AVG Internet Security 2011

Manual del usuario

Revisión del documento 2011.21 (16.5.2011)

Contenido

1. Introducción

Este manual del usuario proporciona documentación completa sobre **AVG Internet Security 2011**.

Enhorabuena por adquirir AVG Internet Security 2011.

AVG Internet Security 2011 es un software de la gama de productos galardonados de AVG que están diseñados para darle tranquilidad a usted y total seguridad a su equipo. Al igual que el resto de productos AVG, **AVG Internet Security 2011** se ha rediseñado íntegramente, de arriba a abajo, para proporcionar la reconocida y acreditada protección de seguridad de AVG de forma novedosa, más eficiente y fácil de usar. El nuevo producto **AVG Internet Security 2011** cuenta con una interfaz optimizada combinada con un análisis más rápido y agresivo. Para su comodidad, se han automatizado más características de seguridad y se han incluido nuevas opciones "inteligentes" de usuario para que pueda adaptarlas a su forma de vida. Se acabó sacrificar la simplicidad de uso en aras de la seguridad.

AVG ha sido diseñado y desarrollado para proteger su actividad informática y de red. Disfrute la experiencia de una protección total con AVG.

Todos los productos AVG ofrecen

- Protección esencial para su forma de utilizar el equipo e Internet: transacciones bancarias y compras, navegación y búsquedas, chat y correo electrónico o descarga de archivos y redes sociales – AVG tiene un producto de protección adecuado para usted
- Protección sin complicaciones en la que confían más de 110 millones de personas en todo el mundo e incentivada por una red global de investigadores altamente experimentados
- Protección respaldada por un soporte técnico experto e ininterrumpido

2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG Internet Security 2011 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 2011, pero sólo sin el componente IDP.*

2.2. Requisitos de hardware mínimos y recomendados

Requisitos de hardware mínimos para **AVG Internet Security 2011**:

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

Requisitos de hardware recomendados para **AVG Internet Security 2011**:

- CPU Intel Pentium de 1,8 GHz
- 512 MB de memoria RAM
- 1400 MB de espacio libre en disco duro (para la instalación)

3. Opciones de instalación de AVG

Es posible instalar AVG desde el archivo de instalación que se encuentra en el CD de instalación, o bien descargando el último archivo de instalación del sitio web de AVG (http://www.avg.com/).

Antes de comenzar a instalar AVG, le recomendamos encarecidamente visitar el sitio web de AVG (http://www.avg.com/) para comprobar la existencia de un nuevo archivo de instalación. De esta forma puede estar seguro de que está instalando la última versión disponible de AVG Internet Security 2011.

Durante el proceso de instalación se le pedirá su número de licencia/venta. Asegúrese de tenerlo a mano antes de comenzar la instalación. El número de venta figura en el paquete del CD. Si compró su copia de AVG en línea, el número de licencia se le habrá enviado por correo electrónico.

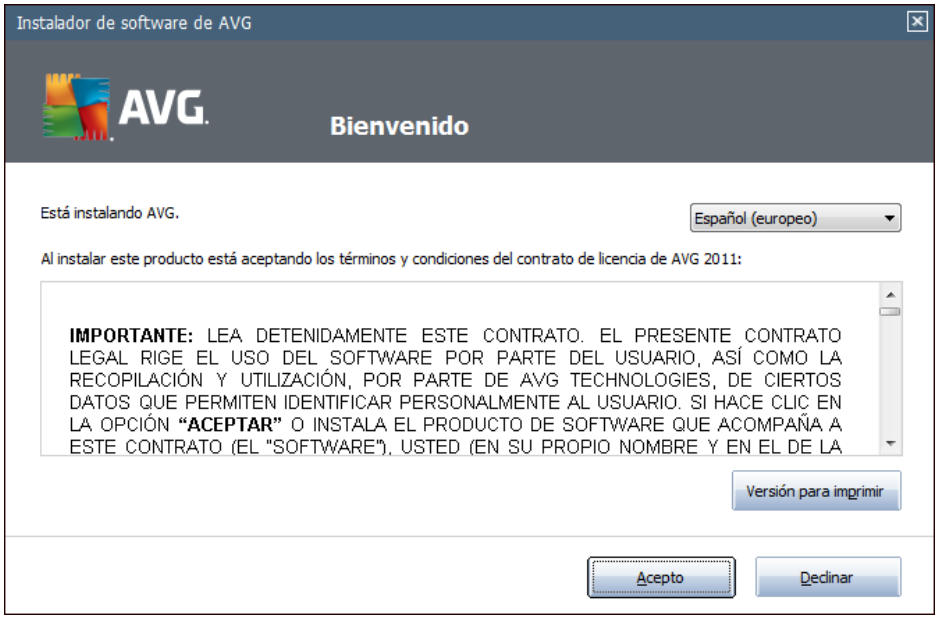
4. Proceso de instalación de AVG

Para instalar **AVG Internet Security 2011** en su equipo, debe obtener el archivo de instalación más reciente. Puede utilizar el archivo de instalación del CD que forma parte de la edición en caja, aunque este archivo podría estar obsoleto. Por este motivo, se recomienda obtener en línea el archivo de instalación más reciente. Puede descargar el archivo del sitio web de AVG (http://www.avg.com/), en la sección ***Centro de soporte / Descargas***.

La instalación es una secuencia de ventanas de cuadro de diálogo con una breve descripción de lo que se debe hacer en cada paso. A continuación ofrecemos una explicación de cada ventana de cuadro de diálogo:

4.1. Bienvenido

El proceso de instalación se inicia con la ventana de cuadro de diálogo ***Bienvenido***. Aquí se selecciona el idioma que se utilizará en el proceso de instalación y el idioma predeterminado para la interfaz de usuario de AVG. En la sección superior de la ventana de cuadro de diálogo encontrará un menú desplegable con la lista de los idiomas que puede elegir:



Atención: *en este paso va a seleccionar el idioma para el proceso de instalación. El idioma que seleccione se instalará como el predeterminado para la interfaz de usuario de AVG junto con el inglés, que se instala automáticamente. Si desea instalar otros idiomas adicionales para la interfaz de usuario, defínalos en uno de los siguientes cuadros de diálogo de configuración denominados* ***Opciones personalizadas****.*

El cuadro de diálogo también incluye 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.

4.2. Active su licencia de AVG

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

Puede encontrar el número de venta en el paquete del CD, dentro de la caja de **AVG Internet Security 2011**. El número de licencia se encontrará en el correo electrónico de confirmación que recibió después de haber comprado **AVG Internet Security 2011** 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.

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

4.3. Seleccione el tipo de instalación

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

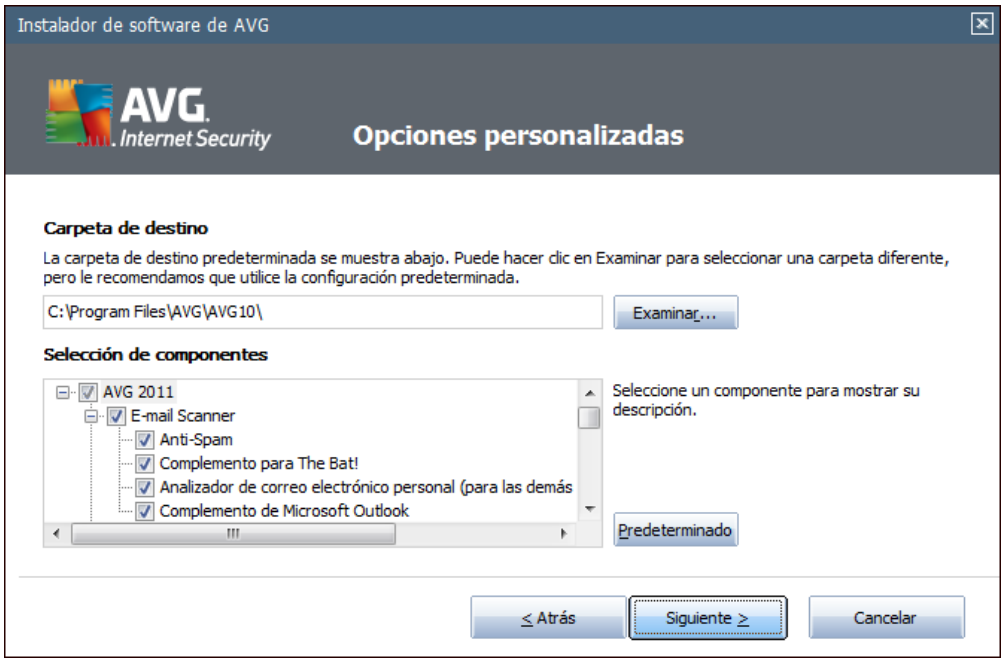
Para la mayoría de los usuarios, se recomienda seleccionar la opción estándar ***Instalación rápida***, la cual instala AVG de manera totalmente automática con la configuración predefinida por el proveedor del programa. Esta configuración ofrece máxima seguridad con un uso óptimo de los recursos. En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

La ***Instalación personalizada*** sólo debería ser utilizada por usuarios expertos que tengan una razón válida para instalar AVG con una configuración diferente de la estándar, es decir, para adecuar el programa a necesidades específicas del sistema. Tras seleccionar esta opción, haga clic en el botón ***Siguiente*** para ir al cuadro de diálogo ***Opciones personalizadas***.

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 2011**; por ejemplo, análisis y actualizaciones.

4.4. 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 2011**. De manera predeterminada, AVG se instalará en la carpeta de archivos de programa situada 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

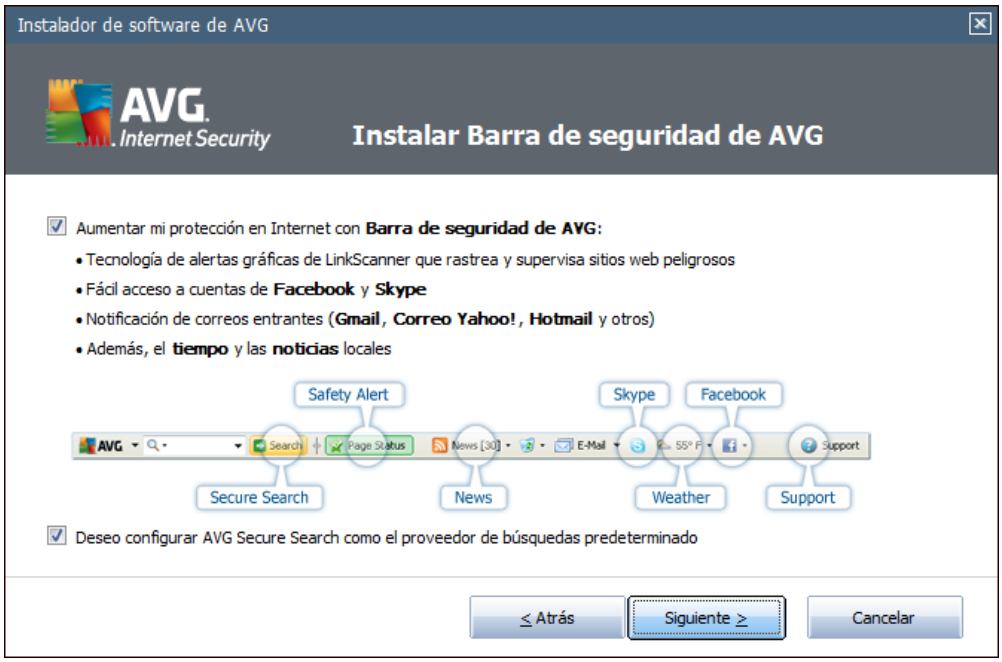
La sección ***Selección de componentes*** muestra una descripción general de todos los componentes de **AVG Internet Security 2011** que se pueden instalar. Si la configuración predeterminada no se ajusta a sus necesidades, puede quitar o agregar componentes específicos.

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***.

Pulse el botón ***Siguiente*** para continuar.

4.5. 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 modifica la configuración predeterminada, este componente se instalará automáticamente en su navegador de Internet (*los navegadores actualmente compatibles son Microsoft Internet Explorer v. 6.0 o superior y Mozilla Firefox v. 3.0 o superior*) para ofrecerle una protección integral en línea mientras navega por Internet.

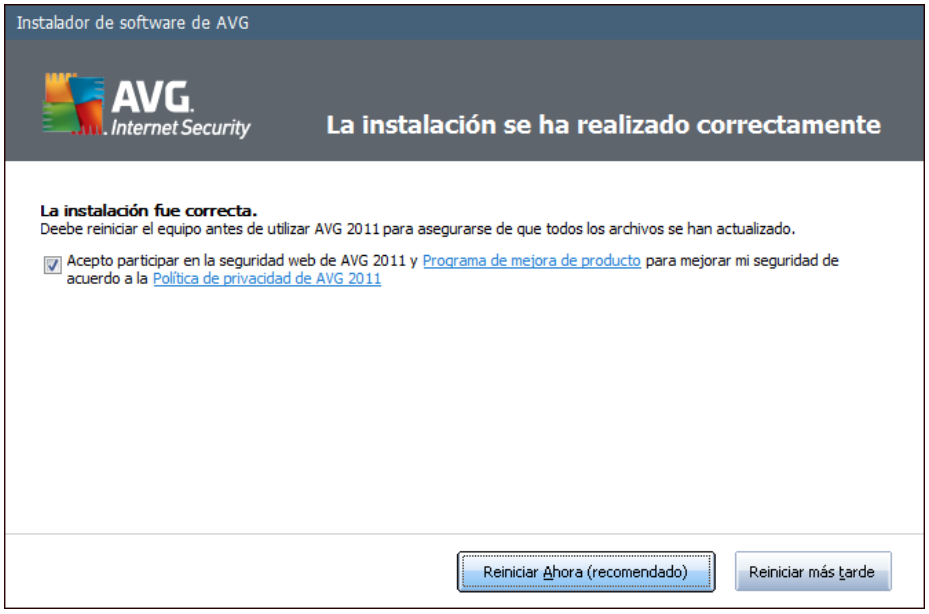
También puede indicar si desea escoger *AVG Secure Search (powered by Google)* como el proveedor de búsqueda predeterminado. Si es así, mantenga la selección de la correspondiente casilla de verificación.

4.6. Progreso de la instalación

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

Tras completarse el preceso de instalación, será redirigido al siguiente cuadro de diálogo.

4.7. La instalación se ha realizado correctamente



El cuadro de diálogo ***La instalación se ha realizado correctamente*** confirma que **AVG Internet Security 2011** se ha instalado y configurado por completo.

En este cuadro de diálogo, facilite su información de contacto para poder recibir información y noticias sobre productos. Debajo del formulario de registro encontrará las dos opciones siguientes:

- ***Sí, mantenerme informado de noticias sobre seguridad y ofertas especiales de AVG 2011 por correo electrónico***: marque esta casilla de verificación para indicar que desea recibir información sobre ofertas especiales de productos AVG, mejoras y actualizaciones, etc.

- ***Acepto participar en la seguridad web de AVG 2011 y Programa de mejora de productos ...***: marque esta casilla de verificación para indicar que desea participar en el programa de mejora de productos (*para obtener detalles, consulte el capítulo Configuración avanzada de AVG / Programa de mejora de productos*), que recopila información anónima sobre amenazas detectadas para aumentar el nivel de seguridad global de Internet.

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

> ***Nota:*** *si utiliza una licencia comercial de AVG y ha seleccionado previamente la instalación del elemento Administración remota (consulte Opciones personalizadas), el cuadro de diálogo La instalación se ha realizado correctamente aparecerá en 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; puede descargarlo en el sitio web de AVG (http://www.avg.com/).*

5. Tras la instalación

5.1. Registro del producto

Cuando haya finalizado la instalación de **AVG Internet Security 2011**, registre el producto en línea en el sitio web de AVG (http://www.avg.com/), en la página de ***Registro*** (*siga las instrucciones que se proporcionan directamente en la página*). 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.

5.2. Acceso a la interfaz de usuario

Se puede acceder a la ***interfaz de usuario de 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 2011/Interfaz de usuario de AVG***
- desde ***la barra de herramientas AVG Security Toolbar,*** a través de la opción ***Ejecutar AVG***

5.3. 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 2011**. 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***.

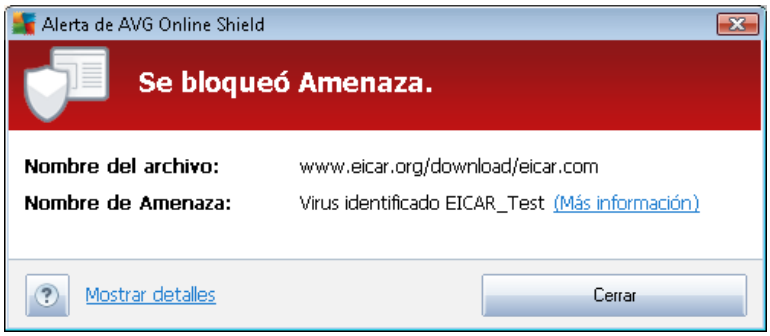
5.4. Prueba Eicar

Para confirmar que **AVG Internet Security 2011** 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 después de

confirmar la descarga del archivo de prueba, ***Online Shield*** reaccionará con una advertencia. 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 el disco local, pero ***Protección residente*** detecta el "virus" en cuanto intenta descomprimirlo. **Si AVG no identifica el archivo de la prueba EICAR como un virus, debe comprobar de nuevo la configuración del programa.**

5.5. Configuración predeterminada de AVG

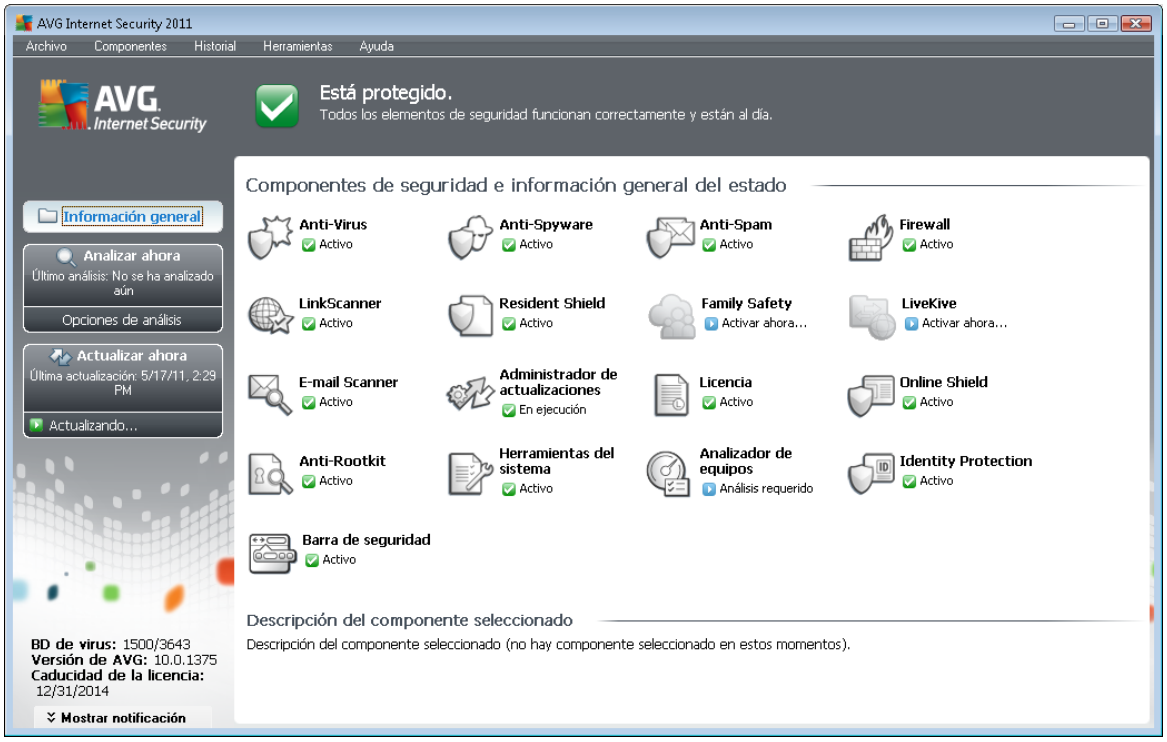
La configuración predeterminada (*es decir, cómo está configurada la aplicación justamente después de la instalación*) de **AVG Internet Security 2011** la realiza el proveedor del software de manera que todos los componentes y funciones ofrezcan un rendimiento óptimo.

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.

6. Interfaz de usuario de AVG

AVG Internet Security 2011 se abre con la ventana principal:



La ventana principal se divide en varias secciones:

- ***Menú del sistema*** *(primera línea del sistema en la ventana)* es la navegación estándar que le permite acceder a todos los componentes, servicios y características de AVG - detalles >>
- ***Información sobre el estado de seguridad*** *(sección superior de la ventana)* le proporciona información sobre el estado actual del programa AVG - detalles >>
- ***Vínculos rápidos*** *(sección izquierda de la ventana)* le permite acceder rápidamente a las tareas de AVG más importantes y frecuentes - detalles >>
- ***Información general de los componentes*** *(sección central de la ventana)* ofrece una vista general de todos los componentes de AVG instalados - detalles >>
- ***Estadísticas*** *(sección inferior izquierda de la ventana)* le proporciona todos los datos estadísticos relacionados con el funcionamiento de los programas - detalles >>
- ***Icono de la bandeja del sistema*** *(esquina inferior derecha del monitor, en la bandeja del sistema)* indica el estado actual de AVG - detalles >>
- ***Gadget de AVG*** *(barra lateral de Windows, compatible con Windows Vista/7)* ofrece acceso rápido al análisis y actualización de AVG - detalles >>

6.1. 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 2011**. 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:

6.1.1. Archivo

- ***Salir***: cierra la interfaz de usuario de **AVG Internet Security 2011**. Sin embargo, la aplicación AVG continuará ejecutándose en segundo plano y su equipo seguirá protegido.

6.1.2. 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*** garantiza la protección de su equipo frente a virus que intentan entrar en él - detalles >>
- ***Anti-Spyware*** garantiza la protección de su equipo frente a spyware y adware - detalles >>
- ***Anti-Spam*** comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como SPAM - detalles >>
- ***Firewall*** controla el intercambio de datos realizado entre el equipo y otros equipos por Internet o a través de la red local - detalles >>
- ***LinkScanner*** comprueba los resultados de búsqueda mostrados en el navegador de Internet - detalles >>
- ***Analizador de correo electrónico*** comprueba todo el correo entrante y saliente en busca de virus - detalles >>
- ***Family Safety*** contribuye a supervisar la actividad en línea de sus hijos y a protegerlos de los contenidos web inadecuados - detalles >>
- ***LiveKive*** proporciona copias de seguridad en línea de sus datos - detalles >>
- ***Protección residente*** se ejecuta en segundo plano y analiza los archivos a medida que se copian, abren o guardan - detalles >>
- ***Administrador de actualizaciones*** controla todas las actualizaciones de AVG - detalles >>

- ***Licencia*** muestra el número de licencia, el tipo y la fecha de caducidad - detalles >>
- ***Online Shield*** analiza todos los datos descargados por el explorador web - detalles >>
- ***Anti-Rootkit*** detecta programas y tecnologías que intentan camuflar software malicioso - 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*** - componente anti-malware cuya finalidad es impedir que los ladrones de identidad roben sus valiosos elementos digitales personales - 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

6.1.3. 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 adjuntos de mensajes de correo electrónico detectados como peligrosos por el componente ***Analizador de correo electrónico***
- ***Resultados de Online Shield***: abre un cuadro de diálogo con información general de las amenazas detectadas por ***Online Shield***
- ***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 2011** registradas
- ***Firewall***: abre la interfaz de configuración del Firewall en la ficha ***Registros***, que contiene información detallada de todas las acciones de este componente

6.1.4. 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 2011**.

- ***Actualizar desde directorio***: ejecuta el proceso de actualización a partir de los archivos de actualización ubicados en una carpeta específica en el 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***, en el que puede editar la configuración de **AVG Internet Security 2011**. 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***.

6.1.5. 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 2011**, *los últimos dos elementos aparecen como* ***Comprar ahora *y* ***Activar***, *que le permiten adquirir de inmediato la versión completa del programa. Si* **AVG Internet Security 2011** *se ha instalado con un número de venta, se muestran los elementos* ***Registrar*** *y* ***Activar***. *Para obtener más información, consulte la sección Licencia de esta documentación.*

- ***Acerca de AVG***: abre el cuadro de diálogo ***Información*** con cinco 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***.

