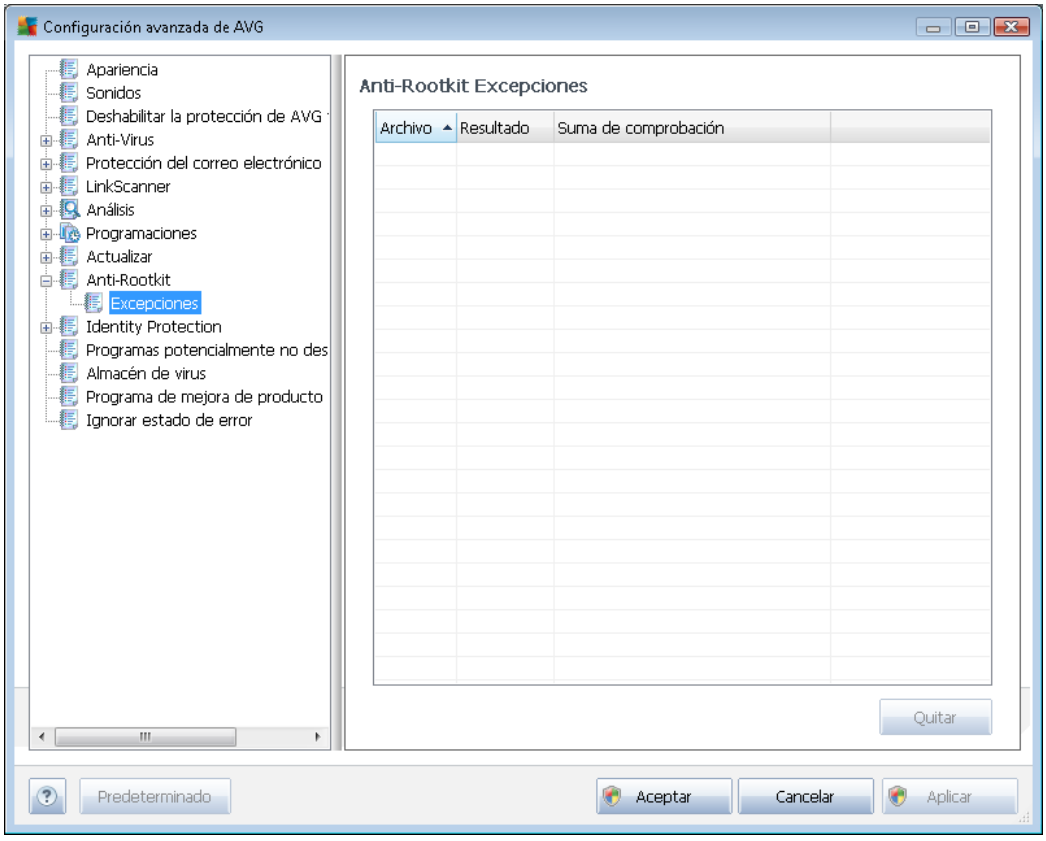
Además, puede seleccionar el modo de análisis de rootkits:

- ***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*), además de todos los discos

locales (*incluyendo el disco flash, pero excluyendo las unidades de disquete y/o CD*)

9.10.1. Excepciones

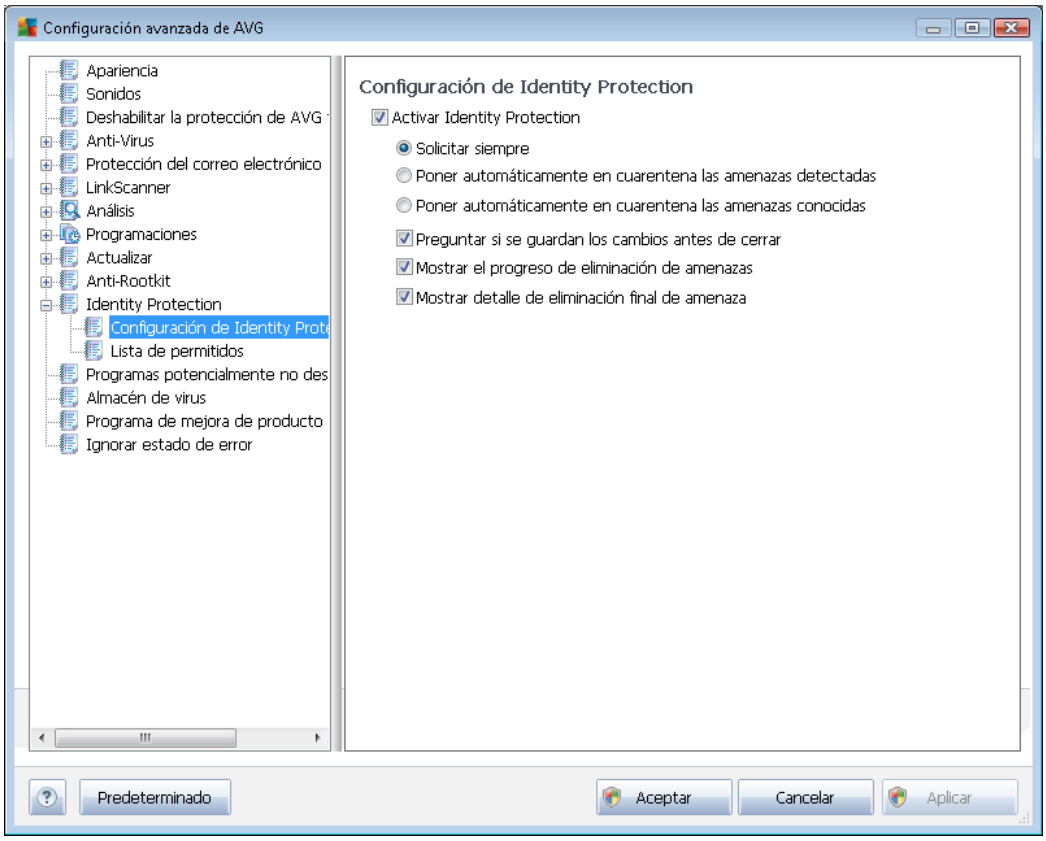
En el cuadro de diálogo ***Excepciones de Anti-Rootkit*** puede definir archivos específicos *(por ejemplo, algunos controladores que podrían ser falsos positivos detectados como rootkits)* que deben ser excluidos del análisis:



9.11. Identity Protection

9.11.1. Configuración de Identity Protection

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



Activar Identity Protection (*activada de manera predeterminada*): deje en blanco esta opción para desactivar el componente Identity Protection.

Recomendamos encarecidamente no hacerlo a menos que sea necesario.

Cuando Identity Protection está activo, puede especificar lo que desea hacer al detectarse una amenaza:

- ***Solicitar siempre*** (*activada de manera predeterminada*): cuando se detecte una amenaza, se le preguntará si debe moverse a la cuarentena para asegurarse de no eliminar ninguna aplicación que desee ejecutar.
- ***Poner automáticamente en cuarentena las amenazas detectadas***: marque esta casilla de verificación para indicar que desea mover inmediatamente todas las amenazas detectadas al espacio seguro del Almacén de virus de. Si se mantiene la configuración predeterminada, cuando se detecte una amenaza se le preguntará si debe moverse a la cuarentena para asegurarse de no eliminar ninguna aplicación que desee ejecutar.
- ***Poner automáticamente en cuarentena las amenazas conocidas***: mantenga seleccionado este elemento si desea que todas las aplicaciones detectadas como posible

malware se muevan de forma automática e inmediata al Almacén de virus de.

A continuación, puede asignar elementos específicos para activar más funciones de Identity Protection:

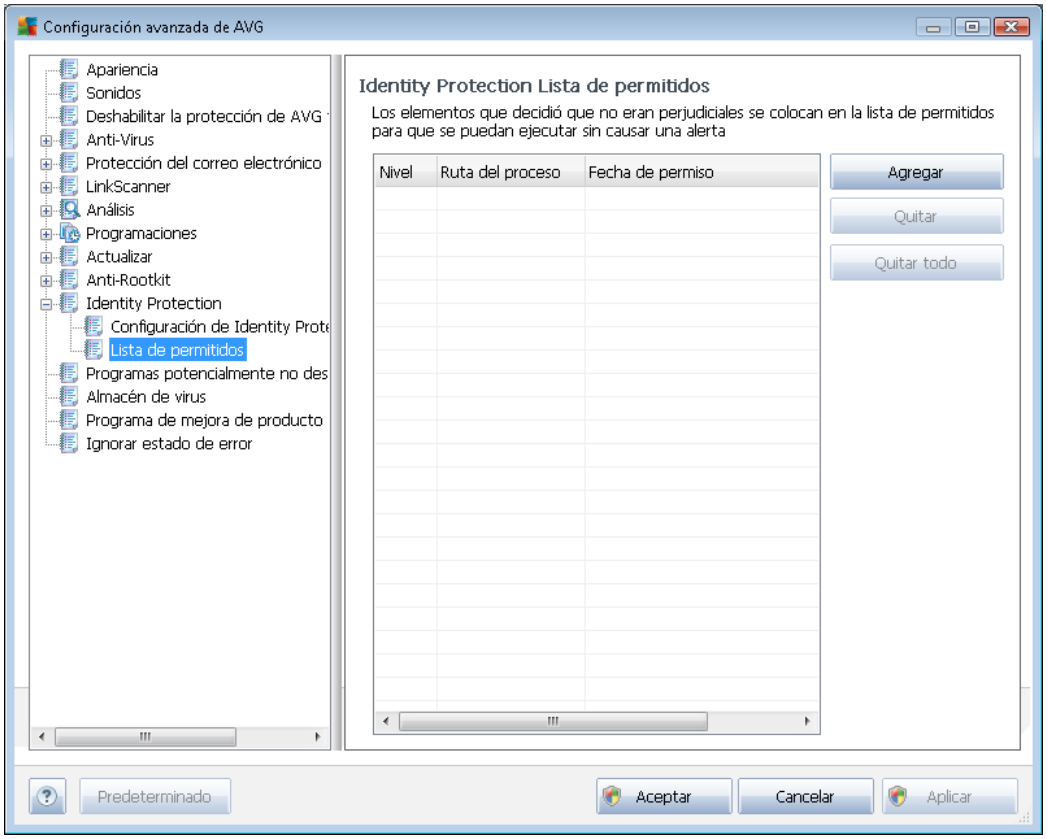
- ***Preguntar si se guarda el trabajo antes de eliminar*** (*activado de manera predeterminada*): mantenga seleccionado este elemento si desea recibir un aviso antes de poner en cuarentena la aplicación detectada como posible malware. En caso de que solamente trabaje con la aplicación, podría perder su proyecto, por lo que debe guardarlo previamente. De manera predeterminada, este elemento está activado y se recomienda encarecidamente dejarlo tal cual.

- ***Mostrar el progreso de la eliminación de malware*** (*activado de manera predeterminada*): cuando este elemento está activado y se detecta un posible malware, se abre un nuevo cuadro de diálogo que muestra el progreso de la puesta en cuarentena.

- ***Mostrar detalles finales de la eliminación de malware*** (*activado de manera predeterminada*): cuando este elemento está activado, ***Identity Protection*** muestra información detallada de cada objeto movido a la cuarentena (*nivel de gravedad, ubicación, etc.*).

9.11.2. Lista de permitidos

Si en el cuadro de diálogo ***Configuración de Identity Protection*** decidió mantener en blanco el elemento ***Poner automáticamente en cuarentena las amenazas detectadas***, cada vez que se detecte malware potencialmente peligroso, se le preguntará si desea eliminarlo. Si a la aplicación sospechosa (*detectada en función de su comportamiento*) le asigna el estado de segura y confirma que debe mantenerse en el equipo, ésta se agregará a la denominada ***Lista de permitidos de Identity Protection*** y no se volverá a notificar como potencialmente peligrosa:



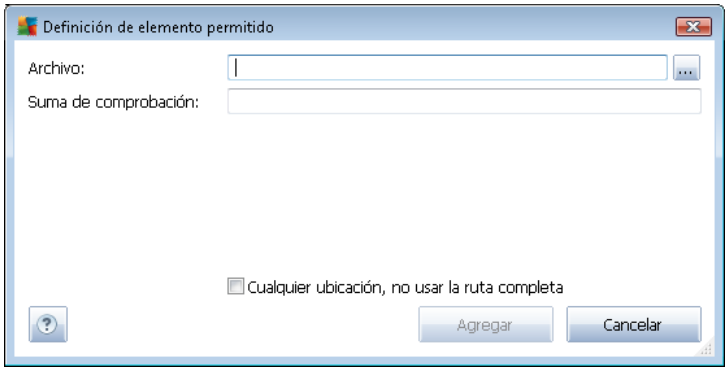
La ***Lista de permitidos de Identity Protection*** proporciona la siguiente información sobre cada aplicación:

- ***Nivel***: identificación gráfica de la gravedad del proceso correspondiente en una escala de cuatro niveles, desde menos importante (■□□□) hasta crítico (■■■■)
- ***Ruta del proceso***: ruta a la ubicación del archivo ejecutable de la aplicación (*proceso*)
- ***Fecha de permiso***: fecha en la que asignó manualmente a la aplicación el estado de segura

Botones de control

Los botones de control disponibles en el cuadro de diálogo ***Lista de permitidos de Identity Protection*** son los siguientes:

- ***Agregar***: pulse este botón para agregar una nueva aplicación a la lista de permitidos. Se abre el siguiente cuadro de diálogo:

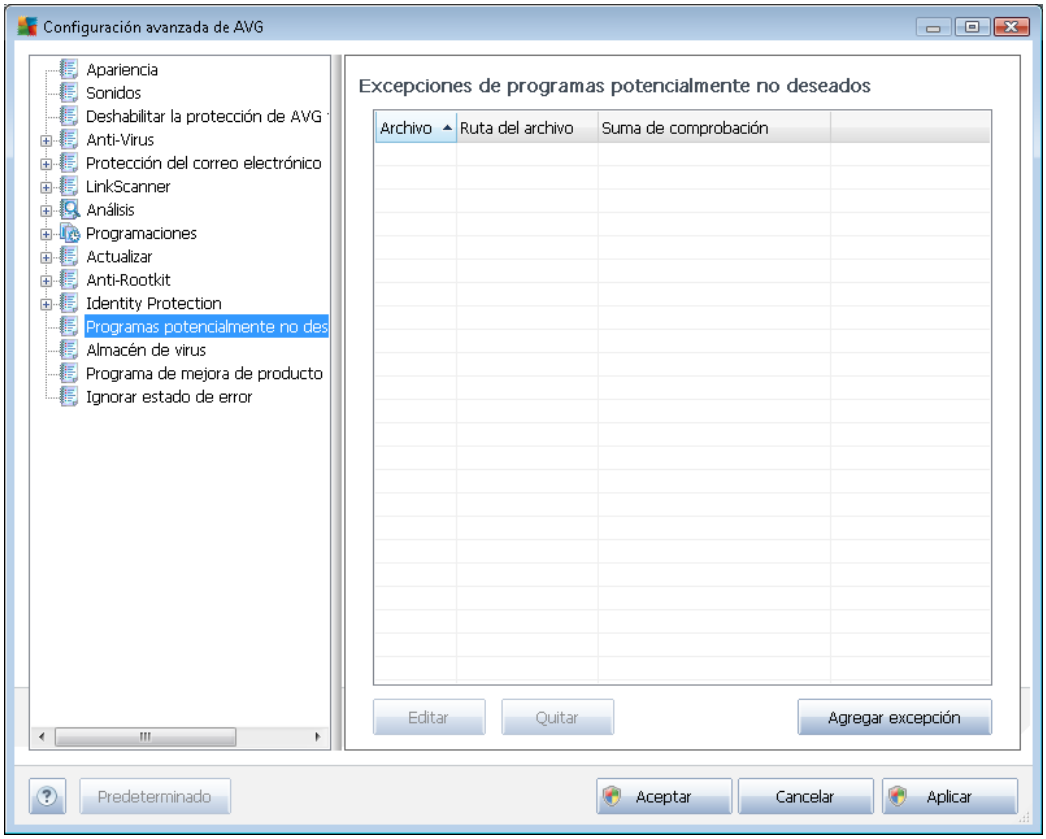


- ***Archivo***: escriba la ruta completa del archivo (*aplicación*) que desea marcar como una excepción
- ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generada automáticamente que permite a AVG distinguir de forma inequívoca el archivo elegido de otros archivos. La suma de comprobación se genera y muestra después de agregar correctamente el archivo.
- ***Cualquier ubicación, no usar la ruta completa***: si desea definir el archivo como una excepción solamente para la ubicación específica, deje esta casilla de verificación en blanco

- ***Quitar***: seleccione esta opción para eliminar de la lista la aplicación elegida
- ***Quitar todo***: seleccione esta opción para eliminar todas las aplicaciones enumeradas

9.12. 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, es posible que el usuario desee mantener determinados programas no deseados en el equipo (programas que se instalaron a propósito). Algunos programas, especialmente los gratuitos, incluyen adware. Este adware podría ser detectado y notificado por **AVG Internet Security 2012** como un *programa potencialmente no deseado*. Si desea mantener dicho programa en el equipo, puede definirlo como una excepción de programa potencialmente no deseado:



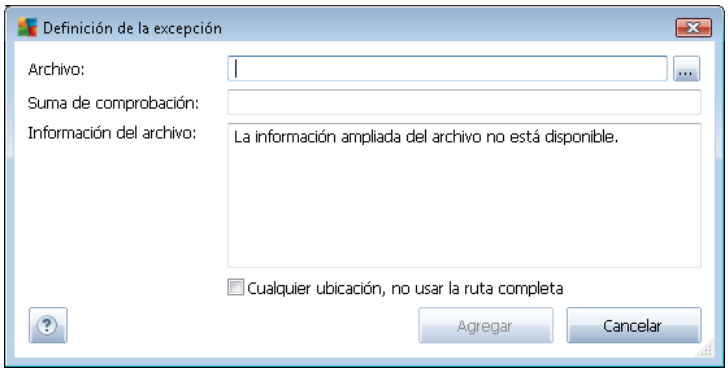
El cuadro de diálogo ***Excepciones de programas potencialmente no deseados*** muestra una lista de excepciones ya definidas y actualmente válidas de programas potencialmente no deseados. Puede editar esta lista, eliminar elementos existentes o añadir nuevas excepciones. En la lista, encontrará la siguiente información para cada una de las excepciones:

- ***Archivo***: proporciona el nombre exacto de la aplicación respectiva
- ***Ruta del archivo***: muestra la ruta 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 generada automáticamente que permite a AVG distinguir de forma inequívoca el archivo elegido de otros archivos. La suma de comprobación se genera y muestra después de agregar correctamente el archivo.

Botones de control

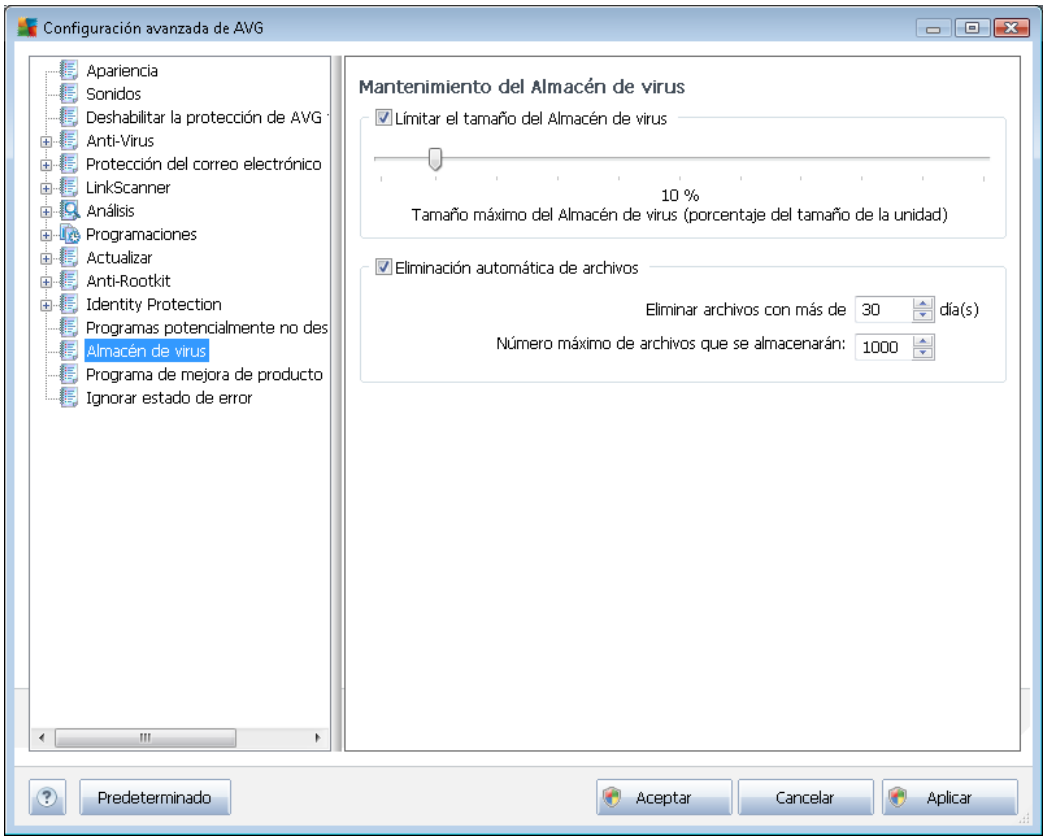
- ***Editar***: abre un cuadro de diálogo de edición (*idéntico al cuadro de diálogo para definición de una nueva excepción, véase a continuación*) para una excepción ya definida, en el que puede modificar los parámetros de la excepción
- ***Quitar***: elimina el elemento seleccionado de la lista de excepciones
- ***Agregar excepción***: abre un cuadro de diálogo de edición en el que puede definir los

parámetros de la nueva excepción que desea crear:



- ***Archivo***: escriba la ruta completa del archivo que desea marcar como excepción
- ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generada automáticamente que permite a AVG distinguir de forma inequívoca el archivo elegido de otros archivos. La suma de comprobación se genera y muestra después de agregar correctamente el archivo.
- ***Información del archivo***: muestra cualquier información adicional que esté disponible sobre el archivo *(licencia/información de la versión, etc.).*
- ***Cualquier ubicación, no usar la ruta completa***: si desea definir el archivo como una excepción solamente para la ubicación específica, deje esta casilla de verificación en blanco. Si la casilla se encuentra marcada, el archivo especificado se definirá como excepción sin importar su ubicación *(sin embargo, de cualquier modo debe escribir la ruta completa al archivo específico; el archivo se utilizará a partir de ese momento como ejemplo único en el caso que aparezcan dos archivos del mismo nombre en el equipo)*.

9.13. Almacén de virus



El cuadro de diálogo ***Mantenimiento del Almacén de virus*** permite definir varios parámetros relativos a la administración de objetos guardados en el Almacén de virus:

- ***Limitar el tamaño del Almacén de virus***: utilice el control deslizante para configurar el tamaño máximo del Almacén de virus. El tamaño se especifica en proporción al tamaño del disco duro local.

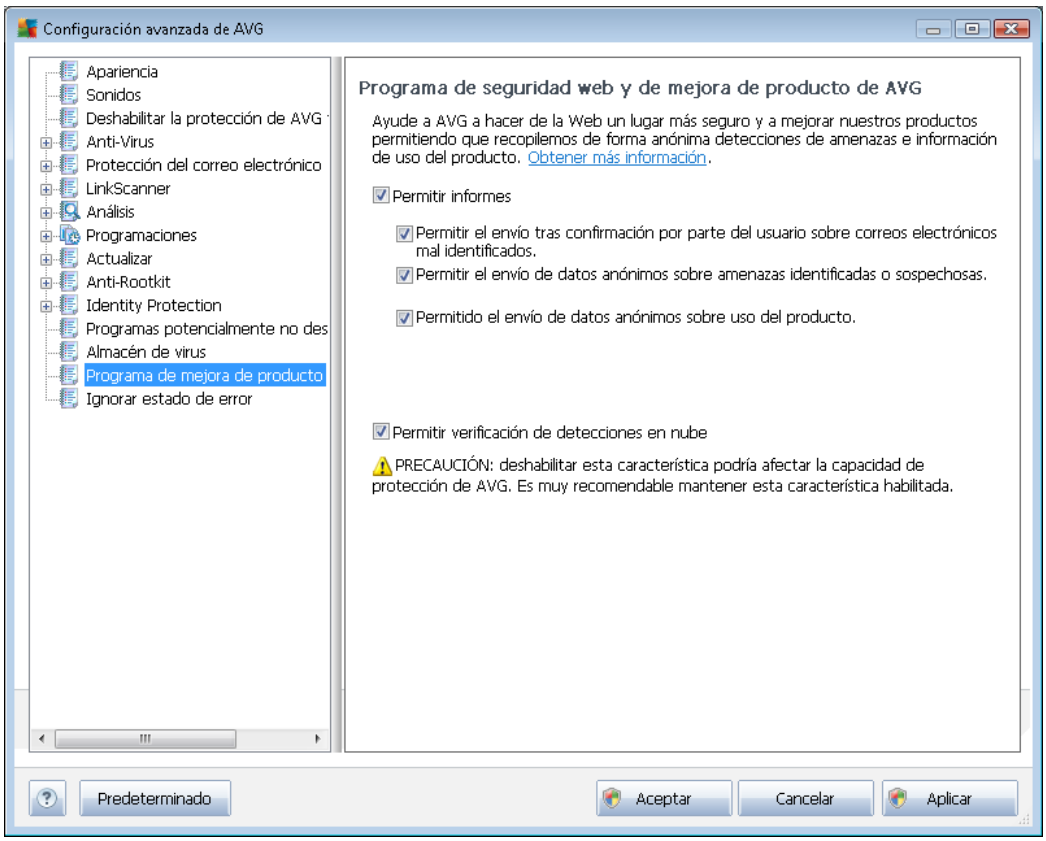
- ***Eliminación automática de archivos***: en esta sección se define el tiempo máximo que los objetos deben permanecer guardados en el Almacén de virus (***Eliminar archivos con más de ... días***) y el número máximo de archivos que se guardarán en el Almacén de virus (***Número máximo de archivos que se almacenarán***).