6.2. Información sobre el estado de seguridad

La sección***Información sobre el estado de seguridad*** está ubicada en la parte superior de la pantalla principal de AVG. En esta sección, siempre encontrará información sobre el estado de seguridad actual de **AVG Internet Security 2011**. A continuación se describen los iconos que pueden aparecer en esta sección y su significado:

 - El icono verde indica que AVG 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 el programa AVG, quizás simplemente se trate de que decidió desactivar alguno de los componentes porque tenía motivos para hacerlo. Sigue estando protegido por AVG. 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.

Este icono también aparece si, por alguna razón, decidió ignorar el estado de error de un componente (*se puede acceder a la opción "Ignorar el estado de este componente" 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*). Es posible que necesite usar esta opción en una situación específica, pero se recomienda estrictamente desactivar "***Ignorar el estado de este componente***" tan pronto como sea posible.

 - El icono rojo indica que AVG se encuentra en estado crítico. Uno o más componentes no funcionan correctamente y AVG 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 no esté configurado para un rendimiento óptimo, aparecerá un botón nuevo llamado Reparar (o Reparar todo si el problema concierne a más de un componente) junto a la información sobre el estado de seguridad. Pulse el botón para

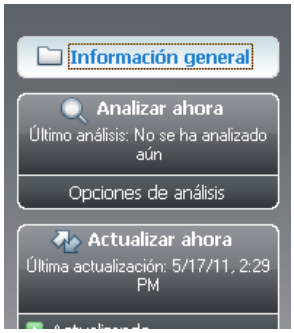
iniciar un proceso automático de comprobación y configuración del programa. Se trata de una manera sencilla de configurar el programa AVG para un rendimiento óptimo y lograr el máximo nivel de seguridad.

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 en cualquier momento desde el icono de AVG en la bandeja del sistema.*

6.3. Vínculos rápidos

Vínculos rápidos *(en la sección izquierda de la interfaz de usuario de AVG)* permite acceder inmediatamente a las características de AVG más importantes y utilizadas:



- ***Información general***: utilice este vínculo para pasar de cualquier interfaz de AVG que tenga abierta a la interfaz predeterminada, que presenta información general de todos los componentes instalados; consulte el capítulo ***Información general de los componentes >>***
- ***Analizar ahora***: de manera predeterminada, este botón proporciona información (*tipo de análisis, fecha en que se ejecutó por última vez*) sobre el último análisis realizado. Puede ejecutar el comando ***Analizar ahora*** para volver a iniciar el mismo análisis o hacer clic en el vínculo ***Opciones de análisis*** para abrir la interfaz de análisis de AVG, en la que puede ejecutar análisis, programarlos o editar sus parámetros; consulte el capítulo ***Análisis de AVG >>***
- ***Actualizar ahora***: este vínculo proporciona la fecha en la que se ejecutó por última vez el proceso de actualización. Pulse el botón para abrir la interfaz de actualización y ejecutar inmediatamente el proceso de actualización de AVG; consulte el capítulo ***Actualizaciones de AVG >>***

Se puede acceder a estos vínculos desda la interfaz de usuario en todo momento. Una vez que haya utilizado un vínculo rápido para ejecutar un proceso específico, la interfaz gráfica del usuario pasará a un nuevo cuadro de diálogo, pero los vínculos rápidos seguirán estando disponibles. Además, el proceso que se está ejecutando se representa también gráficamente.

6.4. Información general de los componentes

La sección ***Información general de los componentes*** se encuentra en la parte central de la interfaz de usuario de AVG. La sección está dividida en dos partes:

- Información general de todos los componentes instalados, que consiste en un panel que muestra el icono de cada componente y la información referida al estado activo o inactivo del componente en cuestión
- Descripción de un componente seleccionado

En **AVG Internet Security 2011**, la sección ***Información general de los componentes*** contiene información sobre los siguientes componentes:

- ***Anti-Virus*** garantiza la protección de su equipo frente a virus que intentan entrar en él - detalles >>
- ***Anti-Spyware*** garantiza la protección de su equipo frente a spyware y adware - detalles >>
- ***Anti-Spam*** comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como SPAM - detalles >>
- ***Firewall*** controla el intercambio de datos realizado entre el equipo y otros equipos por Internet o a través de la red local - detalles >>
- ***LinkScanner*** comprueba los resultados de búsqueda mostrados en el navegador de Internet - detalles >>
- ***Analizador de correo electrónico*** comprueba todo el correo entrante y saliente en busca de virus - detalles >>
- ***Protección residente*** se ejecuta en segundo plano y analiza los archivos a medida que se copian, abren o guardan - detalles >>
- ***Family Safety*** contribuye a supervisar la actividad en línea de sus hijos y a protegerlos de los contenidos web inadecuados - detalles >>
- ***LiveKive*** proporciona copias de seguridad en línea de sus datos - detalles >>
- ***Administrador de actualizaciones*** controla todas las actualizaciones de AVG - detalles >>
- ***Licencia*** muestra el número de licencia, el tipo y la fecha de caducidad - detalles >>
- ***Online Shield*** analiza todos los datos descargados por el explorador web - detalles >>
- ***Anti-Rootkit*** detecta programas y tecnologías que intentan camuflar software malicioso - 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*** - componente anti-malware cuya finalidad es impedir que los ladrones de identidad roben sus valiosos elementos digitales personales - 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

Haga un solo clic en el icono de cualquier componente para resaltarlo en la información general de los componentes. Al mismo tiempo, en la parte inferior de la interfaz de usuario aparece una descripción de la funcionalidad básica del componente. Haga doble clic en el icono para abrir la interfaz propia del componente con una lista de datos estadísticos básicos.

Haga clic con el botón derecho del ratón sobre el icono de un componente para expandir un menú contextual: además de abrir la interfaz gráfica del componente, también puede seleccionar ***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 AVG siga así y no quiere que se le advierta mediante el cambio en el icono de la bandeja del sistema.

6.5. Estadísticas

La sección ***Estadísticas*** está ubicada en la parte inferior izquierda de la ***interfaz de usuario de AVG***. Ofrece una lista con información relativa al funcionamiento del programa:

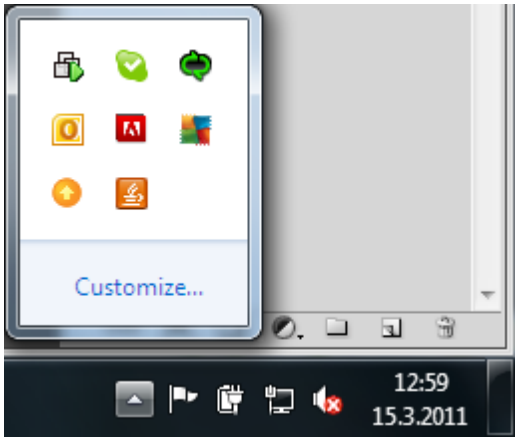
- ***Base de datos de virus***: informa sobre la versión actualmente instalada de la base de datos de virus

- ***Versión de AVG***: informa sobre la versión de AVG instalada *(cuyo formato es 10.0.xxxx, donde 10.0 es la versión de la línea de producto y xxxx hace referencia al número de compilación)*

- ***Caducidad de la licencia***: muestra la fecha en que caduca la licencia de AVG

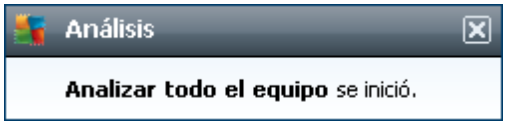
6.6. Icono de la bandeja del sistema

El icono de la bandeja del sistema (*en la barra de tareas de Windows*) indica el estado actual de **AVG Internet Security 2011**. Resulta visible en todo momento en la bandeja del sistema, sin importar si la ventana principal de AVG está abierta o cerrada:



Si está a todo color, el ***icono de la bandeja del sistema*** indica que todos los componentes de AVG están activos y funcionando correctamente. Del mismo modo, el icono de la bandeja del sistema de AVG puede mostrarse a todo color si se encuentra en un estado de error pero el usuario es plenamente consciente de esta situación y ha decidido deliberadamente ***Ignorar el estado de este componente***. Un icono con un signo de exclamación indica un problema (*componente inactivo, estado de error, etc.*). Haga doble clic en el ***icono de la bandeja del sistema*** para abrir la ventana principal y editar un componente.

El icono de la bandeja del sistema presentará información sobre las actividades actuales de AVG y posibles cambios de estado del programa (*por ejemplo, el inicio automático de una actualización o análisis 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 AVG en la bandeja del sistema:



El ***icono de la bandeja del sistema*** también puede utilizarse como vínculo rápido para acceder a la ventana principal de AVG en el momento en que lo desee; sólo debe hacer doble clic en el icono. Al hacer clic con el botón secundario en el ***icono de la bandeja del sistema***, aparecerá un breve menú contextual con las opciones siguientes:

- ***Abrir Interfaz de usuario de AVG***: haga clic aquí para abrir la interfaz de usuario de AVG
- ***Análisis***: haga clic aquí para abrir el menú contextual de
- ***Firewall***: haga clic aquí para abrir el menú contextual de las opciones de configuración de Firewall, donde podrá editar los principales parámetros: Estado de Firewall (*Firewall habilitado/Firewall deshabilitado/Modo de emergencia*), activación/desactivación del modo de juego y Perfiles de Firewall
- ***Ejecutar Analizador de equipos***: haga clic aquí para iniciar el componente Analizador de equipos
- ***Ejecutando análisis***: este elemento aparece sólo en caso de que haya un análisis

ejecutándose actualmente en el equipo. 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

6.7. Gadget de AVG

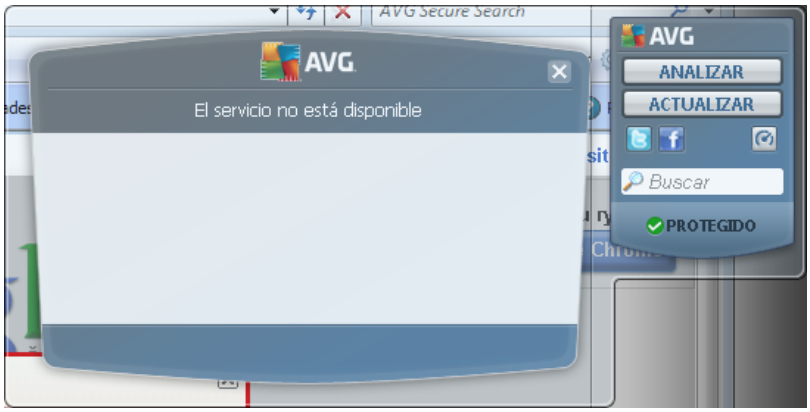
El ***gadget de AVG*** se muestra en el escritorio de Windows (*Barra lateral de Windows*). Esta aplicación solamente es compatible con los sistemas operativos Windows Vista y Windows 7. El ***gadget de AVG*** ofrece acceso inmediato a las funciones más importantes de **AVG Internet Security 2011**, es decir, análisis y actualización:

El ***gadget de AVG*** proporciona las siguientes opciones de acceso rápido:

- ***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 resltados de los análisis correspondintes se enumerarán en ***Análisis del gadget de la barra lateral***).

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

- ***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

- ***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

7. Componentes de AVG

7.1. Anti-Virus

7.1.1. Principios de Anti-Virus

El motor de análisis del software antivirus analiza todos los archivos y la actividad de los mismos (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. 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.

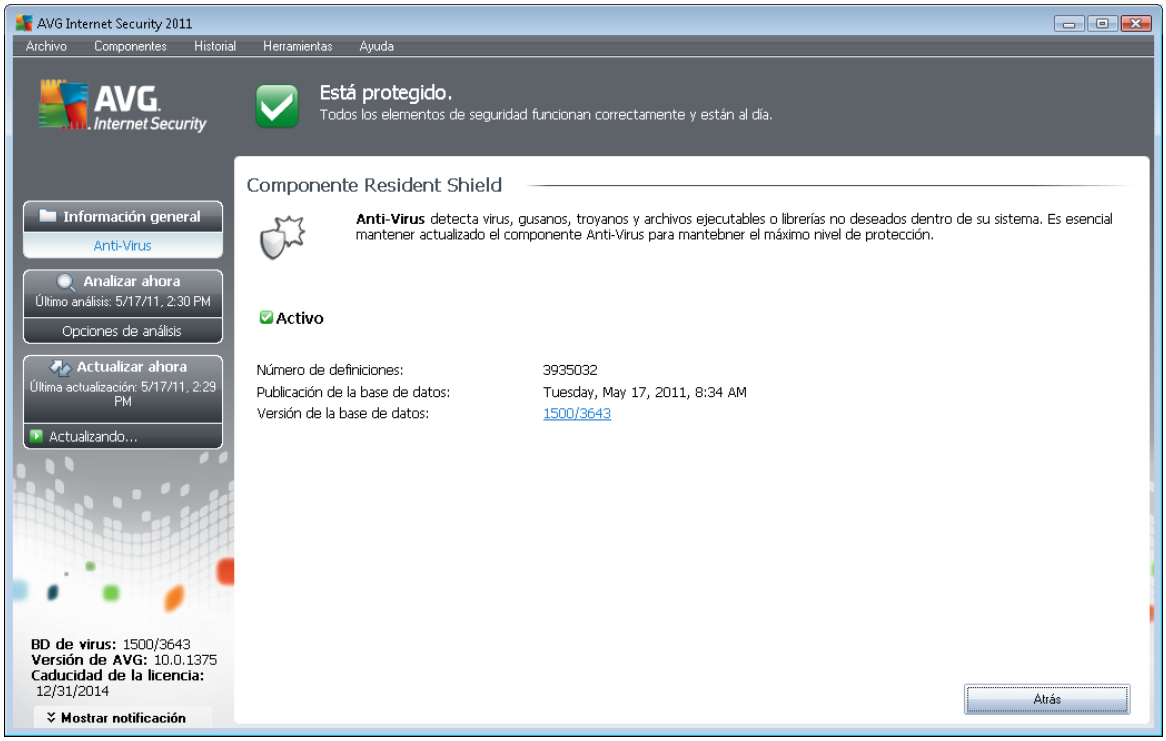
La característica esencial de la protección antivirus es que ningún virus conocido puede ejecutarse en el equipo.

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:

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

AVG también puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas en el sistema. Dichas amenazas se denominan programas potencialmente no deseados (como diversos tipos de spyware, adware, etc.). Asimismo, AVG analiza el Registro del sistema en busca de entradas sospechosas, archivos temporales de Internet y cookies de seguimiento, y permite tratar todos los elementos potencialmente dañinos de la misma manera que cualquier otra infección.

7.1.2. Interfaz de Anti-Virus



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

- ***Número de definiciones***: proporciona el recuento de virus definidos en la versión actualizada de la base de datos de virus
- ***Publicación de la base de datos***: especifica la fecha y hora de la última actualización de la base de datos de virus
- ***Versión de la base de datos***: define el número de la versión de la base de datos de virus instalada, que se incrementa con cada actualización de la base de datos de virus

En la interfaz de este componente solamente hay un botón operativo disponible (***Atrás***). Pulse este botón para volver a la interfaz de usuario de AVG predeterminada (*información general de los componentes*).

7.2. Anti-Spyware

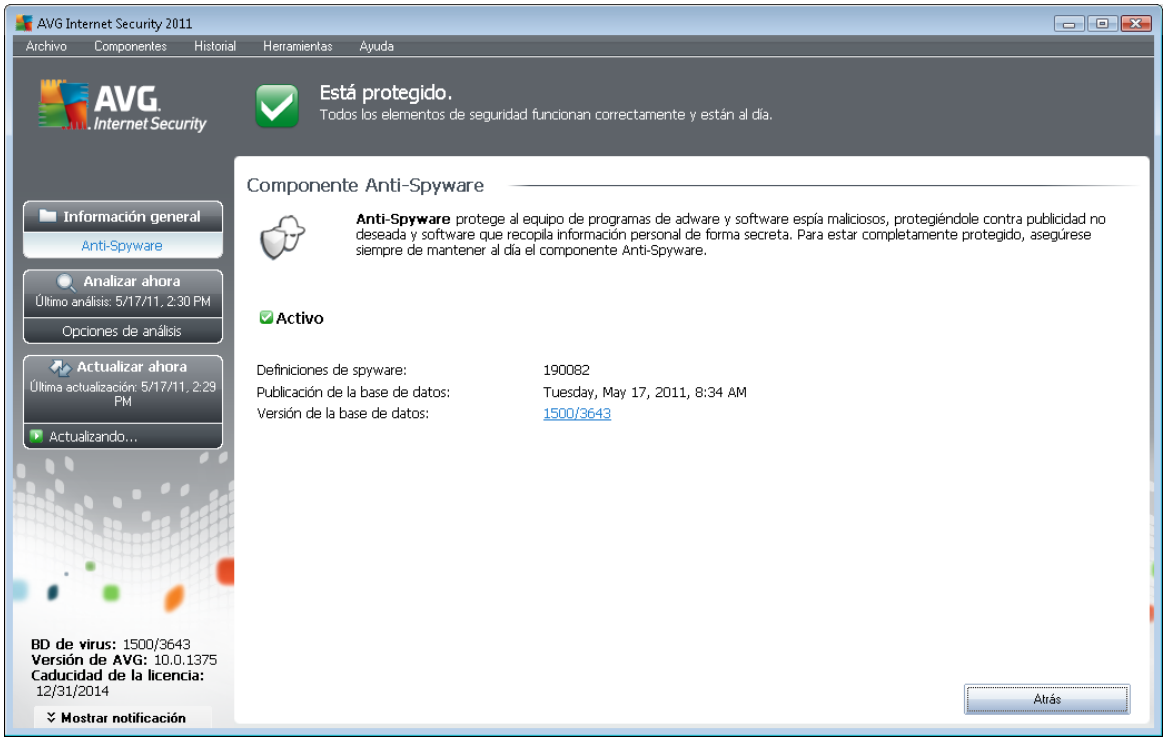
7.2.1. Principios de Anti-Spyware

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.

También existe el riesgo potencial de que se haya transmitido malware al equipo antes de instalar AVG o de que no haya mantenido **AVG Internet Security 2011** al día con las últimas actualizaciones de la base de datos y del programa. Por este motivo, AVG permite analizar el equipo completo en busca de malware y spyware utilizando la característica de análisis. También detecta malware inactivo o en letargo, es decir, el que ha sido descargado, pero que aún no se ha activado.

7.2.2. Interfaz de Anti-Spyware



La interfaz del componente ***Anti-Spyware*** proporciona una breve descripción de la funcionalidad del componente, información sobre su estado actual y algunas estadísticas de ***Anti-Spyware***:

- ***Definiciones de spyware***: proporciona el recuento de muestras de spyware definidas en la última versión de la base de datos de spyware

- ***Publicación de la base de datos***: especifica la fecha y hora de actualización de la base de datos de spyware

- ***Versión de la base de datos***: define el número de la última versión de la base de datos de spyware, que aumenta cada vez que se actualiza la base de datos de virus

En la interfaz de este componente solamente hay un botón operativo disponible (***Atrás***). Pulse este botón para volver a la interfaz de usuario de AVG predeterminada (*información general de los componentes*).

7.3. Anti-Spam

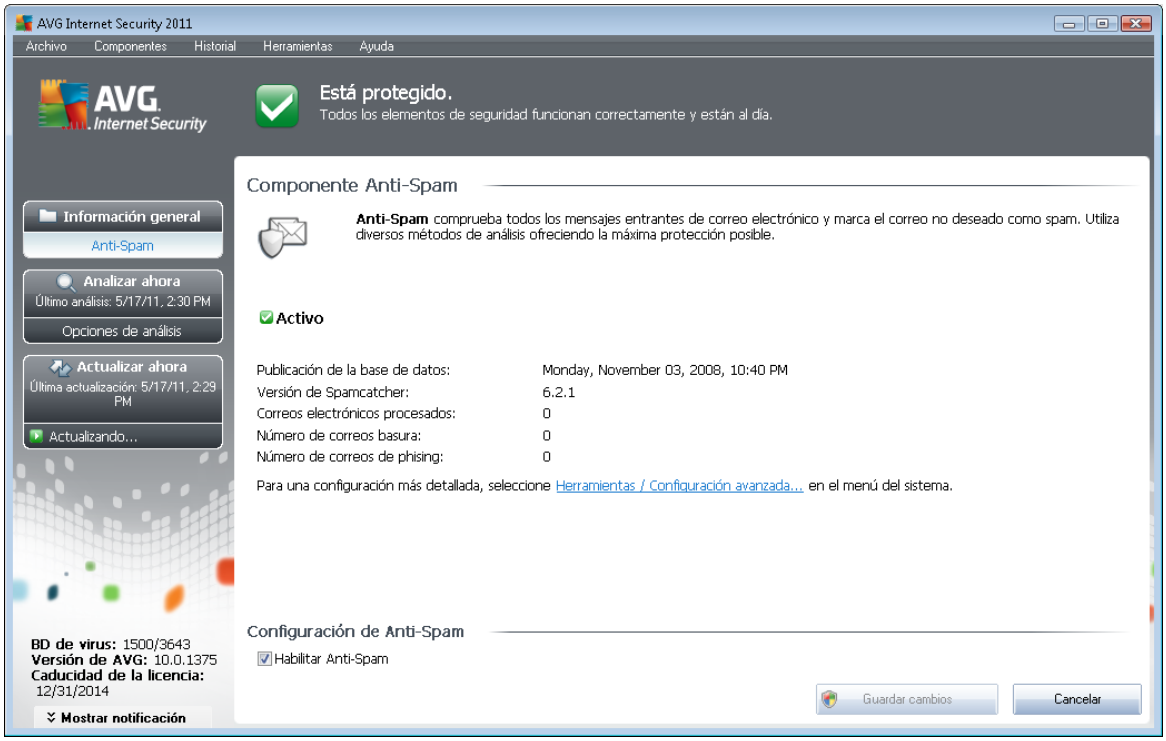
El spam se refiere al correo electrónico no solicitado, generalmente anunciando un producto o servicio, que se envía masiva y simultáneamente a un gran número de direcciones de correo electrónico, llenando los buzones de los destinatarios. El spam no hace referencia al correo comercial legítimo al que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

7.3.1. Principios de Anti-Spam

AVG Anti-Spam comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como spam. ***AVG 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 ***AVG Anti-Spam*** utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado. ***AVG 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*).

7.3.2. Interfaz de Anti-Spam



En el cuadro de diálogo del componente ***Anti-Spam*** encontrará una breve descripción acerca de su funcionalidad, información sobre su estado actual y las siguientes estadísticas:

- ***Publicación de la base de datos***: especifica la fecha y hora de actualización y publicación de la base de datos de spam
- ***Versión de Spamcatcher***: define el número de la última versión del motor anti-spam
- ***Correos electrónicos procesados***: especifica cuántos mensajes de correo electrónico se han analizado desde el último inicio del motor anti-spam
- ***Número de correos no deseados***: especifica cuántos de los mensajes de correo electrónico analizados se han marcado como spam
- ***Número de correos de phising***: especifica cuántos de los mensajes de correo electrónico analizados se han identificado como intentos de phishing

El cuadro de diálogo ***Anti-Spam*** también proporciona el vínculo ***Herramientas/Configuración avanzada***. Este vínculo conduce al entorno de configuración avanzada de todos los componentes de **AVG Internet Security 2011** .

Nota: *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.*

En la interfaz de este componente solamente hay un botón operativo disponible (***Atrás***). Pulse este

botón para volver a la interfaz de usuario de AVG predeterminada (*información general de los componentes*).

7.4. 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 algún 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 los equipos individuales de los ataques realizados por usuarios internos de otros equipos de la red.

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.*

7.4.1. Principios de Firewall

En AVG, el componente ***Firewall*** controla el tráfico en todos los puertos de red del equipo. Basándose en las reglas definidas, el ***Firewall*** evalúa las aplicaciones que se están ejecutando en el equipo (y que desean conectarse a Internet o a la red local) o las aplicaciones que intentan conectarse con el equipo desde el exterior. Para cada una de esas aplicaciones, el ***Firewall*** puede, entonces, permitir o impedir la comunicación en los puertos de la 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.

Nota: *AVG Firewall no ha sido diseñado para 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

7.4.2. 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)*. No es posible duplicar ni eliminar este perfil del sistema, ni tampoco puede modificarse su configuración.

- ***Bloquear todas***: un perfil de ***Firewall*** del sistema preconfigurado por el fabricante y que está siempre presente. Cuando se activa este perfil, se bloquean todas las comunicaciones de la red y no es posible acceder al equipo desde redes externas, ni tampoco el equipo puede iniciar comunicaciones hacia el exterior. No es posible duplicar ni eliminar este perfil del sistema, ni tampoco puede modificarse su configuración.

- ***Perfiles personalizados***:

    - ***Directamente conectado a Internet***: adecuado para los equipos domésticos de escritorio comunes que están conectados directamente a Internet o los portátiles que se conectan a Internet fuera del entorno seguro de la empresa. Seleccione esta opción si va a conectarse desde su hogar o si se encuentra en una pequeña red de empresa sin control central. Asimismo, seleccione esta opción cuando viaje y conecte su portátil desde sitios desconocidos y posiblemente peligrosos (*cibercafé, habitación de hotel, etc.*). Se crearán reglas más restrictivas, ya que se supone que estos equipos no tienen protección adicional y, por ello, requieren la máxima protección.

    - ***Equipo en un dominio***: adecuado para equipos conectados a una red local; por ejemplo, en una red corporativa o escolar. Se supone que la red está protegida por medidas adicionales, por lo que el nivel de seguridad puede ser inferior al utilizado para equipos independientes.

    - ***Pequeña red doméstica o de oficina***: adecuado para equipos que se conectan a una red de tamaño reducido, por ejemplo, en el hogar o en una empresa pequeña. Por lo general, se trata de varios equipos que se conectan entre sí, sin un administrador "central".

Cambio de perfil

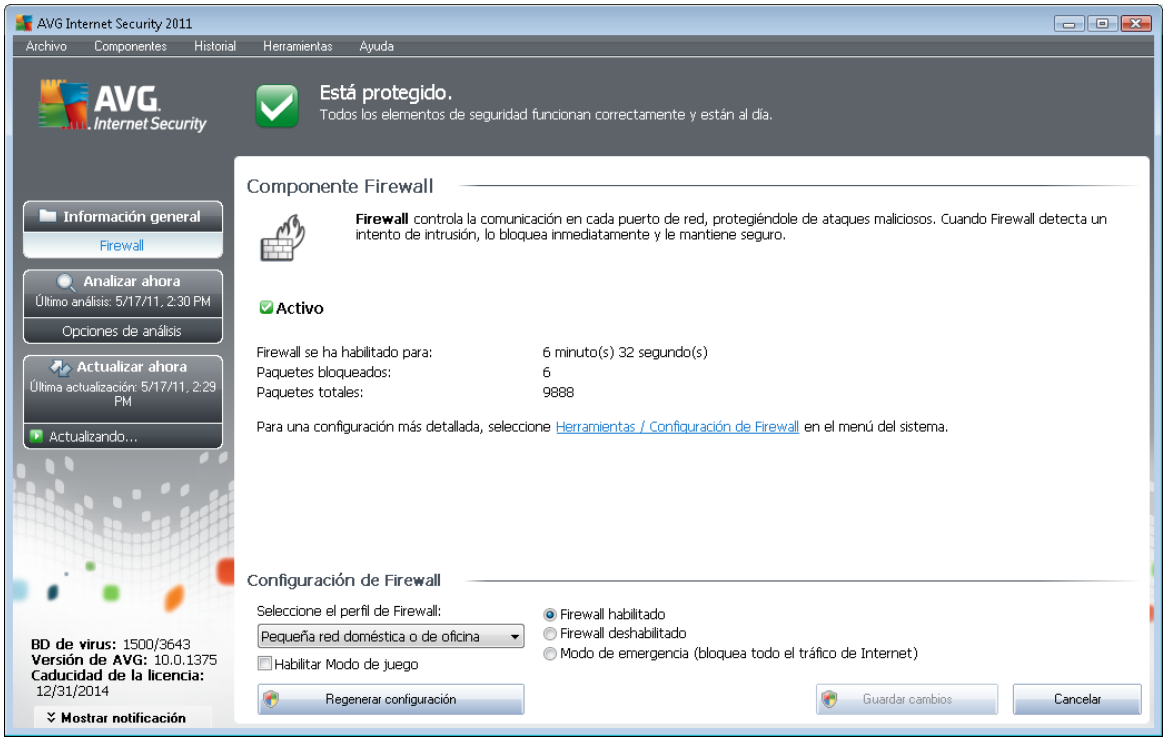
La característica de cambio de perfil permite que el ***Firewall*** cambie automáticamente al perfil

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.

7.4.3. Interfaz de Firewall



La interfaz de ***Firewall*** proporciona información básica sobre la funcionalidad del componente, su estado y una breve descripción de las estadísticas del ***Firewall***:

- ***Firewall se ha habilitado para***: 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 total de paquetes comprobados durante la ejecución del Firewall

Configuración de Firewall

- ***Seleccione el perfil de Firewall***: en el menú desplegable, seleccione uno de los perfiles definidos; siempre hay dos perfiles disponibles (los *perfiles predeterminados denominados* ***Permitir todas*** *y* ***Bloquear todas***) y otros se añadieron manualmente mediante la edición de perfiles en el cuadro de diálogo ***Perfiles*** de ***Configuración de Firewall***.

- ***Habilitar modo de 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.

- ***Estado de Firewall***:

  - ***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 ***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; ***Firewall*** se seguirá ejecutando, pero se detendrá todo el tráfico de red

Nota: *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 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 volver a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*)

7.5. LinkScanner

7.5.1. Principios de 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.

La tecnología de ***LinkScanner*** consta de dos características: ***Search-Shield*** y ***Surf-Shield***:

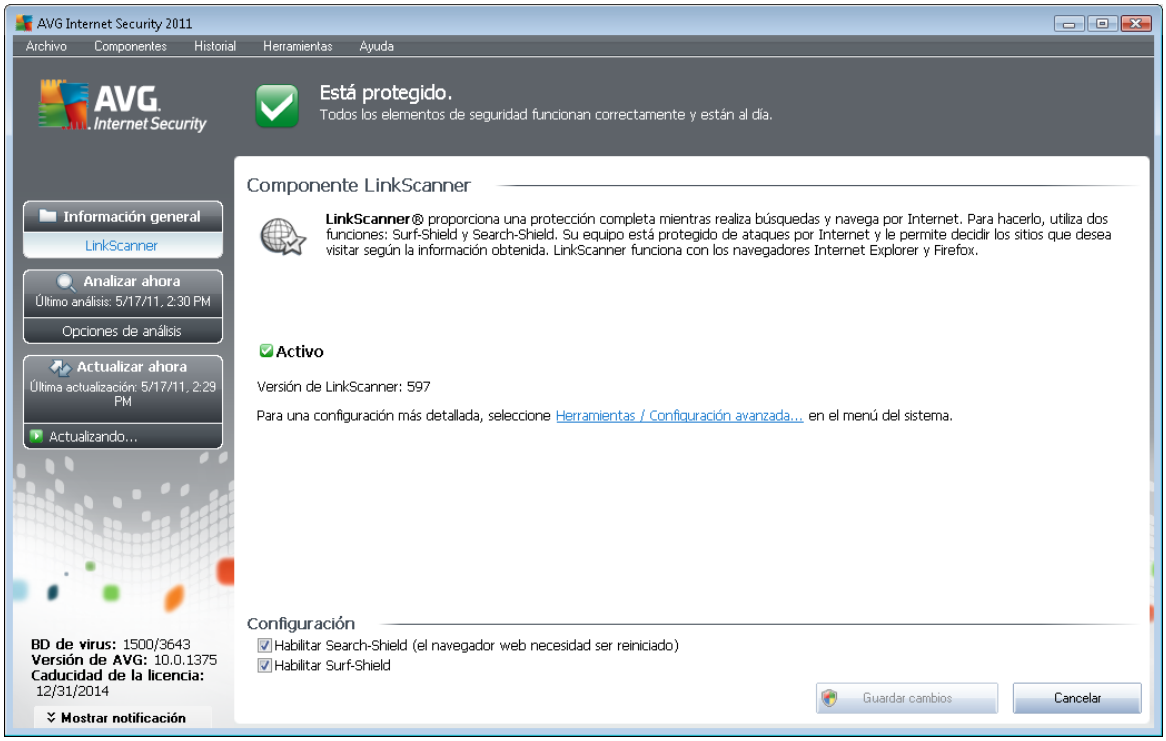
- ***Search-Shield*** contiene una lista de sitios web (*direcciones URL*) que se sabe que son peligrosos. Al realizar búsquedas con Google, Yahoo!, JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot, todos los resultados de la búsqueda se analizan según esta lista y se muestra un icono que indica lo determinado por el análisis (*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 con malware uno que estaba limpio*), ***Surf-Shield*** lo detectará y lo bloqueará cuando intente visitarlo.

Nota: *LinkScanner no ha sido diseñado para plataformas de servidor.*

7.5.2. Interfaz de LinkScanner

La interfaz del componente ***LinkScanner*** proporciona una breve descripción acerca de la funcionalidad del componente y su estado actual. También puede encontrar información sobre el último número de versión de la base de datos de ***LinkScanner*** (*versión de LinkScanner*).



Configuración de LinkScanner

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

- ***Habilite Search-Shield*** (*activado 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 o 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*).

7.5.3. 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, ***AVG 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 JP*).

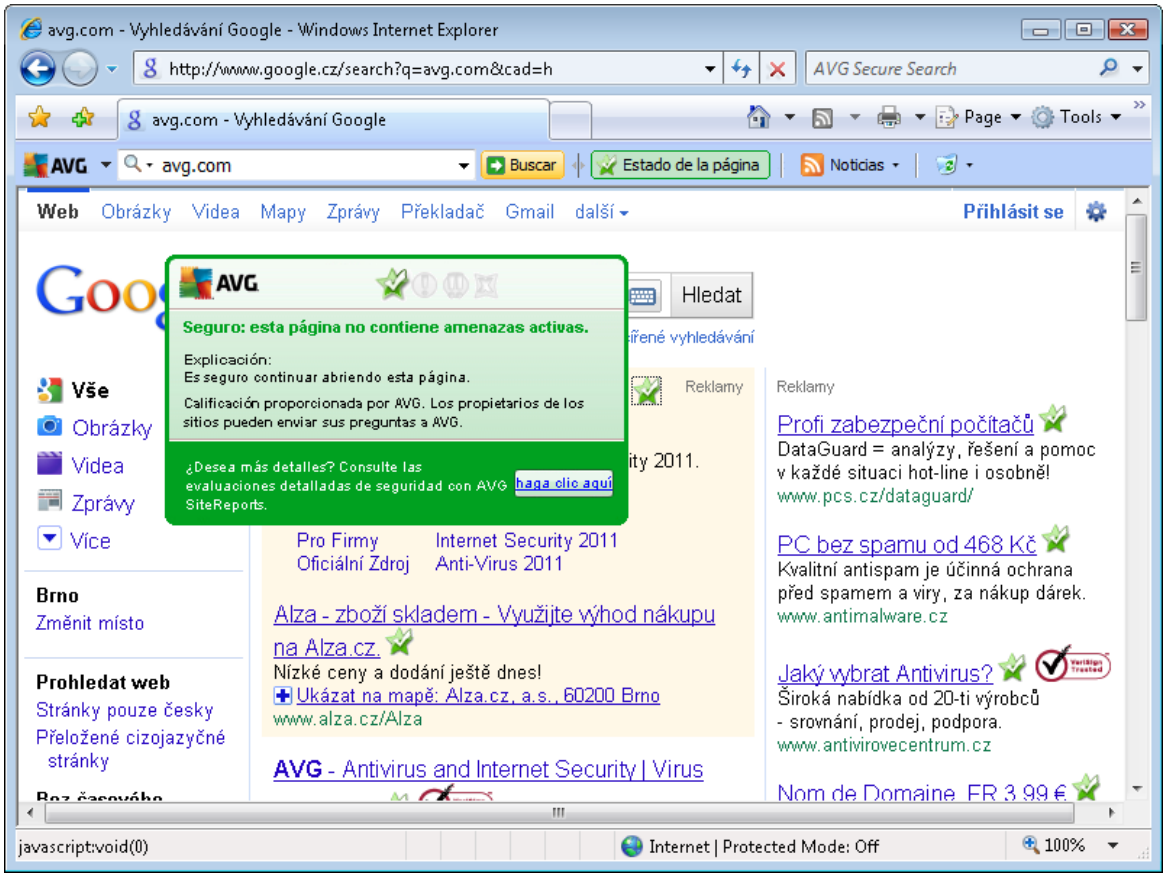
La página vinculada no contiene amenazas, pero es sospechosa (*dudosa por su origen o propósito, por lo que no se recomienda para compras en línea, etc.*).

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.

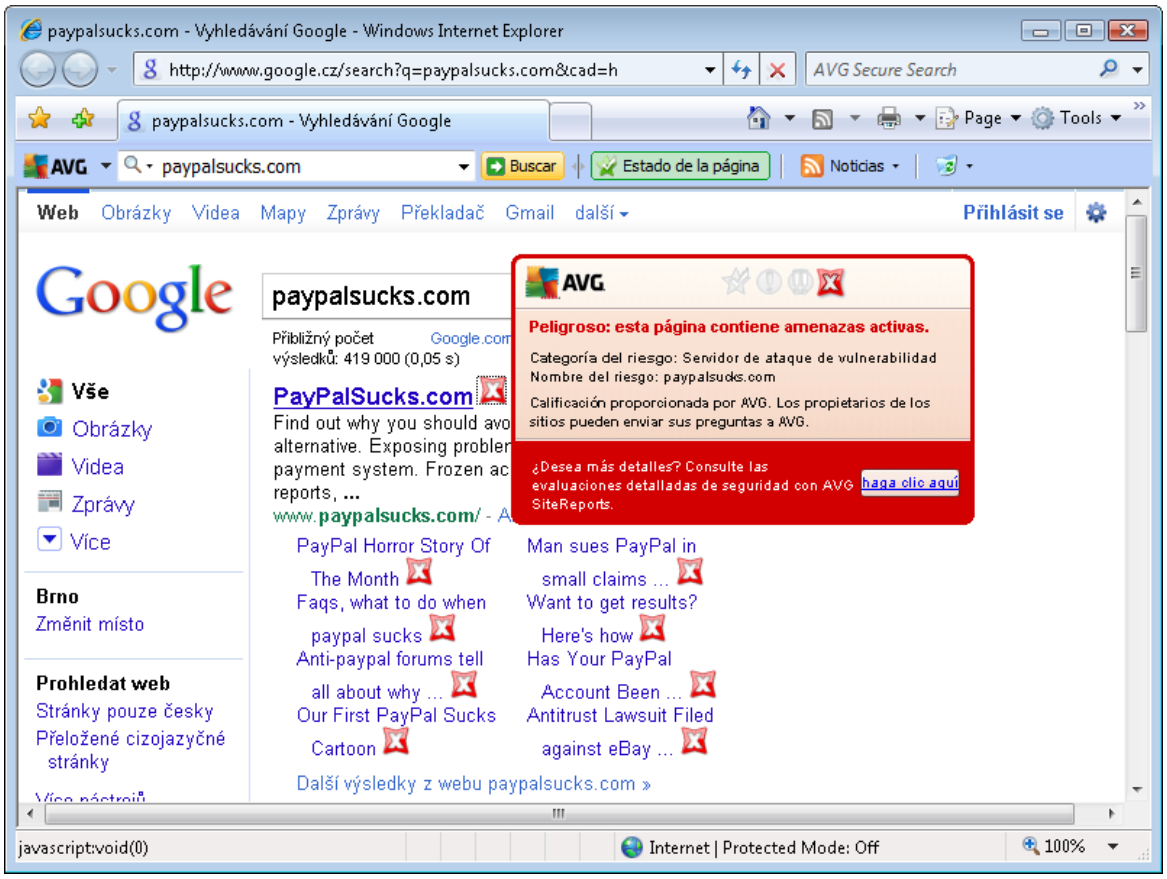
Al desplazar el puntero sobre un icono de calificación concreto, se mostrarán los detalles sobre el vínculo en cuestión. La información incluye detalles adicionales de la amenaza (*si los hubiera*):



7.5.4. 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, ***AVG LinkScanner*** no permitirá que el navegador la muestre.

Si se encuentra con un sitio web malicioso, ***AVG 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.

7.6. Protección residente

7.6.1. Principios de Protección residente

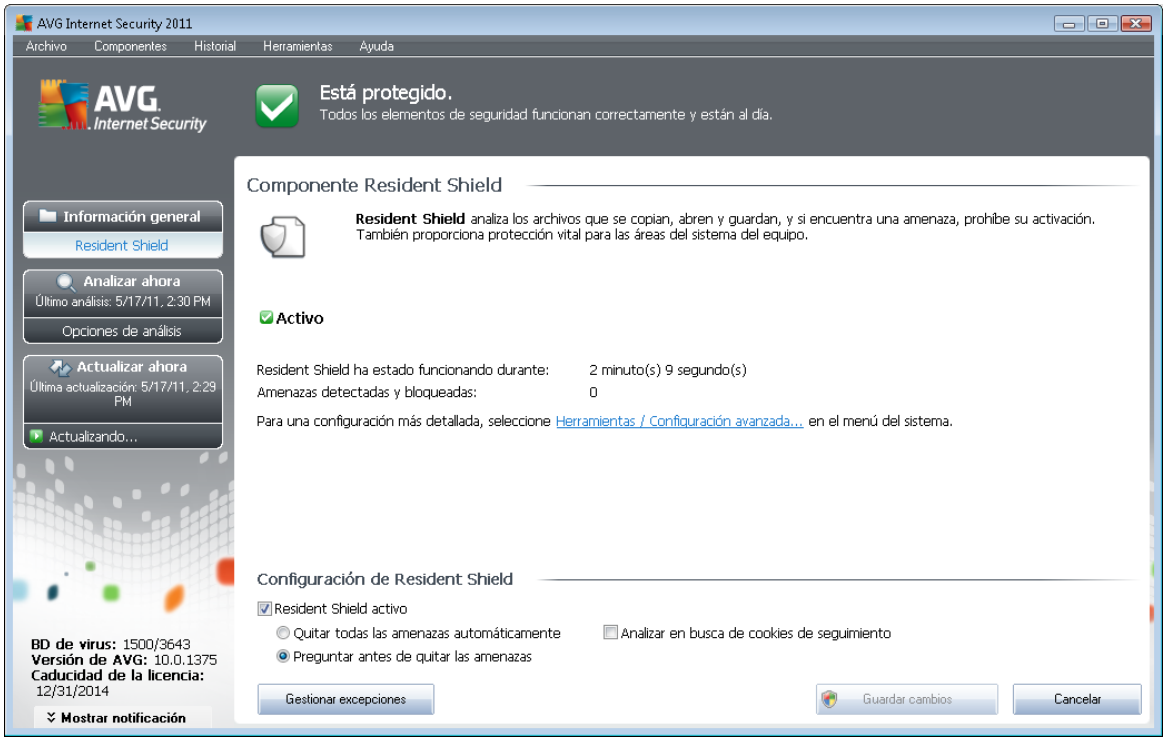
El componente ***Protección residente*** proporciona protección continua al equipo. Analiza todos los archivos que se abren, guardan o copian y protege las áreas del sistema del equipo. Cuando la ***Protección residente*** descubre un virus en un archivo al que se está accediendo, detiene la operación que se está ejecutando y no permite que el virus se active. Normalmente, no notará el proceso, ya que se ejecuta "en segundo plano" y solamente recibirá una notificación cuando se encuentren amenazas; al mismo tiempo, ***Protección residente*** bloquea la activación de la amenaza y la elimina. ***Protección residente*** se carga en la memoria del equipo durante el arranque del sistema.

Protección residente puede:

- Analizar en busca de tipos específicos de amenazas
- Analizar medios extraíbles (*discos flash, etc.*)
- Analizar archivos con extensiones específicas o sin ninguna extensión
- Permitir excepciones del análisis: archivos o carpetas específicas que nunca deben analizarse

Advertencia: Protección residente se carga en la memoria del equipo durante el arranque y es esencial mantenerlo habilitado permanentemente.

7.6.2. Interfaz de Protección residente



Además de presentar información general sobre las funciones de ***Protección residente*** y el estado

del componente, la interfaz de ***Protección residente*** ofrece también algunos datos estadísticos:

- ***Protección residente ha estado funcionando durante***: muestra el tiempo transcurrido desde la última vez que se inició el componente
- ***Amenazas detectadas y bloqueadas***: la cantidad de infecciones detectadas que Protección residente impidió que se ejecutaran o se abrieran (*en caso necesario, este valor se puede reiniciar, por ejemplo, con fines estadísticos: Restablecer valor*)

Configuración de Protección residente

En la parte inferior de la ventana de cuadro de diálogo encontrará la sección llamada ***Configuración de Protección residente***, donde podrá editar algunas opciones básicas de la configuración de las funciones del componente (*la configuración detallada, al igual que para todos los demás componentes, está disponible mediante el elemento Herramientas/Configuración avanzada del menú del sistema*).

La opción ***Protección residente está activo*** permite activar o desactivar fácilmente este componente. De manera predeterminada, esta función se encuentra activada. Con la protección residente activada, puede decidir de qué manera deben tratarse (eliminarse) las infecciones detectadas:

- de forma automática (***Quitar todas las amenazas automáticamente***)
- o sólo tras la aprobación del usuario (***Preguntar antes de quitar las amenazas***)

Esta elección no tiene ningún impacto en el nivel de seguridad y sólo refleja las preferencias del usuario.

En ambos casos, igualmente puede seleccionar si desea ***Analizar en busca de cookies de seguimiento***. En casos específicos puede activar esta opción para conseguir un nivel de seguridad máximo; sin embargo, está desactivada de manera predeterminada. (*cookies = 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 autenticar, rastrear y mantener información específica sobre los usuarios, como sus preferencias de Internet o el contenido de sus carros de compra electrónicos*).

Nota: 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 la interfaz de ***Protección residente*** son los siguientes:

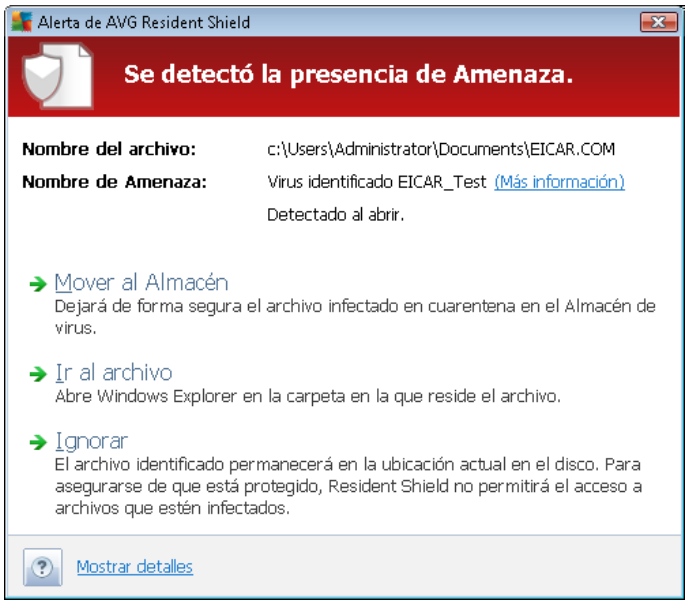
- ***Gestionar excepciones***: abre el cuadro de diálogo ***Protección residente - Elementos***

excluidos, donde puede definir los archivos o carpetas que deben dejarse fuera del análisis efectuado por la ***Protección residente***

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

7.6.3. Detección de Protección residente

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 ese momento. Las opciones disponibles son las siguientes:

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***

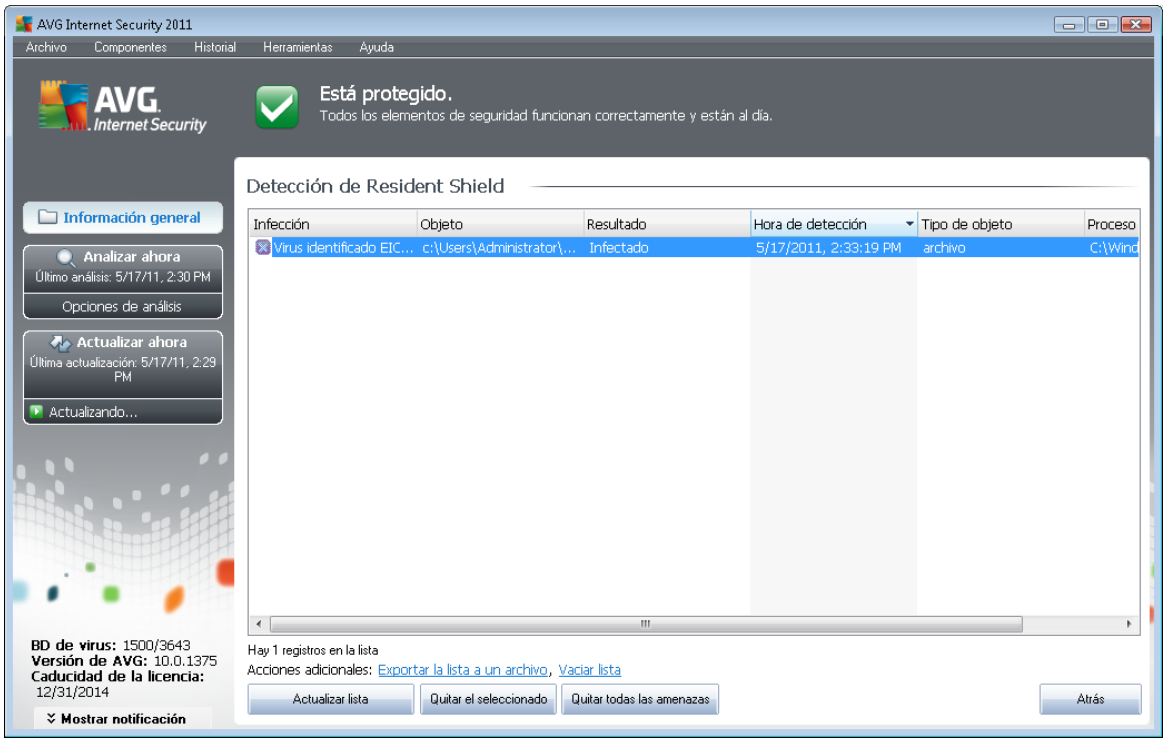
- ***Ir al archivo***: esta opción permite ir a la ubicación exacta donde se encuentra el objeto sospechoso (*abre una ventana nueva del Explorador de Windows*)

- ***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.