9.14. Programa de mejora de productos

El cuadro de diálogo ***Seguridad web y programa de mejora de productos de AVG*** le invita a participar en la mejora de los productos de AVG y a ayudarnos a incrementar el nivel de seguridad general en Internet. Marque la opción ***Permitir informes*** para habilitar el envío de informes de las amenazas detectadas a AVG. Esto nos ayuda a recopilar información actualizada sobre las amenazas más recientes de parte de personas del mundo entero, lo cual nos permite ofrecer una mejor protección a todos nuestros usuarios.

El informe se recibe de manera automática, por lo que no le genera ninguna molestia. En

estos informes no se incluye ningún dato personal. El envío de informes de amenazas detectadas es opcional, aunque recomendamos mantener esta opción activada. Nos ayuda a mejorar su protección y la de otros usuarios de AVG.



Hoy en día, hay muchas más amenazas que los simples virus. Los autores de códigos maliciosos y sitios web peligrosos son muy innovadores, y continuamente surgen nuevas amenazas, la mayoría de las cuales se encuentran en Internet. A continuación se incluyen algunas de las más habituales:

- ***Un virus*** es un código malicioso que se copia y se propaga por sí mismo, a menudo pasando inadvertido hasta que el daño ya está hecho. Algunos virus son una amenaza grave ya que eliminan o cambian deliberadamente los archivos que se van encontrando a su paso, mientras que otros realizan acciones aparentemente inofensivas, como reproducir una pieza musical. Sin embargo, todos los virus son peligrosos debido a su capacidad para multiplicarse – incluso el virus más simple puede ocupar toda la memoria del equipo en un instante y provocar una avería.

- ***Un gusano*** es una subcategoría de virus que, a diferencia del virus normal, no necesita un objeto "portador" al que adjuntarse; se envía por sí mismo a otros equipos, generalmente por correo electrónico y, como resultado de ello, suele sobrecargar los servidores de correo electrónico y los sistemas de red.

- ***El spyware*** se define generalmente como programas que abarcan una categoría de malware (*malware = cualquier software malicioso, incluidos los virus*), normalmente troyanos, que tienen el objetivo de robar información personal, contraseñas, números de

tarjetas de crédito o de infiltrarse en un equipo y permitir al atacante controlarlo remotamente; todo ello, por supuesto, sin el conocimiento o consentimiento del propietario del equipo.

- ***Los programas potencialmente no deseados*** (PUP) constituyen un tipo de spyware que puede ser peligroso para el equipo, aunque no necesariamente. Un ejemplo específico de PUP es el adware, un software diseñado para distribuir avisos publicitarios, por lo general, mediante avisos emergentes, lo cual es molesto, pero no realmente dañino.

- ***Las cookies de seguimiento*** también pueden considerarse un tipo de spyware, dado que estos pequeños archivos, que se almacenan en el navegador web y se envían automáticamente al sitio web "madre" cuando el usuario vuelve a visitarlo, pueden contener datos tales como el historial de navegación y otra información similar.

- ***El ataque de vulnerabilidad*** es un código malicioso que aprovecha algún fallo o alguna vulnerabilidad del sistema operativo, navegador de Internet u otro programa esencial.

- ***El phishing*** es un intento de obtener datos personales confidenciales suplantando a una organización conocida y fiable. Generalmente se contacta con las víctimas potenciales a través de un correo electrónico masivo en el que se les pide, por ejemplo, que actualicen los detalles de su cuenta bancaria. Para ello, se les invita a seguir un vínculo que les lleva a un sitio web falso del banco.

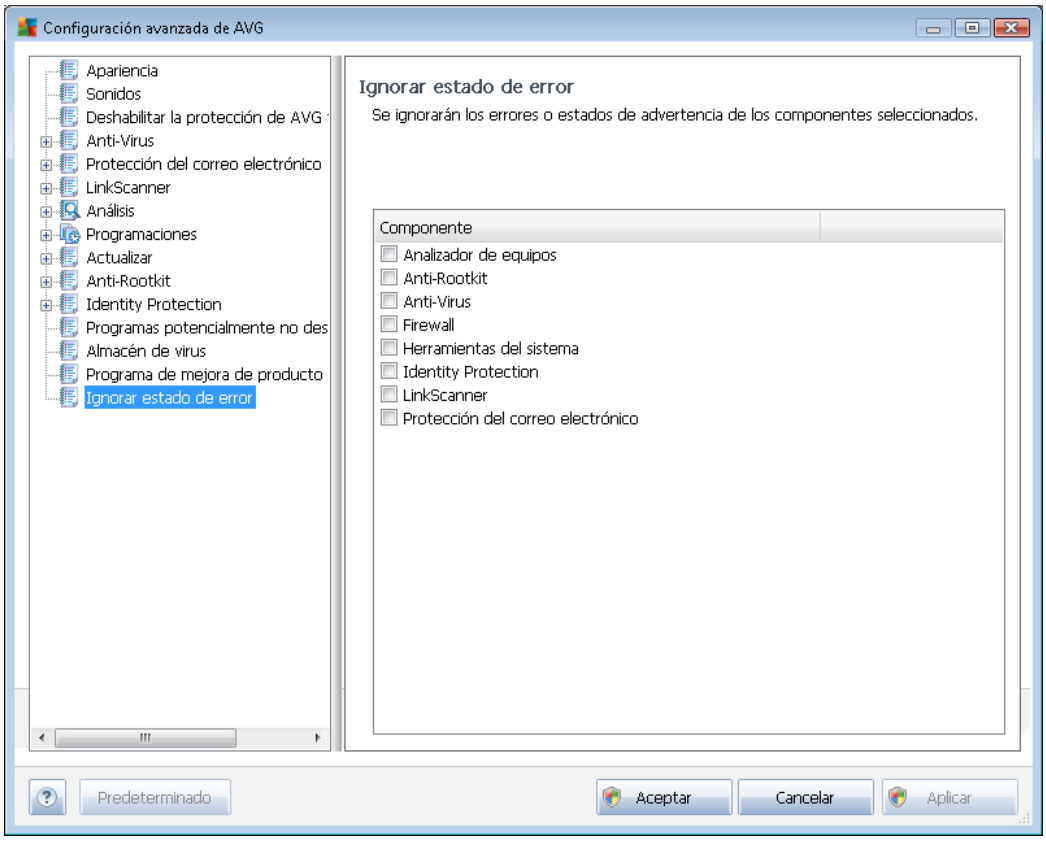
- ***El engaño (hoax)*** es un correo electrónico masivo que contiene información peligrosa, alarmante o simplemente preocupante e inútil. Muchas de las amenazas mencionadas emplean mensajes engañosos de correo electrónico para propagarse.

- ***Los sitios web maliciosos*** son los que instalan deliberadamente software malicioso en su equipo, mientras que los sitios pirateados hacen lo mismo, pero con la diferencia de que se trata de sitios web legítimos que han sido convertidos para que infecten a sus visitantes.

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

9.15. Ignorar estado de error

En el cuadro de diálogo ***Ignorar estado de error*** puede seleccionar aquellos componentes sobre los que no desea ser informado:



De manera predeterminada, no hay ningún componente seleccionado en esta lista. Esto significa que si cualquier componente entra en estado de error, será informado inmediatamente a través de:

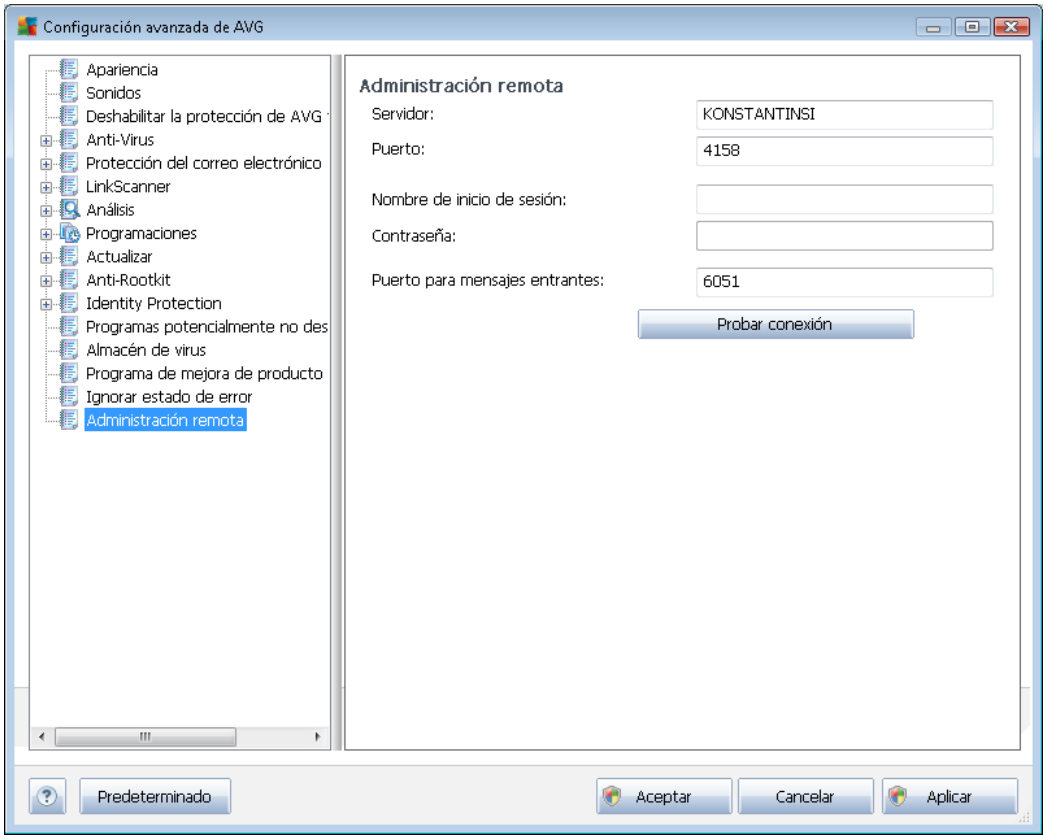
- el icono de la bandeja del sistema: mientras todos los componentes de AVG funcionan correctamente, el icono muestra cuatro colores; por el contrario, cuando se produce un error, el icono aparece con un signo de exclamación amarillo,
- una descripción textual del problema existente en la sección Información sobre el estado de seguridad de la ventana principal de AVG

Puede haber situaciones en las que, por algún motivo, necesite desactivar temporalmente un componente (*puede suceder, aunque no se recomienda. Debe intentar mantener todos los componentes constantemente activos y con la configuración predeterminada*). En tal caso, el icono de la bandeja del sistema informará automáticamente sobre el estado de error del componente. Sin embargo, en este caso en concreto no podemos hablar de error propiamente, ya que ha sido provocado deliberadamente por usted y es consciente del posible riesgo. Al mismo tiempo, una vez adquiere color gris, el icono no puede informar sobre ningún posible error posterior que pueda aparecer.

En dicha situación, en el cuadro de diálogo superior puede seleccionar los componentes que pueden encontrarse en estado de error (*o desactivados*) y sobre los que no desea recibir información. La misma opción *(Ignorar el estado de este componente)* también está disponible para componentes específicos directamente desde la información general de los componentes en la ventana principal de AVG.

9.16. Administración remota

El elemento ***Administración remota*** y su cuadro de diálogo respectivo sólo se mostrarán en el árbol de navegación si ha instalado **AVG Internet Security 2012** con una de las licencias de AVG Business Edition y ha confirmado durante el proceso de instalación que deseaba instalar el componente ***Administración remota***. Para obtener información detallada sobre la instalación y configuración de la administración remota, consulte la documentación de AVG Network Edition correspondiente que se encuentra disponible en el sitio web de AVG (http://www.avg.com/), en la sección Centro de soporte / Descarga.



La configuración de ***Administración remota*** hace referencia a la conexión entre la estación del cliente de AVG y el sistema de administración remoto. Si tiene la intención de conectar la estación respectiva a la administración remota, especifique los parámetros siguientes:

- ***Servidor***: nombre (o dirección IP) del servidor en el que está instalado el Servidor de administración de AVG
- ***Puerto***: escriba el número de puerto que el cliente de AVG utiliza para comunicarse con el

Servidor de administración de AVG (*el puerto número 4158 se considera predeterminado, por lo que, si utiliza este puerto, no es necesario que lo especifique de manera explícita*)

- ***Inicio de sesión***: si la comunicación entre el cliente de AVG y el Servidor de administración de AVG se ha definido como "segura", escriba su nombre de usuario...
- ***Contraseña***: ... y su contraseña
- ***Puerto para mensajes entrantes***: el número del puerto a través del cual el cliente de AVG acepta mensajes entrantes del Servidor de administración de AVG

Botones de control

El botón ***Probar conexión*** permite verificar que todos los datos antes detallados son válidos y pueden utilizarse efectivamente para establecer la conexión con el Centro de datos.

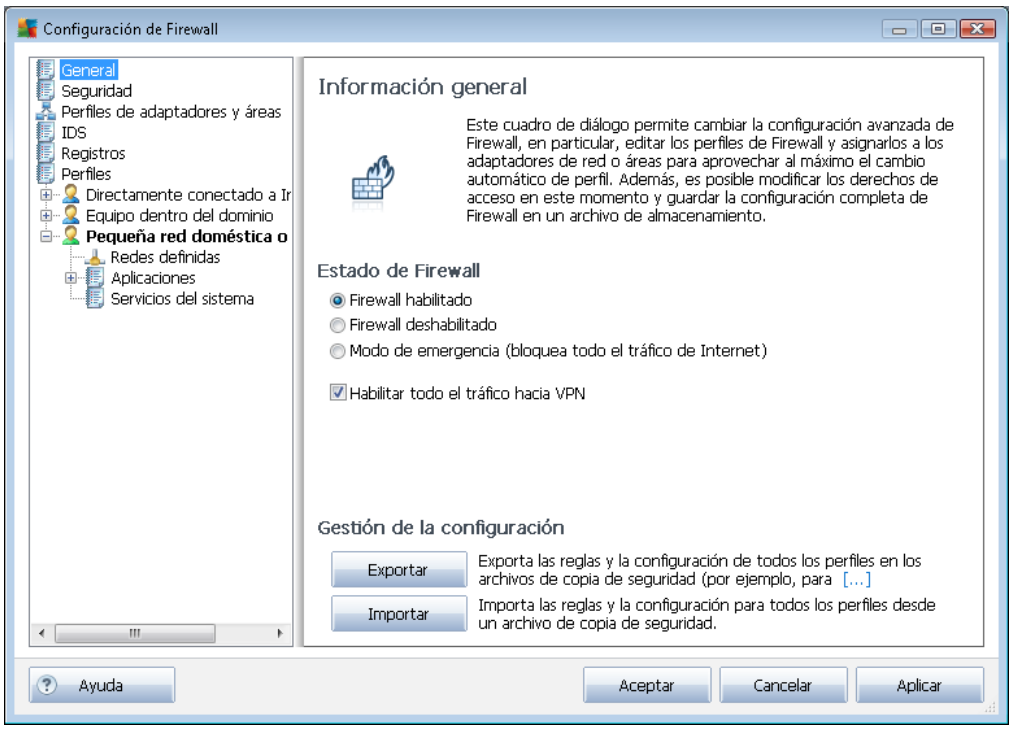
10. Configuración de Firewall

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

Sin embargo, el proveedor del software ha configurado todos los componentes de AVG Internet Security 2012 para ofrecer un rendimiento óptimo. A menos que tenga una buena razón para hacerlo, no cambie la configuración predeterminada. Cualquier cambio en la configuración debería realizarlo únicamente un usuario experimentado.

10.1. General

El cuadro de diálogo ***Información general*** se divide en dos secciones:



Estado de Firewall:

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

- ***Firewall habilitado***: seleccione esta opción para permitir la comunicación a las aplicaciones identificadas como "permitidas" en el conjunto de reglas definidas en el perfil de Firewall seleccionado.
- ***Firewall deshabilitado***: con esta opción se desactiva por completo el Firewall y se permite todo el tráfico de red sin comprobación.
- ***Modo de emergencia (bloquea todo el tráfico de Internet)***: seleccione esta opción para

bloquear el tráfico en todos los puertos de red; el Firewall se seguirá ejecutando, pero se detendrá todo el tráfico de red.

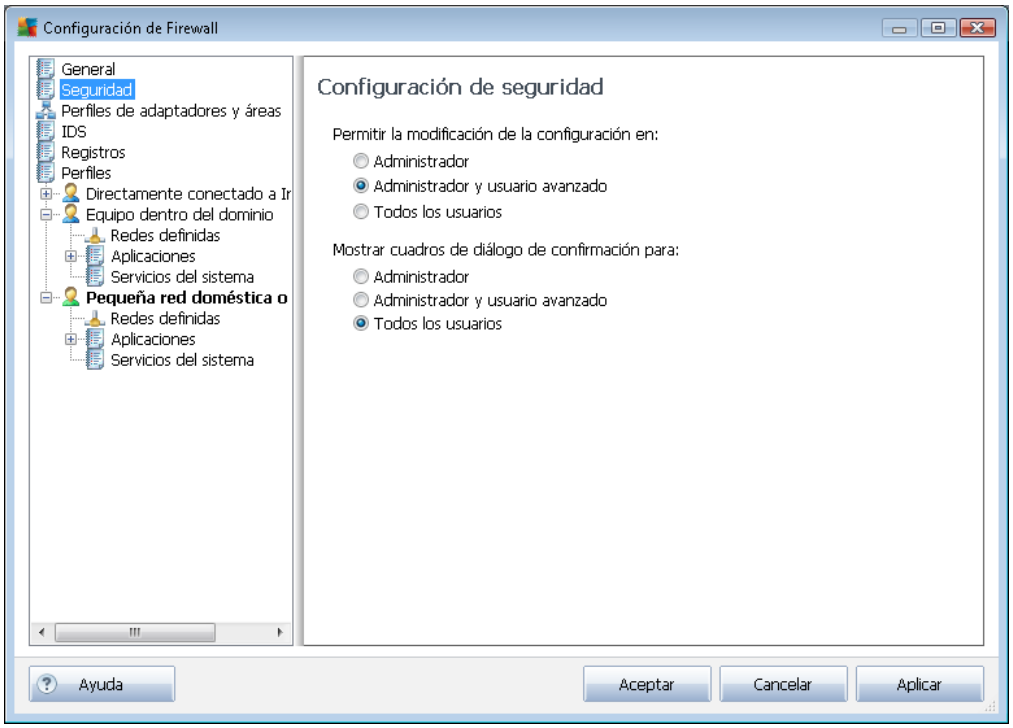
- ***Habilitar todo el tráfico hacia VPN*** *(activada de manera predeterminada)*: si utiliza una conexión VPN *(Red privada virtual)*, por ejemplo, para conectarse a la oficina desde casa, se recomienda marcar esta casilla. ***AVG Firewall*** buscará automáticamente entre los adaptadores de red para encontrar los que se utilizan para la conexión VPN, y permitirá que todas las aplicaciones se conecten a la red de destino *(sólo se aplica a las aplicaciones sin regla específica de Firewall asignada)*. En un sistema estándar con adaptadores de red comunes, este simple paso le evitará tener que crear una regla específica para cada aplicación que necesite usar con VPN.

Nota: *para habilitar la conexión VPN para todas, es necesario permitir la comunicación a los siguientes protocolos del sistema: GRE, ESP, L2TP, PPTP. Esto puede hacerse mediante el cuadro de diálogo Servicios del sistema.*

Gestión de la configuración

En la sección ***Gestión de la configuración*** puede ***Exportar*** o ***Importar*** la configuración del Firewall ; por ejemplo, puede exportar la configuración y las reglas definidas del Firewall a los archivos de copia de seguridad, o bien importar el archivo completo de copia de seguridad.

10.2. Seguridad



En el cuadro de diálogo ***Configuración de seguridad*** puede definir reglas generales para el comportamiento de Firewall, independientemente del perfil seleccionado:

- ***Permitir la modificación de la configuración en***: permite especificar quién está autorizado a modificar la configuración del Firewall.

- ***Mostrar cuadros de diálogo de confirmación para***: permite especificar a quién deben mostrarse los cuadros de diálogo *(cuadros de diálogo que solicitan al usuario que decida sobre una situación no contemplada por ninguna de las reglas definidas del Firewall)*.

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

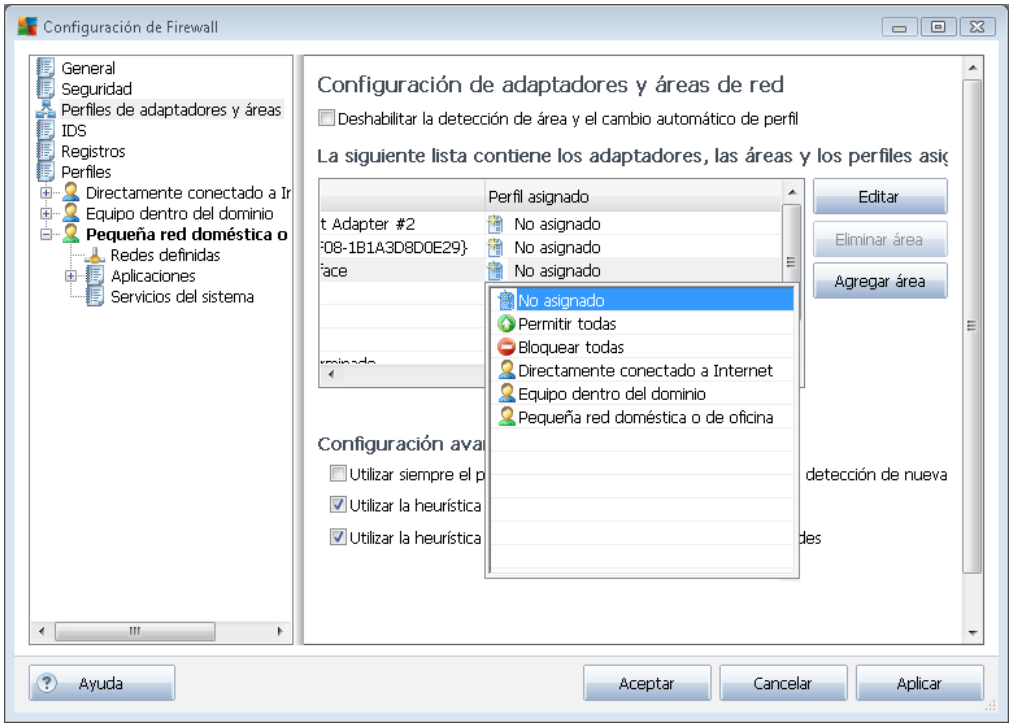
- ***Administrador***: controla el equipo completamente y tiene el derecho de asignar cada usuario a grupos con permisos específicamente definidos.

- ***Administrador y usuario avanzado***: el administrador puede asignar cualquier usuario a un grupo especificado (*Usuario avanzado*) y definir permisos para los miembros del grupo.

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

10.3. Perfiles de adaptadores y áreas

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



- ***Deshabilitar la detección de área y el cambio automático de perfil*** *(desactivada de forma predeterminada)*: se puede asignar uno de los perfiles predefinidos a cada tipo de

interfaz de red, respectivamente a cada área. Si no desea definir perfiles específicos, se utilizará un perfil común. No obstante, si decide diferenciar perfiles y asignarlos a áreas y adaptadores específicos y, posteriormente, desea cambiar temporalmente por algún motivo esta configuración, marque la opción ***Deshabilitar la detección de área y el cambio automático de perfil***.

- ***Lista de adaptadores, áreas y perfiles asignados***: en esta lista puede encontrar información general de los adaptadores y áreas detectados. Puede asignar a cada uno de ellos un perfil específico desde el menú de perfiles definidos. Para abrir este menú, haga clic sobre el elemento correspondiente de la lista de adaptadores *(en la columna Perfil asignado)* y seleccione el perfil desde el menú contextual.

Configuración avanzada

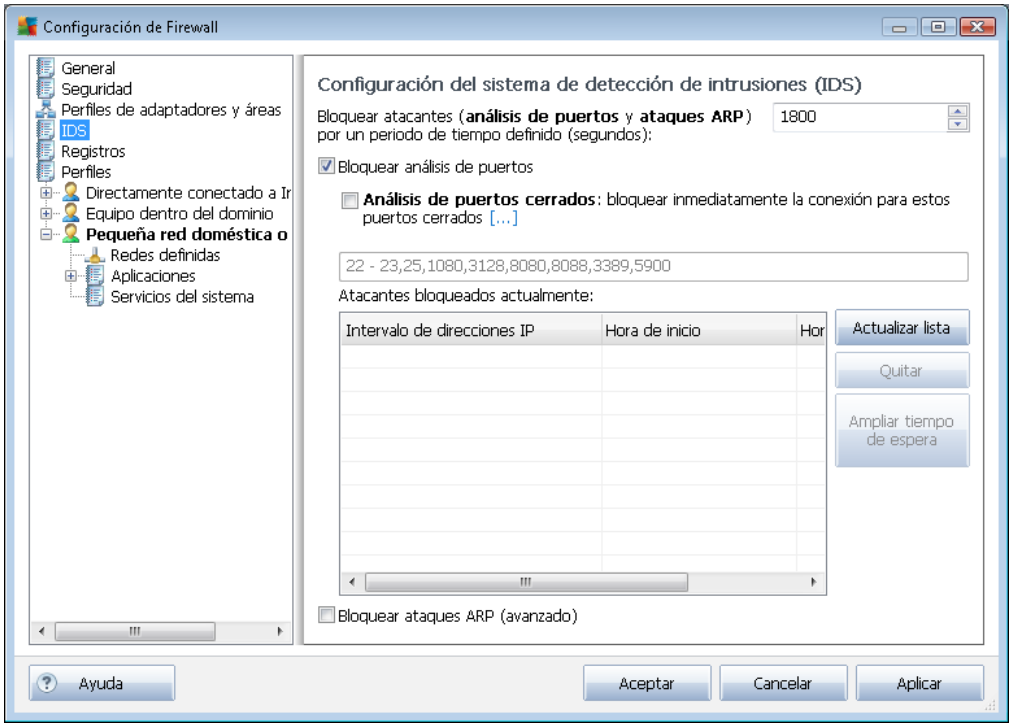
- ***Utilizar siempre el perfil predeterminado y no mostrar diálogo de detección de nueva red***: siempre que su equipo se conecte a una nueva red, el Firewall le alertará y mostrará un cuadro de diálogo para que seleccione un tipo de conexión de red y le asigne un perfil de Firewall. Si no desea que se muestre el cuadro de diálogo, marque esta casilla.

- ***Utilizar la heurística de AVG para la detección de nuevas redes***: permite recopilar información sobre una nueva red detectada con el mecanismo propio de AVG (*sin embargo, esta opción solo está disponible en Windows VISTA o superior*).

- ***Utilizar la heurística de Microsoft para la detección de nuevas redes***: permite recopilar información sobre una nueva red detectada desde el servicio de Windows (*esta opción solo está disponible en Windows Vista o superior*).

10.4. IDS

El Sistema de detección de intrusiones es una característica de análisis de comportamiento especial diseñada para identificar y bloquear intentos de comunicación sospechosos en determinados puertos 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)*** contiene las siguientes opciones de configuración:

- ***Bloquear atacantes (análisis de puertos y ataques ARP) por un periodo de tiempo definido***: aquí puede especificar durante cuántos segundos debe estar bloqueado un puerto cuando se detecta en él un intento de comunicación sospechoso. De manera predeterminada, el intervalo de tiempo está configurado como 1.800 segundos (*30 minutos*).

- ***Bloquear análisis de puertos*** *(activada de manera predeterminada)*: marque la casilla para bloquear intentos de comunicación en todos los puertos TCP y UDP que llegan al equipo desde el exterior. Para cualquiera de estas conexiones se permiten cinco intentos, el sexto se bloquea. La opción está activada de forma predeterminada, y se recomienda mantener esta configuración. Si mantiene activada la opción ***Bloquear análisis de puertos***, puede configurar más opciones *(de lo contrario, la siguiente opción estará desactivada)*:

    - ***Analisis de puertos cerrados***: marque la casilla para bloquear inmediatamente cualquier intento de comunicación a través de los puertos especificados en el campo de texto de abajo. Cada puerto o intervalos de puertos deben separarse con comas. Existe una lista predefinida de puertos recomendados si desea utilizar esta característica.

    - Atacantes bloqueados actualmente: esta sección muestra cualquier intento de comunicación que está siendo bloqueado actualmente por el Firewall. El historial completo de intentos bloqueados se puede ver en el cuadro de diálogo Registros (*ficha Registros de análisis de puertos*).

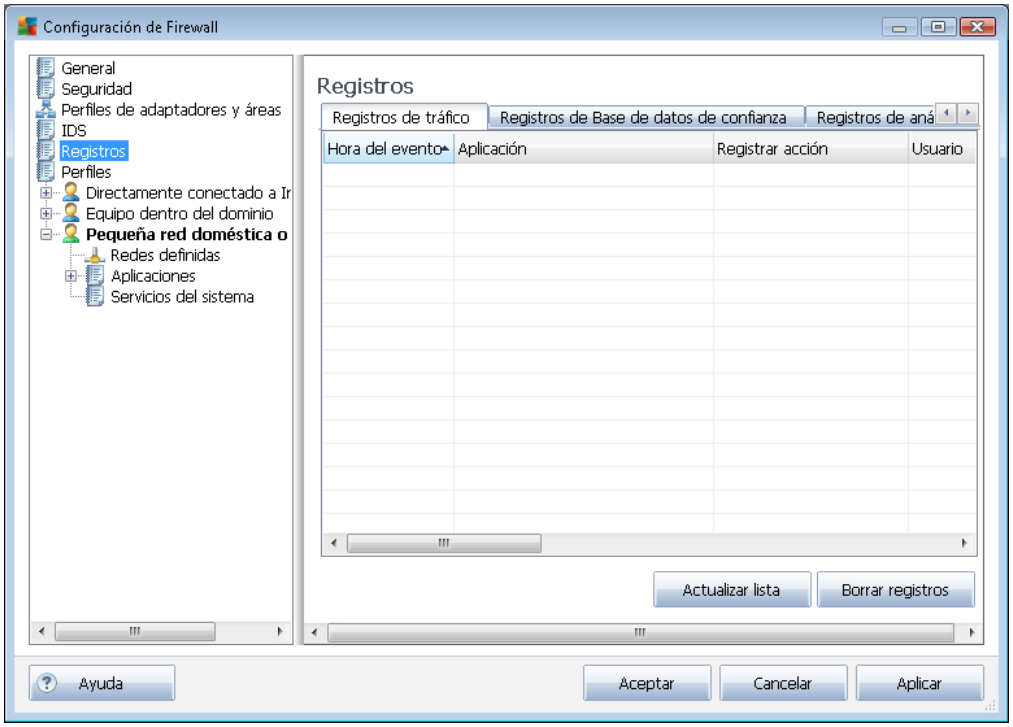
- ***Bloquear ataques ARP (avanzado)*** *(desactivada de manera predeterminada)*: marque esta

opción para activar el bloqueo de tipos especiales de intentos de comunicación dentro de una red local detectados por el ***IDS*** como potencialmente peligrosos. Se aplica el tiempo configurado en ***Bloquear atacantes por un periodo de tiempo definido.*** Se recomienda que sólo utilicen esta característica los usuarios avanzados que estén familiarizados con el tipo y el nivel de riesgo de sus redes locales.

Botones de control

- ***Actualizar lista***: pulse el botón para actualizar la lista (*para incluir cualquier intento bloqueado recientemente*)
- ***Quitar***: pulse el botón para cancelar un bloqueo seleccionado
- ***Ampliar tiempo de espera***: pulse el botón para prolongar el tiempo que un intento seleccionado permanece bloqueado. Aparecerá un nuevo cuadro de diálogo con más opciones, donde podrá establecer una hora y fecha específicas o una duración ilimitada.

10.5. Registros



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

- ***Registros de tráfico***: muestra información sobre la actividad de todas las aplicaciones que hayan intentado conectarse con la red.

- ***Registros de Base de datos de confianza***: *una base de datos de confianza* es una base de datos interna de AVG que recopila información sobre aplicaciones certificadas y de confianza a las que siempre se les puede permitir comunicarse en línea. La primera vez que una aplicación nueva intenta conectarse con la red (*es decir, cuando todavía no hay ninguna regla del firewall especificada para esa aplicación*), es necesario evaluar si debería permitirse o no la comunicación de esa aplicación con la red. Primero, AVG busca en la *Base de datos de confianza* y, si la aplicación figura allí, se le otorgará acceso a la red de forma automática. Sólo después de ese paso y siempre que la base de datos no contenga información sobre esa aplicación, se le preguntará en un cuadro de diálogo independiente si desea permitir que esa aplicación acceda a la red.

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

- ***Registros 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.

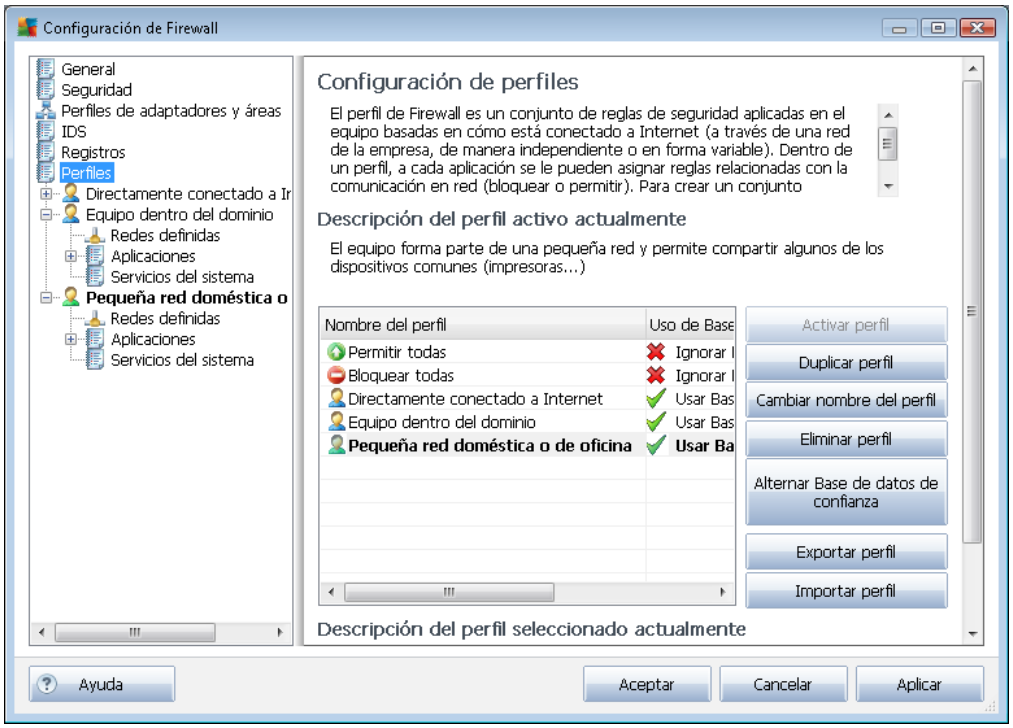
Botones de control

- ***Actualizar lista***: todos los parámetros registrados pueden ordenarse según el atributo seleccionado: cronológicamente (*fechas*) o alfabéticamente (*las otras columnas*); simplemente haga clic en el título de la columna deseada. Utilice el botón ***Actualizar lista*** para actualizar la información que aparece en este momento en pantalla.

- ***Borrar registros***: pulse este botón para eliminar todas las entradas de la tabla.

10.6. Perfiles

En el cuadro de diálogo ***Configuración de perfiles*** puede encontrar una lista de todos los perfiles disponibles:



Los perfiles del sistema *(Permitir todas, Bloquear todas)* no puede editarse. Sin embargo, todos los perfiles personalizados *(Directamente conectado a Internet, Equipo dentro del dominio, Pequeña red doméstica o de oficina)* pueden editarse posteriormente en este cuadro de diálogo a través de los botones de control siguientes:

- ***Activar perfil***: este botón establece el perfil seleccionado como activo, lo que significa que la configuración del perfil elegido será utilizada por el Firewall para controlar el tráfico de la red.
- ***Duplicar perfil***: permite crear una copia idéntica del perfil seleccionado, que luego se podrá editar y cambiar de nombre para crear un nuevo perfil basado en el perfil original duplicado.
- ***Cambiar nombre del perfil***: permite establecer un nombre nuevo para el perfil seleccionado.
- ***Eliminar perfil***: elimina el perfil seleccionado de la lista.
- ***Alternar Base de datos de confianza***: para el perfil seleccionado, puede decidir usar la información de la *Base de datos de confianza* (*la Base de datos de confianza es una base de datos interna de AVG que recopila información sobre aplicaciones certificadas y de confianza a las que siempre se les permitirá comunicarse en línea*).

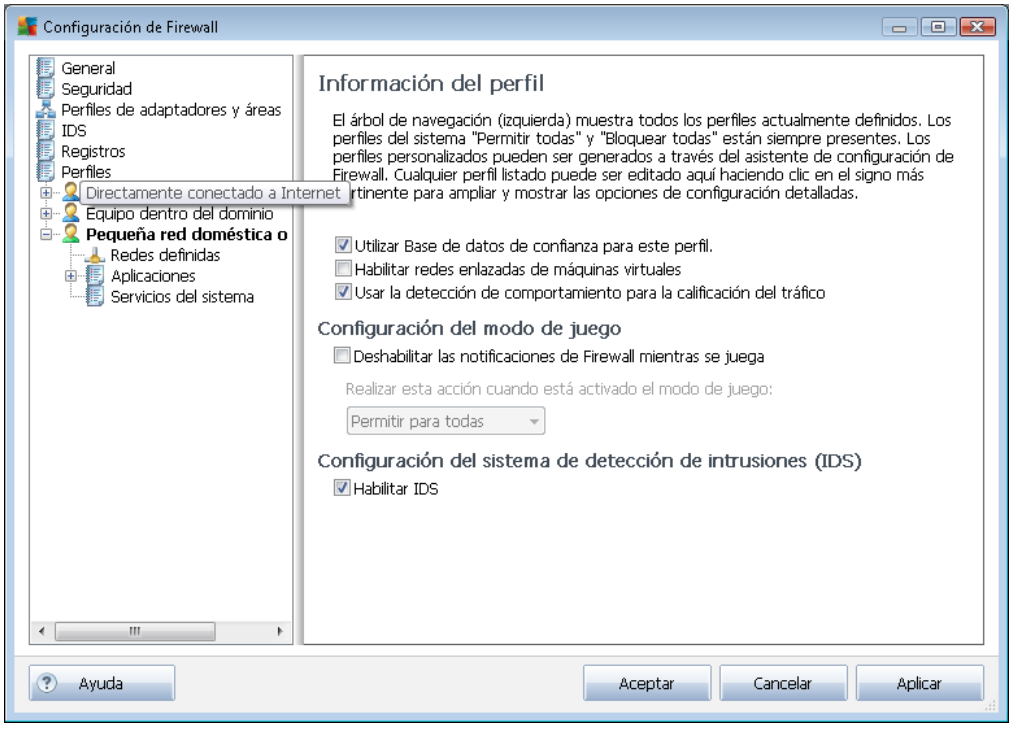
- ***Exportar perfil***: escribe la configuración del perfil seleccionado en un archivo que se guardará para su posible uso en el futuro.

- ***Importar perfil***: realiza la configuración del perfil seleccionado según los datos exportados del archivo de copia de seguridad de la configuración.

En la sección inferior del cuadro de diálogo puede encontrar la descripción del perfil actualmente seleccionado en la lista de arriba.

Según la cantidad de perfiles definidos que aparezcan en la lista del cuadro de diálogo ***Perfil***, se modificará la estructura del menú de navegación de la izquierda. Cada perfil definido crea una rama específica debajo del elemento ***Perfil***. Así, es posible editar perfiles específicos en los siguientes cuadros de diálogo (*que son idénticos para todos los perfiles*):

10.6.1. Información del perfil



El cuadro de diálogo ***Información del perfil*** es el primer cuadro de diálogo de una sección en la que puede editar la configuración de cada perfil en cuadros de diálogo independientes que se refieren a parámetros específicos del perfil.

- ***Utilizar Base de datos de confianza para este perfil*** (*activada de manera predeterminada*): marque esta opción para activar la *Base de datos de confianza* (*es decir, la base de datos interna de AVG que recopila información sobre las aplicaciones certificadas y de confianza que se comunican en línea. Si no existe ninguna regla especificada para una aplicación determinada, debe decidirse si se puede otorgar acceso a la red a esa aplicación. Primero, AVG busca en la base de datos de confianza y, si la aplicación figura allí, se considerará segura y se le permitirá comunicarse a través de la red. Si no figura, se le solicitará que decida si desea permitir que esa aplicación se comunique a través de la*

red) para el perfil correspondiente

- ***Habilitar redes enlazadas de máquinas virtuales*** (*desactivada de manera predeterminada*): marque esta opción para permitir que las máquinas virtuales de VMware se conecten directamente a la red.

- ***Usar la detección de comportamiento para la calificación del tráfico*** (*activada de manera predeterminada*): marque esta opción para permitir que el Firewall emplee la función Identity Protection al evaluar una aplicación. Identity Protection puede determinar si la aplicación tiene algún comportamiento sospechoso o si se puede confiar en ella para permitirle comunicarse en línea.

Configuración del modo de juego

En la sección ***Configuración del modo de juego*** puede decidir y confirmar marcando el elemento respectivo si desea que se muestren los mensajes informativos del Firewall aunque se esté ejecutando una aplicación de pantalla completa en el equipo (*normalmente, juegos, pero también puede aplicarse a aplicaciones a pantalla completa como una presentación PTT*), ya que los mensajes informativos pueden interrumpir.

Si marca el elemento ***Deshabilitar las notificaciones de Firewall mientras se juega***, seleccione en el menú desplegable qué acción se debe realizar en caso de que una aplicación nueva sin reglas especificadas intente comunicarse a través de la red (*son aplicaciones que, por lo general, harían que se abriera un cuadro de diálogo de pregunta*). Las opciones posibles son permitir o bloquear todas las aplicaciones de ese tipo.

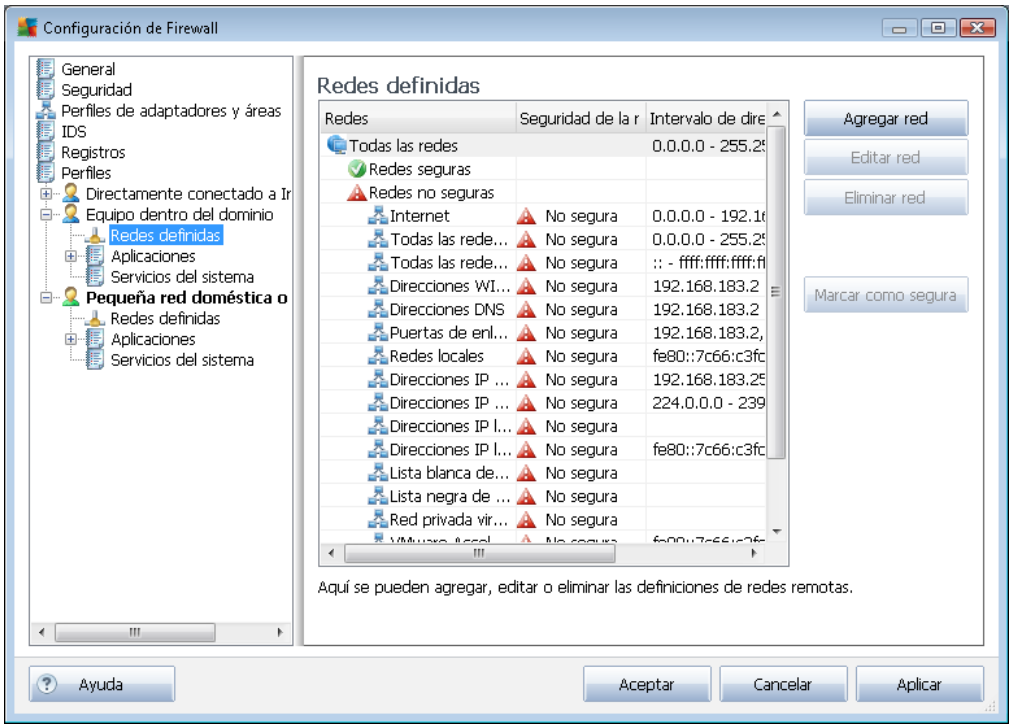
Cuando el modo de juego está activado, todas las tareas programadas (*análisis, actualizaciones*) se posponen hasta que se cierra la aplicación.

Configuración del sistema de detección de intrusiones (IDS)

Marque la casilla de verificación ***Habilitar IDS*** para activar una característica de análisis de comportamiento especial diseñada para identificar y bloquear intentos de comunicación sospechosos en puertos específicos del equipo *(para obtener más información sobre la configuración de esta característica, consulte el capítulo sobre IDS en esta misma documentación).*

10.6.2. Redes definidas

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

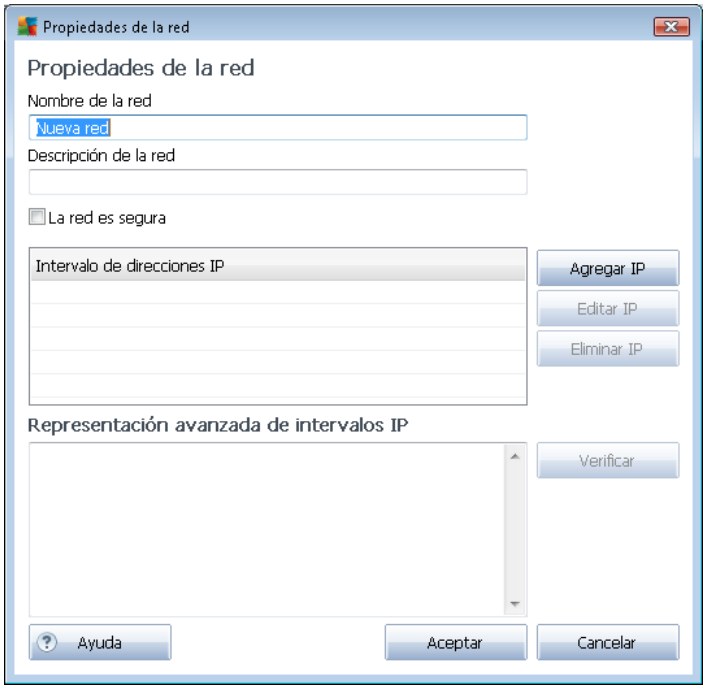


La lista proporciona la siguiente información sobre cada red detectada:

- ***Redes***: proporciona una lista con los nombres de todas las redes a las que el equipo está conectado.
- ***Seguridad de la red***: de manera predeterminada, todas las redes se consideran no seguras y sólo si tiene la certeza de que una red determinada es segura, puede asignarle tal estado (*haga clic en el elemento de la lista correspondiente a la red en cuestión y seleccione Segura en el menú contextual*); todas las redes seguras se incluirán en el grupo de redes con las que la aplicación puede comunicarse cuando la regla de la aplicación establecida sea Permitir para seguras.
- ***Intervalo de direcciones IP***: cada red se detectará automáticamente y se especificará en forma de intervalo de direcciones IP.

Botones de control

- ***Agregar red***: abre el cuadro de diálogo ***Propiedades de la red***, donde puede editar los parámetros de la red que acaba de definir:



En este cuadro de diálogo puede especificar el ***Nombre de la red***, proporcionar una ***Descripción de la red*** y, posiblemente, asignar a la red el estado de segura. La nueva red se puede definir manualmente en un cuadro de diálogo independiente que se abre a través del botón ***Agregar IP*** (o ***Editar IP*** / ***Eliminar IP***). En este cuadro de diálogo puede especificar la red indicando su intervalo o máscara IP. Si debe definir un número amplio de redes como parte de una red creada recientemente, puede utilizar la opción ***Representación avanzada de intervalos IP***: introduzca la lista de todas las redes en el campo de texto correspondiente (*se admite cualquier formato estándar*) y pulse el botón ***Verificar*** para asegurarse de que el formato es reconocible. A continuación, pulse ***Aceptar*** para confirmar y guardar los datos.

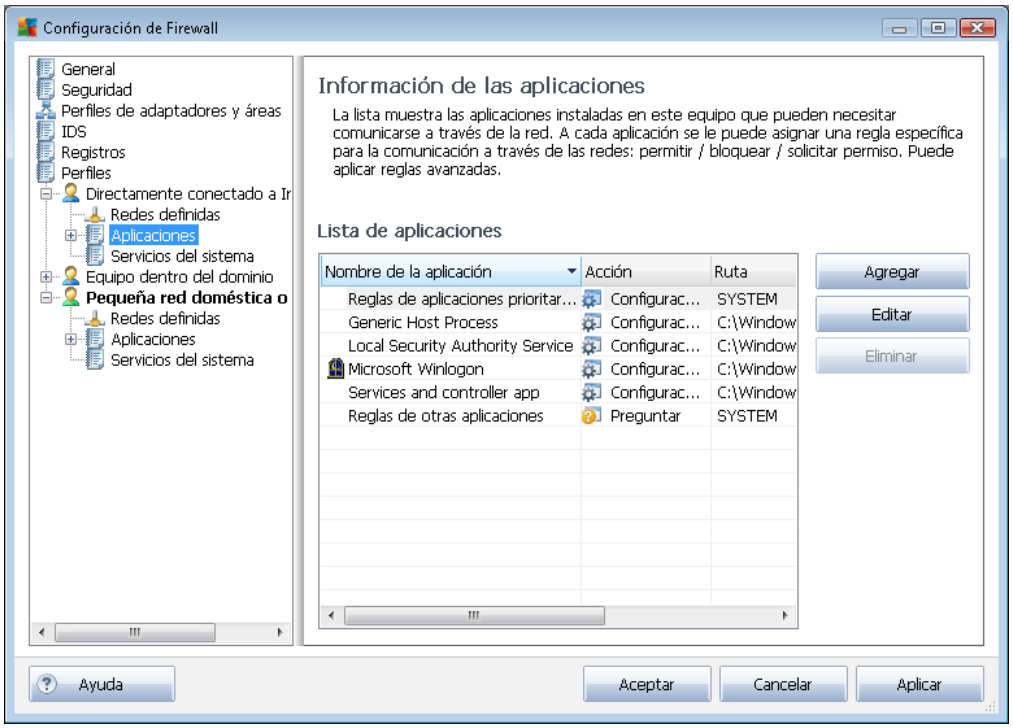
- ***Editar red***: abre la ventana de cuadro de diálogo ***Propiedades de la red*** (*ver más arriba*), donde puede editar los parámetros de una red ya definida (*el cuadro de diálogo es idéntico al que sirve para agregar una nueva red; consulte la descripción del párrafo anterior*).

- ***Eliminar red***: quita la red seleccionada de la lista de redes.

- ***Marcar como segura***: de manera predeterminada, todas las redes se consideran no seguras y sólo si tiene la certeza de que la red respectiva es segura, puede utilizar este botón para establecerla como tal (*y viceversa, una vez que la red es clasificada como segura, el texto del botón cambia a "Marcar como no segura"*).