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 a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*).

7.7. Family Safety

AVG 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.

Este componente sólo está activo cuando se instala el producto ***AVG Family Safety*** en el equipo. Si el producto ***AVG Family Safety*** no está instalado, haga clic en el correspondiente icono en la interfaz de usuario de **AVG Internet Security 2011,** que le redigirá al sitio web del producto donde encontrará toda la información necesaria.

7.8. AVG LiveKive

AVG 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.

Este componente sólo está activo cuando se instala el producto ***AVG LiveKive*** en el equipo. Si el producto ***AVG LiveKive*** no está instalado, haga clic en el correspondiente icono en la interfaz de usuario de **AVG Internet Security 2011,** que le redigirá al sitio web del producto donde encontrará toda la información necesaria.

7.9. Analizador de 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.

7.9.1. Principios de 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*).

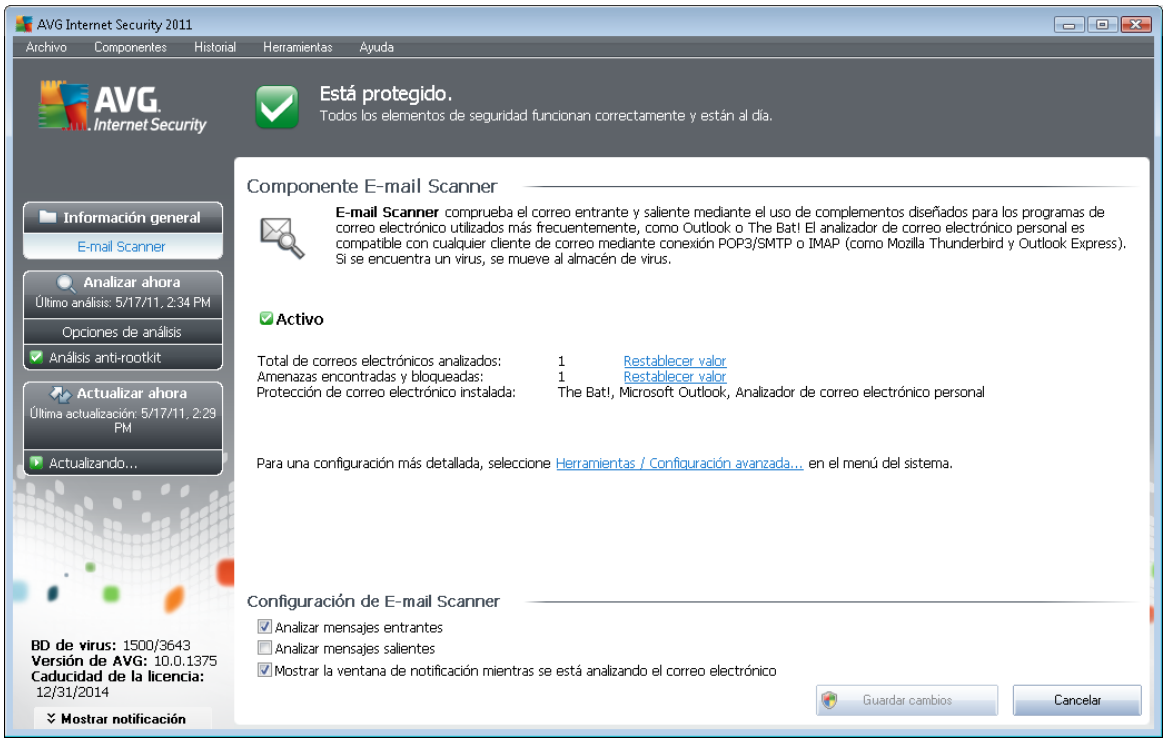
El ***Analizador de correo electrónico*** funciona como una interfaz entre el cliente de correo electrónico y los servidores de correo electrónico en Internet.

- ***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*).

Nota: *el Analizador de correo electrónico AVG no ha sido diseñado para plataformas de servidor.*

7.9.2. Interfaz de Analizador de correo electrónico



En el cuadro de diálogo del componente ***Analizador de correo electrónico*** encontrará un breve texto que describe la funcionalidad del mismo y ofrece información sobre su estado actual y las siguientes estadísticas:

- ***Total de correos electrónicos analizados***: cuántos mensajes de correo electrónico se han analizado desde la última vez que se inició el ***Analizador de correo electrónico*** (*en caso necesario, este valor se puede reiniciar, por ejemplo con fines estadísticos, con la opción Restablecer valor*)
- ***Amenazas encontradas y bloqueadas***: proporciona el número de infecciones detectadas en mensajes de correo electrónico desde la última vez que se inició el ***Analizador de correo electrónico***
- ***Protección de correo electrónico instalada***: información sobre un determinado complemento de protección de correo electrónico relativo a su cliente de correo instalado de manera predeterminada

Configuración del Analizador de correo electrónico

En la parte inferior del cuadro de diálogo encontrará la sección denominada ***Configuración del Analizador de correo electrónico***, donde puede editar algunas características elementales de la funcionalidad del componente:

- ***Analizar mensajes entrantes***: active este elemento para especificar que todos los correos

electrónicos entregados en su cuenta deben analizarse en busca de virus. De manera predeterminada, este elemento está activado y se recomienda no modificar esta configuración.

- ***Analizar mensajes salientes***: active este elemento para confirmar que todo el correo electrónico enviado desde su cuenta debe analizarse en busca de virus. De manera predeterminada, este elemento está desactivado.

- ***Mostrar la ventana de notificación mientras se está analizando el correo electrónico***: active este elemento para confirmar que desea ser informado mediante un cuadro de diálogo de notificación que se muestra sobre el icono de AVG en la bandeja del sistema durante el análisis de su correo realizado por el componente ***Analizador de correo electrónico***. De manera predeterminada, este elemento está activado y se recomienda no modificar esta configuración.

A la configuración avanzada del componente ***Analizador de correo electrónico*** se accede a través del elemento del menú del sistema ***Herramientas/Configuración avanzada***; no obstante, la configuración avanzada sólo está recomendada para usuarios experimentados.

Nota: *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.*

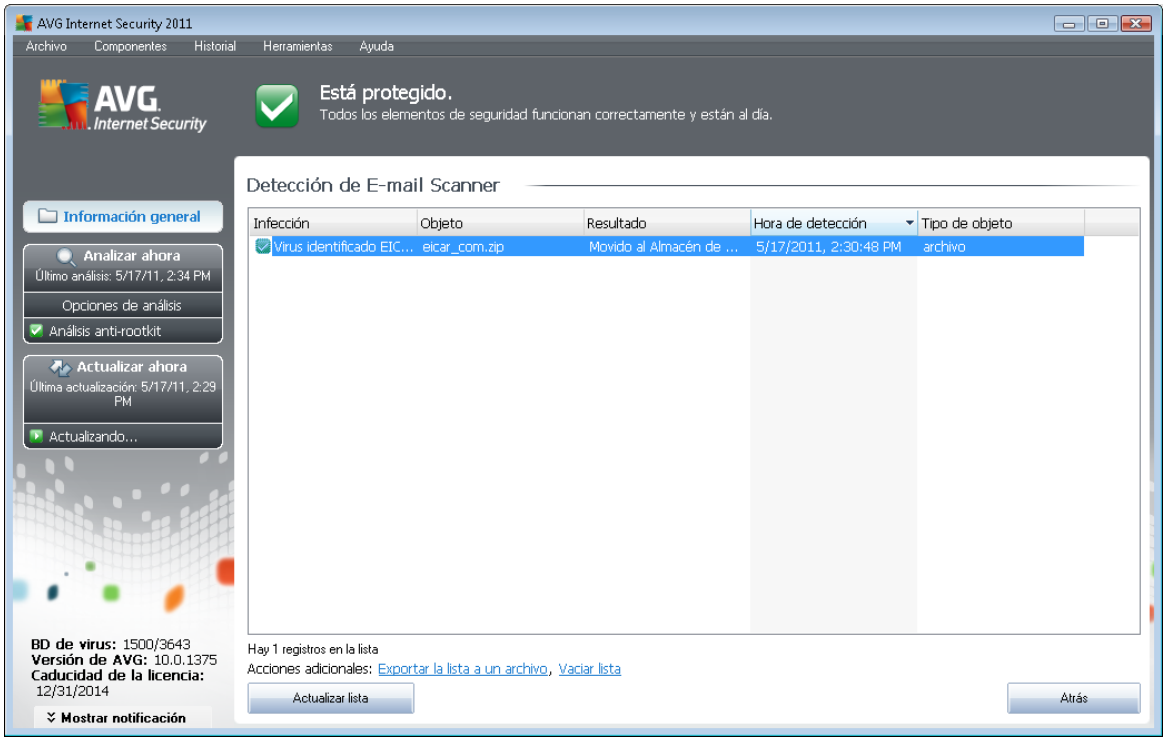
Botones de control

Los botones de control disponibles en la interfaz de ***Analizador de 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 volver a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*)

7.9.3. Detección de Analizador de correo electrónico



En el cuadro de diálogo ***Detección de Analizador de correo electrónico*** (*al que se accede a través de la opción del menú del sistema Historial / Detección de Analizador de correo electrónico*), podrá ver una lista de todos los resultados detectados por el componente ***Analizador de 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 anterior

7.10. Administrador de actualizaciones

7.10.1. Principios de Administrador de actualizaciones

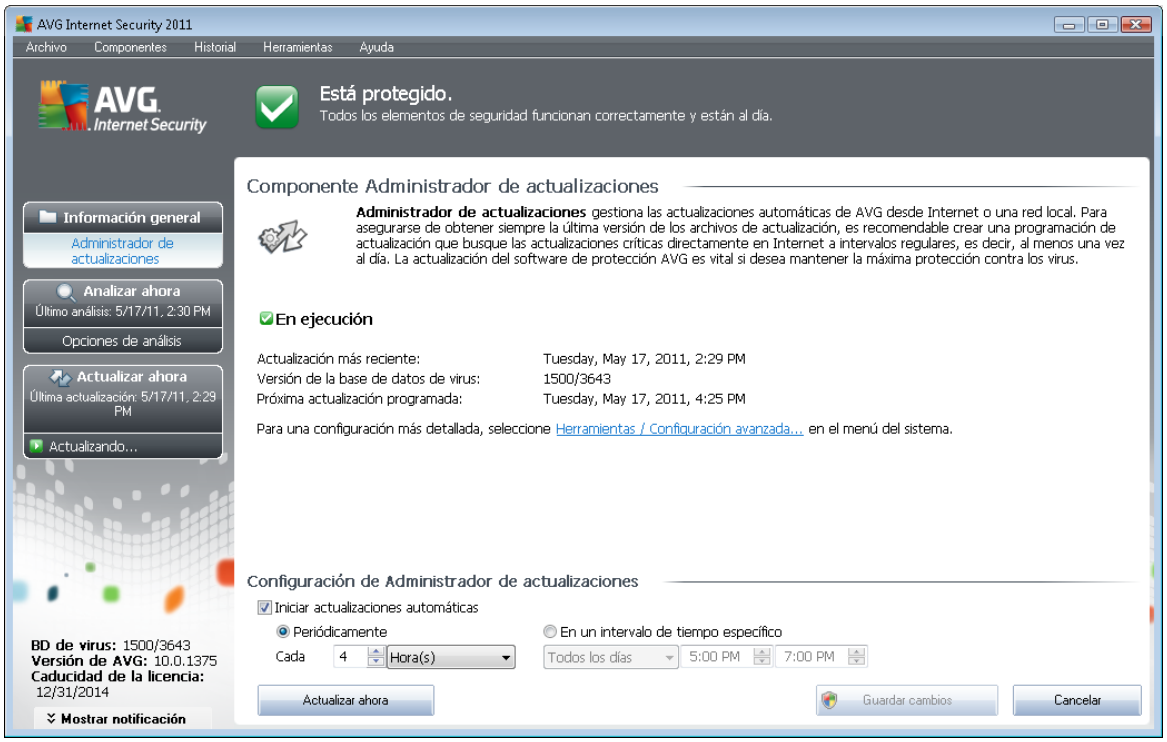
Ningún software de seguridad puede garantizar una verdadera protección contra los diversos tipos de amenazas a menos que se actualice regularmente. Los creadores de virus están siempre a la búsqueda de nuevos fallos que puedan aprovechar tanto del software como de los sistemas operativos. Cada día aparecen 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.

Es crucial actualizar regularmente la instalación de AVG.

El ***Administrador de actualizaciones*** ayuda en el control de las actualizaciones regulares. Con este componente puede programar descargas automáticas de archivos de actualización, ya sea desde Internet o desde la red local. Las actualizaciones de las definiciones de virus esenciales deben ser diarias si es posible. Las actualizaciones del programa menos urgentes pueden hacerse semanalmente.

Nota: *consulte el capítulo Actualizaciones de AVG si desea obtener más información sobre los tipos y niveles de actualización.*

7.10.2. Interfaz de Administrador de actualizaciones



La interfaz de ***Administrador de actualizaciones*** muestra información de la funcionalidad del componente, su estado actual y algunos datos estadísticos relevantes:

- ***Actualización más reciente***: especifica la fecha y hora de actualización más reciente de la base de datos
- ***Versión de la base de datos de virus***: define el número de versión de la base de datos de virus instalada actualmente, que se incrementa con cada actualización de la base de datos de virus
- ***Próxima actualización programada***: especifica la fecha y hora de la próxima actualización de la base de datos

Configuración del Administrador de actualizaciones

En la parte inferior del cuadro de diálogo se encuentra la sección ***Configuración del Administrador de actualizaciones***, donde puede realizar algunas modificaciones de las reglas del proceso de inicio de las actualizaciones. Es posible definir si desea que se descarguen automáticamente los archivos de actualización (Iniciar actualizaciones automáticas***) o bajo demanda. La opción*** Iniciar actualizaciones automáticas ***está activada de forma predeterminada, y se recomienda mantenerla así. La descarga de los archivos de actualización más recientes a intervalos regulares es crucial para el correcto funcionamiento de cualquier software de seguridad.***

A continuación, es posible definir la frecuencia a la que deberá iniciarse la actualización:

- ***Periódicamente***: defina el intervalo de tiempo
- ***En un intervalo de tiempo específico***: defina la hora exacta en la que se iniciará la actualización

De forma predeterminada, la actualización está configuración para realizarse cada cuatro horas. Se recomienda encarecidamente mantener está configuración a menos que tenga un buen motivo para modificarla.

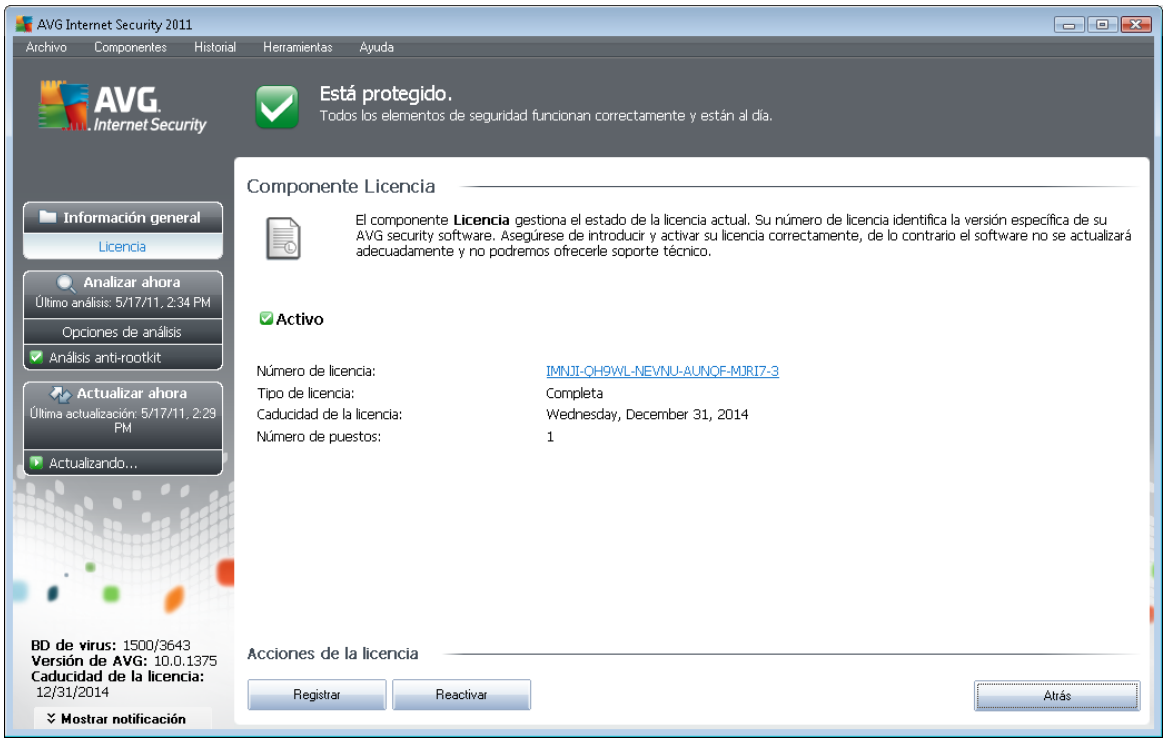
Nota: el *proveedor del software ha configurado todos los componentes de AVG para ofrecer un rendimiento óptimo. A menos que tenga un buen motivo para hacerlo, no modifique la configuración de AVG. Cualquier cambio de configuración debe realizarlo únicamente un usuario experimentado. Si necesita cambiar 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 la interfaz del ***Administrador de actualizaciones*** son los siguientes:

- ***Actualizar ahora***: inicia una actualización inmediata bajo demanda
- ***Guardar cambios***: pulse este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo
- ***Cancelar***: pulse este botón para volver a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*)

7.11. Licencia



En la interfaz del componente ***Licencia***, encontrará una breve descripción acerca de la funcionalidad del componente, su estado actual y la siguiente información:

- ***Número de licencia***: proporciona la forma abreviada del número de licencia (*por razones de seguridad, los últimos cuatro símbolos no se muestran*). El número de licencia debe escribirse con absoluta precisión, exactamente como figura. Por lo tanto, recomendamos encarecidamente que utilice siempre el método "copiar y pegar" para realizar cualquier manipulación con el número de licencia.

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

- ***Caducidad de la licencia***: esta fecha determina el período de validez de la licencia. Si desea continuar utilizando **AVG Internet Security 2011** después de esta fecha, deberá renovar la licencia. La renovación de la licencia puede realizarse en línea en el sitio web de AVG.

- ***Número de puestos***: la cantidad de estaciones de trabajo en las que se le permite instalar **AVG Internet Security 2011**.

Botones de control

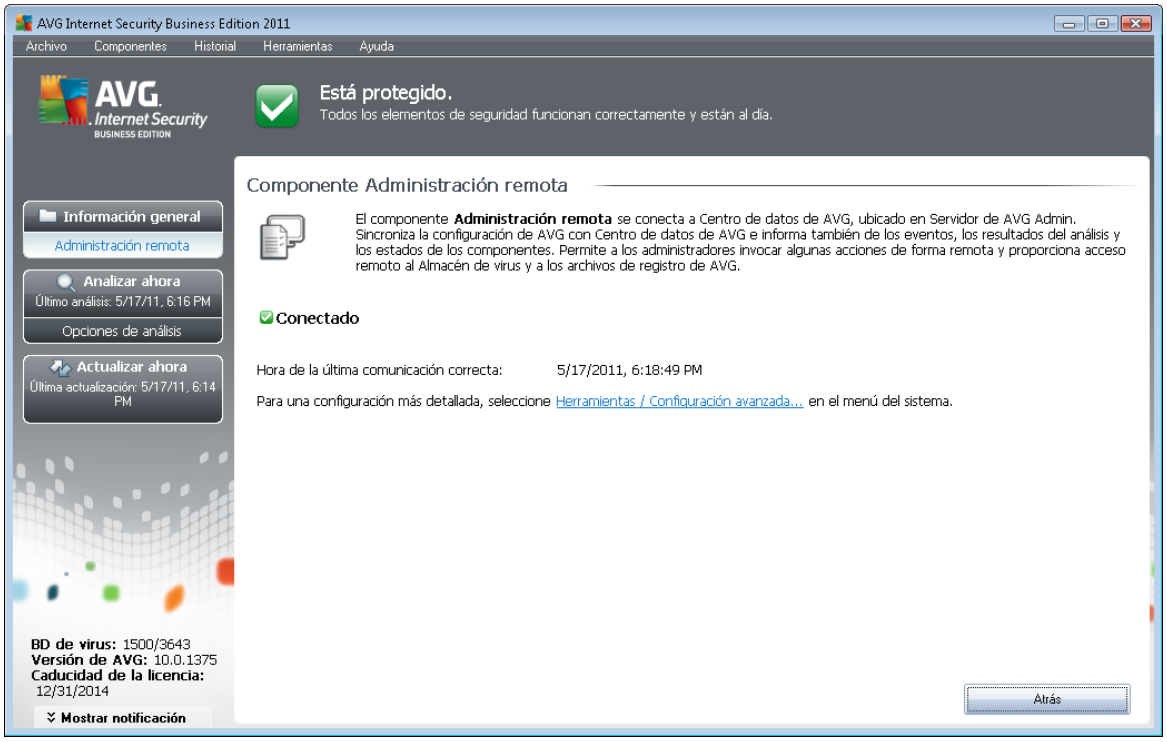
- ***Registrar***: conecta con la página de registro del sitio web de AVG (http://www.avg.com/). Introduzca sus datos de registro; solamente los clientes que registran su producto AVG pueden recibir soporte técnico gratuito.

- ***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*).

Nota: *si utiliza la versión de prueba de* **AVG Internet Security 2011**, *los botones aparecen como* ***Comprar ahora*** *y* ***Activar*** *y le permiten adquirir de inmediato la versión completa del programa. Si* **AVG Internet Security 2011** *se ha instalado con un número de venta, los botones que se muestran serán* ***Registrar*** *y* ***Activar***.

- ***Atrás***: pulse este botón para volver a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*).

7.12. Administración remota



El componente ***Administración remota*** sólo se muestra en la interfaz de usuario de **AVG Internet Security 2011** si instaló la edición Business del producto (*consulte el componente* ***Licencia***). En el cuadro de diálogo ***Administración remota*** podrá ver si el componente se encuentra 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. Puede descargar tal documentación del sitio web de AVG (www.avg.com), en la sección ***Centro de soporte / Descargas / Documentación***.

Botones de control

- ***Atrás***: pulse este botón para volver a la interfaz de usuario de AVG predeterminada (*información general de los componentes*).

7.13. Online Shield

7.13.1. Principios de Online Shield

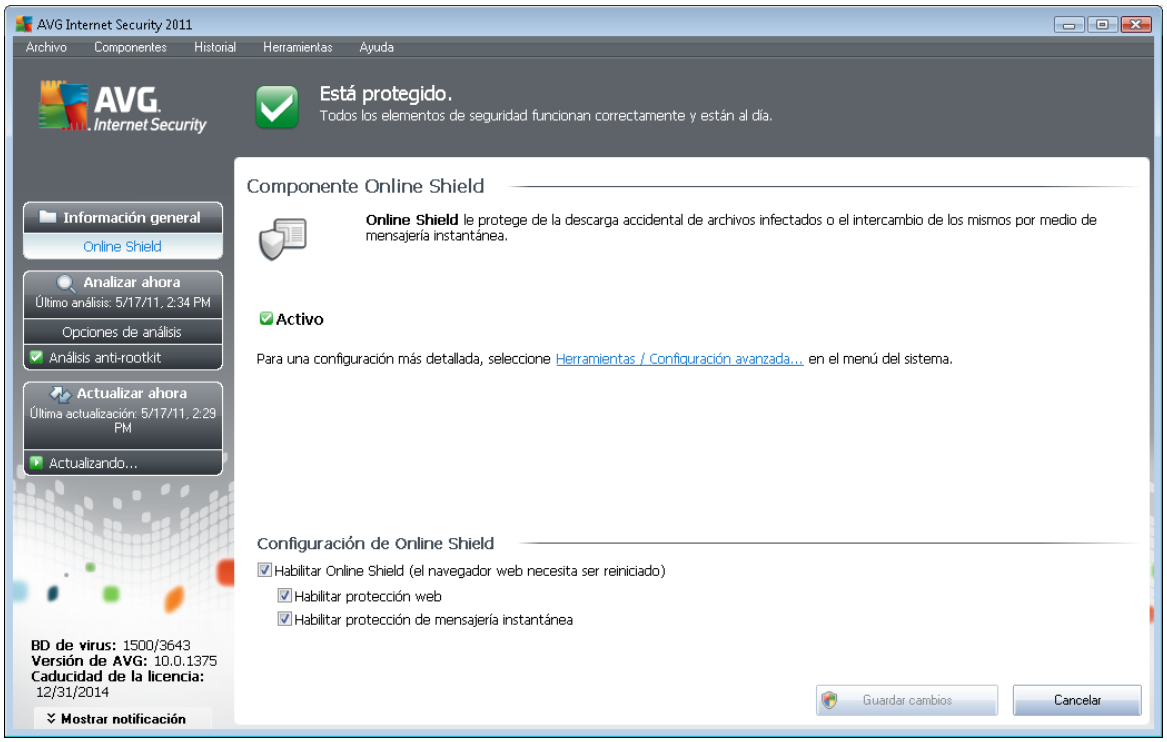
Online Shield es un tipo de protección residente en tiempo real; analiza el contenido de las páginas web visitadas (*y los posibles archivos incluidos en ellas*) antes incluso de que aparezcan en el navegador web o se descarguen en el equipo.

Online Shield detecta que la página que se dispone a visitar incluye algún javascript peligroso e impide que ésta se abra. Asimismo, reconoce el malware contenido en una página y detiene inmediatamente su descarga para que no entre en el equipo.

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

7.13.2. Interfaz de Online Shield

La interfaz del componente ***Online Shield*** describe el comportamiento de este tipo de protección. Además, es posible encontrar información del estado actual del componente. En la parte inferior del cuadro de diálogo se incluyen las opciones de edición básicas de la funcionalidad del componente:



Configuración de Online Shield

En primer lugar, existe la opción de activar o desactivar ***Online Shield*** inmediatamente marcando el elemento ***Habilitar Online Shield***. Esta opción está habilitada de forma predeterminada, estando activo el componente ***Online Shield***. A menos que tenga un buen motivo para modificar esta configuración, se recomienda mantener el componente activo. Si el elemento está marcado y ***Online Shield*** se está ejecutando, se activan otras dos opciones de configuración:

- ***Habilitar protección web***: esta opción confirma que ***Online Shield*** llevará a cabo el análisis del contenido de las páginas web.
- ***Habilitar protección de mensajería instantánea***: marque este elemento si desea que ***Online Shield*** verifique que las comunicaciones de mensajería instantánea (*por ejemplo, ICQ, MSN Messenger, etc.*) no contienen virus.

Nota: 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.*

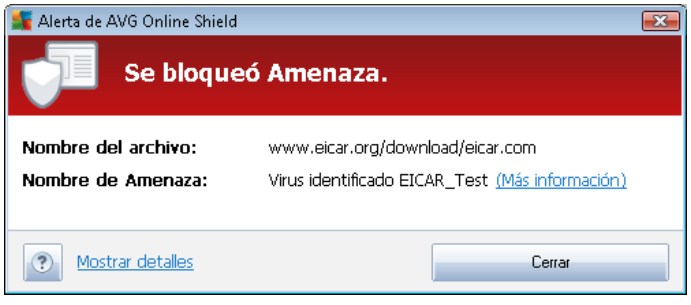
Botones de control

Los botones de control disponibles en la interfaz de ***Online Shield*** 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 volver a la ***interfaz de usuario de AVG predeterminada*** (*información general de los componentes*)

7.13.3. Detección 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:



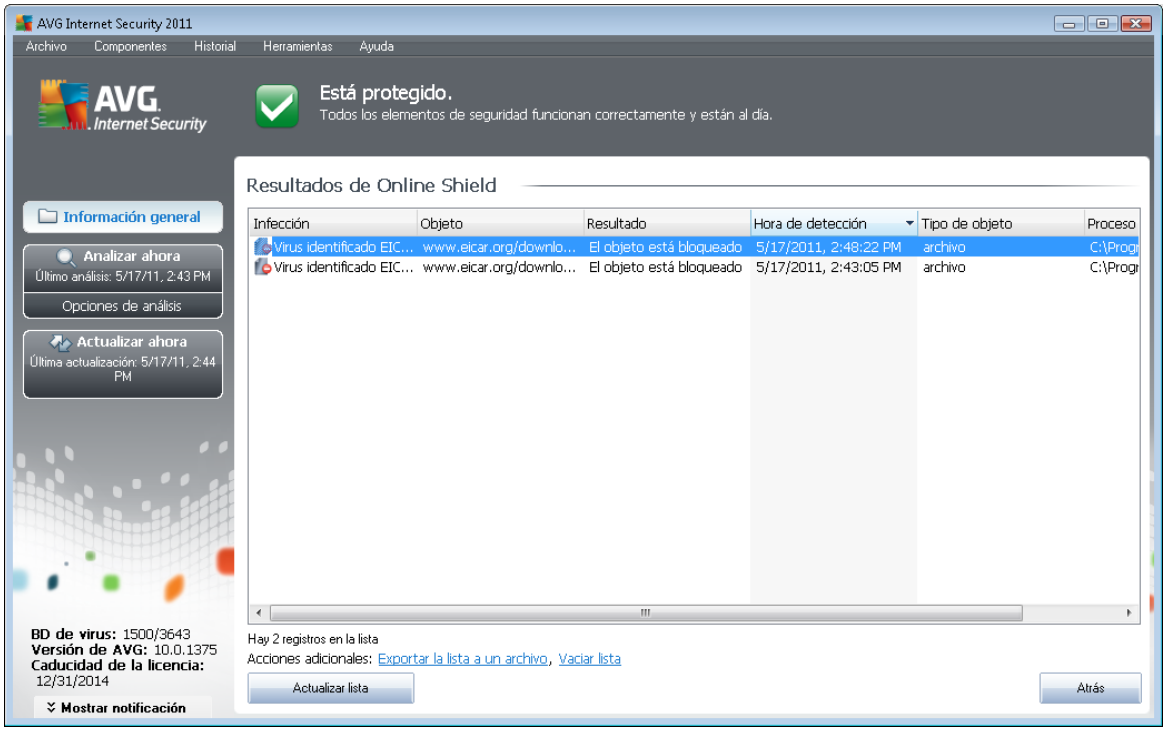
En este cuadro de diálogo de advertencia, encontrará datos sobre el archivo detectado y marcado

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***). El botón ***Actualizar lista*** actualizará la lista de objetos detectados por ***Online Shield***. El botón ***Atrás*** le devuelve a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*).

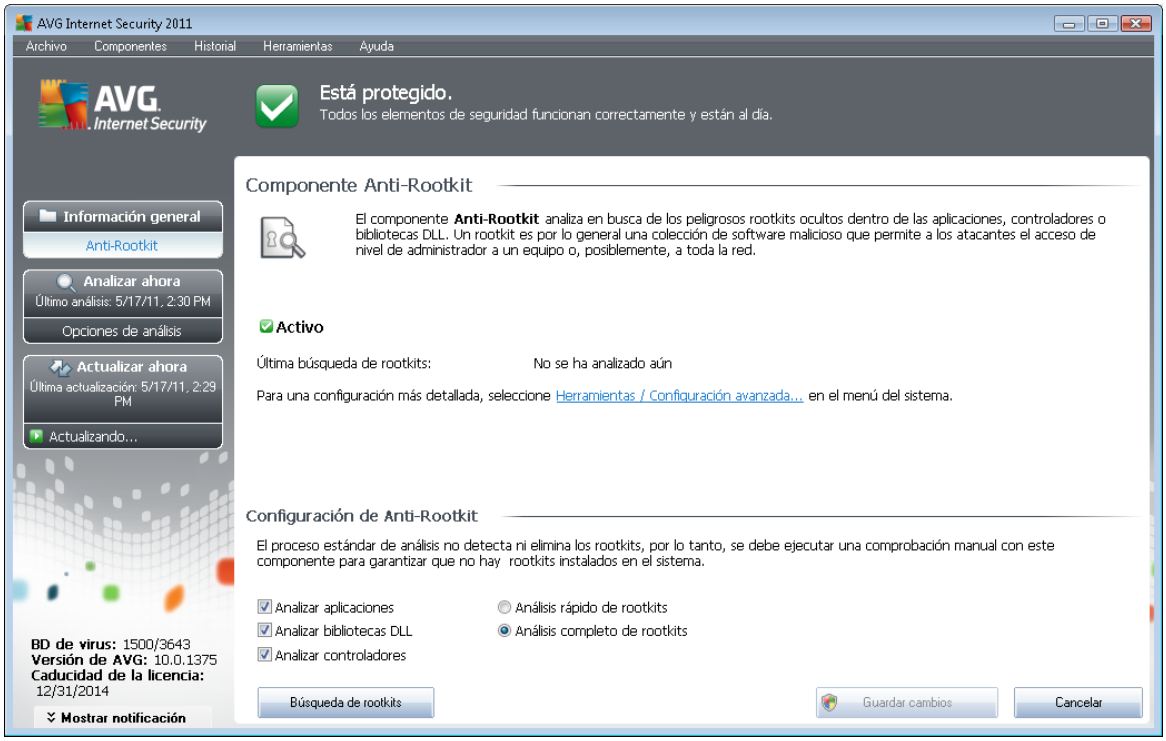
7.14. Anti-Rootkit

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.

7.14.1. Principios de Anti-Rootkit

AVG 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. ***AVG 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 ***AVG 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.

7.14.2. Interfaz de Anti-Rootkit



La interfaz del usuario de ***Anti-Rootkit*** proporciona una breve descripción de la funcionalidad del componente, informa sobre su estado actual 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***.

Nota: *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 de Anti-Rootkit

En la parte inferior del cuadro de diálogo encontrará la sección ***Configuración de Anti-Rootkit***, donde 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 (*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*)

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 a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*)
- ***Cancelar***: pulse este botón para volver a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*) sin guardar los cambios realizados

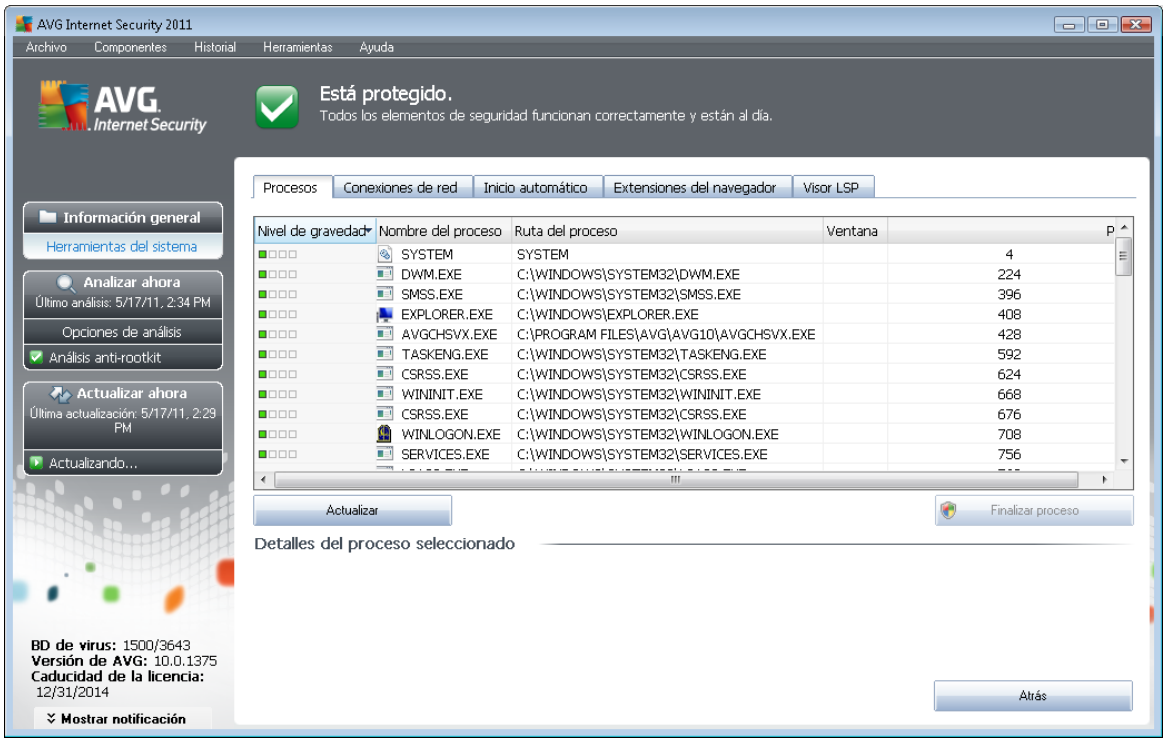
7.15. Herramientas del sistema

Herramientas del sistema se refiere a las herramientas que ofrecen un resumen detallado del entorno de **AVG Internet Security 2011** 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.

7.15.1. 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

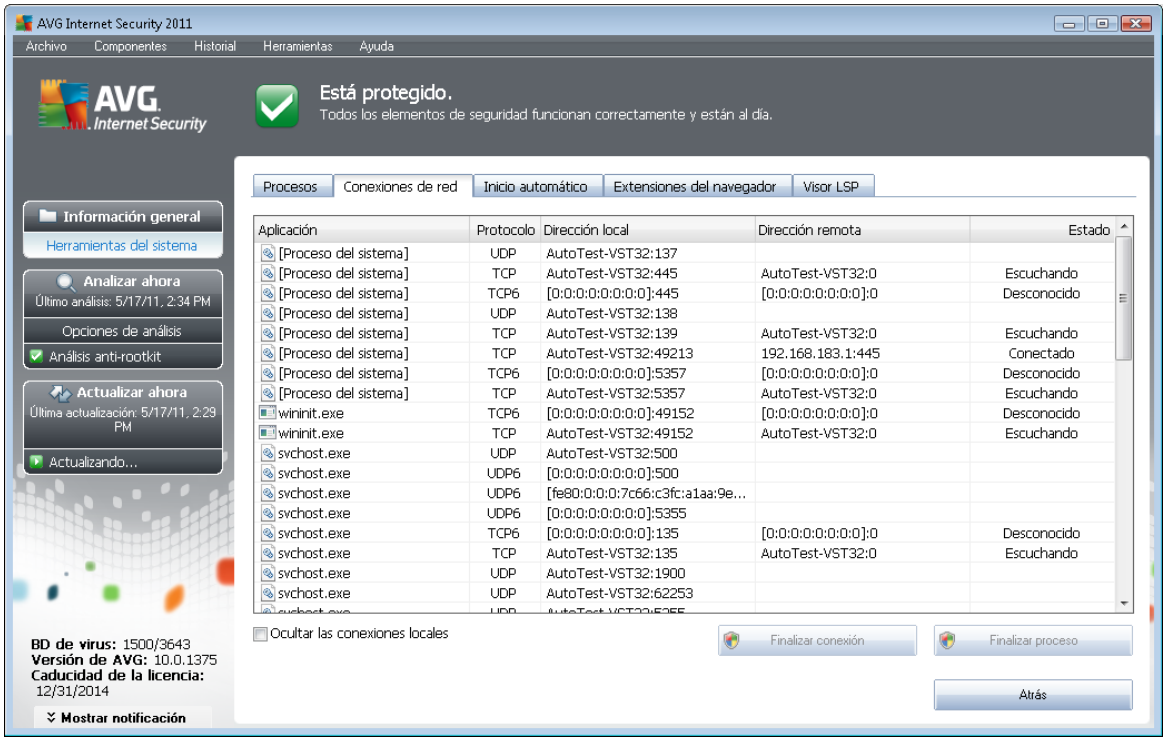
Botones de control

Los botones de control disponibles dentro de la interfaz de ***Herramientas del sistema*** 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 a la interfaz de usuario de AVG predeterminada (*información general de los componentes*)

7.15.2. 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.

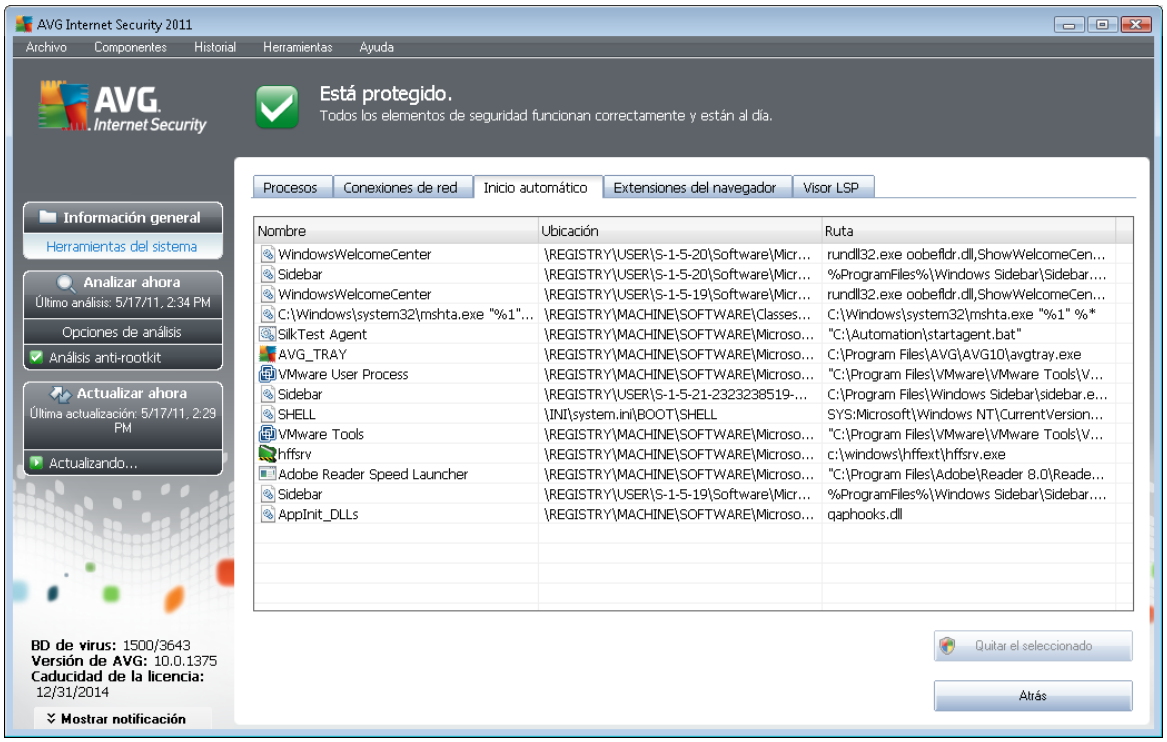
Botones de control

Los botones de control disponibles 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 a la interfaz de usuario de AVG ***predeterminada*** (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.

7.15.3. Inicio automático



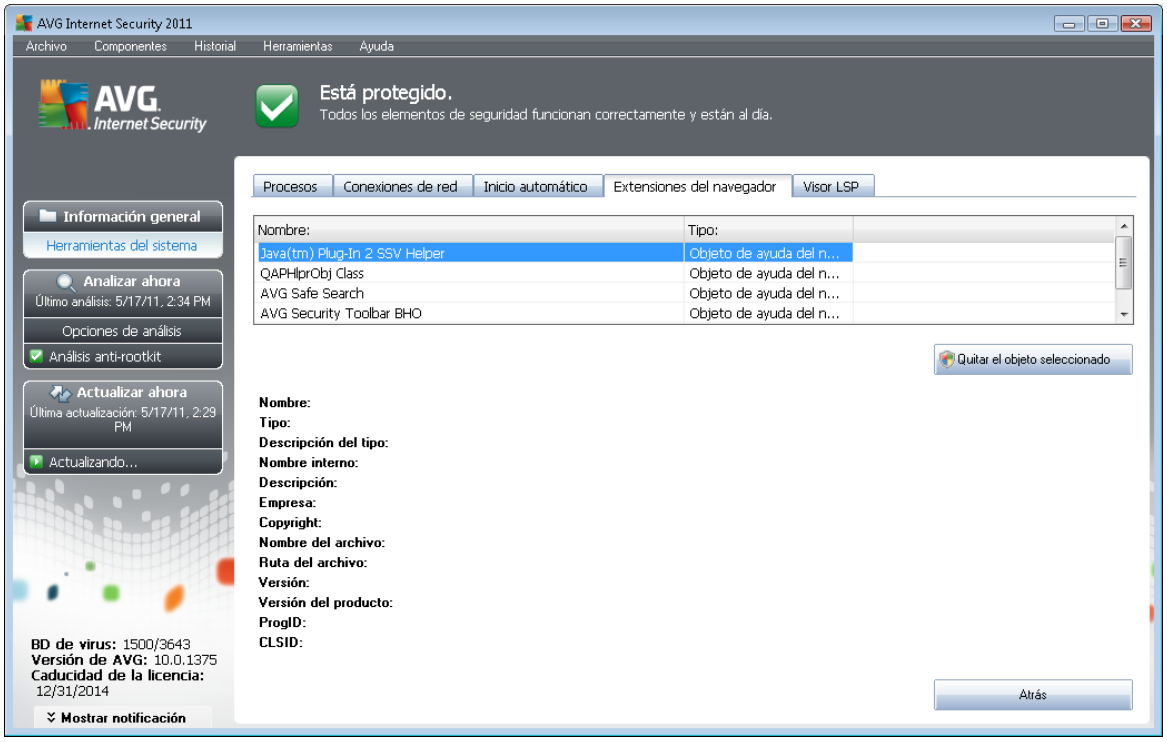
El cuadro de diálogo ***Inicio automático*** muestra una lista de todas las aplicaciones que se ejecutan en el inicio del sistema Windows. Muy a menudo, varias aplicaciones de malware se agregan automáticamente a la entrada de inicio del Registro.

Puede eliminar una o más entradas seleccionándolas y pulsando el botón ***Quitar el seleccionado***.

El botón ***Atrás*** le devuelve a la interfaz de usuario de AVG predeterminada (*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.

7.15.4. 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.