10.6.3. Aplicaciones

El cuadro de diálogo ***Información de las aplicaciones*** muestra todas las aplicaciones instaladas que puede ser que necesiten comunicarse a través de la red y los iconos para la acción asignada:



Las aplicaciones incluidas en ***Lista de aplicaciones*** son las que se detectan en su equipo (*y a las que se asignan las acciones correspondientes*). Se pueden utilizar los siguientes tipos de acción:

- - Permitir comunicación para todas las redes
- - Permitir comunicación sólo para las redes definidas como seguras
- - Bloquear comunicación
- - Mostrar cuadro de diálogo de pregunta (*el usuario podrá decidir si desea autorizar 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 aplicaciones ya instaladas; si instala una nueva aplicación posteriormente, tendrá que definir reglas de Firewall para ella. De manera predeterminada, cuando la nueva aplicación intente conectarse a través de la red por primera vez, el Firewall creará automáticamente una regla para ella según la base de datos de confianza o le preguntará si desea autorizar o bloquear la comunicación. En el segundo caso, podrá guardar su respuesta como regla permanente (y se incluirá en este cuadro de diálogo).

Por supuesto, también puede definir inmediatamente reglas para la nueva aplicación. En este

cuadro de diálogo, pulse ***Agregar*** y rellene los detalles de la aplicación.

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

- ***Reglas de aplicaciones prioritarias*** (*en la parte superior de la lista*) son las que tienen prioridad y que siempre se aplican antes de las reglas de cualquier aplicación individual.
- ***Reglas de otras aplicaciones*** (*en la parte inferior de la lista*) son las que se aplican en "última instancia", cuando no se aplica ninguna regla de aplicación específica; por ejemplo, en el caso de una aplicación desconocida no definida.

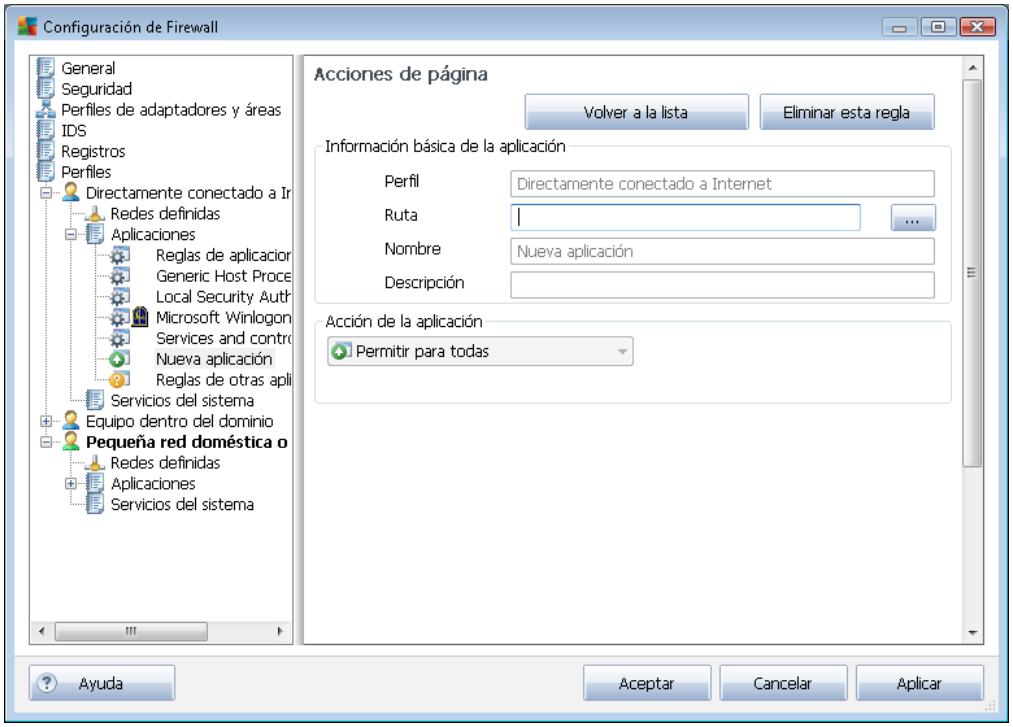
Estos elementos tienen opciones de configuración diferentes de las aplicaciones comunes y sólo deben usarlos los usuarios experimentados. Recomendamos encarecidamente no modificar la configuración.

Botones de control

Puede editar la lista empleando los siguientes botones de control:

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

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



Botones de control

Hay dos botones de control disponibles en la parte superior del cuadro de diálogo:

- ***Volver a la lista***: pulse el botón para mostrar la información general de todas las reglas de aplicación definidas.
- ***Eliminar esta regla***: pulse el botón para borrar la regla de aplicación mostrada actualmente. ***Tenga en cuenta que esta acción no se puede deshacer.***

Información básica de la aplicación

En esta sección, escriba el ***Nombre*** de la aplicación y, de manera opcional, una ***Descripción*** (*un breve comentario para su información*). En el campo ***Ruta***, escriba la ruta completa para llegar a la aplicación (*el archivo ejecutable*) en el disco. También puede buscar la aplicación en la estructura de árbol pulsando el botón "***...***".

Acción de la aplicación

En el menú desplegable, puede seleccionar la regla de Firewall para la aplicación, es decir, qué

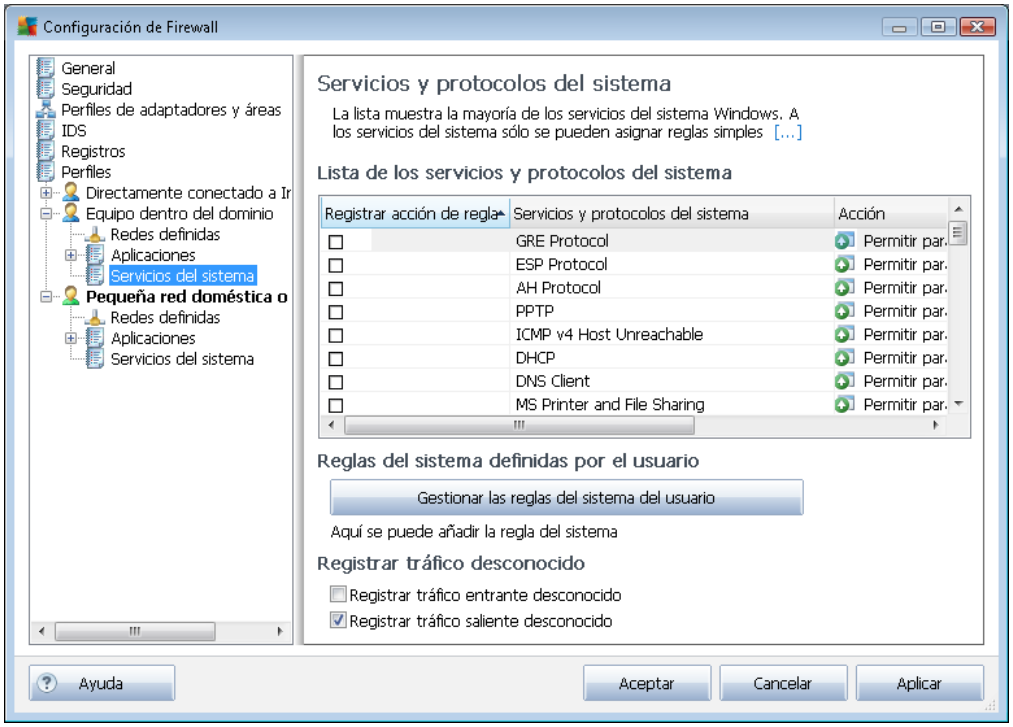
debe hacer el Firewall cuando la aplicación intenta comunicarse a través de la red:

- ***Permitir para todas***: permite a la aplicación comunicarse con todas las redes y adaptadores definidos sin limitaciones.
- ***Permitir para seguras***: permite a la aplicación comunicarse solo conredes definidas como seguras *(de confianza)*.
- ***Bloquear***: impide la comunicación automáticamente; la aplicación no podrá conectarse con 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 ampliadas y detalladas en la parte inferior del cuadro de diálogo, en la sección ***Reglas de detalle de aplicación***. Los detalles se aplicarán según el orden en que aparezcan en la lista, por lo que puede ***Subir*** o ***Bajar*** las reglas en la lista según sea necesario para establecer su prioridad. Después de hacer clic en una regla específica de la lista, la descripción general de los detalles de la regla se mostrará en la parte inferior del cuadro de diálogo. Cualquiera de los valores que aparezcan subrayados en azul pueden modificarse haciendo clic en el cuadro de diálogo de configuración respectivo. Para eliminar la regla resaltada, simplemente pulse ***Quitar***. Para definir una regla nueva, use el botón ***Agregar*** para abrir el cuadro de diálogo ***Cambiar detalle de la regla***, donde podrá especificar todos los detalles necesarios.

10.6.4. Servicios del sistema

Cualquier tipo de modificación en el cuadro de diálogo Servicios y protocolos del sistema ÚNICAMENTE DEBE SER REALIZADA POR USUARIOS EXPERTOS.

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



Lista de los servicios y protocolos del sistema

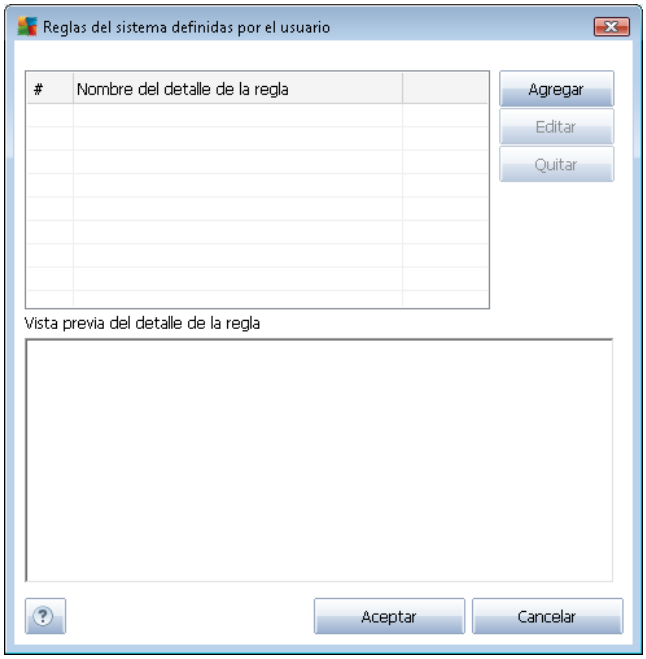
La tabla contiene las siguientes columnas:

- ***Registrar acción de regla***: esta casilla permite activar el registro de cada regla de aplicación en los registros.
- ***Servicios y protocolos del sistema***: esta columna muestra el nombre del correspondiente servicio del sistema.
- ***Acción***: esta columna muestra el icono correspondiente a la acción asignada:
  - Permitir comunicación para todas las redes
  - Permitir comunicación sólo para las redes definidas como seguras
  - Bloquear comunicación
- ***Redes***: esta columna informa sobre la red específica a la que se aplica la regla del sistema.

Para editar la configuración de cualquier elemento de la lista (*incluidas las acciones asignadas*), haga clic con el botón secundario sobre el elemento y seleccione ***Editar***. ***Sin embargo, la edición de las reglas del sistema debería ser realizada únicamente por usuarios avanzados. Lo más recomendable es no editar las reglas del sistema.***

Reglas del sistema definidas por el usuario

Para abrir un nuevo cuadro de diálogo con el fin de definir su propia regla del servicio del sistema (*véase la imagen a continuación*), pulse el botón ***Gestionar las reglas del sistema del usuario***. La sección superior del cuadro de diálogo ***Reglas del sistema definidas por el usuario*** muestra un resumen de los detalles de la regla del sistema actualmente editada, mientras que la sección inferior muestra el detalle seleccionado. Los detalles de la regla del sistema definida por el usuario se pueden editar, agregar o eliminar con su correspondiente botón; los detalles de la regla definida por el fabricante solamente se pueden editar:



Tenga en cuenta que la configuración de reglas de detalles es una tarea avanzada y está destinada básicamente a los administradores de red que necesitan tener 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., le recomendamos no modificar esta configuración. Si es realmente necesario modificar la configuración, consulte los archivos de ayuda del cuadro de diálogo correspondiente para ver detalles específicos.

Registrar tráfico desconocido

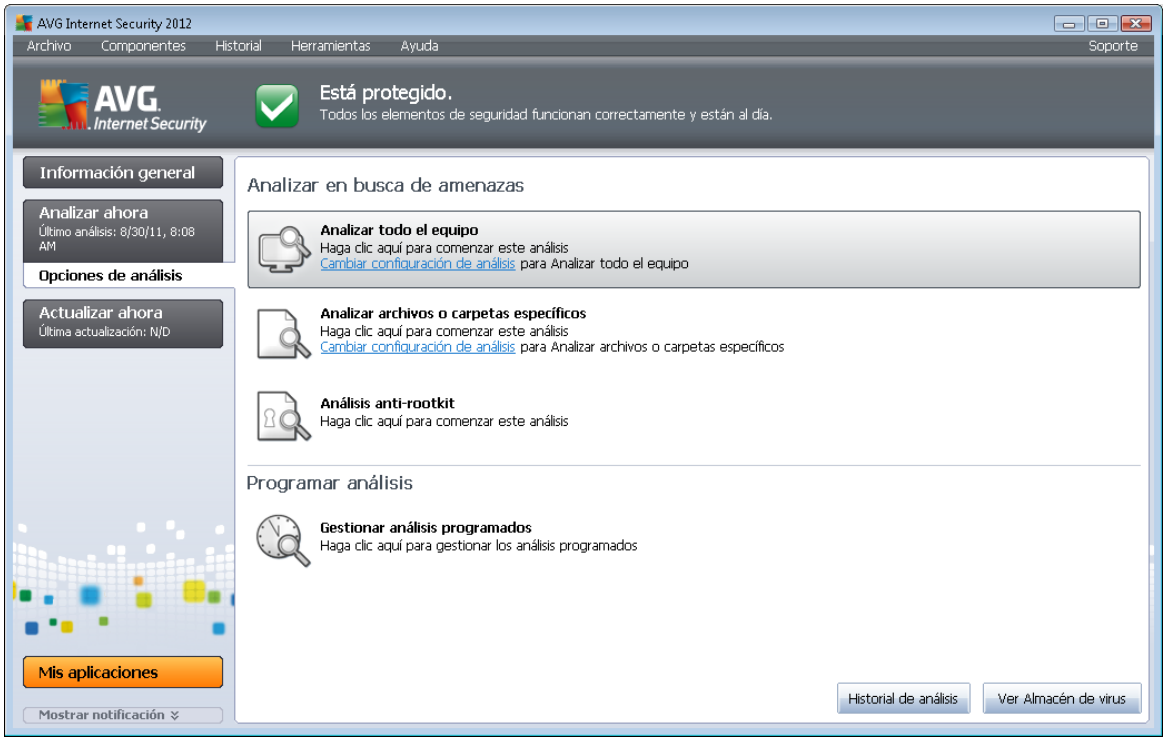
- ***Registrar tráfico entrante desconocido*** *(desactivada de manera predeterminada)*: marque la casilla para registrar en Registros todos los intentos desconocidos de conexión al equipo desde el exterior.

- ***Registrar tráfico saliente desconocido*** *(desactivada de manera predeterminada)*: marque la casilla para registrar en Registros todos los intentos desconocidos de conexión desde equipo a una ubicación exterior.

11. Análisis de AVG

Por defecto, **AVG Internet Security 2012** no ejecuta ningún análisis, ya que desde el análisis inicial, debe quedar perfectamente protegido por los componentes residentes de **AVG Internet Security 2012** que siempre están en guardia, y no permiten que ningún código malicioso entre en su equipo. Por supuesto, puede programar un análisis para que se ejecute en intervalos periódicos, o iniciar manualmente un análisis según sus necesidades en cualquier momento.

11.1. Interfaz de análisis



Se puede acceder a la interfaz de análisis de AVG mediante el vínculo rápido ***Opciones de análisis***. Haga clic en este vínculo para dirigirse al cuadro de diálogo ***Analizar en busca de amenazas***. En este cuadro de diálogo encontrará lo siguiente:

- información general de análisis predefinidos; hay tres tipos de análisis definidos por el proveedor del software que pueden utilizarse de inmediato bajo demanda o mediante programación:
    - Análisis del equipo completo
    - Analizar archivos o carpetas específicos
    - Análisis anti-rootkit
- sección de programación de análisis; aquí puede definir nuevos análisis y crear nuevas programaciones según sea necesario.

Botones de control

Los botones de control disponibles dentro de la interfaz de análisis son los siguientes:

- ***Historial de análisis***: muestra el cuadro de diálogo Información general de los resultados del análisis, donde se encuentra todo el historial de análisis
- ***Ver Almacén de virus***: abre una nueva ventana con el Almacén de virus, un espacio en el que las infecciones detectadas se ponen en cuarentena

11.2. Análisis predefinidos

Una de las características principales de **AVG Internet Security 2012** es el análisis bajo demanda. Los análisis bajo demanda han sido diseñados para comprobar varias partes del equipo cada vez que surge la sospecha de una posible infección de virus. De todos modos, se recomienda realizar tales análisis regularmente, aunque no sospeche que el equipo pueda tener algún virus.

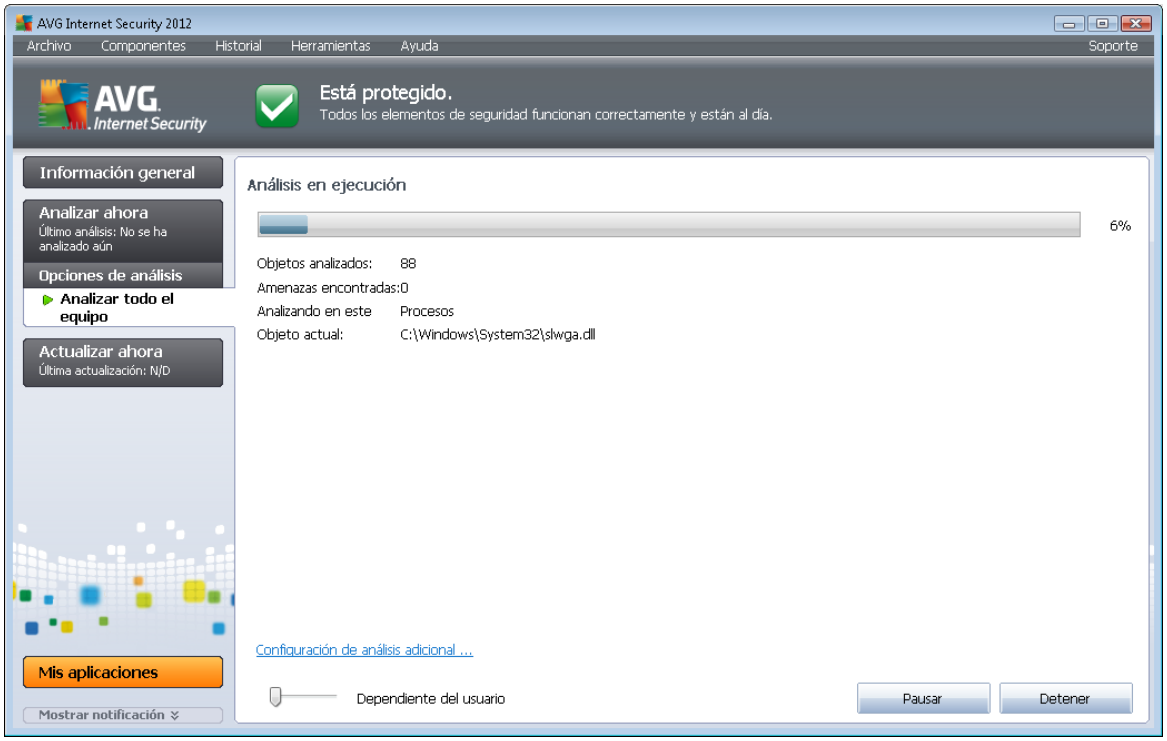
En **AVG Internet Security 2012**, encontrará los siguientes tipos de análisis predefinidos por el proveedor de software:

11.2.1. Análisis del equipo completo

Análisis del equipo completo: analiza todo el equipo en busca de posibles infecciones o programas potencialmente no deseados. En este análisis se comprobarán todos los discos duros del equipo, se detectarán y repararán los virus encontrados o se moverán las infecciones al Almacén de virus. El análisis del equipo completo debería programarse en la estación de trabajo al menos una vez a la semana.

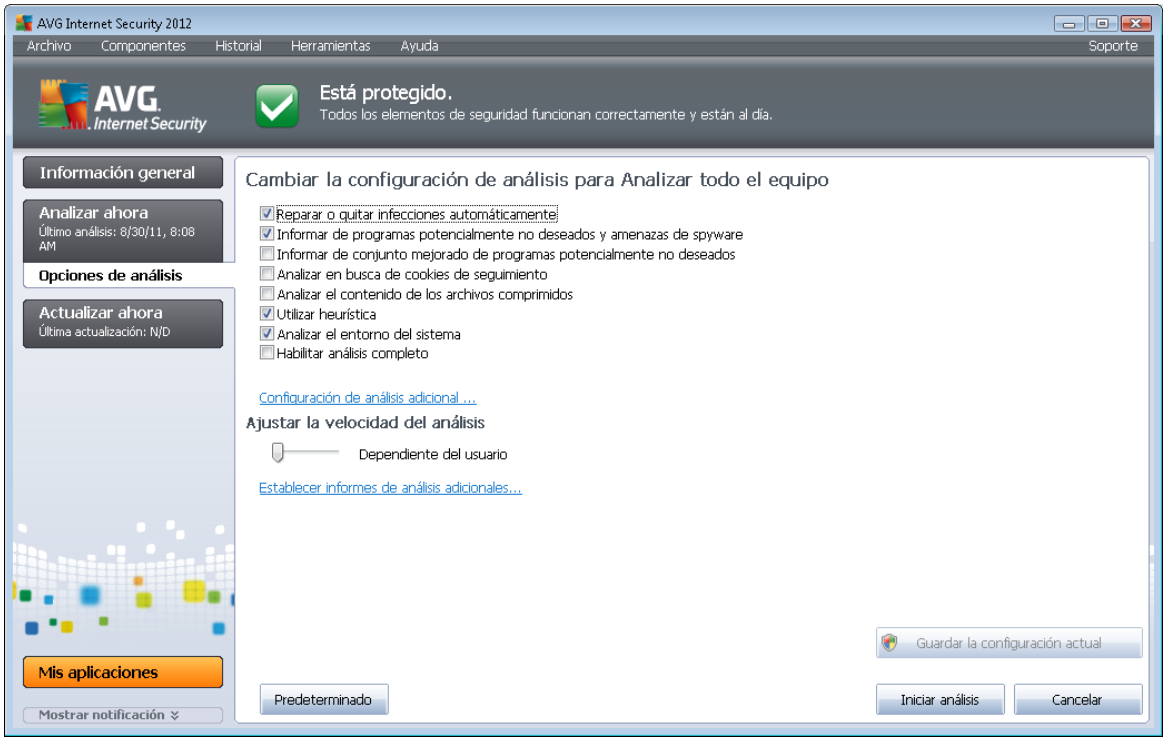
Inicio del análisis

El ***Análisis del equipo completo*** se puede iniciar directamente desde la interfaz de análisis haciendo clic en el icono del análisis. Para este tipo de análisis no es necesario configurar más parámetros; se iniciará inmediatamente en el cuadro de diálogo ***Análisis en ejecución*** (*consulte la captura de pantalla*). En caso necesario, el análisis se puede interrumpir temporalmente (***Pausar***) o cancelar (***Detener***).



Edición de la configuración del análisis

Puede editar la configuración predefinida del ***Análisis del equipo completo***. Pulse el vínculo ***Cambiar configuración de análisis*** para abrir el cuadro de diálogo ***Cambiar la configuración de análisis para Análisis del equipo completo*** *(accesible desde la interfaz de análisis a través del vínculo Cambiar configuración de análisis para el Análisis del equipo completo)*. ***Se recomienda mantener la configuración predeterminada a menos que tenga un buen motivo para modificarla.***



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

    - ***Reparar o quitar infecciones automáticamente*** (*activada de manera predeterminada*): si durante el análisis se identifica algún virus, éste se puede reparar automáticamente en caso de que haya alguna cura disponible. Si el archivo infectado no puede repararse automáticamente, el objeto infectado se moverá al Almacén de virus.

    - ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de manera predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.

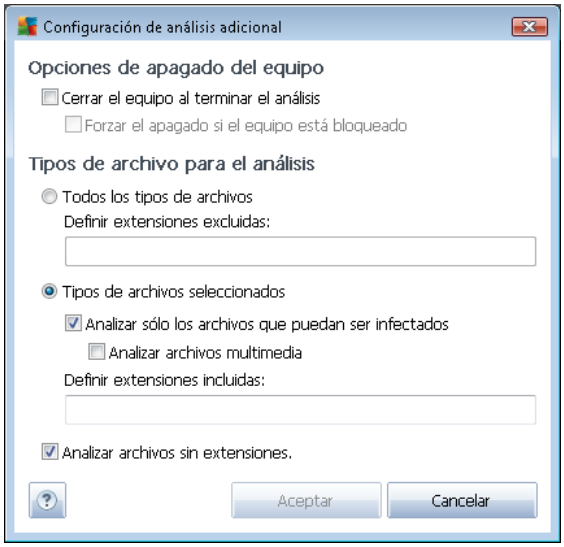
    - ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

    - ***Analizar en busca de cookies de seguimiento*** (*desactivado de manera predeterminada*): este parámetro del componente Anti-Spyware indica que las cookies deben detectarse (*las cookies HTTP se utilizan para autenticar, rastrear y*

mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos).