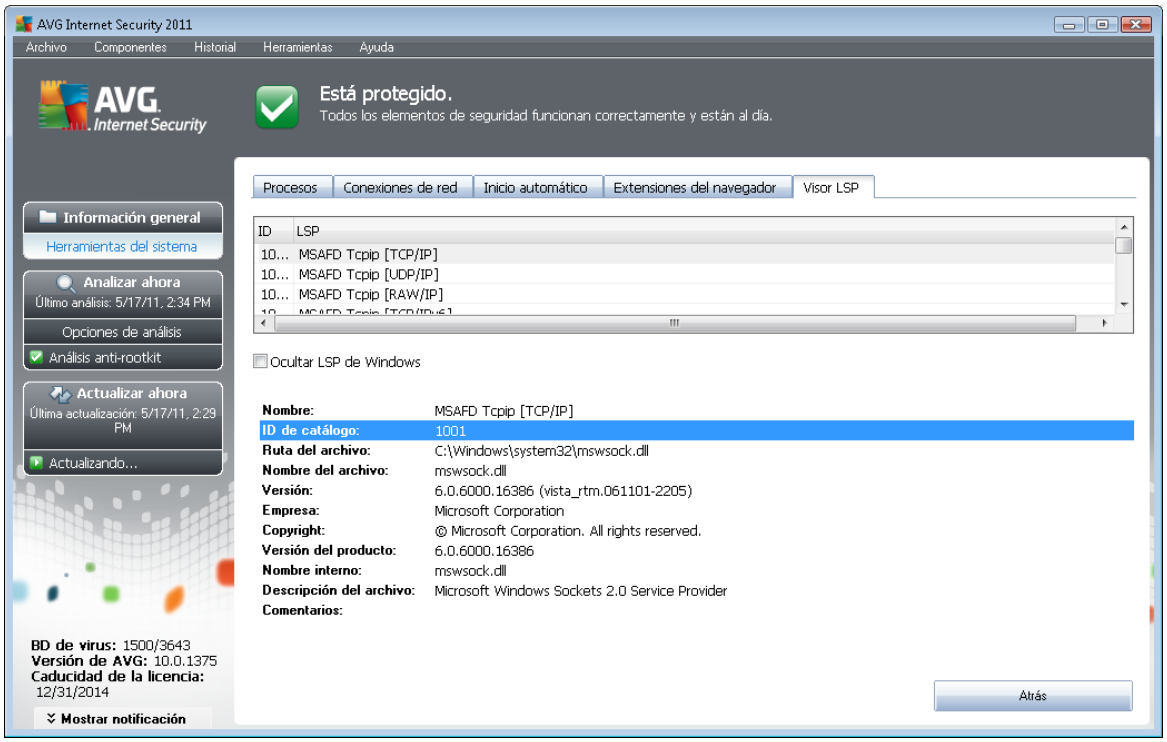
Botones de control

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 a la interfaz de usuario de***AVG*** predeterminada (información general de los componentes)

7.15.5. Visor LSP



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

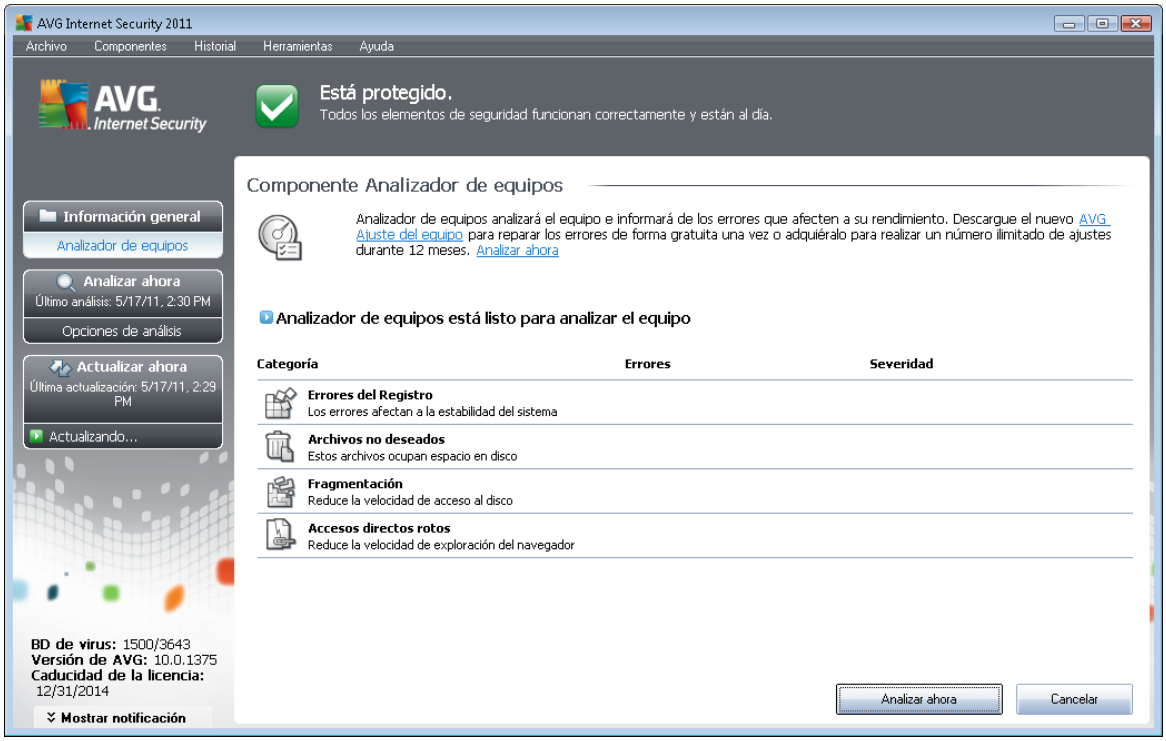
Un ***proveedor de servicios por capas*** (LSP) es un controlador del sistema vinculado a los servicios de red del sistema operativo Windows. Tiene acceso a todos los datos que entran y salen del equipo y puede, además, modificar dichos datos. Algunos LSP son necesarios para que Windows pueda conectarle 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.

Para incluir LSP de Windows en la lista, desactive la casilla ***Ocultar LSP de Windows***. El botón ***Atrás*** le devuelve a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*).

7.16. 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:



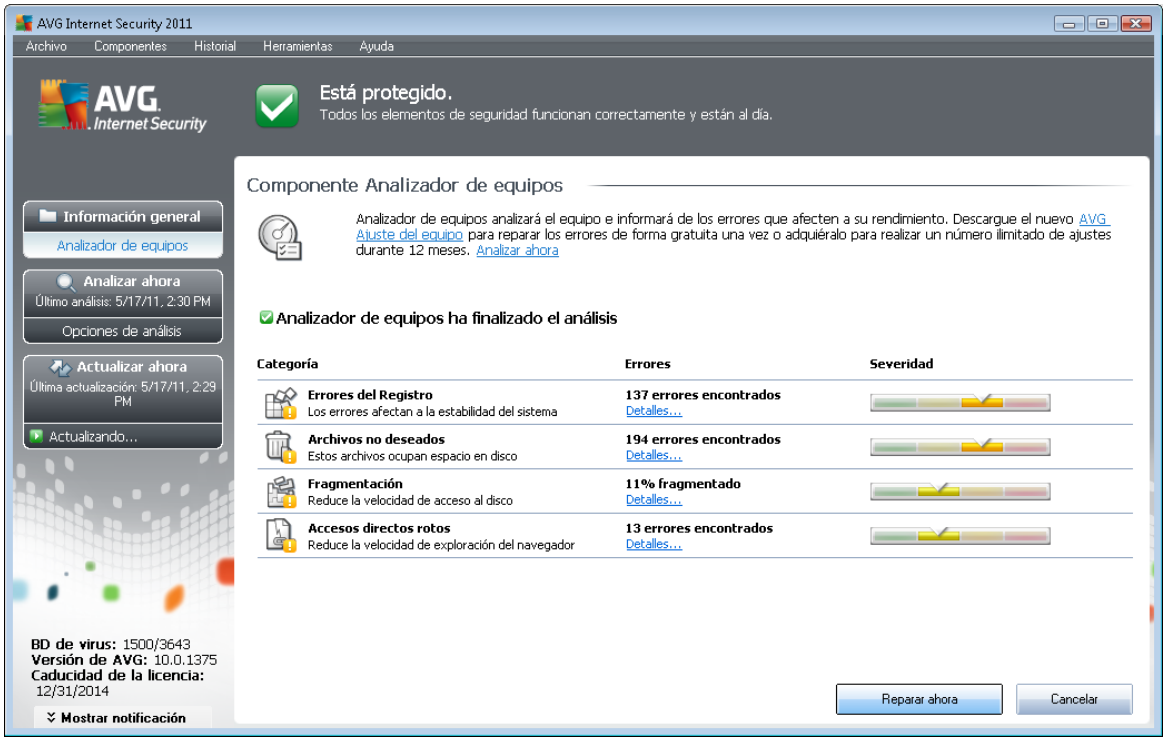
- ***Errores del Registro*** le dará la cantidad de errores que hay en el Registro de Windows. Dado que para corregir el Registro se requieren conocimientos bastante avanzados, no es recomendable intentar solucionar los errores por uno mismo.

- ***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 ir 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 a la interfaz de usuario de AVG predeterminada (*información general de los componentes*) una vez finalizado el análisis

7.17. Identity Protection

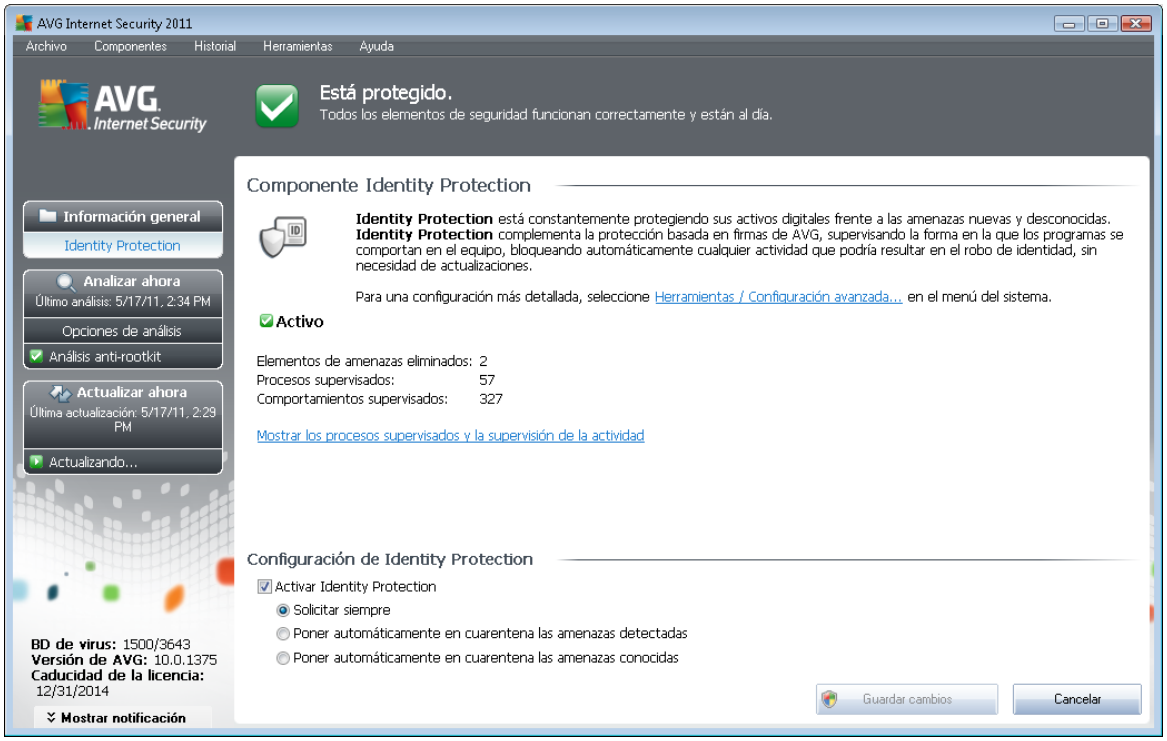
AVG Identity Protection es un producto anti-malware cuya finalidad es impedir que los ladrones de identidad roben sus contraseñas, los detalles de su cuenta bancaria, sus números de tarjetas de crédito y otros valiosos elementos digitales personales, y protegerlos de todo tipo de software malicioso (*malware*) que ataque a su equipo. Se asegura de que todos los programas que se ejecutan en el equipo funcionan correctamente. ***AVG Identity Protection*** detecta y bloquea constantemente los comportamientos sospechosos y protege el equipo frente a todo el malware nuevo.

7.17.1. Principios de Identity Protection

AVG 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. Teniendo en cuenta que el malware es cada vez más sofisticado y adopta la forma de programas normales que permiten al atacante remoto abrir el equipo para robar su identidad, ***AVG Identity Protection*** le protege de este nuevo malware basado en la ejecución. Es un complemento de ***AVG Anti-Virus*** que le protege frente a los virus basados en archivos y los virus conocidos utilizando el mecanismo de firma y el análisis.

Recomendamos encarecidamente instalar tanto AVG Anti-Virus como AVG Identity Protection para obtener una protección completa del equipo.

7.17.2. Interfaz de Identity Protection



La interfaz de ***Identity Protection*** proporciona una breve descripción de la funcionalidad del componente, su estado y algunos datos estadísticos:

- ***Elementos de malware eliminados***: indica el número de aplicaciones detectadas como malware y eliminadas
- ***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 de Identity Protection

En la parte inferior del cuadro de diálogo, encontrará la sección ***Configuración de Identity Protection***, donde 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

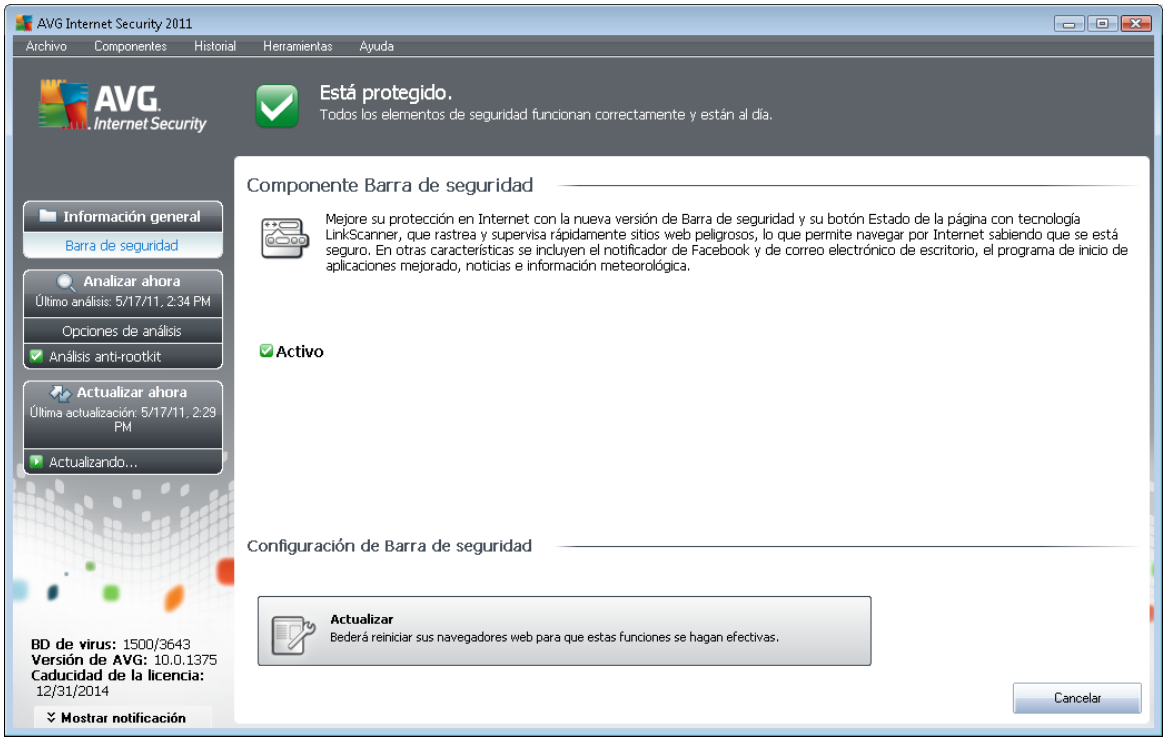
Botones de control

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 este botón para volver a la ***interfaz de usuario de AVG*** predeterminada (*información general de los componentes*)

7.18. Security Toolbar

Security Toolbar es una barra de herramientas del navegador web opcional que ofrece protección AVG mejorada y acceso a diversas características y herramientas mientras se navega por Internet. Actualmente, ***Security Toolbar*** es compatible con los navegadores web Internet Explorer (*versión 6.0 o superior*) y Mozilla Firefox *(versión 3.0 o superior*):



Toda la configuración del componente ***Security Toolbar*** es accesible directamente mediante ***Security Toolbar*** en el navegador web.

8. AVG Security Toolbar

AVG Security Toolbar es una nueva herramienta que funciona junto con el componente ***LinkScanner*** . La ***barra de herramientas AVG Security Toolbar*** se puede usar para controlar las funciones de ***LinkScanner*** y para ajustar su comportamiento.

Si selecciona instalar la barra de herramientas durante la instalación de **AVG Internet Security 2011**, se añadirá a su navegador web (*Internet Explorer 6.0 o superior y Mozilla Firefox 3.0 o superior*) de forma automática. Por el momento, no es compatible con otros navegadores de Internet.

Nota: *en caso de que utilice algún navegador de Internet diferente (p. ej. Avant Browser) puede encontrarse con un comportamiento inesperado.*

8.1. Interfaz de AVG Security Toolbar

La ***barra de herramientas AVG Security Toolbar*** está diseñada para funcionar con ***MS Internet Explorer*** (*versión 6.0 o superior*) y ***Mozilla Firefox*** (*versión 3.0 o superior*). Si decidió instalar ***AVG Security Toolbar*** (*durante el proceso de instalación de AVG, se le preguntó si deseaba o no instalar este componente*), el componente estará ubicado en el navegador web, justo debajo de la barra de dirección:

La ***barra de herramientas AVG Security Toolbar*** consta de lo siguiente:

8.1.1. Botón de logotipo de AVG

Este botón proporciona acceso a los elementos de la barra de herramientas general. Haga clic en el botón de logotipo para ser redirigido al sitio web de AVG. Si hace clic en el puntero situado junto al icono de AVG, se abrirá lo siguiente:

- ***Información de la barra de herramientas***: vínculo a la página principal de la ***barra de herramientas AVG Security Toolbar*** con información detallada sobre la protección de dicha barra de herramientas
- ***Ejecutar AVG***: abre la ***interfaz de usuario***
- ***Información de AVG***: abre un menú contextual con una serie de vínculos que llevan a información importante de seguridad relacionada con **AVG Internet Security 2011**:
  - *Acerca de las amenazas*: abre el sitio web de AVG en la página que proporciona los datos más importantes sobre las mayores amenazas, recomendaciones para la eliminación de virus, información sobre las actualizaciones de AVG, acceso a la base de datos de virus y otra información relevante
  - *Noticias AVG*: abre la página web que proporciona los últimos comunicados de prensa sobre AVG

- *Nivel actual de amenaza*: abre la página web del laboratorio de virus con una representación gráfica del nivel actual de la amenaza en Internet

- *Laboratorios de amenazas de AVG*: abre el sitio web de AVG Site Reports, donde puede buscar amenazas específicas por su nombre y obtener información detallada sobre cada una de ellas

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

- ***Eliminar historial***: permite eliminar desde la ***barra de herramientas AVG Security Toolbar*** el historial completo, o bien borrar por separado el historial de búsqueda, el historial de descargas y las cookies.

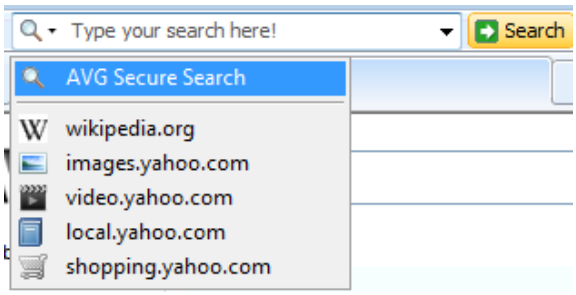
- ***Actualizar***: busca nuevas actualizaciones de la ***barra de herramientas de AVG Security Toolbar***

- ***Ayuda***: proporciona opciones para abrir el archivo de ayuda, contactar con el soporte técnico de AVG, enviar sus comentarios sobre el producto o ver los detalles de la versión actual de la barra de herramientas

8.1.2. Cuadro de búsqueda con tecnología de AVG Secure Search (powered by Google)

El cuadro ***AVG Secure Search (powered by Google)*** es una manera sencilla y segura de hacer búsquedas en la web utilizando AVG Secure Search (powered by Google). Escriba una palabra o frase en el cuadro de búsqueda y pulse el botón Buscar ***o la tecla*** Intro ***para iniciar la búsqueda directamente en el servidor*** AVG Secure Search (powered by Google), independientemente de la página mostrada en ese momento. El cuadro de búsqueda también muestra el historial de búsquedas. Las búsquedas hechas a través de este cuadro se analizan utilizando la protección de ***Search-Shield***.

Como alternativa, en el campo de búsqueda se puede cambiar a Wikipedia o a algún otro servicio específico de búsqueda; consulte la imagen:



8.1.3. Estado de la página

Ubicado directamente en la barra de herramientas, este botón muestra la evaluación de la página web actualmente en pantalla según los criterios establecidos en el componente ***Surf-Shield***:

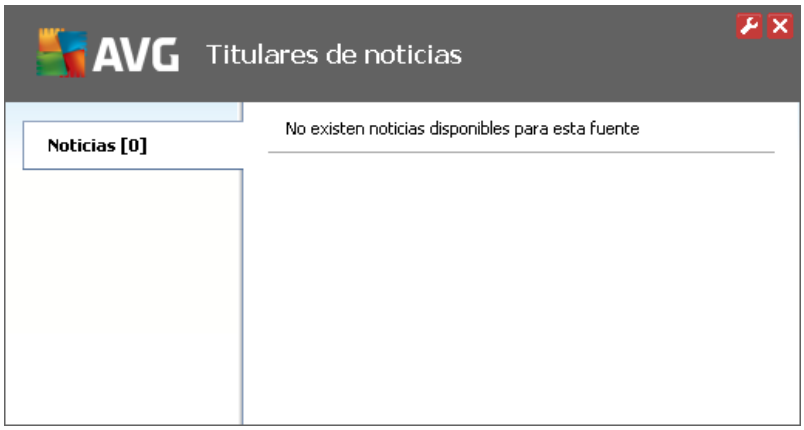
- - La página vinculada es segura

-  - La página es un tanto sospechosa.
-  - La página contiene vínculos a páginas verdaderamente peligrosas.
-  - 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.

Haga clic en el botón para abrir un panel de información con datos detallados sobre la página web específica.

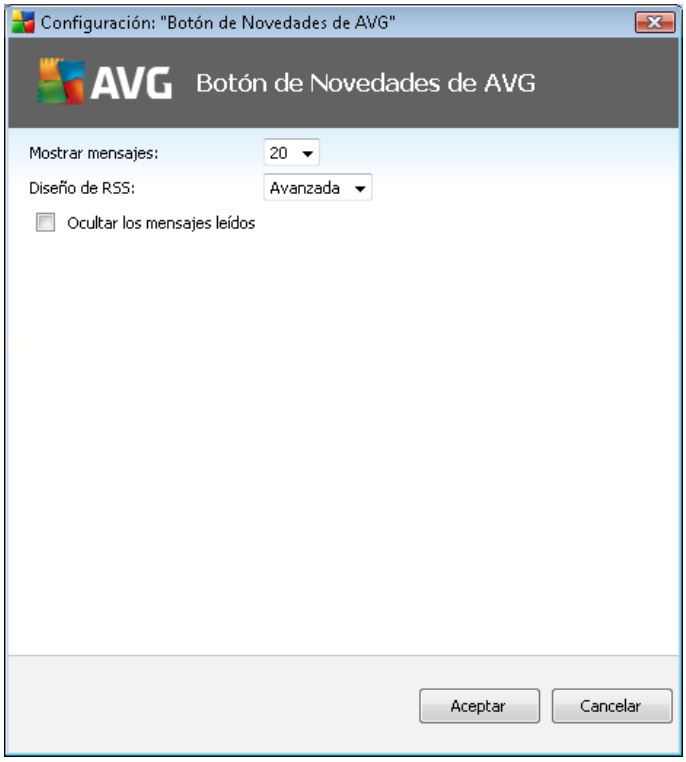
8.1.4. Noticias AVG

Situado directamente en la ***barra de herramientas AVG Security Toolbar***, este botón abre una vista de los últimos ***titulares de noticias*** relacionados con AVG, tanto noticias de prensa como comunicados de la empresa.



En la esquina superior derecha verá dos botones de control de color rojo:

-  : este botón abre el cuadro de diálogo de edición, donde puede especificar los parámetros del botón ***Noticias AVG*** mostrado en la ***barra de herramientas AVG Security Toolbar***:

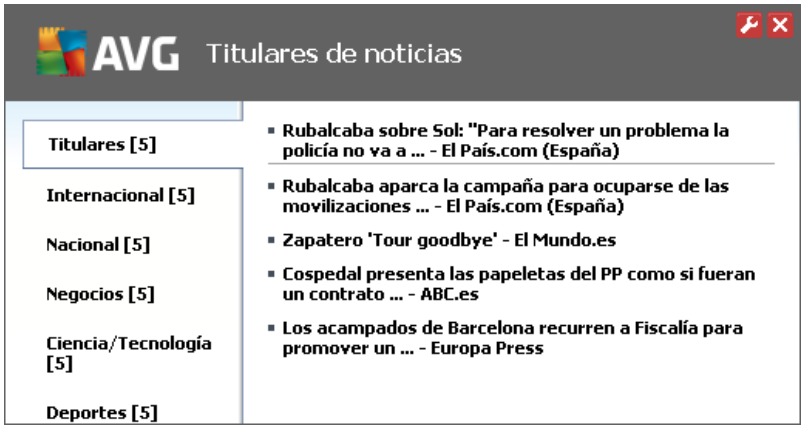


- o ***Mostrar mensajes***: cambie el número deseado de mensajes mostrados simultáneamente
- o ***Diseño de RSS***: seleccione el modo avanzado o básico para la visualización actual de la vista de noticias (*de manera predeterminada está seleccionado el modo avanzado; consulte la imagen anterior*)
- o ***Ocultar los mensajes leídos***: marque este elemento para confirmar que no se vuelvan a mostrar los mensajes leídos, de forma que se puedan ofrecer mensajes nuevos

- : haga clic en este botón para cerrar la vista general de noticias actualmente abierta

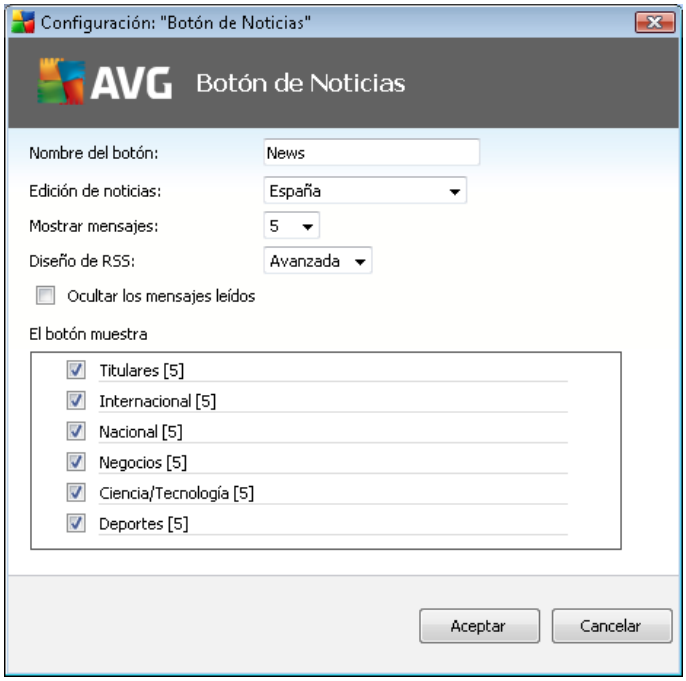
8.1.5. Noticias

De manera similar, directamente desde la ***barra de herramientas AVG Security Toolbar***, este botón abre una vista general de las noticias más recientes en los medios seleccionados dividida en varias secciones:



En la esquina superior derecha verá dos botones de control de color rojo:

- : este botón abre el cuadro de diálogo de edición, donde puede especificar los parámetros del botón ***Noticias*** mostrado en la ***barra de herramientas AVG Security Toolbar***:



- ***Nombre del botón***: puede cambiar el nombre del botón que se ve en la ***barra de herramientas AVG Security Toolbar***

- ***Edición de noticias***: seleccione un país de la lista para ver noticias de la región seleccionada.
- ***Mostrar mensajes***: especifique la cantidad de mensajes que desea que se muestren simultáneamente
- ***Diseño de RSS***: permite pasar de la opción básica a la avanzada, y viceversa, para seleccionar el diseño con que se verá la vista general de noticias (***de forma predeterminada está seleccionado el diseño avanzado; consulte la imagen de arriba***).
- ***Ocultar los mensajes leídos***: marque este elemento para confirmar que los mensajes leídos

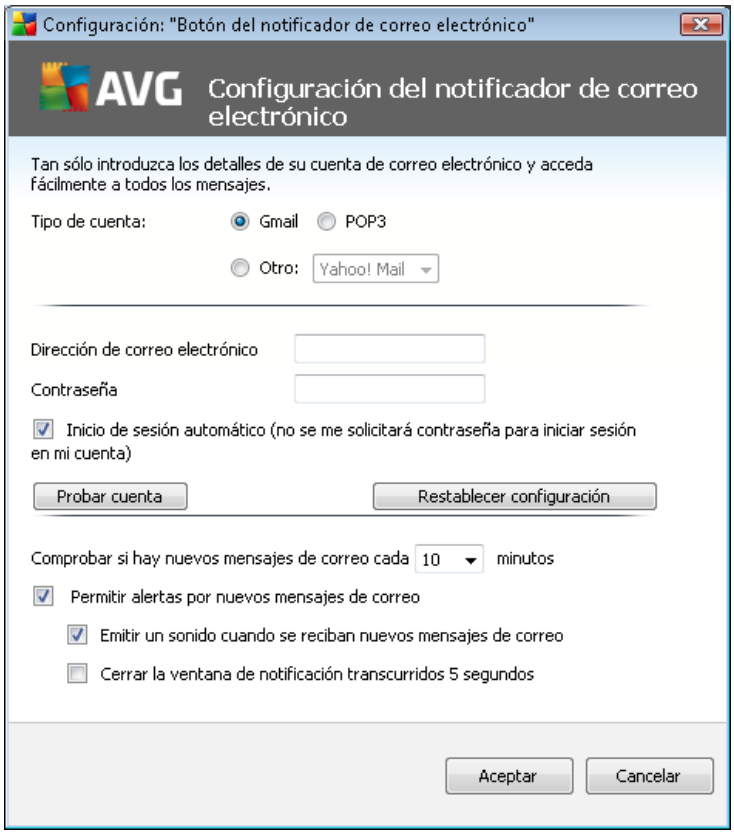
dejen de aparecer en la vista general de noticias y sean reemplazados por encabezados nuevos
- o ***El botón muestra***: en este campo puede asignar qué tipo de noticias se mostrarán en la vista general de noticias en la ***barra de herramientas AVG Security Toolbar***.
  - : haga clic en este botón para cerrar la vista general de noticias actualmente abierta

8.1.6. Eliminar historial

Con este botón puede eliminar el historial del navegador, tal como lo haría desde ***logotipo de AVG -> Eliminar historial***.

8.1.7. Notificador de correo electrónico

El botón ***Notificador de correo electrónico*** permite activar la opción de recibir información sobre los mensajes de correo electrónico que acaban de llegar directamente en la interfaz de la ***barra de herramientas AVG Security Toolbar***. El botón abre el siguiente cuadro de diálogo de edición, donde puede definir los parámetros de su cuenta de correo electrónico y las reglas de visualización del correo electrónico. Siga las instrucciones del cuadro de diálogo:



- ***Tipo de cuenta***: especifique el tipo de protocolo que utiliza su cuenta de correo electrónico. Puede elegir entre las siguientes alternativas: *Gmail*, *POP3* o seleccionar el nombre del servidor en el menú desplegable del elemento *Otro* (*por el momento, puede usar esta opción si tiene una cuenta en Correo Yahoo! JP Mail o Hotmail*). Si no está seguro del tipo de servidor de correo electrónico que utiliza su cuenta, intente solicitar información a su proveedor de correo electrónico o de servicios de Internet.

- ***Inicio de sesión***: en la sección inferior, introduzca su *dirección de correo electrónico* exacta y su correspondiente *contraseña*. Mantenga marcada la opción *Inicio de sesión automático* para no tener que escribir repetidamente los datos.

- ***Probar cuenta***: utilice este botón para probar los datos introducidos.

- ***Restablecer configuración***: elimina de forma rápida los detalles de la dirección electrónica introducidos más arriba.

- ***Comprobar si hay nuevos mensajes de correo cada ... minutos***: defina el intervalo de tiempo para comprobar si hay nuevos mensajes de correo electrónico (*entre 5 y 120 minutos*) e indique si desea recibir información sobre la llegada de nuevos mensajes y cómo recibirla.

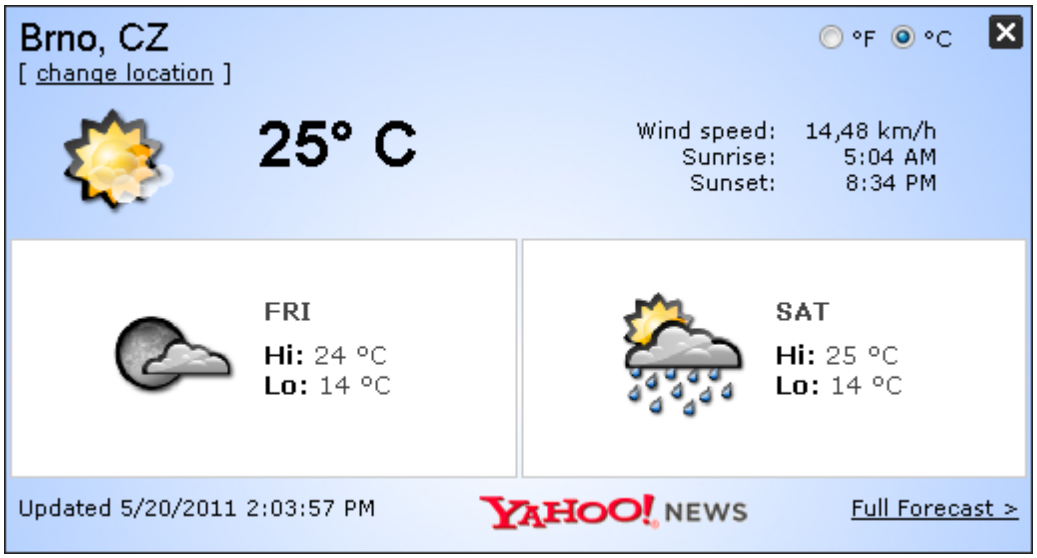
- ***Permitir alertas por nuevos mensajes de correo***: deje esta casilla en blanco para desactivar las notificaciones visuales de llegada de nuevos mensajes.

    - ***Emitir un sonido cuando se reciban nuevos mensajes de correo:*** deje esta casilla en blanco para desactivar las notificaciones sonoras de llegada de nuevos mensajes.

    - ***Cerrar la ventana de notificación transcurridos 5 segundos:*** marque esta opción para cerrar automáticamente la ventana de notificación visual de llegada de nuevos mensajes una vez transcurridos 5 segundos.

8.1.8. Información metereológica

El botón ***Tiempo*** muestra información sobre la temperatura actual (*actualizada cada 3-6 horas*) en el destino seleccionado directamente en la interfaz de la ***barra de herramientas AVG Security Toolbar***. Haga clic en el botón para abrir un nuevo panel informativo con detalles generales de la situación meteorológica:



Las opciones de edición son las siguientes:

- ***Cambiar ubicación***: haga clic en el texto ***Cambiar ubicación*** para mostrar un nuevo cuadro de diálogo denominado ***Busque su ubicación***. Introduzca la ubicación deseada en el campo de texto y confírmela haciendo clic en el botón ***Buscar***. A continuación, seleccione el destino buscado en la lista de ubicaciones con el mismo nombre. Finalmente, se mostrará el panel informativo de nuevo con la información metereológica de la ubicación seleccionada.

- ***Convertidor de Fahrenheit/Celsius***: en la esquina superior derecha del panel informativo puede elegir mostrar los grados en la escala Fahrenheit o Celsius. Según la selección, la información de la temperatura se proporcionará en adelante en la escala elegida.

- ***Previsión completa***: si desea una previsión completa y detallada, utilice el vínculo ***Previsión completa*** para acceder al sitio web especializado en el tiempo.

8.1.9. Facebook

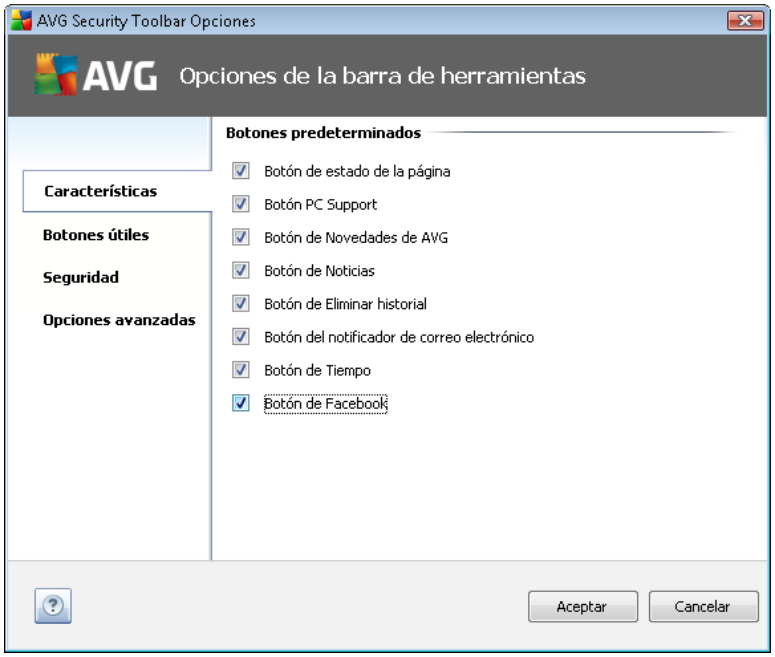
El botón ***Facebook*** le permite conectarse a la red social Facebook directamente desde la ***barra de herramientas AVG Security Toolbar***. Al hacer clic en el botón, aparecerá una invitación para iniciar sesión; haga clic de nuevo para abrir el cuadro de diálogo ***Acceso a Facebook***. Facilite sus datos de acceso y pulse el botón ***Conectar***. Si aún no tiene cuenta en Facebook, puede crearla directamente utilizando el vínculo ***Registrarse en Facebook***.

Una vez realizado el proceso de registro en Facebook, se le invitará a permitir la aplicación ***AVG Social Extension***. La funcionalidad de esta aplicación es esencial para la conexión a Facebook en la barra de herramientas, por lo que se recomienda permitir su funcionamiento; asegúrese de hacerlo. La conexión a Facebook se activará y el botón ***Facebook*** de la ***barra de herramientas AVG Security Toolbar*** ofrecerá las opciones de menú estándar de Facebook.

8.2. Opciones de AVG Security Toolbar

Se puede acceder a la configuración de todos los parámetros de la ***barra de herramientas AVG Security Toolbar*** directamente en el panel de ***AVG Security Toolbar***. La interfaz de edición se abre a través del elemento de menú de la barra de herramientas *AVG / Opciones* en un nuevo cuadro de diálogo denominado ***Opciones de la barra de herramientas*** que está dividido en cuatro secciones:

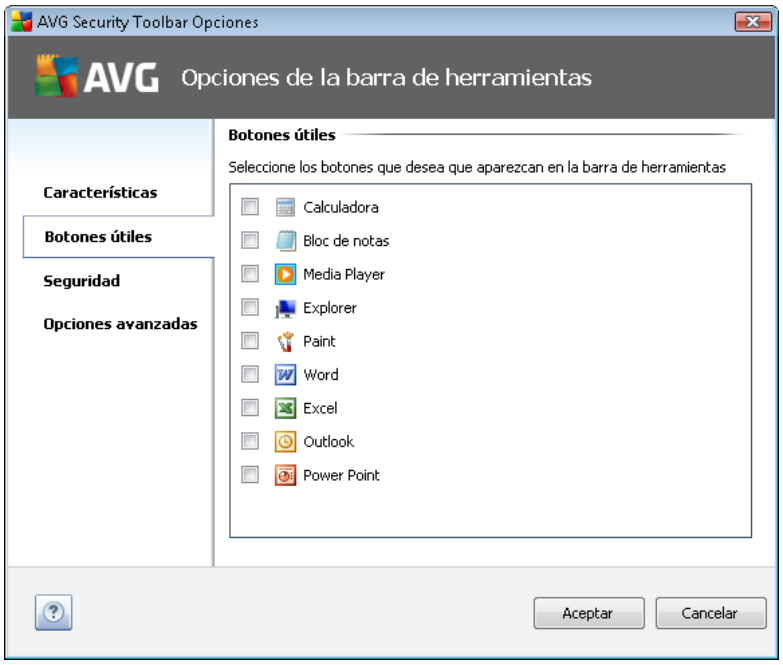
8.2.1. Ficha General



En esta ficha, puede especificar los botones de control de la barra de herramientas que deberían mostrarse u ocultarse dentro del panel de ***AVG Security Toolbar***. Marque cualquiera de las opciones si desea que se muestre el botón correspondiente. A continuación se describe la función de cada uno de los botones de la barra de herramientas:

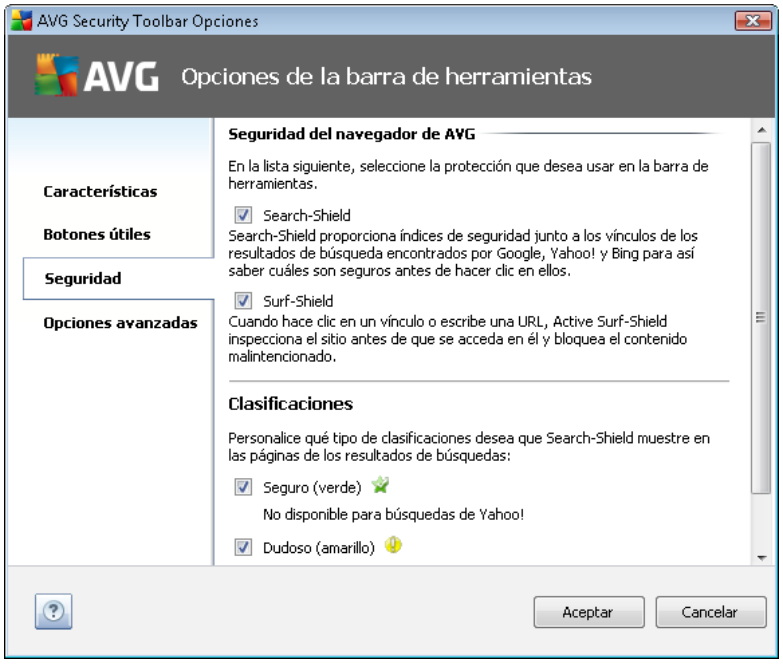
- ***Botón Estado de la página***: este botón ofrece la posibilidad de ver información sobre la página de estado de seguridad actualmente abierta dentro de la ***barra de herramientas AVG Security Toolbar***
- ***Botón Noticias AVG***: este botón abre una página web que muestra los últimos comunicados de prensa sobre AVG
- ***Botón Noticias***: este botón muestra un resumen estructurado de noticias de actualidad extraídas de la prensa diaria
- ***Botón Eliminar historial***: este botón permite borrar todo el historial, el historial de búsqueda, el historial de navegación, el historial de descargas o las cookies directamente desde el panel de AVG Security Toolbar
- ***Botón Notificador de correo electrónico***: este botón permite ver los mensajes de correo nuevos dentro de la interfaz de la ***barra de herramientas AVG Security Toolbar***
- ***Botón Tiempo***: este botón permite ver información inmediata sobre el estado meteorológico en un sitio determinado
- ***Botón de Facebook***: este botón ofrece conexión directa con la red social Facebook

8.2.2. Ficha Botones útiles



La ficha ***Botones útiles*** permite seleccionar aplicaciones de una lista y hacer que su icono se muestre en la interfaz de la barra de herramientas. De esta forma, el icono actúa como vínculo rápido para iniciar la aplicación correspondiente de inmediato.

8.2.3. Ficha Seguridad



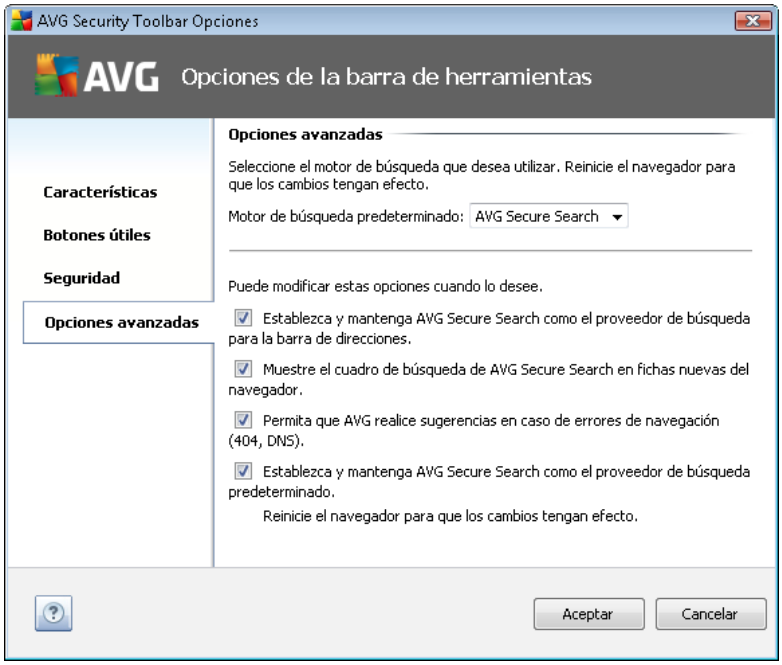
La ficha ***Seguridad*** se divide en dos secciones, ***Seguridad del navegador de AVG*** y

Clasificaciones, donde puede marcar las casillas de verificación específicas para asignar la función de la ***barra de herramientas AVG Segurity Toolbar*** que desea utilizar:

- ***Seguridad del navegador de AVG***: marque este elemento para activar o desactivar el servicio ***Search-Shield*** y/o ***Surf-Shield***.
- ***Clasificaciones***: seleccione los símbolos gráficos que desea que se empleen para indicar la clasificación de los resultados de búsqueda realizada por el componente ***Search-Shield***:
  - o la página es segura
  - o la página es un tanto sospechosa
  - o la página contiene vínculos a páginas verdaderamente peligrosas
  - o la página contiene amenazas activas
  - o no se puede acceder a esta página, por lo que no fue posible analizarla

Marque la opción que corresponda para confirmar que desea ser informado sobre este nivel de amenaza específico. Tenga en cuenta que no es posible desactivar la visualización de una marca roja junto a las páginas que contienen amenazas activas y peligrosas. ***Nuevamente, se recomienda mantener la configuración predeterminada establecida por el proveedor del programa a menos que se tenga un buen motivo para modificarla.***

8.2.4. Ficha Opciones avanzadas



En la ficha ***Opciones avanzadas***, seleccione primero el motor de búsqueda que desea utilizar de forma predeterminada. Puede elegir entre *AVG Secure Search (powered by Google), Baidu, WebHledani*, *Yandex y Yahoo! JP*. Una vez cambiado el motor de búsqueda predeterminado, reinicie el navegador de Internet para que el cambio tenga efecto.

También puede activar o desactivar parámetros específicos de la ***barra de herramientas AVG Security Toolbar*** *(el ejemplo que se muestra hace referencia a los parámetros predeterminados de AVG Secure Search (powered by Google))*:

- ***Establezca y mantenga AVG Secure Search (powered by Google) como el proveedor de búsqueda para la barra de direcciones***: si esta opción está marcada, permite escribir una palabra clave directamente en la barra de direcciones del navegador de Internet y el servicio de Google se utilizará de manera automática para buscar sitios web que coincidan con esa palabra.

- ***Permitir que AVG realice sugerencias en caso de errores de navegación (404, DNS)***: si, al buscar en Internet, aparece el mensaje de que la página no existe o que no es posible mostrarla (error 404), automáticamente se le redirigirá a una página web donde podrá ver una lista de páginas alternativas relacionadas con el mismo tema.