- ***Analizar el contenido de los archivos comprimidos*** (*desactivado de forma predeterminada*): este parámetro establece que el análisis debe comprobar todos los archivos que se encuentren dentro de archivos comprimidos, tales como ZIP, RAR, etc.
- ***Utilizar heurística*** (*activada de manera predeterminada*): el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos utilizados para detectar virus durante el análisis.
- ***Analizar el entorno del sistema*** (*activada de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*si sospecha que su equipo ha sido infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

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

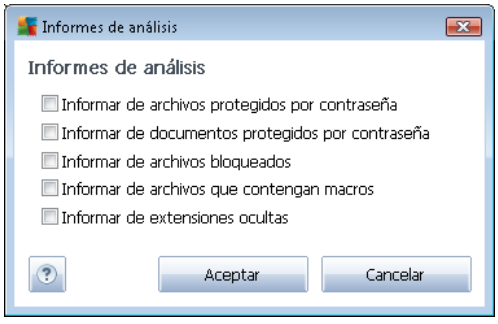


- ***Opciones de apagado del equipo***: indique si el equipo debe cerrarse automáticamente al finalizar la ejecución del proceso de análisis. Una vez confirmada esta opción (***Cerrar el equipo al terminar el análisis***), se activa una nueva opción que permite apagar el equipo aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).
- ***Tipos de archivos para el análisis***: permite definir con más detalle los tipos de

archivos que desea analizar:

- ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis, proporcionando una lista de extensiones de archivo separadas por comas que no deben analizarse;
- ***Tipos de archivos seleccionados***: puede especificar que desea analizar solamente los archivos que puedan estar infectados (*no se analizarán los archivos que no se pueden infectar, por ejemplo, algunos archivos de texto sin formato u otro tipo de archivos no ejecutables*), incluyendo archivos multimedia (*archivos de vídeo y audio - si deja esta casilla en blanco, se reducirá aún más el tiempo del análisis, ya que estos archivos suelen ser grandes y no es demasiado probable que estén infectados por un virus*). Del mismo modo, puede especificar las extensiones de los archivos que se analizarán siempre.
- Opcionalmente, puede indicar que desea ***Analizar archivos sin extensiones***: esta opción está activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

- ***Ajustar la velocidad del análisis***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos del sistema. Como alternativa, puede ejecutar el proceso de análisis de forma más lenta, lo que significa que se minimiza la carga de los recursos del sistema (*resulta útil cuando necesita trabajar en el equipo pero no le importa tanto el tiempo que tarde el análisis*), o más rápida, con mayor exigencia de recursos del sistema (*por ejemplo, cuando el equipo se desatiende temporalmente*).
- ***Establecer informes de análisis adicionales***: este vínculo abre un nuevo cuadro de diálogo ***Informes de análisis***, donde puede seleccionar el tipo de resultados que deben notificarse:



Advertencia: *esta configuración de análisis es idéntica a la que se emplea para un análisis recién 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 predeterminada para que la utilicen todos los análisis del equipo completo que se realicen en el futuro.*

11.2.2. Analizar archivos o carpetas específicos

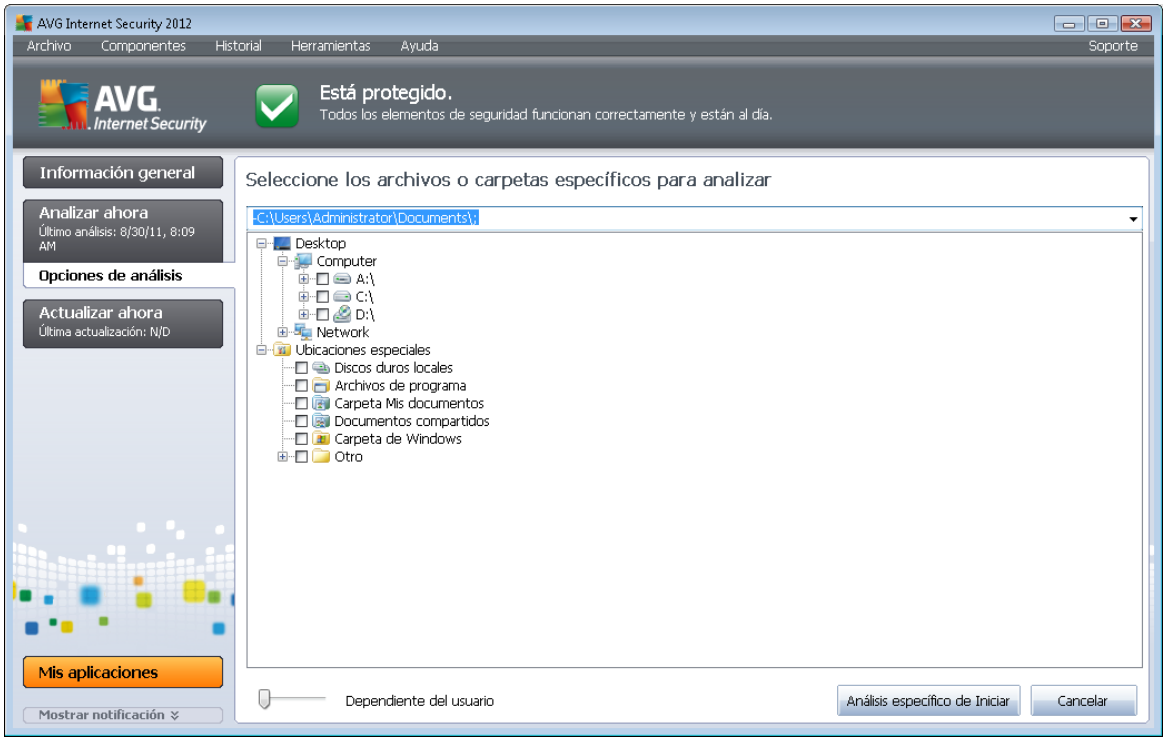
Analizar archivos o carpetas específicos: analiza únicamente aquellas áreas del equipo marcadas para ser analizadas (*carpetas, discos duros, disquetes, CD, etc. seleccionados*). En caso de que se detecte un virus, el progreso del análisis y el tratamiento de la amenaza detectada serán iguales que en el análisis del equipo completo: todos los virus encontrados se reparan o se envían al Almacén de virus. Puede utilizar el análisis de archivos o carpetas específicos para configurar análisis personalizados y programarlos según sus propias necesidades.

Inicio del análisis

El ***Análisis de archivos o carpetas específicos*** se puede iniciar directamente desde la interfaz de análisis haciendo clic en el icono del análisis. Se abrirá un nuevo cuadro de diálogo llamado ***Seleccione los archivos o carpetas específicos para analizar***. En la estructura de árbol del equipo, seleccione las carpetas que desea que se analicen. La ruta a cada carpeta seleccionada se generará automáticamente y se mostrará en el cuadro de texto ubicado en la parte superior de este cuadro de diálogo.

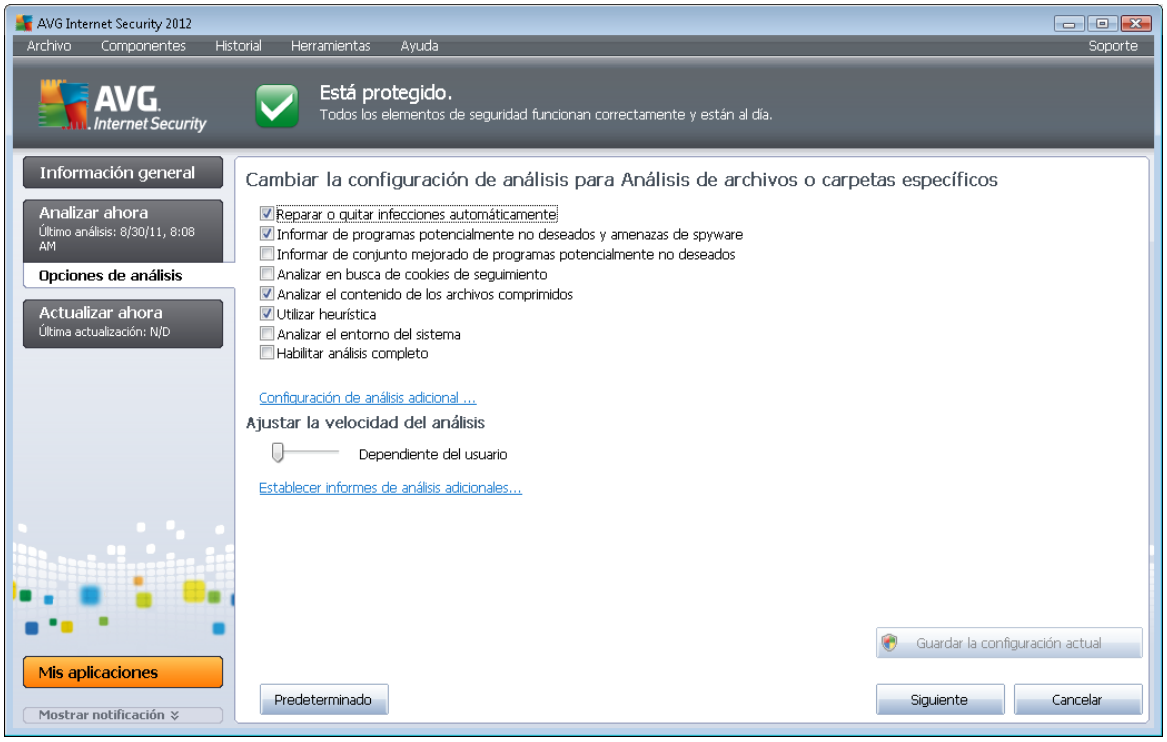
También existe la posibilidad de analizar una carpeta específica excluyendo del análisis todas sus subcarpetas. Para ello, escriba un signo menos "**-**" delante de la ruta que se genera de manera automática (*consulte la captura de pantalla*). Para excluir del análisis toda la carpeta, utilice el parámetro "**!**" .

Por último, para iniciar el análisis, pulse el botón ***Iniciar análisis***; el proceso de análisis en sí es básicamente idéntico al Análisis del equipo completo.



Edición de la configuración del análisis

Puede editar la configuración predefinida del ***Análisis de archivos o carpetas específicos***. Pulse el vínculo ***Cambiar configuración de análisis*** para ir al cuadro de diálogo ***Cambiar la configuración de análisis para Análisis de archivos o carpetas específicos***. ***Se recomienda mantener la configuración predeterminada a menos que tenga un buen motivo para modificarla.***



- ***Parámetros de análisis***: en la lista de parámetros de análisis, puede activar o desactivar parámetros específicos según sea necesario:
    - ***Reparar o quitar infecciones automáticamente*** (*activada de manera predeterminada*): si durante el análisis se identifica algún virus, éste se puede reparar automáticamente en caso de que haya alguna cura disponible. Si el archivo infectado no puede repararse automáticamente, el objeto infectado se moverá al Almacén de virus.
    - ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de manera predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.
    - ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas correctos e inofensivos si proceden

directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

- ***Analizar en busca de cookies de seguimiento*** (*desactivado de manera predeterminada*): este parámetro del componente Anti-Spyware indica que las cookies deben detectarse (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos*).

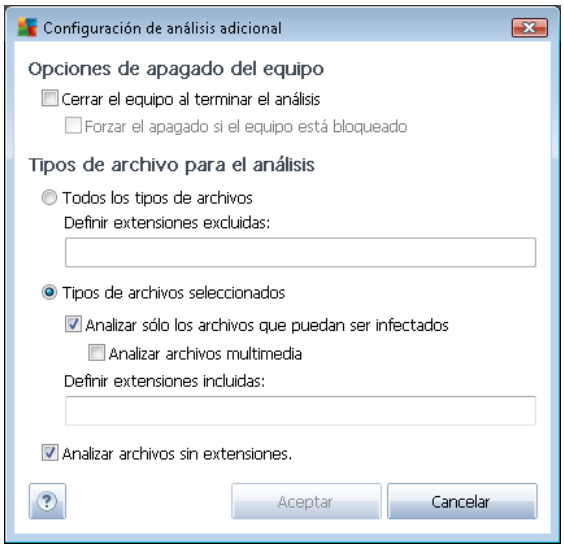
- ***Analizar el contenido de los archivos comprimidos*** (*activado de forma predeterminada*): este parámetro establece que el análisis debe comprobar todos los archivos que se encuentren dentro de archivos comprimidos, tales como ZIP, RAR, etc.

- ***Utilizar heurística*** (*desactivada de manera predeterminada*): el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos utilizados para detectar virus durante el análisis.

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

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*si sospecha que su equipo ha sido infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

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



- ***Opciones de apagado del equipo***: indique si el equipo debe cerrarse automáticamente al finalizar la ejecución del proceso de análisis. Una vez confirmada esta opción (***Cerrar el equipo al terminar el análisis***), se activa una nueva opción que permite apagar el equipo aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

- ***Tipos de archivos para el análisis***: permite definir con más detalle los tipos de archivos que desea analizar:

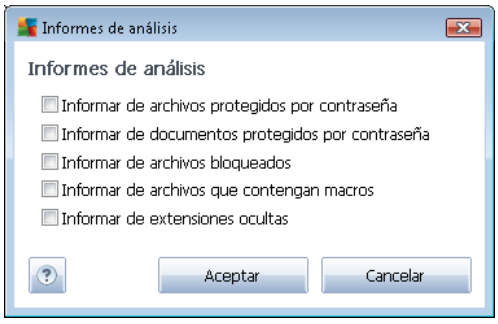
  - ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis, proporcionando una lista de extensiones de archivo separadas por comas que no deben analizarse;

  - ***Tipos de archivos seleccionados***: puede especificar que desea analizar solamente los archivos que puedan estar infectados (*no se analizarán los archivos que no se pueden infectar, por ejemplo, algunos archivos de texto sin formato u otro tipo de archivos no ejecutables*), incluyendo archivos multimedia (*archivos de vídeo y audio - si deja esta casilla en blanco, se reducirá aún más el tiempo del análisis, ya que estos archivos suelen ser grandes y no es demasiado probable que estén infectados por un virus*). Del mismo modo, puede especificar las extensiones de los archivos que se analizarán siempre.

  - Opcionalmente, puede indicar que desea ***Analizar archivos sin extensiones***: esta opción está activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

- ***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 se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos del sistema. Como alternativa, puede ejecutar el proceso de análisis de forma más lenta, lo que significa que se minimiza la carga de los recursos del sistema (*resulta útil cuando necesita trabajar en el equipo pero no le importa tanto el tiempo que tarde el análisis*), o más rápida, con mayor exigencia de recursos del sistema (*por ejemplo, cuando el equipo se desatiende temporalmente*).

- ***Establecer informes de análisis adicionales***: este vínculo abre un nuevo cuadro de diálogo ***Informes de análisis***, donde puede seleccionar el tipo de resultados que deben notificarse:



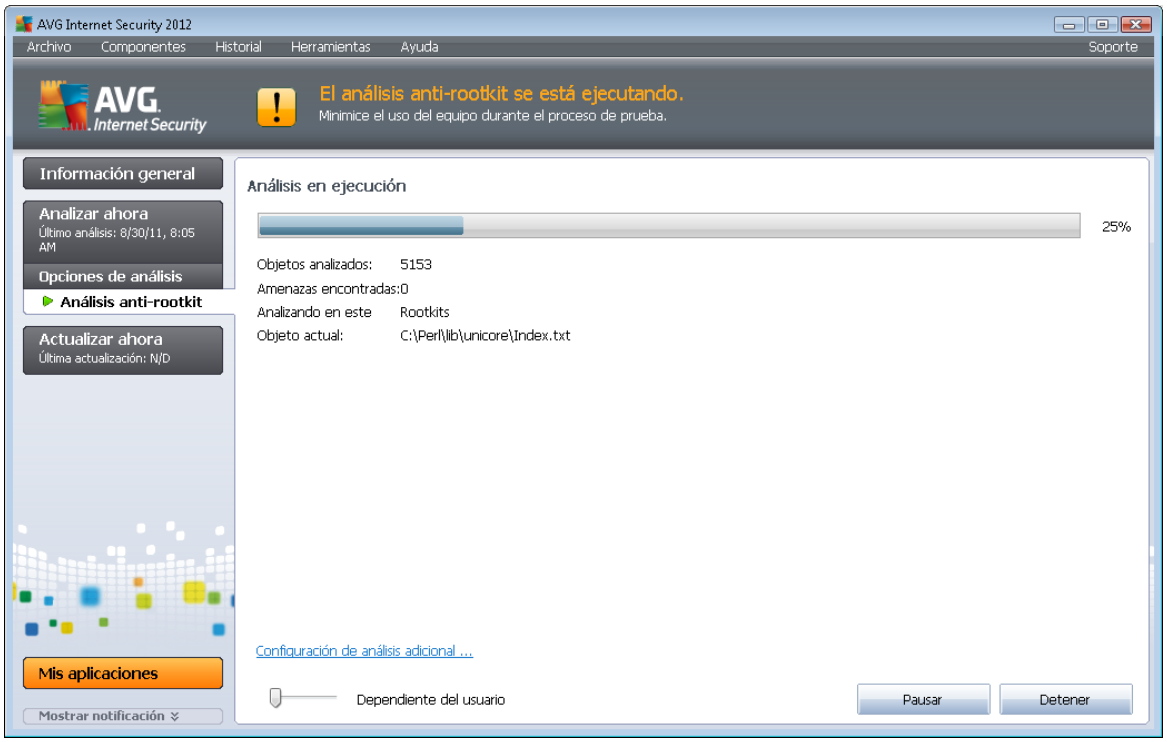
Advertencia: *esta configuración de análisis es idéntica a la que se emplea para un análisis recién definido, tal como se describe en el capítulo Análisis de AVG / Programación de análisis / Cómo analizar. Si decide cambiar la configuración predeterminada de la opción* ***Analizar archivos o carpetas específicos****, puede guardar la nueva configuración como predeterminada para que la utilicen todos los análisis de archivos o carpetas específicos que se realicen en el futuro. Asimismo, esta configuración se utilizará a modo de plantilla para todos los análisis nuevos que se programen (todos los análisis personalizados se basan en la configuración actual de la opción Analizar archivos o carpetas específicos).*

11.2.3. Análisis anti-rootkit

El ***análisis anti-rootkit*** busca posibles rootkits en el equipo (*programas y tecnologías que pueden encubrir una actividad de malware en el sistema*). Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, determinados controladores o secciones de aplicaciones normales se pueden detectar erróneamente como rootkits.

Inicio del análisis

El ***análisis anti-rootkit*** se puede iniciar directamente desde la interfaz de análisis haciendo clic en el icono de análisis. Para este tipo de análisis no es necesario configurar más parámetros, el análisis se iniciará inmediatamente en el cuadro de diálogo ***Análisis en ejecución*** (*consulte la captura de pantalla*). En caso necesario, el análisis se puede interrumpir temporalmente (***Pausar***) o cancelar (***Detener***).

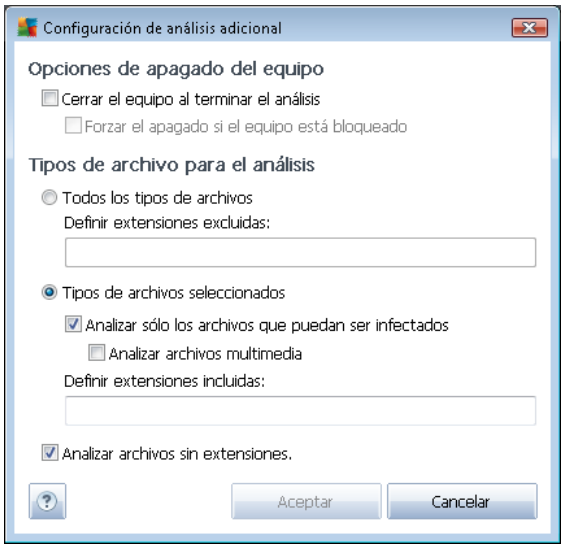


Edición de la configuración del análisis

El ***análisis anti-rootkit*** se inicia siempre con la configuración predeterminada y sus parámetros solamente se pueden editar en el cuadro de diálogo Configuración avanzada de AVG / Anti-Rootkit. En la interfaz de análisis está disponible la siguiente configuración, pero únicamente mientras se está ejecutando el análisis:

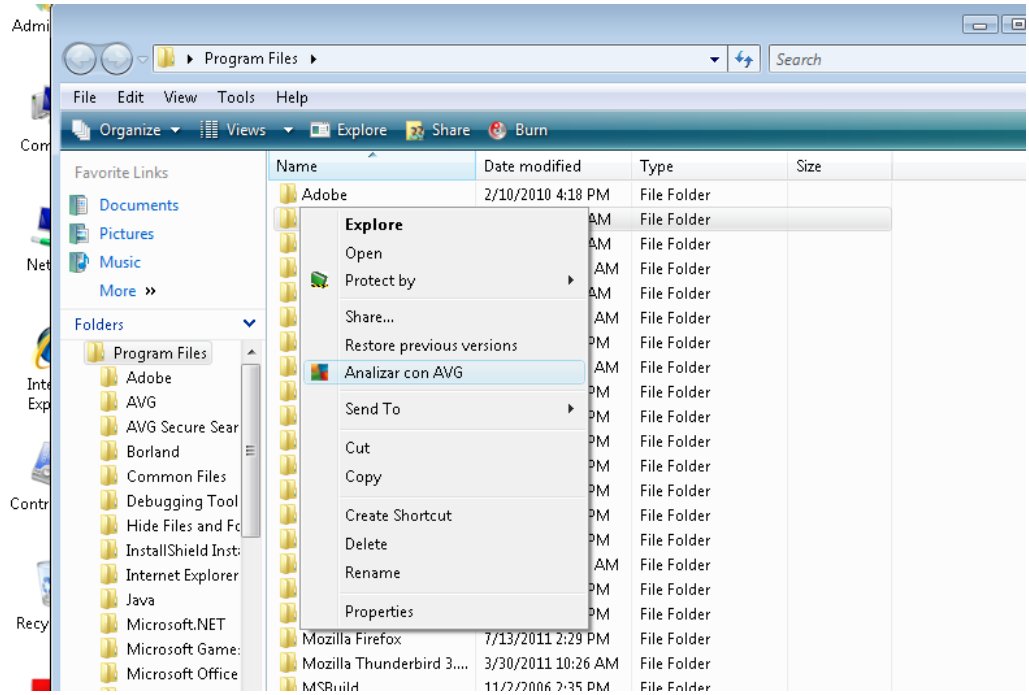
- ***Análisis automático***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos del sistema. Como alternativa, puede ejecutar el proceso de análisis de forma más lenta, lo que significa que se minimiza la carga de los recursos del sistema (*resulta útil cuando necesita trabajar en el equipo pero no le importa tanto el tiempo que tarde el análisis*), o más rápida, con mayor exigencia de recursos del sistema (*por ejemplo, cuando el equipo se desatiende temporalmente*).

- ***Configuración de análisis adicional***: este vínculo abre un nuevo cuadro de diálogo ***Configuración de análisis adicional***, donde puede definir posibles condiciones para el cierre del equipo en relación con el ***análisis anti-rootkit*** (***Cerrar el equipo al terminar el análisis***, *posiblemente* ***Forzar el apagado si el equipo está bloqueado***):



11.3. Análisis en el Explorador de Windows

Además de los análisis predefinidos que comprueban el equipo entero o sólo áreas seleccionadas, **AVG Internet Security 2012** también ofrece la opción de realizar un 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 bajo demanda. Siga estos pasos:



- Desde el Explorador de Windows, resalte el archivo *(o carpeta)* que desea comprobar
- Haga clic con el botón secundario en el objeto para abrir el menú contextual
- Seleccione la opción ***Analizar con AVG*** para que **AVG Internet Security 2012**

11.4. Análisis desde la línea de comandos

En **AVG Internet Security 2012** existe la opción de ejecutar el análisis desde la línea de comandos. Puede utilizar esta opción, por ejemplo, en servidores, o bien al crear un script por lotes que se ejecutará automáticamente tras el arranque del 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 iniciar el análisis de AVG desde la línea de comandos, ejecute el siguiente comando en la carpeta donde AVG esté instalado:

- ***avgscanx*** para sistemas operativos de 32 bits
- ***avgscana*** para sistemas operativos de 64 bits

Sintaxis del comando

La sintaxis del comando es la siguiente:

- ***avgscanx /parámetro***... por ejemplo, ***avgscanx /comp*** para analizar el equipo completo

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

- si un parámetro requiere introducir un valor específico (por ejemplo, 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 con punto y coma, por ejemplo: ***avgscanx /scan=C:\;D:***

Parámetros de análisis

Para mostrar la información completa de los parámetros disponibles, escriba el comando seguido del parámetro /? o /HELP (p. ej. ***avgscanx /?***). El único parámetro obligatorio es /SCAN, que especifica qué áreas del equipo se deben analizar. Para obtener una explicación más detallada de las opciones, consulte la introducción a los parámetros de la línea de comandos.

Para ejecutar el análisis, pulse ***Intro***. Durante el análisis, se puede detener el proceso pulsando ***Ctrl+C*** o ***Ctrl+Pausa***.

Análisis desde CMD iniciado desde la interfaz gráfica

Si se ejecuta el equipo en el modo seguro de Windows, también existe la posibilidad de iniciar el análisis desde la línea de comandos en la interfaz gráfica de usuario. El análisis en sí mismo se iniciará desde la línea de comandos, el cuadro de diálogo ***Compositor de línea de comandos*** solamente le permite especificar la mayoría de los parámetros de análisis de forma cómoda en la interfaz gráfica.

Puesto que a este cuadro de diálogo sólo se puede acceder en el modo seguro de Windows, consulte el archivo de ayuda que se abre directamente desde el cuadro de diálogo para obtener una descripción detallada del mismo.

11.4.1. Parámetros del análisis desde CMD

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

- ***/SCAN*** Analizar archivos o carpetas específicos /SCAN=ruta;ruta *(por ejemplo, /SCAN=C:\;D:\)*
- ***/COMP*** Análisis del equipo completo
- ***/HEUR*** Utilizar análisis heurístico
- ***/EXCLUDE*** Excluir ruta o archivos del análisis
- ***/@*** Archivo de comando /nombre de archivo/
- ***/EXT*** Analizar estas extensiones /por ejemplo, EXT=EXE,DLL/
- ***/NOEXT*** No analizar estas extensiones /por ejemplo, NOEXT=JPG/

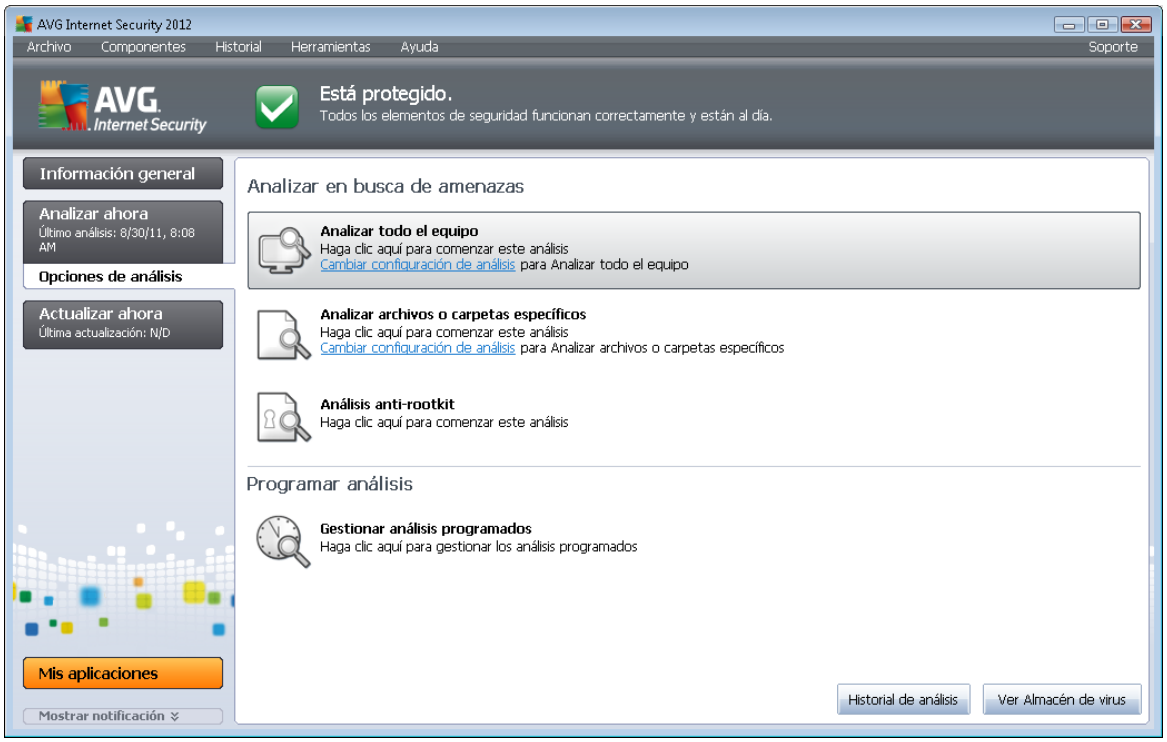
- ***/ARC*** Analizar archivos comprimidos
- ***/CLEAN*** Limpiar automáticamente
- ***/TRASH*** Mover archivos infectados a Almacén de virus
- ***/QT*** Análisis rápido
- ***/MACROW*** Informar de macros
- ***/PWDW*** Informar de archivos protegidos por contraseña
- ***/IGNLOCKED*** Ignorar archivos bloqueados
- ***/REPORT*** Informar en archivo /nombre de archivo/
- ***/REPAPPEND*** Añadir al archivo de informe
- ***/REPOK*** Informar de archivos no infectados como correctos
- ***/NOBREAK*** No permitir CTRL-BREAK para anular
- ***/BOOT*** Habilitar comprobación MBR/BOOT
- ***/PROC*** Analizar procesos activos
- ***/PUP*** Informar 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 la prioridad del análisis /Baja, Automática, Alta *(consulte Configuración avanzada/Análisis)*
- ***/SHUTDOWN*** Cerrar el equipo al terminar el análisis
- ***/FORCESHUTDOWN*** Forzar el cierre del equipo al terminar el análisis
- ***/ADS*** Analizar secuencias de datos alternativas *(sólo NTFS)*
- ***/ARCBOMBSW*** Informar de archivos repetidamente comprimidos

11.5. Programación de análisis

Con **AVG Internet Security 2012**, puede ejecutar análisis bajo demanda (por ejemplo, si sospecha que puede haber una infección en el equipo) o según una programación definida. Se recomienda encarecidamente ejecutar los análisis de manera programada; así podrá asegurarse de que el equipo está protegido contra cualquier posibilidad de infección y no tendrá que preocuparse por el análisis ni cuándo realizarlo.

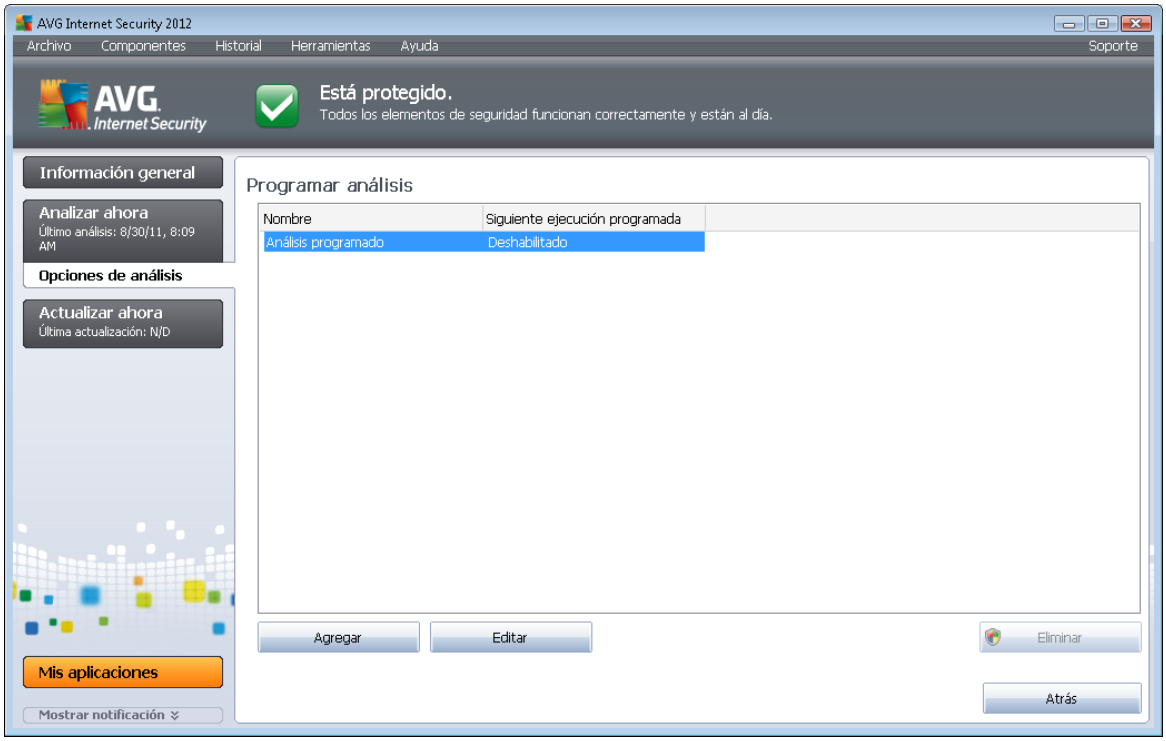
El Análisis del equipo completo debería ejecutarse regularmente, al menos una vez por semana. Sin embargo, de ser posible, lo ideal es realizar el análisis del equipo completo a diario, tal como lo establece la configuración predeterminada de la programación de análisis. Si el equipo está continuamente encendido, los análisis se pueden programar para que se realicen fuera de las horas de trabajo. Si el equipo se apaga en ocasiones, entonces programe que los análisis se realicen al iniciar el equipo cuando se haya pasado por alto dicha tarea.

Para crear nuevas programaciones de análisis, vaya a la interfaz de análisis de AVG y busque la sección inferior llamada ***Programar análisis***:



Programar análisis

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



Puede editar o añadir análisis con los botones de control siguientes:

- ***Agregar programación de análisis***: este botón abre el cuadro de diálogo ***Configuración del análisis programado***, en la ficha Configuración de la programación. En este cuadro de diálogo puede especificar los parámetros del análisis recién definido.

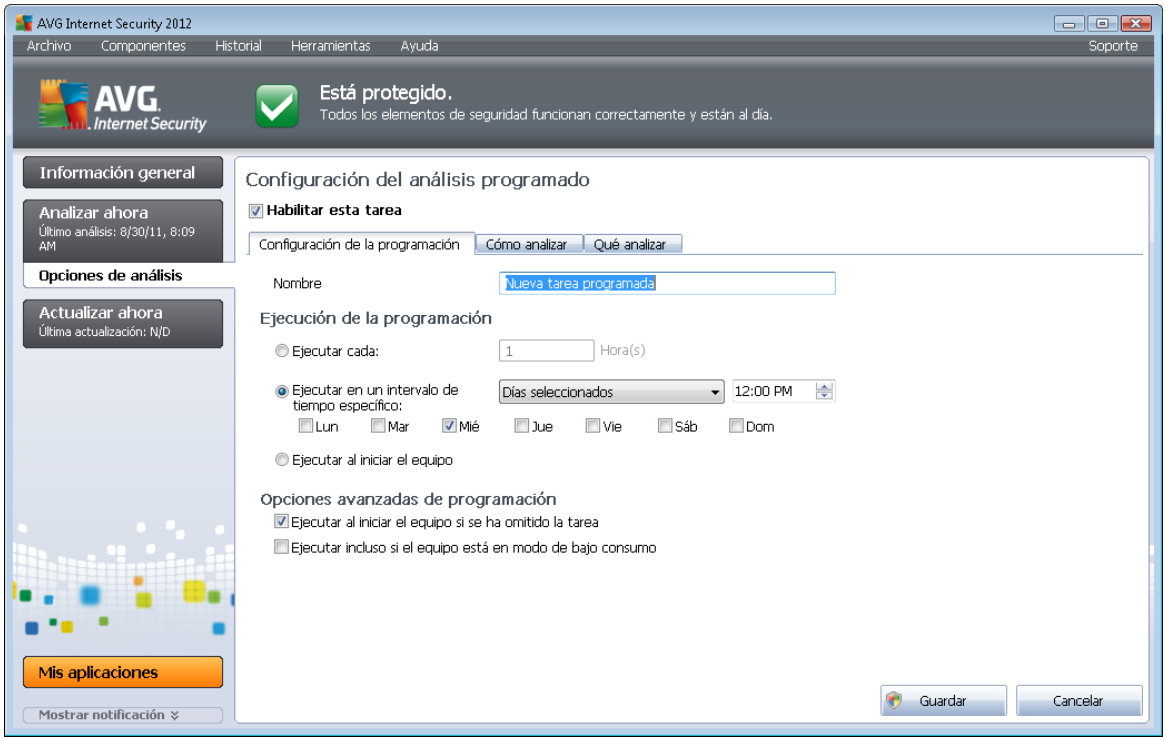
- ***Editar programación de análisis***: sólo puede utilizar este botón si ya seleccionó alguno de los análisis existentes en la lista de análisis programados. En ese caso, el botón se muestra activo y puede hacer clic en él para pasar al cuadro de diálogo ***Configuración del análisis programado***, en la ficha Configuración de la programación. Los parámetros del análisis seleccionado ya se encuentran especificados aquí y pueden editarse.

- ***Eliminar programación de análisis***: este botón también se encuentra activo si ya seleccionó alguno de los análisis existentes en la lista de análisis programados. En ese caso, puede eliminar los análisis de la lista pulsando el botón de control. No obstante, únicamente puede eliminar los análisis que haya creado; no es posible eliminar la ***Programación de análisis del equipo completo*** predefinida dentro de la configuración predeterminada.

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

11.5.1. Configuración de la programación

Si desea programar un nuevo análisis y su ejecución periódica, abra el cuadro de diálogo ***Configuración del análisis programado*** (*haga clic en el botón* ***Agregar programación de análisis*** *dentro del cuadro de diálogo* ***Programar análisis***). El cuadro de diálogo está dividido en tres fichas: ***Configuración de la programación*** *(consulte la imagen a continuación; la ficha predeterminada a la que se le redireccionará automáticamente*), Cómo analizar y Qué analizar.



En la ficha ***Configuración de la programación*** puede seleccionar o dejar en blanco el elemento ***Habilitar esta tarea*** simplemente para desactivar temporalmente el análisis programado y activarlo de nuevo cuando sea necesario.

A continuación, elija un nombre para el análisis que está a punto de crear y programar. Escriba el nombre en el campo de texto que se encuentra junto al elemento ***Nombre***. Trate de usar nombres breves, descriptivos y adecuados para los análisis con el objeto de facilitar su reconocimiento posterior.

Ejemplo: *no resulta apropiado llamar al análisis con el nombre de "Análisis nuevo" o "Mi análisis" puesto que estos nombres no hacen referencia a lo que realmente se comprueba en el análisis. En cambio, un ejemplo de un buen nombre descriptivo podría ser "Análisis de las áreas del sistema", etc. Del mismo modo, no es necesario especificar en el nombre del análisis si se trata de un análisis de todo el equipo o sólo de ciertos archivos o carpetas: los análisis creados por el usuario siempre serán una versión concreta del análisis de archivos o carpetas específicos.*

En este cuadro de diálogo puede definir aún más los parámetros siguientes del análisis:

- ***Ejecución de la programación***: permite especificar los intervalos de tiempo para el inicio del análisis que se acaba de programar. Los intervalos se pueden definir mediante el inicio repetido del análisis tras un período de tiempo (***Ejecutar cada...***), indicando una fecha y hora exactas (***Ejecutar en un intervalo...***) o posiblemente definiendo un evento al que debe asociarse el inicio del análisis (***Basada en acciones: Al iniciar el equipo***).

- ***Opciones avanzadas de programación***: esta sección permite definir bajo qué condiciones deberá iniciarse o no el análisis si el equipo está en modo de bajo consumo o apagado completamente.

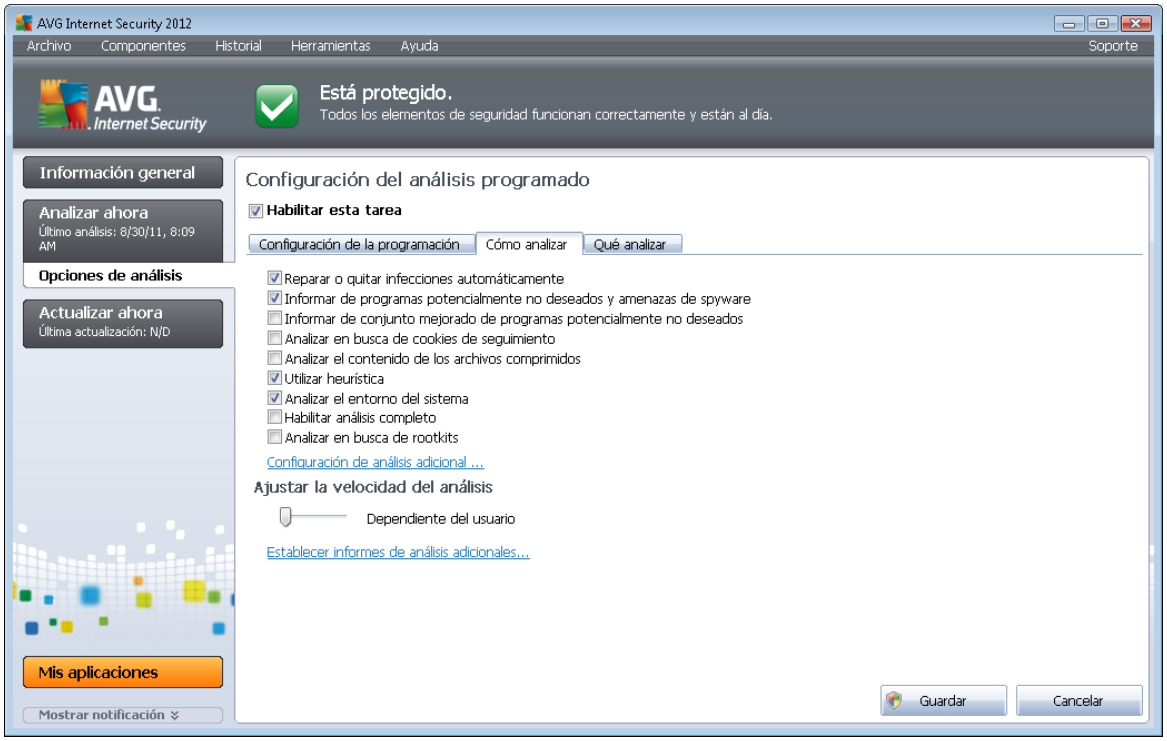
Botones de control del cuadro de diálogo Configuración del análisis programado

Hay dos botones de control disponibles en las tres fichas del cuadro de diálogo ***Configuración del análisis programado*** *(Configuración de la programación, Cómo analizar y Qué analizar)* y todos tienen las mismas funcionalidades sin que importe la ficha en la que se encuentre actualmente:

- ***Guardar***: guarda todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por ello, si desea configurar los parámetros del análisis en todas las fichas, pulse el botón para guardarlos únicamente después de haber especificado todos sus requisitos.

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

11.5.2. Cómo analizar



En la ficha ***Cómo analizar*** encontrará una lista de parámetros de análisis que pueden activarse o desactivarse de manera opcional. De manera predeterminada, la mayoría de los parámetros están activados y las funciones se aplicarán durante el análisis. A menos que tenga un buen motivo para modificarla, se recomienda mantener la configuración predefinida:

- ***Reparar o quitar infecciones automáticamente*** (*activada de manera predeterminada*): si durante el análisis se identifica algún virus, éste se puede reparar automáticamente en caso de que haya alguna cura disponible. Si el archivo infectado no se puede reparar

automáticamente o si decide desactivar esta opción, se le notificará la detección de un virus y deberá decidir qué hacer con la infección detectada. La acción recomendada es trasladar el archivo infectado al Almacén de virus.

- ***Informar de programas potencialmente no deseados y amenazas de spyware*** (*activada de manera predeterminada*): marque esta opción para activar el motor Anti-Spyware y analizar en busca de spyware y virus. El spyware representa una categoría dudosa de malware: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos mantener activada esta característica ya que aumenta la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): marque esta opción para detectar paquetes ampliados de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

- ***Analizar en busca de cookies de seguimiento*** (*desactivado de manera predeterminada*): este parámetro del componente Anti-Spyware indica que deben detectarse cookies durante el análisis (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos*).

- ***Analizar el contenido de los archivos comprimidos*** (*desactivado de manera predeterminada*): este parámetro indica que se deben analizar todos los archivos, incluso si se encuentran dentro de archivos comprimidos, por ejemplo, ZIP, RAR...

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

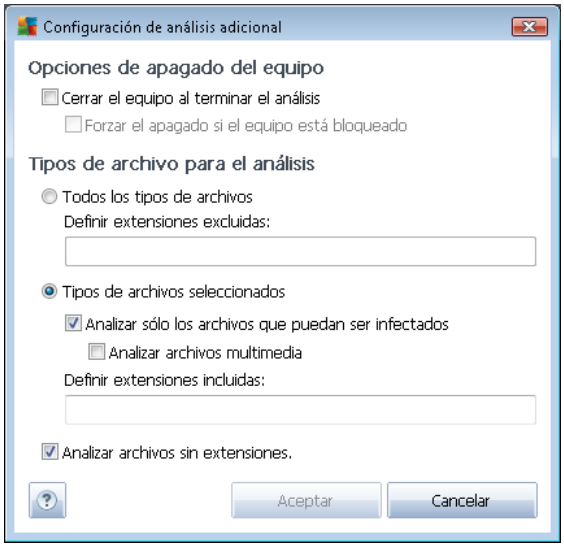
- ***Analizar el entorno del sistema*** (*activado de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo.

- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas situaciones (*si sospecha que su equipo ha sido infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados que analizarán incluso las áreas del equipo más difíciles de infectar, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

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

A continuación, puede modificar la configuración del análisis de la siguiente manera:

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



- ***Opciones de apagado del equipo***: indique si el equipo debe cerrarse automáticamente al finalizar la ejecución del proceso de análisis. Una vez confirmada esta opción (***Cerrar el equipo al terminar el análisis***), se activa una nueva opción que permite apagar el equipo aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

- ***Tipos de archivos para el análisis***: permite definir con más detalle los tipos de archivos que desea analizar:

  - ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis, proporcionando una lista de extensiones de archivo separadas por comas que no deben analizarse;

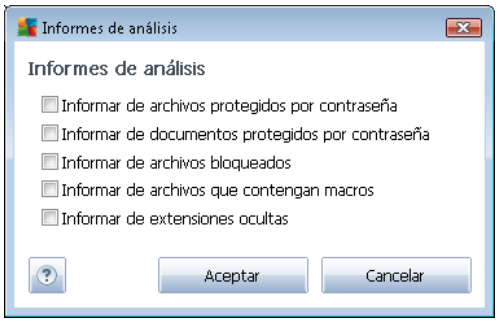
  - ***Tipos de archivos seleccionados***: puede especificar que desea analizar solamente los archivos que puedan estar infectados (*no se analizarán los archivos que no se pueden infectar, por ejemplo, algunos archivos de texto sin formato u otro tipo de archivos no ejecutables*), incluyendo archivos multimedia (*archivos de vídeo y audio - si deja esta casilla en blanco, se reducirá aún más el tiempo del análisis, ya que estos archivos suelen ser grandes y no es demasiado probable que estén infectados por un virus*). Del mismo modo, puede especificar las extensiones de los archivos que se analizarán siempre.

  - Opcionalmente, puede indicar que desea ***Analizar archivos sin extensiones***: esta opción está activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

- ***Ajustar la velocidad del análisis***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos del sistema. Como alternativa, puede ejecutar el proceso de análisis de forma más lenta, lo que significa que se minimiza la carga de los recursos del sistema (*resulta útil cuando necesita trabajar en el equipo pero no le importa tanto el tiempo que tarde el análisis*), o

más rápida, con mayor exigencia de recursos del sistema (*por ejemplo, cuando el equipo se desatiende temporalmente*).

- ***Establecer informes de análisis adicionales***: este vínculo abre un nuevo cuadro de diálogo ***Informes de análisis***, donde puede seleccionar el tipo de resultados que deben notificarse:



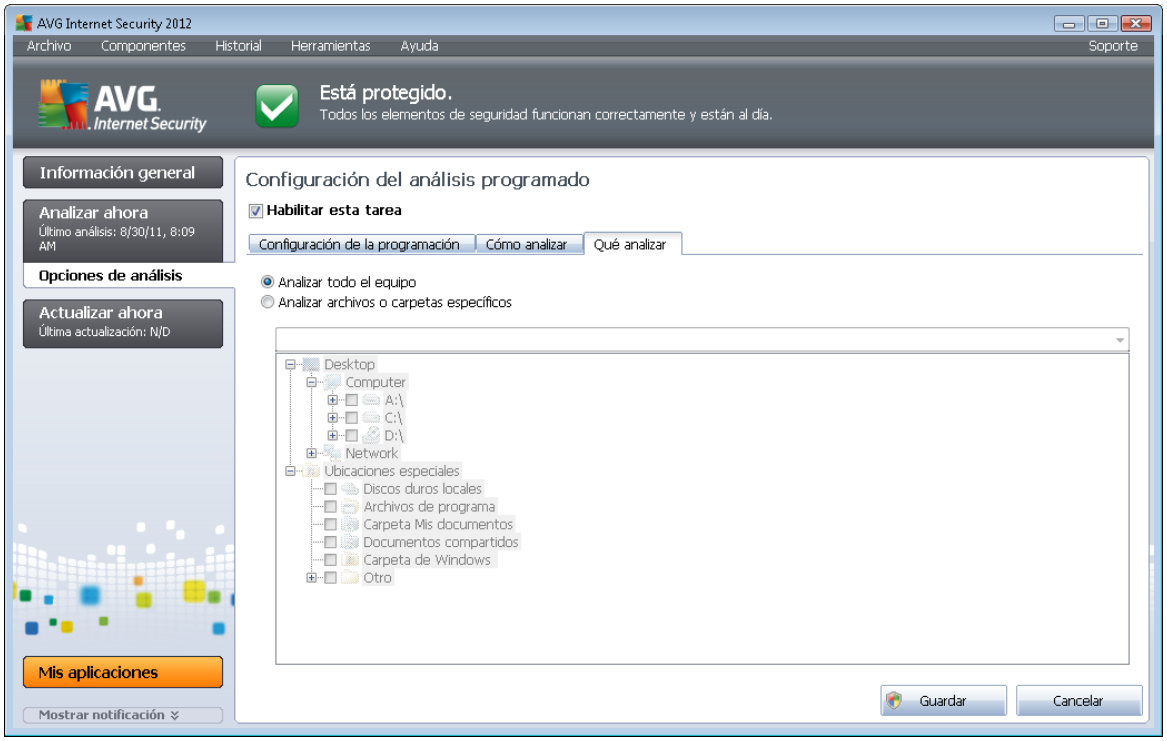
Botones de control

Hay dos botones de control disponibles en las tres fichas del cuadro de diálogo ***Configuración del análisis programado*** (*Configuración de la programación*, *Cómo analizar* y *Qué analizar*) y todos tienen las mismas funcionalidades sin que importe la ficha en la que se encuentre actualmente:

- ***Guardar***: guarda todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por ello, si desea configurar los parámetros del análisis en todas las fichas, pulse el botón para guardarlos únicamente después de haber especificado todos sus requisitos.

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

11.5.3. Qué analizar



En la ficha ***Qué analizar*** se puede definir si se desea programar el análisis del equipo completo o el análisis de archivos o carpetas específicos.

En caso de que se seleccione el análisis de archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activa la estructura de árbol mostrada, pudiéndose especificar las carpetas a analizar (*expanda los elementos haciendo clic en el nodo con el signo más hasta que encuentre la carpeta que desea analizar*). Puede seleccionar varias carpetas activando su correspondiente casilla. Las carpetas seleccionadas aparecerán en el campo de texto, en la parte superior del cuadro de diálogo, y el menú desplegable conservará el historial de los análisis seleccionados para su posterior uso. Como alternativa, puede introducir manualmente la ruta completa de la carpeta deseada (*si introduce varias rutas, es necesario separarlas con punto y coma, sin espacio adicional*).

En la estructura del árbol también existe una rama denominada ***Ubicaciones especiales***. A continuación se ofrece una lista de ubicaciones que se analizarán cuando se marque la correspondiente casilla de verificación:

- ***Discos duros locales***: todos los discos duros del equipo
- ***Archivos de programa***
  - C:\Archivos de programa\
  - *en versiones de 64 bits* C:\Archivos de programa (x86)

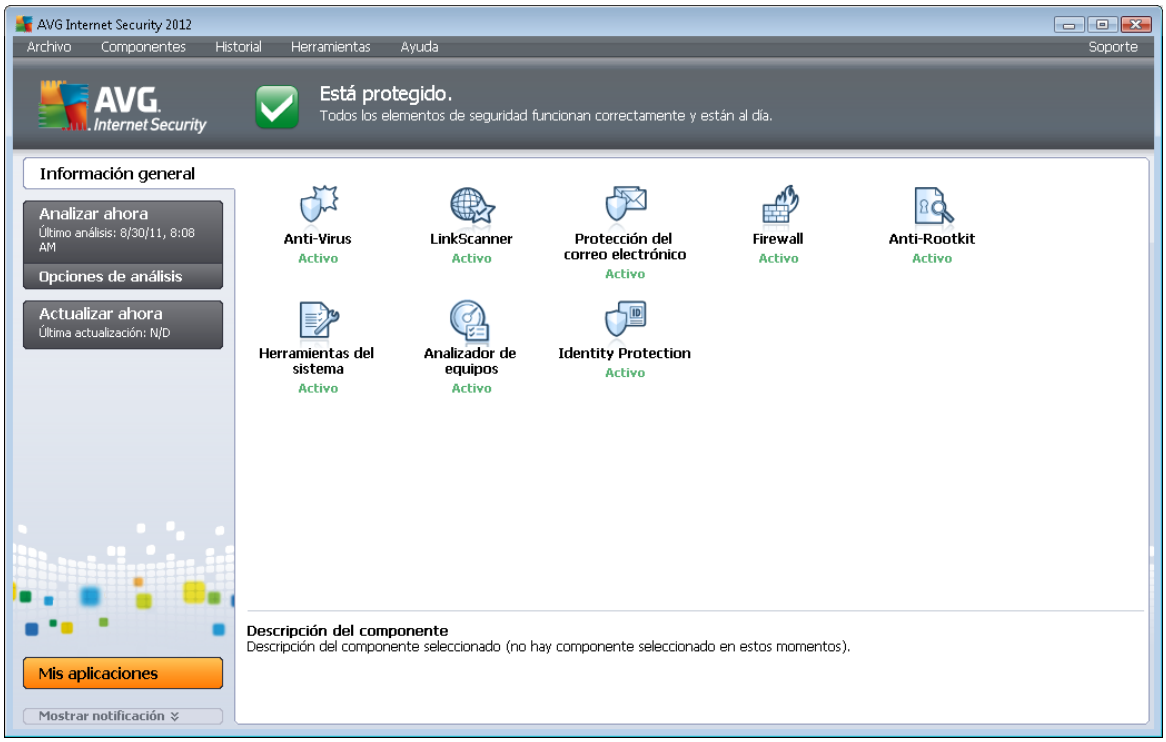
- ***Carpeta Mis documentos***
    - *para Windows XP:* C:\Documents and Settings\Default User\Mis documentos\
    - *para Windows Vista/7*: C:\Usuarios\usuario\Documentos\
- ***Documentos compartidos***
    - *para Windows XP*: C:\Documents and Settings\All Users\Documentos compartidos\
    - *para Windows Vista/7*: C:\Usuarios\Acceso público\Documentos públicos\
- ***Carpeta de Windows*** - C:\Windows\
- ***Otras***
    - *Unidad del sistema*: la unidad de disco duro en la que está instalado el sistema operativo (generalmente C:)
    - *Carpeta del sistema*: C:\Windows\System32\
    - *Carpeta de archivos temporales*: C:\Documents and Settings\usuario\Configuración local\ (*Windows XP*) o C:\Usuarios\usuario\AppData\Local\Temp\ (*Windows Vista/7*)
    - *Archivos temporales de Internet* - C:\Documents and Settings\usuario\Configuración local\Archivos temporales de Internet\ (Windows XP*) o C: \Usuarios\usuario\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7*)

Botones de control

Los dos mismos botones de control están disponibles en las tres fichas del cuadro de diálogo ***Configuración del análisis programado*** *(Configuración de la programación, Cómo analizar y Qué analizar*:

- ***Guardar***: guarda todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por ello, si desea configurar los parámetros del análisis en todas las fichas, pulse el botón para guardarlos únicamente después de haber especificado todos sus requisitos.
- ***Cancelar***: cancela todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG.

11.6. Información general de los resultados del análisis



Se puede acceder al cuadro de diálogo ***Información general de los resultados del análisis*** desde la interfaz de análisis de AVG, mediante el botón ***Historial de análisis***. Este cuadro de diálogo muestra una lista de todos los análisis realizados anteriormente e información sobre sus resultados:

- ***Nombre***: designación del análisis; puede ser el nombre de uno de los análisis predefinidos o un nombre que el usuario le haya dado a su análisis programado personalizado. Cada uno de los nombres incluye un icono que indica el resultado del análisis:

  - el icono verde indica que no se detectó ninguna infección durante el análisis

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

  - el icono rojo advierte que se detectó una infección durante el análisis y que no fue posible eliminarla

  Los iconos pueden ser de un solo color o estar divididos en dos partes: un icono de un solo color indica que el análisis se completó correctamente; un icono de dos colores indica que el análisis se canceló o se interrumpió.

  Nota: *para ver información detallada sobre cada análisis, abra el cuadro de diálogo Resultados del análisis, al que puede acceder mediante el botón Ver detalles (ubicado en la parte inferior de este cuadro de 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 probados***: número de objetos que se comprobaron durante el análisis
- ***Infecciones***: número de infecciones de virus detectadas / eliminadas
- ***Spyware***: número de casos de spyware detectados / eliminados
- ***Advertencias***: número de objetos sospechosos detectados
- ***Rootkits***: número de rootkits detectados
- ***Información del registro del análisis***: información relacionada con el transcurso y resultado del análisis (por lo general, con su finalización o interrupción)

Botones de control

Los botones de control del cuadro de diálogo ***Información general de los resultados del análisis*** son los siguientes:

- ***Ver detalles***: pulse este botón para pasar al cuadro de diálogo Resultados del análisis, donde podrá ver datos detallados sobre el análisis seleccionado
- ***Eliminar resultado***: pulse este botón para eliminar el elemento seleccionado de la información general de los resultados del análisis
- ***Atrás***: permite volver al cuadro de diálogo predeterminado de la interfaz de usuario de AVG

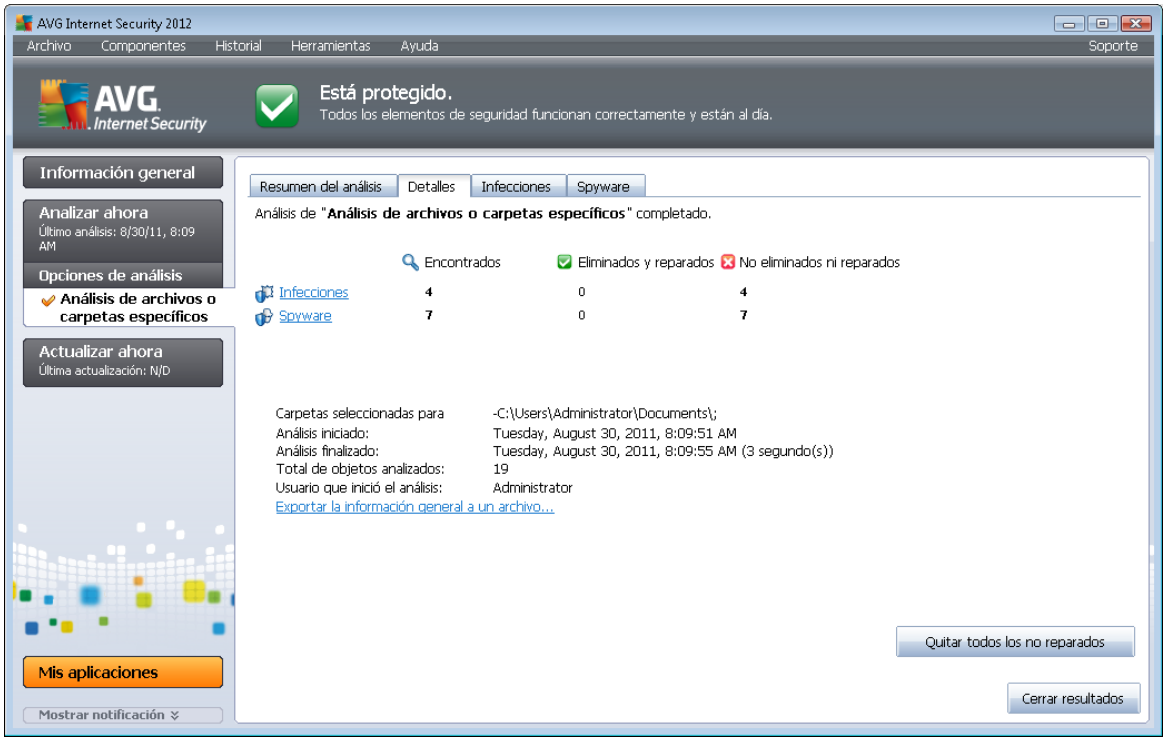
11.7. Detalles de los resultados del análisis

Si hay un análisis específico seleccionado en el cuadro de diálogo Información general de los resultados del análisis, puede hacer clic en el botón ***Ver detalles*** para pasar al cuadro de diálogo ***Resultados del análisis***, que ofrece datos detallados sobre el transcurso y el resultado del análisis seleccionado. El cuadro de diálogo está dividido en varias fichas:

- Información general de los resultados: esta ficha está visible en todo momento y proporciona datos estadísticos que describen el progreso del análisis
- Infecciones: esta ficha aparece únicamente si se detectó una infección de virus durante el análisis
- Spyware: esta ficha aparece únicamente si se detectó spyware durante el análisis
- Advertencias: esta ficha aparece, por ejemplo, si se detectaron cookies durante el análisis
- Rootkits: esta ficha aparece únicamente si se detectaron rootkits durante el análisis
- Información: esta ficha aparece sólo si se detectaron posibles amenazas que no pueden clasificarse como ninguna de las categorías antes mencionadas. La ficha muestra un mensaje de advertencia sobre el hallazgo. Del mismo modo, aquí encontrará información

sobre objetos que no pudieron analizarse *(p. ej., archivos comprimidos protegidos por contraseña)*..

11.7.1. Ficha Información general de los resultados



En la ficha ***Resultados del análisis***, encontrará estadísticas detalladas con información sobre:

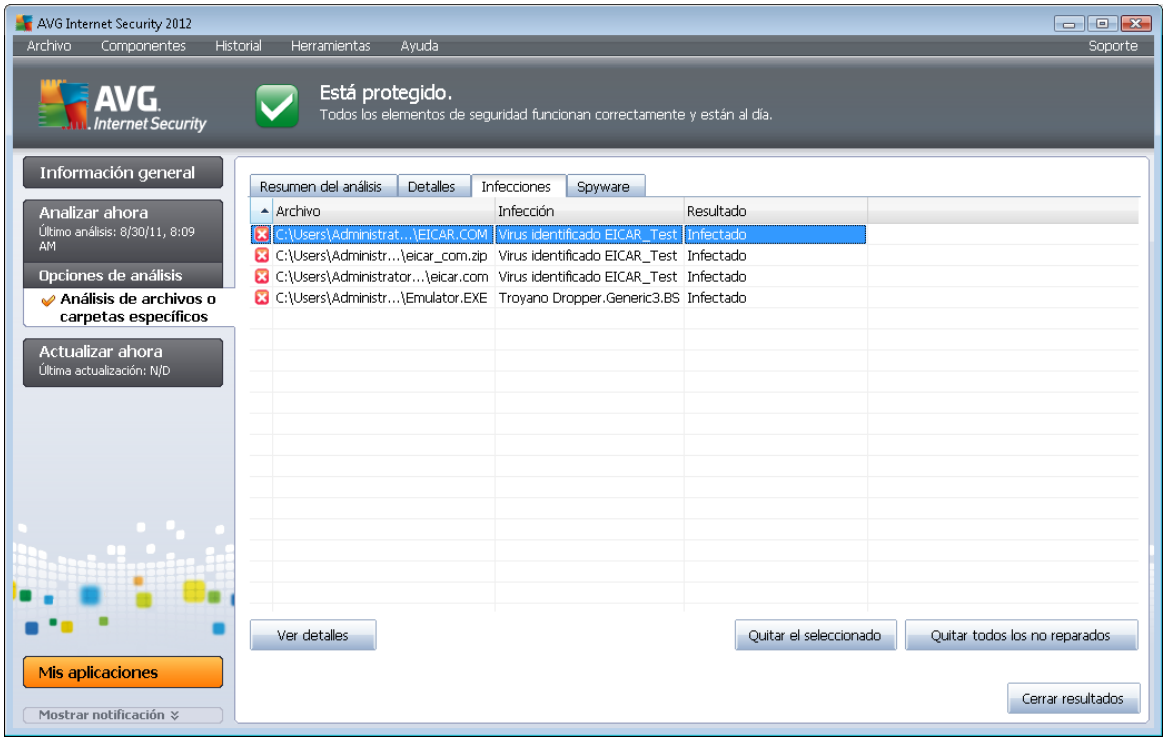
- infecciones de virus / spyware detectados
- infecciones de virus / spyware eliminados
- el número de infecciones de virus / spyware que no pudieron eliminarse ni repararse

Además, encontrará información sobre la fecha y hora exactas en que se inició el análisis, la cantidad total de objetos analizados, la duración del análisis y el número de errores que se produjeron durante el análisis.

Botones de control

Sólo hay un botón de control disponible en este cuadro de diálogo. Mediante el botón ***Cerrar resultados*** se vuelve al cuadro de diálogo Información general de los resultados del análisis.

11.7.2. Ficha Infecciones



La ficha ***Infecciones*** sólo se muestra en el cuadro de diálogo ***Resultados del análisis*** si durante el análisis se detecta una infección de virus. La ficha se divide en tres secciones que proporcionan la siguiente información:

- ***Archivo***: ruta completa a 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 que se ha detectado durante el análisis:
    - ***Infectado***: el objeto infectado se ha detectado y se ha dejado en su ubicación original (*por ejemplo, si ha desactivado la opción de reparación automática en la configuración de un análisis concreto*)
    - ***Reparado***: el objeto infectado se ha reparado automáticamente y se ha dejado en su ubicación original
    - ***Movido al Almacén de virus***: el objeto infectado se ha movido a la cuarentena del Almacén de virus
    - ***Eliminado***: el objeto infectado ha sido eliminado
    - ***Añadido a excepciones PUP***: el resultado se ha evaluado como una excepción y se

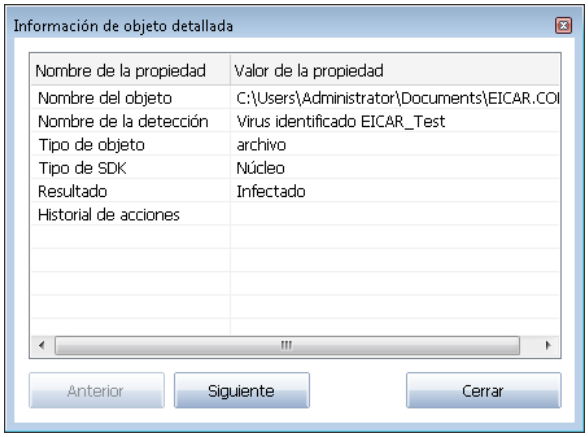
ha agregado a la lista de excepciones PUP *(configuradas en el cuadro de diálogo Excepciones PUP de la configuración avanzada)*

- ***Archivo bloqueado. No analizado***: el objeto en cuestión está bloqueado, por lo que AVG no puede analizarlo
- ***Objeto potencialmente peligroso***: el objeto ha sido detectado como potencialmente peligroso pero no infectado (*por ejemplo, puede contener macros*); la información debe considerarse únicamente como una advertencia
- ***Para finalizar la acción, debe reiniciar el equipo***: el objeto infectado no se puede eliminar, para eliminarlo por completo es necesario reiniciar el equipo

Botones de control

Hay tres botones de control disponibles en este cuadro de diálogo:

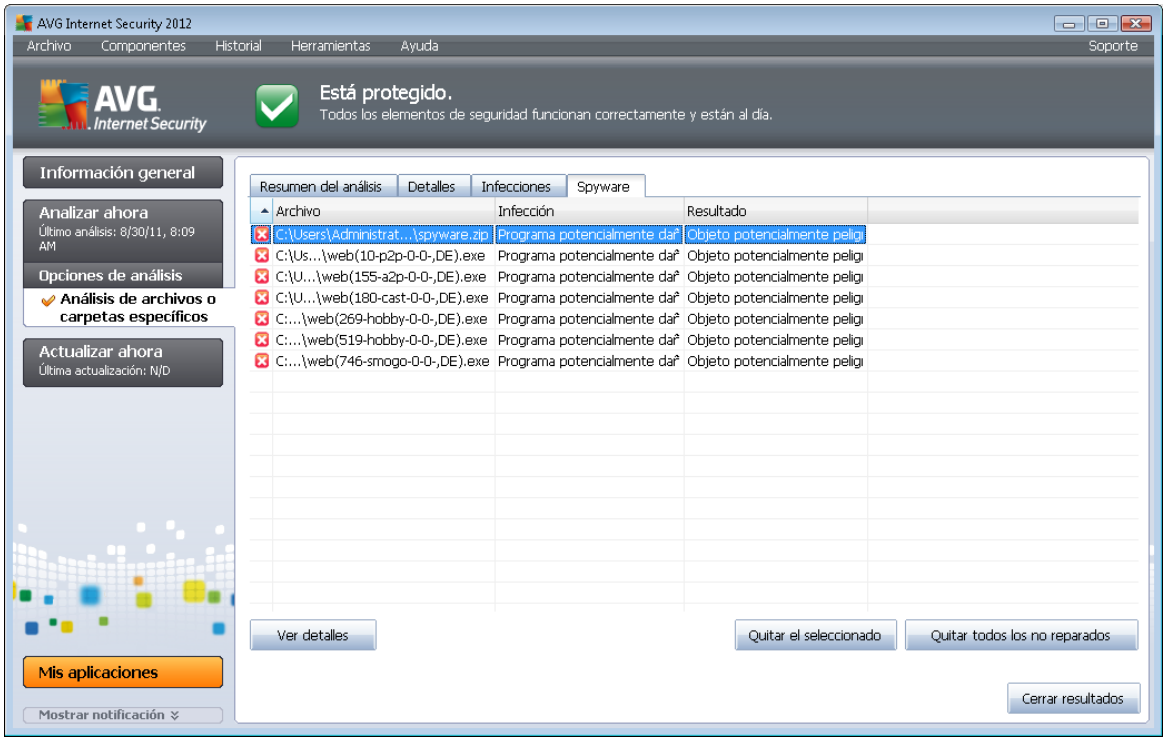
- ***Ver detalles***: el botón abre una nueva ventana de cuadro de diálogo denominada ***Información de objeto detallada***:



  En este cuadro de diálogo, encontrará información detallada sobre el objeto infeccioso detectado (*por ejemplo, nombre y ubicación del objeto infectado, tipo de objeto, tipo de SDK, resultado de la detección e historial de las acciones relativas al objeto detectado*). Utilizando los botones ***Anterior*** / ***Siguiente*** puede visualizar información sobre resultados específicos. Use el botón ***Cerrar*** para cerrar este cuadro de diálogo.

- ***Quitar el seleccionado***: use el botón para mover el resultado seleccionado al Almacén de virus
- ***Quitar todos los no reparados***: este botón elimina todos los resultados que no se pueden reparar ni mover al Almacén de virus
- ***Cerrar resultados***: finaliza la vista de información detallada y vuelve al cuadro de diálogo Información general de los resultados del análisis

11.7.3. Ficha Spyware



La ficha ***Spyware*** sólo se muestra en el cuadro de diálogo ***Resultados del análisis*** si durante el análisis se detecta spyware. La ficha se divide en tres secciones que proporcionan la siguiente información:

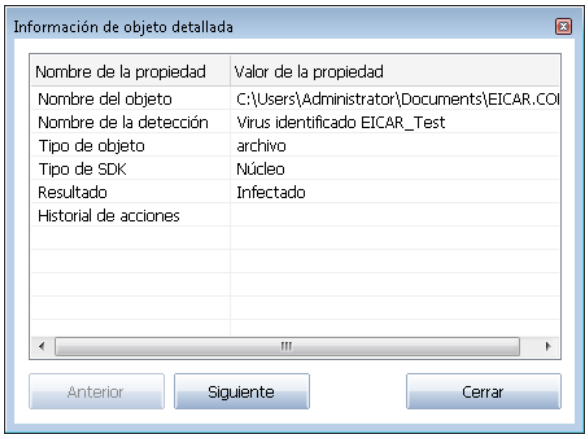
- ***Archivo***: ruta completa a la ubicación original del objeto infectado
- ***Infecciones***: nombre del spyware detectado *(para obtener más detalles sobre los virus específicos, consulte la Enciclopedia de virus en línea)*
- ***Resultado***: define el estado actual del objeto detectado durante el análisis:
  - ***Infectado***: el objeto infectado se ha detectado y se ha dejado en su ubicación original *(por ejemplo, si ha desactivado la opción de reparación automática en la configuración de un análisis concreto)*
  - ***Reparado***: el objeto infectado se ha reparado automáticamente y se ha dejado en su ubicación original
  - ***Movido al Almacén de virus***: el objeto infectado se ha movido a la cuarentena del Almacén de virus
  - ***Eliminado***: el objeto infectado ha sido eliminado
  - ***Añadido a excepciones PUP***: el resultado se ha evaluado como una excepción *y se ha agregado a la lista de excepciones PUP (configuradas en el cuadro de diálogo Excepciones PUP de la configuración avanzada)*

- ***Archivo bloqueado. No analizado***: el objeto en cuestión está bloqueado, por lo que AVG no puede analizarlo
- ***Objeto potencialmente peligroso***: el objeto ha sido detectado como potencialmente peligroso pero no infectado (por ejemplo, puede contener macros); la información es únicamente una advertencia
- ***Para finalizar la acción, debe reiniciar el equipo***: el objeto infectado no se puede eliminar, para eliminarlo por completo es necesario 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 de cuadro de diálogo denominada ***Información de objeto detallada***:



  En este cuadro de diálogo, encontrará información detallada sobre el objeto infeccioso detectado (*por ejemplo, nombre y ubicación del objeto infectado, tipo de objeto, tipo de SDK, resultado de la detección e historial de las acciones relativas al objeto detectado*). Utilizando los botones ***Anterior*** / ***Siguiente*** puede visualizar información sobre resultados específicos. Use el botón ***Cerrar*** para salir de este cuadro de diálogo.

- ***Quitar el seleccionado***: use el botón para mover el resultado seleccionado al Almacén de virus
- ***Quitar todos los no reparados***: este botón elimina todos los resultados que no se pueden reparar ni mover al Almacén de virus
- ***Cerrar resultados***: finaliza la vista de información detallada y vuelve al cuadro de diálogo Información general de los resultados del análisis

11.7.4. Ficha Advertencias

La ficha ***Advertencias*** muestra información sobre objetos "sospechosos" (*normalmente archivos*) detectados durante el análisis. Cuando estos archivos son detectados por Protección residente, se impide el acceso a ellos. Ejemplos típicos de este tipo de detecciones son archivos ocultos, cookies, claves del Registro sospechosas, archivos comprimidos o documentos protegidos por contraseña, etc. Estos archivos no presentan ninguna amenaza directa al equipo o a la seguridad. La información sobre estos archivos resulta generalmente útil en caso de que se detecte adware o spyware en el equipo. Si únicamente se han detectado advertencias en un análisis de **AVG Internet Security 2012**, no es necesario realizar ninguna acción.

La siguiente es una breve descripción de los ejemplos más comunes de tales objetos:

- ***Archivos ocultos***: de forma predeterminada, los archivos ocultos no son visibles en Windows, por lo que algunos virus u otras amenazas pueden intentar evitar su detección almacenando sus archivos con este atributo. Si **AVG Internet Security 2012** informa de un archivo oculto que sospecha que es malicioso, puede moverlo al Almacén de virus.
- ***Cookies***: las cookies son archivos de texto sin formato utilizados por los sitios web para almacenar información específica del usuario, que se utilizará posteriormente para cargar diseños personalizados de los sitios web, presentar el nombre del usuario, etc.
- ***Claves del Registro sospechosas***: existe software malicioso que almacena información en el Registro de Windows para asegurarse de que se carga al inicio o para ampliar su efecto en el sistema operativo.

11.7.5. Ficha Rootkits

La ficha ***Rootkits*** muestra información sobre los rootkits detectados durante el análisis si ha iniciado el Análisis anti-rootkit.

Un rootkit es un programa diseñado para asumir el control de un equipo sin autorización de los propietarios y los administradores legítimos del sistema. El acceso al hardware normalmente no es necesario, ya que el rootkit está diseñado para tomar el control del sistema operativo que se ejecuta en el hardware. Generalmente, 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 se presentan en forma de troyanos, engañando a los usuarios para hacerles creer que es seguro ejecutarlos en sus sistemas. Las técnicas que se utilizan para conseguir este propósito incluyen ocultar los procesos en ejecución a los programas de supervisión o esconder archivos o datos del sistema al sistema operativo.

La estructura de esta ficha es básicamente la misma que la de la ficha Infecciones o la ficha Spyware.

11.7.6. Ficha Información

La ficha ***Información*** contiene datos sobre los "resultados" que no se pueden catalogar como infecciones, spyware, etc. No pueden clasificarse propiamente como peligrosos, pero merecen su atención. **El análisis de AVG Internet Security 2012** puede detectar archivos que pueden no estar infectados, pero que son sospechosos. Estos archivos son notificados como Advertencia o como Información.

Se puede notificar una gravedad del tipo ***Información*** por los siguientes motivos:

- ***Empaquetado en tiempo de ejecución***: el archivo se empaquetó con uno de los empaquetadores en tiempo de ejecución menos habituales, lo que puede indicar un intento de impedir el análisis de dicho archivo. Sin embargo, no todas las notificaciones sobre tales archivos indican un virus.

- ***Empaquetado en tiempo de ejecución recurrente***: similar al anterior, aunque es menos frecuente en el software habitual. Estos archivos son sospechosos y deberían ser eliminados o enviados para su posterior análisis.

- ***Archivo comprimido o documento protegido por contraseña***: los archivos protegidos por contraseña no pueden ser analizados por **AVG Internet Security 2012** (*ni por otros programas anti-malware*).

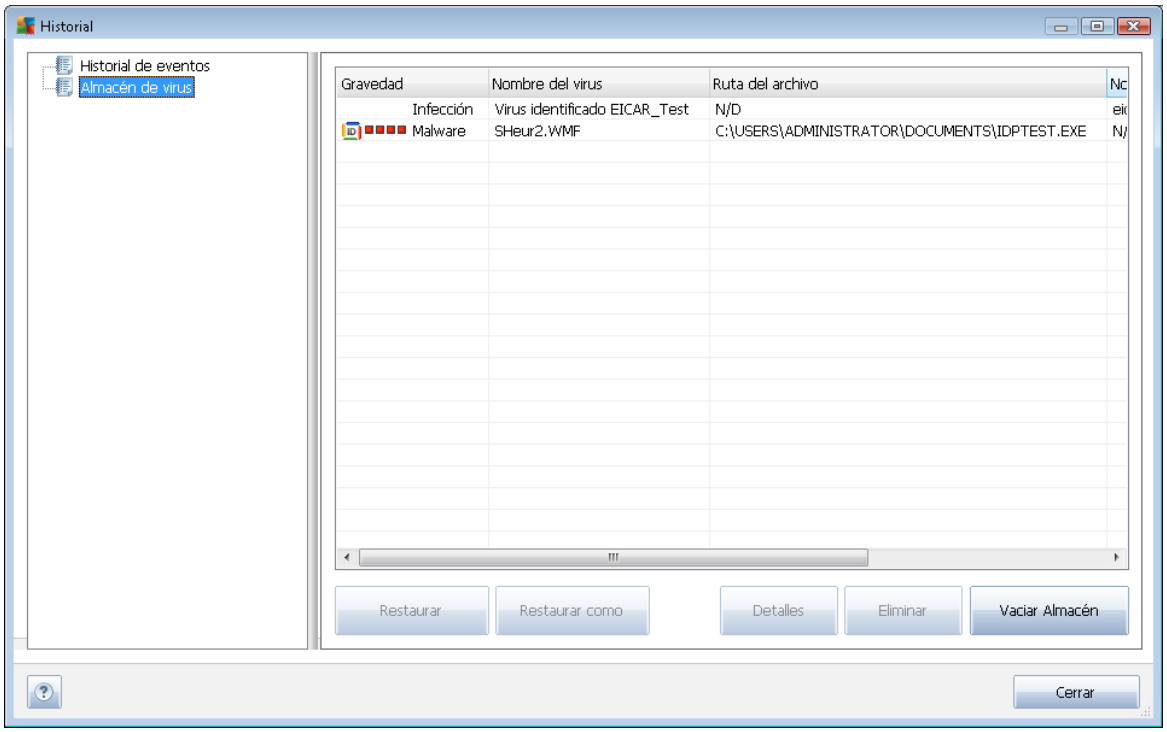
- ***Documento con macros***: el documento notificado contiene macros, lo que puede ser malicioso.

- ***Extensión oculta***: los archivos con extensión oculta pueden parecer, por ejemplo, imágenes, pero en realidad son archivos ejecutables (*por ejemplo, imagen.jpg.exe*). La segunda extensión no es visible en Windows de manera predeterminada, y **AVG Internet Security 2012** notifica sobre dichos archivos a fin de impedir su apertura accidental.

- ***Ruta de archivo incorrecta***: si algún archivo de sistema importante se está ejecutando desde una ruta que no es la predeterminada (*p. ej., winlogon.exe ejecutándose desde otra carpeta que no sea la de Windows*), **AVG Internet Security 2012** notifica esta discrepancia. En algunos casos, los virus usan nombres de procesos habituales del sistema para hacer que su presencia resulte menos evidente.

- ***Archivo bloqueado***: el archivo notificado está bloqueado y no puede ser analizado por **AVG Internet Security 2012**. Esto suele significar que algún archivo está siendo utilizado constantemente por el sistema (*por ejemplo, un archivo de intercambio*).

11.8. Almacén de virus



El ***Almacén de virus*** es un entorno seguro para la gestión de objetos sospechosos o infectados detectados en los análisis de AVG. Cuando se detecta un objeto infectado durante el análisis y AVG no puede repararlo automáticamente, se le solicita que decida lo que se hará con el objeto sospechoso. La acción recomendada es mover el archivo infectado al ***Almacén de virus*** para su posterior tratamiento. La finalidad principal del ***Almacén de virus*** es guardar cualquier archivo eliminado durante un tiempo determinado para que pueda asegurarse de que ya no lo necesita en su ubicación original. Si observa que la ausencia del archivo causa problemas, puede enviar el archivo en cuestión para que sea analizado o restaurarlo a la ubicación original.

La interfaz del ***Almacén de virus*** se abre en una ventana independiente y ofrece información general de los objetos infectados puestos en cuarentena:

- ***Gravedad***: si decidió instalar el componente Identity Protection con **AVG Internet Security 2012**, en esta sección se proporcionará una identificación gráfica de la gravedad de cada hallazgo en una escala de cuatro niveles, desde incuestionable (■□□□) a muy peligroso (■■■■), así como información del tipo de infección (*según su nivel infeccioso, pudiendo estar positiva o potencialmente infectados*)
- ***Nombre del virus***: especifica el nombre de la infección detectada según la Enciclopedia de virus *(en línea)*
- ***Ruta del archivo***: ruta completa a la ubicación original del archivo infeccioso detectado
- ***Nombre del objeto original***: todos los objetos detectados enumerados en la tabla se etiquetan según el nombre estándar proporcionado por AVG durante el proceso de análisis.

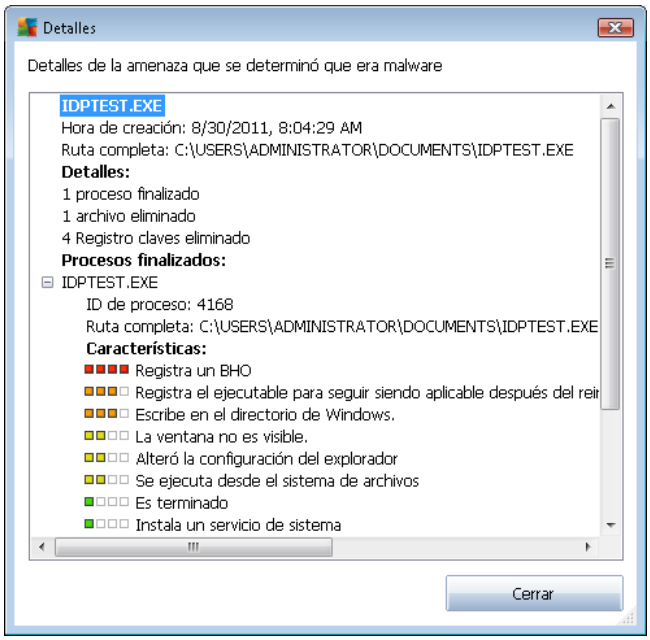
En el caso de que el objeto tuviese un nombre original específico conocido (*por ejemplo, el nombre de un adjunto que de hecho no corresponda con el contenido del mismo*), se proporcionará en esta columna.

- ***Fecha de almacenamiento***: fecha y hora en la que se detectó el archivo sospechoso y se movió al Almacén de virus

Botones de control

En la interfaz del ***Almacén de virus*** están disponibles los siguientes botones de control:

- ***Restaurar***: vuelve a colocar el archivo infectado en su ubicación original en el disco
- ***Restaurar como***: mueve el archivo infectado a una carpeta seleccionada
- ***Detalles***: este botón sólo es aplicable a las amenazas detectadas por Identity Protection. Al hacer clic en él, muestra un resumen sinóptico de los detalles de la amenaza (*los archivos/procesos afectados, las características del proceso, etc.*). Tenga en cuenta que para los elementos no detectados por IDP, este botón aparece atenuado y está inactivo.



- ***Eliminar***: quita el archivo infectado del ***Almacén de virus*** de manera completa e irreversible
- ***Vaciar Almacén***: quita todo el contenido del ***Almacén de virus***. Al quitar los archivos del ***Almacén de virus***, desaparecen del disco de manera irreversible (*no se mueven a la Papelera de reciclaje*).

12. Actualizaciones de AVG

Ningún software de seguridad puede garantizar una verdadera protección contra los diversos tipos de amenazas a menos que se actualice regularmente. Los creadores de virus están siempre a la búsqueda de nuevos fallos que puedan aprovechar tanto del software como de los sistemas operativos. Cada día aparecen nuevos virus, nuevo software malicioso y nuevos ataques de piratas informáticos. Por esta razón, los fabricantes de software están continuamente publicando actualizaciones y parches de seguridad para solucionar las brechas que se descubren.

Teniendo en cuenta las nuevas amenazas que emergen y la velocidad con que se difunden, es absolutamente esencial que actualice **AVG Internet Security 2012** regularmente. La mejor solución es mantener la configuración predeterminada del programa, donde está configurada la actualización automática. Tenga en cuenta que si la base de datos de virus de **AVG Internet Security 2012** no está actualizada, el programa no podrá detectar las últimas amenazas.

Es crucial actualizar regularmente la instalación de AVG. Las actualizaciones de las definiciones de virus esenciales deben ser diarias si es posible. Las actualizaciones del programa menos urgentes pueden hacerse semanalmente.

12.1. Inicio de la actualización

Para proporcionar la máxima seguridad disponible, **AVG Internet Security 2012** está definido de manera predeterminada para buscar actualizaciones nuevas cada cuatro horas. Puesto que las actualizaciones de AVG no se publican en función de un calendario fijo, sino como reacción al volumen y a la gravedad de las nuevas amenazas, esta comprobación es fundamental para asegurarse de que la base de datos de virus de AVG se encuentra actualizada en todo momento.

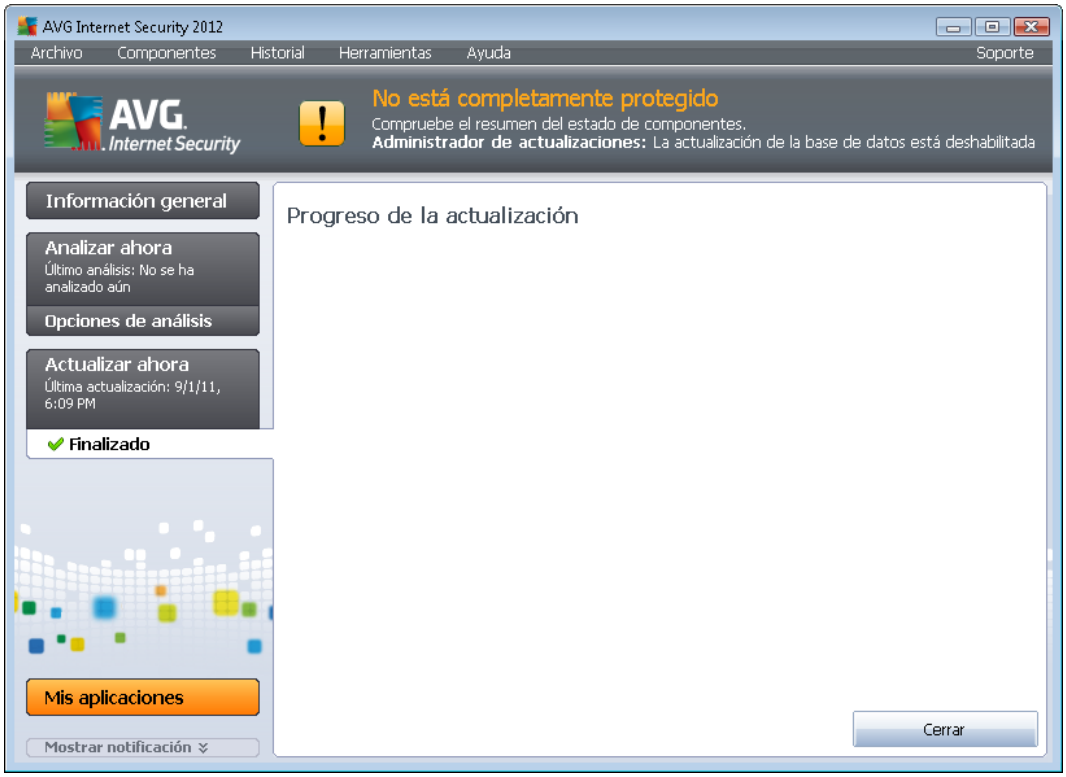
En caso de que desee reducir el número de inicios de la actualización, puede configurar sus propios parámetros para este proceso. En todo caso, se recomienda encarecidamente que se inicie la actualización al menos una vez al día. La configuración puede editarse desde la sección Configuración avanzada/Programaciones, específicamente en los cuadros de diálogo siguientes:

- Programación de actualización de definiciones
- Programación de actualización del programa
- Programación de actualización de Anti-Spam

Si desea comprobar si hay nuevos archivos de actualización inmediatamente, utilice el vínculo rápido Actualizar ahora en la interfaz de usuario principal. Este vínculo está disponible en todo momento desde cualquier cuadro de diálogo de la interfaz de usuario.

12.2. Progreso de la actualización

Una vez iniciada la actualización, AVG verificará primero si hay disponibles nuevos archivos de actualización. Si es así, **AVG Internet Security 2012** comienza a descargarlos e inicia el proceso de actualización en sí. Durante el proceso de actualización, se le redirigirá a la interfaz de ***actualización***, donde podrá ver el progreso del proceso en una representación gráfica, así como una descripción general de los parámetros estadísticos relevantes (*tamaño del archivo de actualización, datos recibidos, velocidad de descarga, tiempo transcurrido, etc.*):



***Nota**: antes de iniciar la actualización del programa AVG, se creará un punto de restauración del sistema. En caso de que falle el proceso de actualización y se bloquee el sistema operativo, este último siempre se podrá restaurar a la configuración original desde este punto. Esta opción es accesible a través del menú de Windows: Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema. Recomendado sólo para usuarios expertos.*

12.3. Niveles de actualización

AVG Internet Security 2012 ofrece dos niveles de actualización entre los que elegir:

- ***Actualización de definiciones*** contiene los cambios necesarios para una protección antivirus, anti-spam y anti-malware fiable. Por lo general, no incluye ningún cambio de código y sólo actualiza la base de datos de definiciones. Esta actualización debe aplicarse tan pronto como esté disponible.
- ***Actualización del programa*** contiene diversos cambios, correcciones y mejoras para el programa.

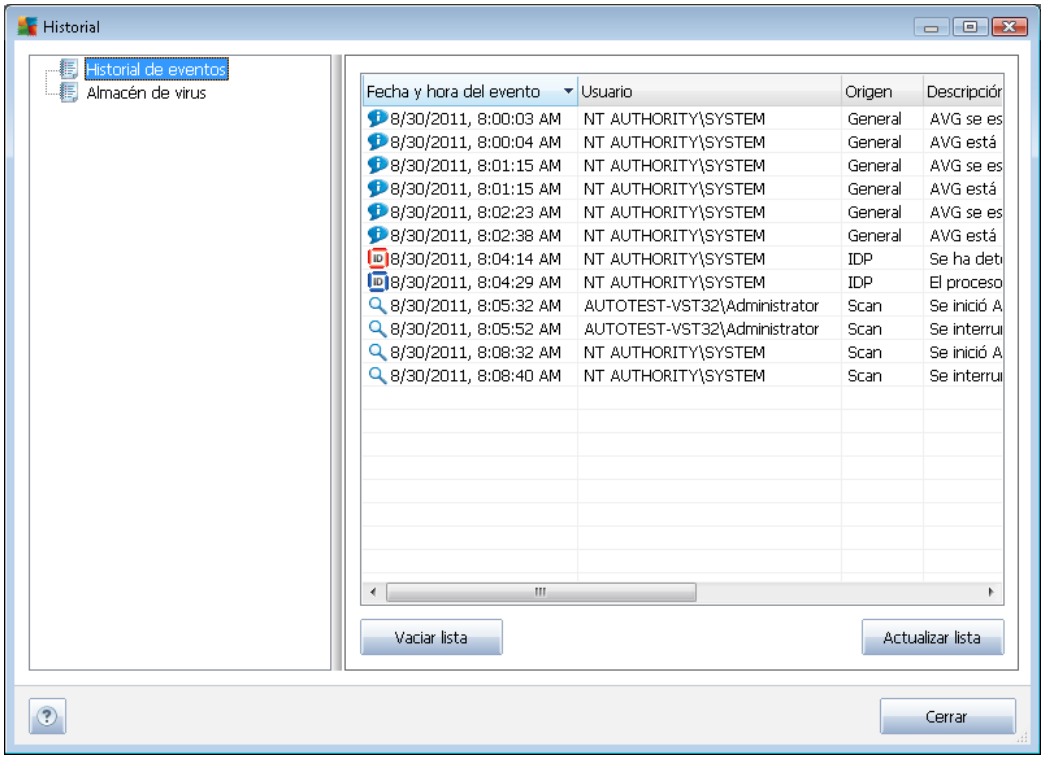
Cuando se programa una actualización, es posible definir parámetros específicos para cada nivel de actualización:

- Programación de actualización de definiciones
- Programación de actualización del programa

***Nota:** si llegase a coincidir el momento de una actualización programada del programa y un análisis*

programado, el proceso de actualización tiene prioridad y, por lo tanto, se interrumpirá el análisis.

13. Historial de eventos



Al cuadro de diálogo ***Historial*** se puede acceder desde el menú del sistema, a través del elemento ***Historial/Registro del historial de eventos***. En este cuadro de diálogo puede encontrar un resumen de los eventos más importantes que ocurrieron durante el funcionamiento de **AVG Internet Security 2012**. ***Historial*** registra los siguientes tipos de eventos:

- Información sobre actualizaciones de la aplicación AVG
- Información sobre el inicio, la finalización o la detención del análisis (*incluidas las pruebas realizadas automáticamente*)
- Información sobre eventos relacionados con la detección de virus (*por parte de la Protección residente o de los análisis*), incluida la ubicación de los casos
- Otros eventos importantes

De cada evento se ofrece la siguiente información:

- ***Fecha y hora del evento*** proporciona la fecha y hora exacta en la que ocurrió el evento
- ***Usuario*** indica el nombre del usuario conectado en el momento en que ocurrió el evento
- ***Origen*** proporciona información sobre el componente de origen u otra parte del sistema de AVG que provocó el evento
- ***Descripción del evento*** proporciona un breve resumen de lo que en realidad ha sucedido

Botones de control

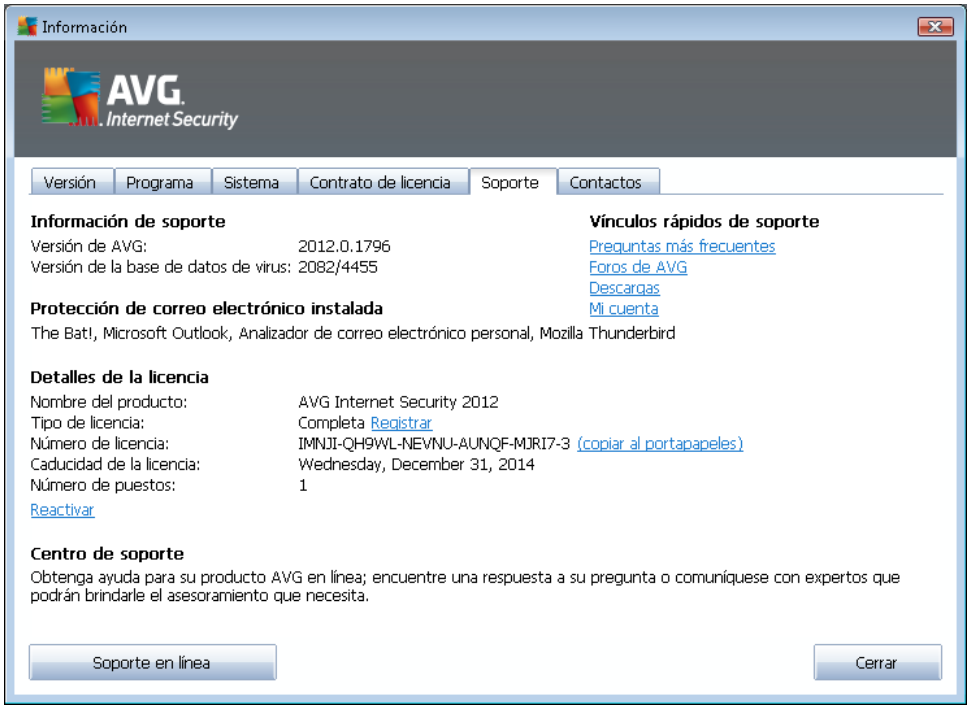
- ***Vaciar lista***: pulse el botón para eliminar todas las entradas de la lista de eventos
- ***Actualizar lista***: pulse el botón para actualizar todas las entradas de la lista de eventos

14. Preguntas más frecuentes (FAQ) y soporte técnico

Si tiene algún problema administrativo o técnico con su aplicación **AVG Internet Security 2012**, hay varias formas de buscar ayuda. Elija entre las siguientes opciones:

- ***Contacto con el servicio de atención al cliente***: desde la aplicación AVG puede contactar con nuestro departamento de atención al cliente. Seleccione la opción del menú principal ***Ayuda / Obtener ayuda en línea*** para ser redirigido al formulario de contacto en línea que le permitirá comunicarse con el departamento de atención al cliente de AVG, disponible las 24 horas, los 7 días de la semana. El campo se completará automáticamente con su número de licencia. Para continuar, siga las instrucciones de la página web.

- ***Soporte (vínculo en el menú principal)***: el menú de la aplicación AVG (*en la parte superior de la interfaz de usuario principal*) incluye el vínculo ***Soporte***, que abre un nuevo cuadro de diálogo con todos los tipos de información que podría necesitar cuando intenta buscar ayuda. El cuadro de diálogo incluye datos básicos sobre su programa AVG instalado (*versión de la base de datos/programa*), datos de licencia y una lista de vínculo rápidos de soporte:



- ***Resolución de problemas en el archivo de ayuda***: hay una nueva sección ***Resolución de problemas*** disponible directamente en el archivo de ayuda incluido en **AVG Internet Security 2012**. Esta sección proporciona una lista de las situaciones que ocurren más frecuentemente cuando un usuario desea buscar ayuda profesional para un problema técnico. Seleccione la situación que mejor describa el problema y haga clic en ella para abrir instrucciones detalladas que llevan a su solución.

- ***Centro de soporte del sitio web de AVG***: también puede buscar la solución a su problema en el sitio web de AVG (http://www.avg.com/). En la sección ***Centro de soporte***

puede encontrar información general estructurada en grupos temáticos que tratan problemas administrativos y técnicos.

- ***Preguntas más frecuentes***: en el sitio web de AVG (http://www.avg.com/) también puede encontrar una sección independiente y estructurada de preguntas frecuentes. Esta sección es accesible a través de la opción de menú ***Centro de soporte / FAQ***. De nuevo, todas las preguntas se dividen de forma bien organizada en las categorías de ventas, cuestiones técnicas y virus.

- ***Acerca de virus y amenazas***: hay un capítulo específico en el sitio web de AVG (http://www.avg.com/) dedicado a temas de virus. En el menú, seleccione ***Centro de soporte / Acerca de virus y amenazas*** para ir a una página que proporciona información general estructurada relacionada con las amenazas en línea. También puede encontrar instrucciones sobre como quitar virus y spyware, además de consejos para mantenerse protegido.

- ***Foro de debate***: también puede utilizar el foro de debate de los usuarios de AVG en http://forums.avg.com.