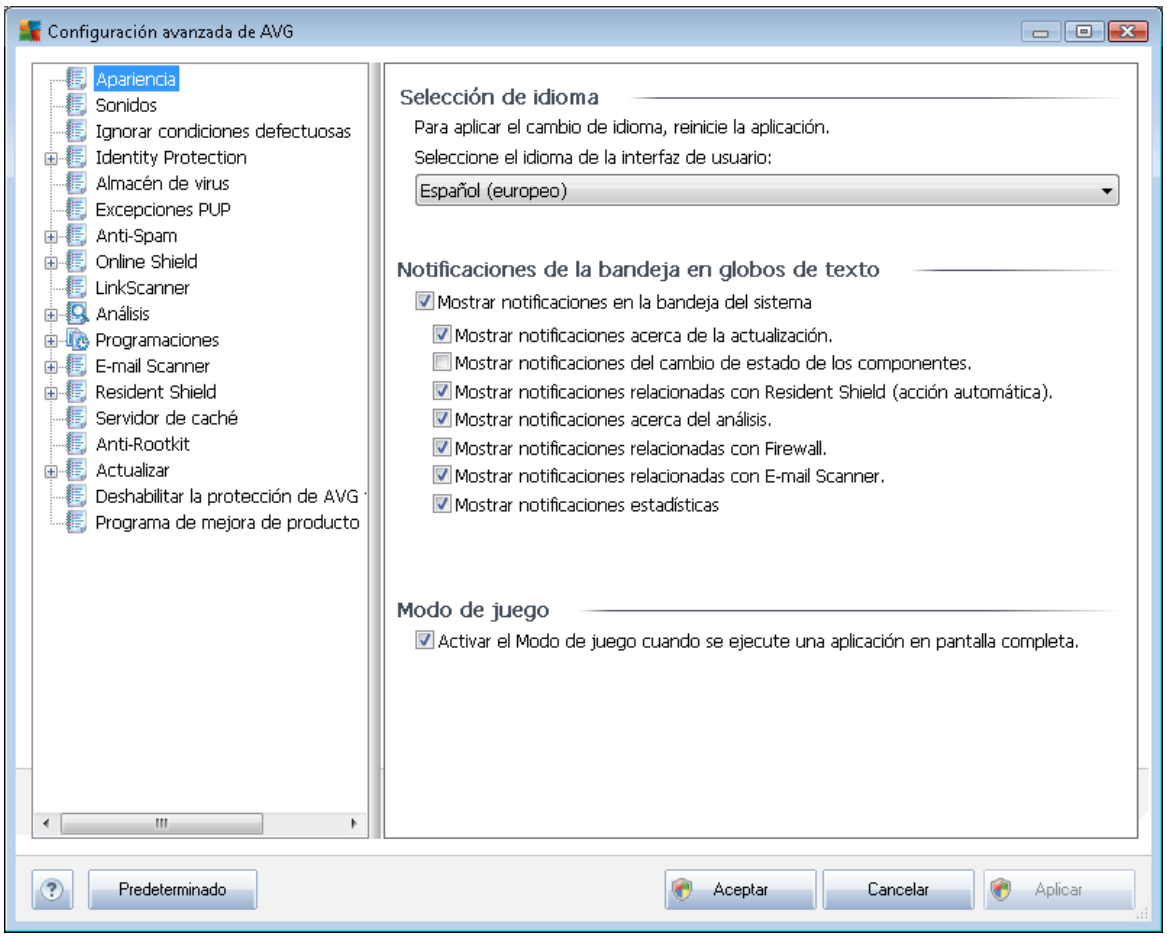
- ***Establezca y mantenga AVG Secure Search (powered by Google) como el proveedor de búsqueda predeterminado***: Google es el motor de búsqueda predeterminado para buscar en la web desde la ***barra de herramientas AVG Security Toolbar*** y, si activa esta opción, también se convertirá en el motor de búsqueda predeterminado para el navegador web.

9. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG Internet Security 2011** 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 y a algunas opciones elementales del comportamiento de la aplicación:

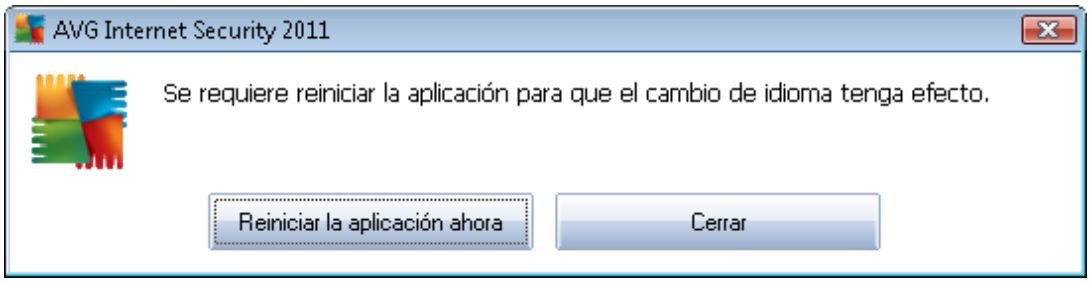


Selección de idioma

En la sección ***Selección de idioma*** puede elegir el idioma que desee en el menú desplegable, el cual se utilizará en toda la interfaz de usuario de AVG. El menú desplegable solamente ofrece los idiomas previamente seleccionados durante el proceso de instalación (*consulte el capítulo Opción personalizada*) además del inglés (*instalado de manera predeterminada*). No obstante, para terminar

de cambiar la aplicación a otro idioma, debe reiniciar la interfaz de usuario; siga los pasos descritos a continuación:

- Seleccione el idioma deseado para la aplicación y confirme su selección pulsando el botón ***Aplicar*** (esquina inferior derecha)
- Pulse el botón ***Aceptar*** para confirmar
- Se abre una nueva ventana de cuadro de diálogo informándole de que el cambio de idioma de la interfaz de usuario de AVG requiere reiniciar la aplicación:



Notificaciones de la bandeja en globos de texto

En esta sección puede hacer que se supriman las notificaciones mediante globos de texto que aparecen en la bandeja del sistema informando sobre el estado de la aplicación. De manera predeterminada, la visualización de notificaciones en globos está autorizada y se recomienda conservar esta configuración. Generalmente, las notificaciones en globos de texto informan sobre el cambio de estado de algún componente de AVG y se les debería prestar atención.

No obstante, si por algún motivo no desea que se muestren estas notificaciones o si solamente desea visualizar ciertas notificaciones (relacionadas con un determinado componente de AVG), puede definir y especificar sus preferencias seleccionando o dejando en blanco las siguientes opciones:

- ***Mostrar notificaciones en la bandeja del sistema***: de manera predeterminada, este elemento está seleccionado (*activo*), por lo que se muestran notificaciones. Deje en blanco este elemento para desactivar por completo la visualización de notificaciones en globos de texto. Cuando está activo, puede seleccionar las notificaciones específicas que deben mostrarse:
  - ***Mostrar notificaciones en la bandeja acerca de la actualización***: indique si debe mostrarse información sobre el inicio, el progreso y la finalización del proceso de actualización de AVG;
  - ***Mostrar notificaciones del cambio de estado de los componentes***: decida si desea que se muestre información relacionada con la actividad o inactividad del componente o sus problemas relacionados. Cuando se notifica el estado de error de un componente, esta opción es igual que la función informativa del icono de la bandeja del sistema (cambio de color) que notifica un problema en algún componente de AVG;

- ***Mostrar notificaciones en la bandeja relacionadas con Protección residente (acción automática)***: indique si la información referente a procesos de guardado, copia y apertura de archivos se debe mostrar o suprimir (*esta configuración solamente aparece si la opción Reparación automática de Protección residente está activa*);

- ***Mostrar notificaciones en la bandeja acerca del análisis***: indique si debe mostrarse información sobre el inicio automático, el progreso y los resultados del análisis programado;

- ***Mostrar notificaciones en la bandeja relacionadas con Firewall***: indique si la información referente al estado y los procesos del Firewall, p. ej. advertencias de activación o desactivación del componente, posible bloqueo del tráfico, etc. debe mostrarse;

- ***Mostrar notificaciones en la bandeja relacionadas con Analizador de correo electrónico***: indique si debe mostrarse información sobre el análisis de todos los mensajes de correo electrónico entrantes y salientes.

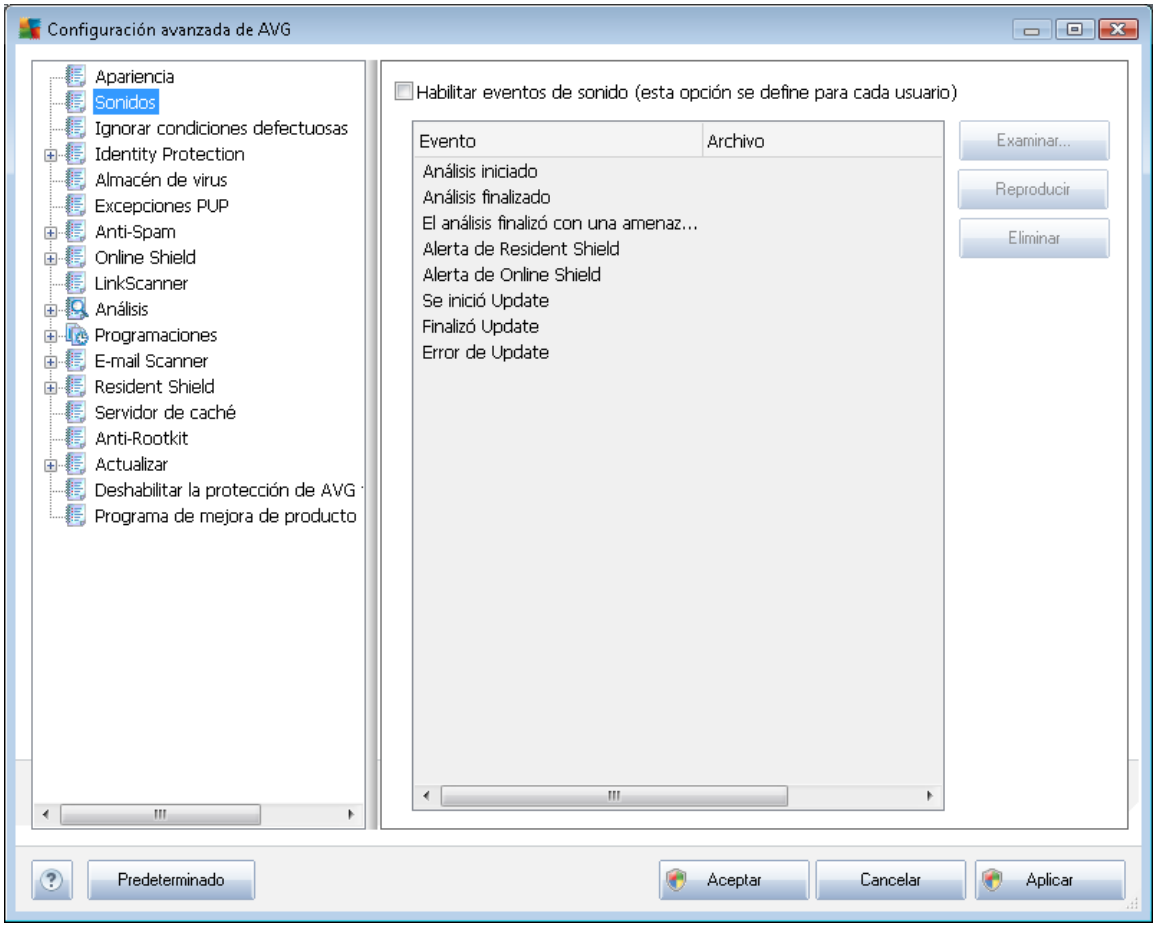
- ***Mostrar notificaciones estadísticas:*** mantenga esta opción marcada para permitir que se muestren en la bandeja del sistema notificaciones de las estadísticas de revisión regulares.

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 mediante una notificación sonora. De ser así, marque la opción ***Habilitar eventos de sonido*** (*desactivada de manera predeterminada*) para activar la lista de acciones de AVG:

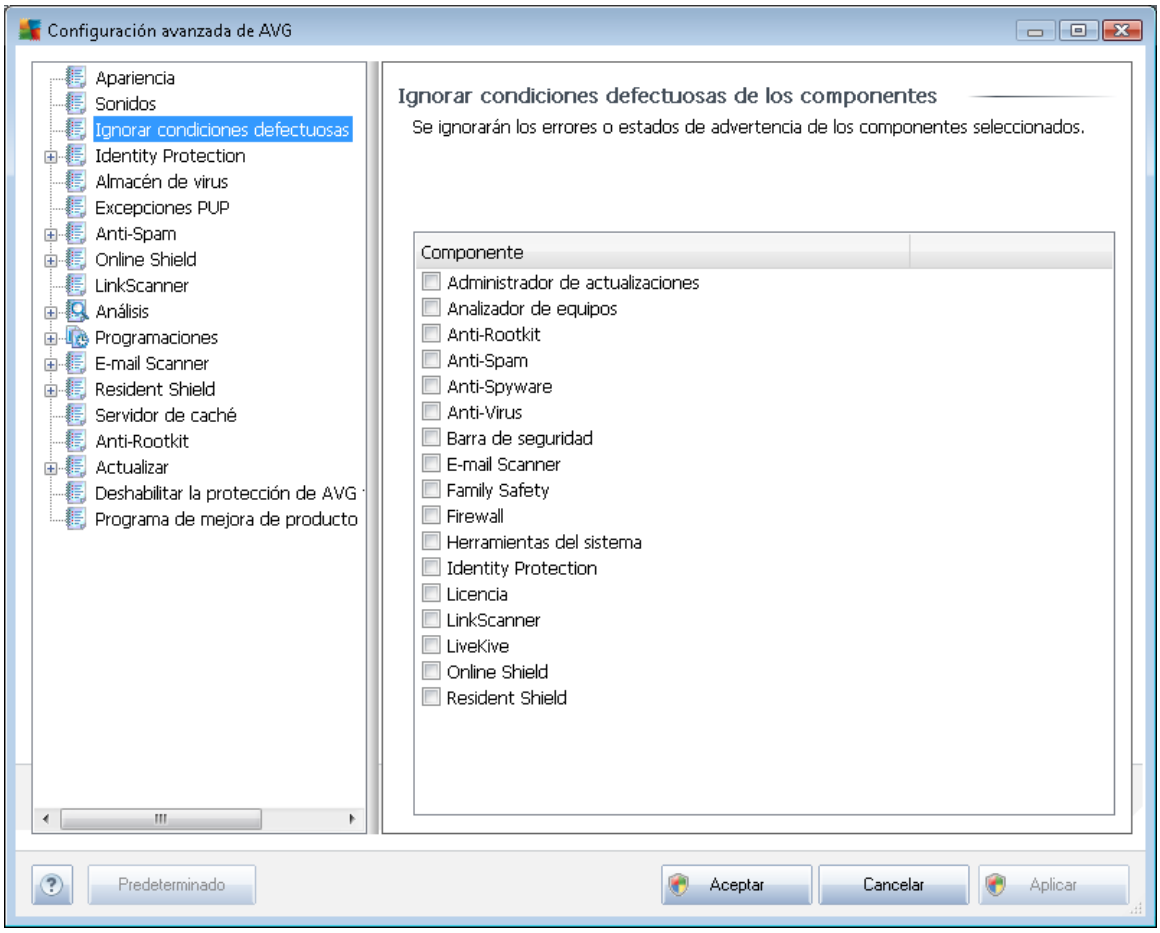


A continuación, seleccione el evento correspondiente de la lista y busque en el disco duro (con ***Examinar***) el sonido que desea asignar a este evento. Para escuchar el sonido seleccionado, resalte el evento en la lista y pulse el botón ***Reproducir***. Emplee el botón ***Eliminar*** para quitar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

Nota: *sólo se admiten sonidos *.wav.*

9.3. Ignorar condiciones defectuosas

En el cuadro de diálogo ***Ignorar condiciones defectuosas de los componentes***, puede marcar los componentes sobre los que no desea recibir información:



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

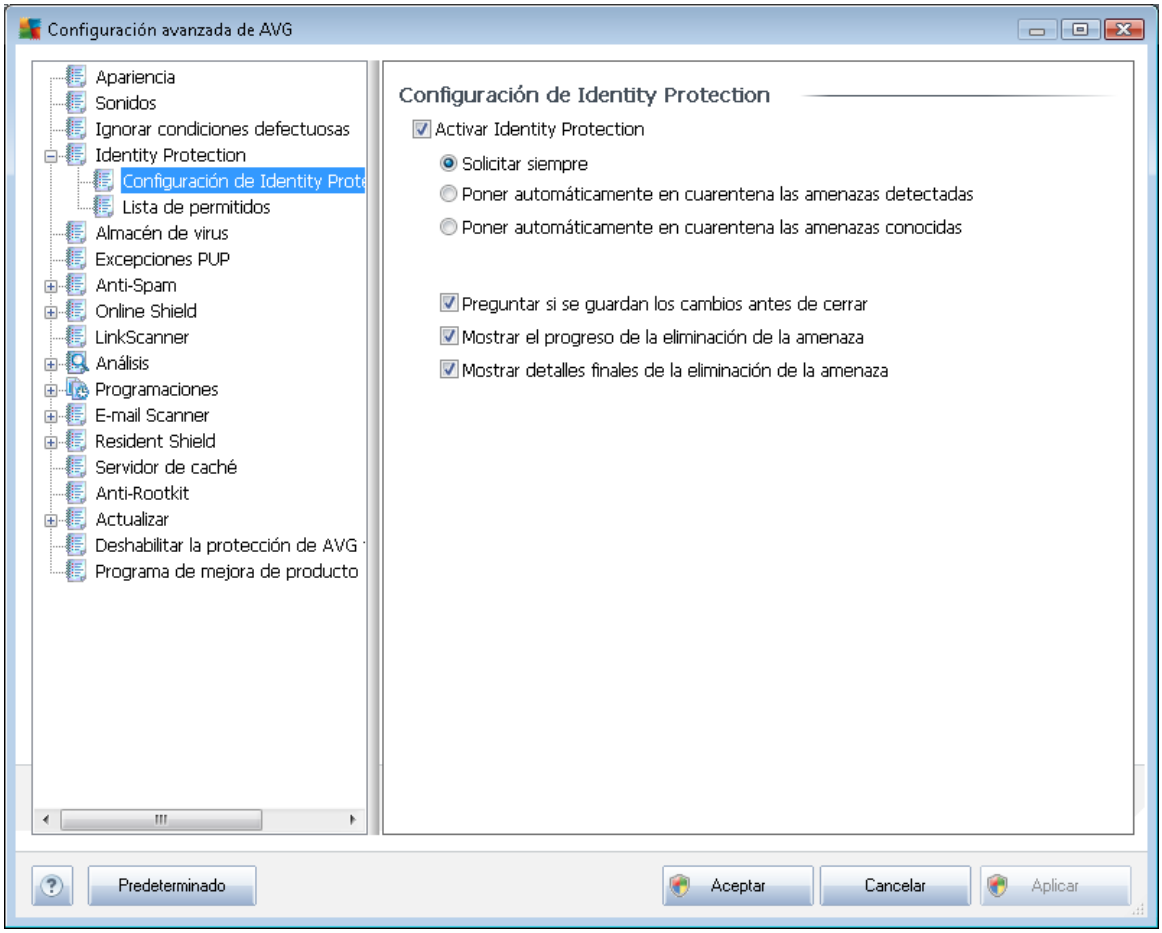
adquiere color gris, el icono no puede informar sobre ningún posible error posterior que pueda aparecer.

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 de ***ignorar el estado del componente*** también está disponible para determinados componentes directamente en la información general de los componentes, en la ventana principal de AVG.

9.4. Identity Protection

9.4.1. 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 AVG***. 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 AVG***.

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

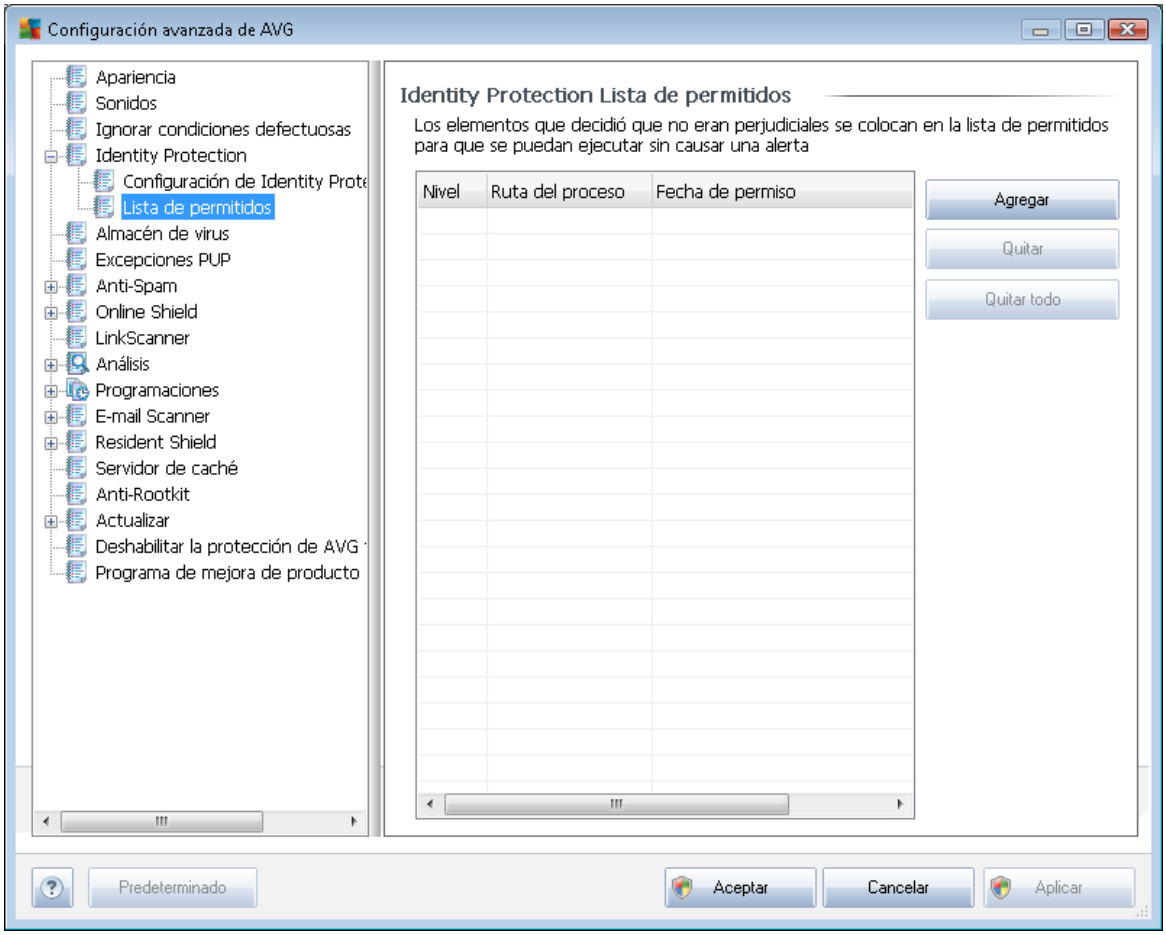
- ***Preguntar si se guarda el trabajo antes de eliminar*** (*activado de manera predeterminada*): mantenga seleccionado este elemento si desea recibir un aviso antes de poner en cuarentena la aplicación detectada como posible malware. En caso de que solamente trabaje con la aplicación, podría perder 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.*).

9.4.2. 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:



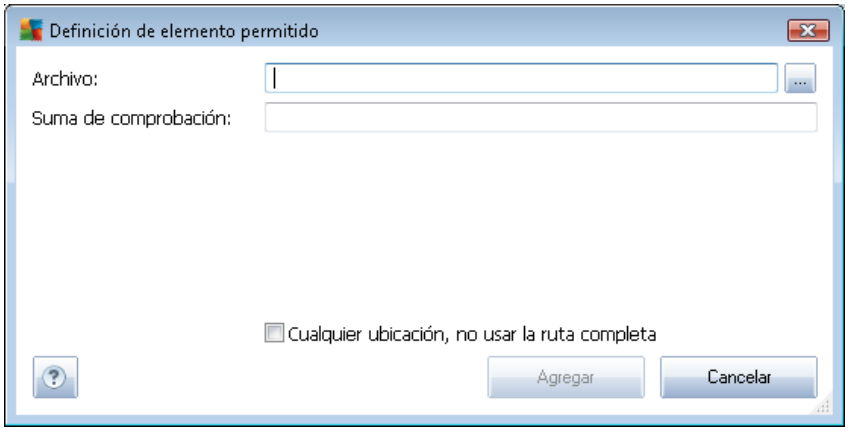
La ***Lista de permitidos de Identity Protection*** proporciona la siguiente información sobre cada aplicación:

- ***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:

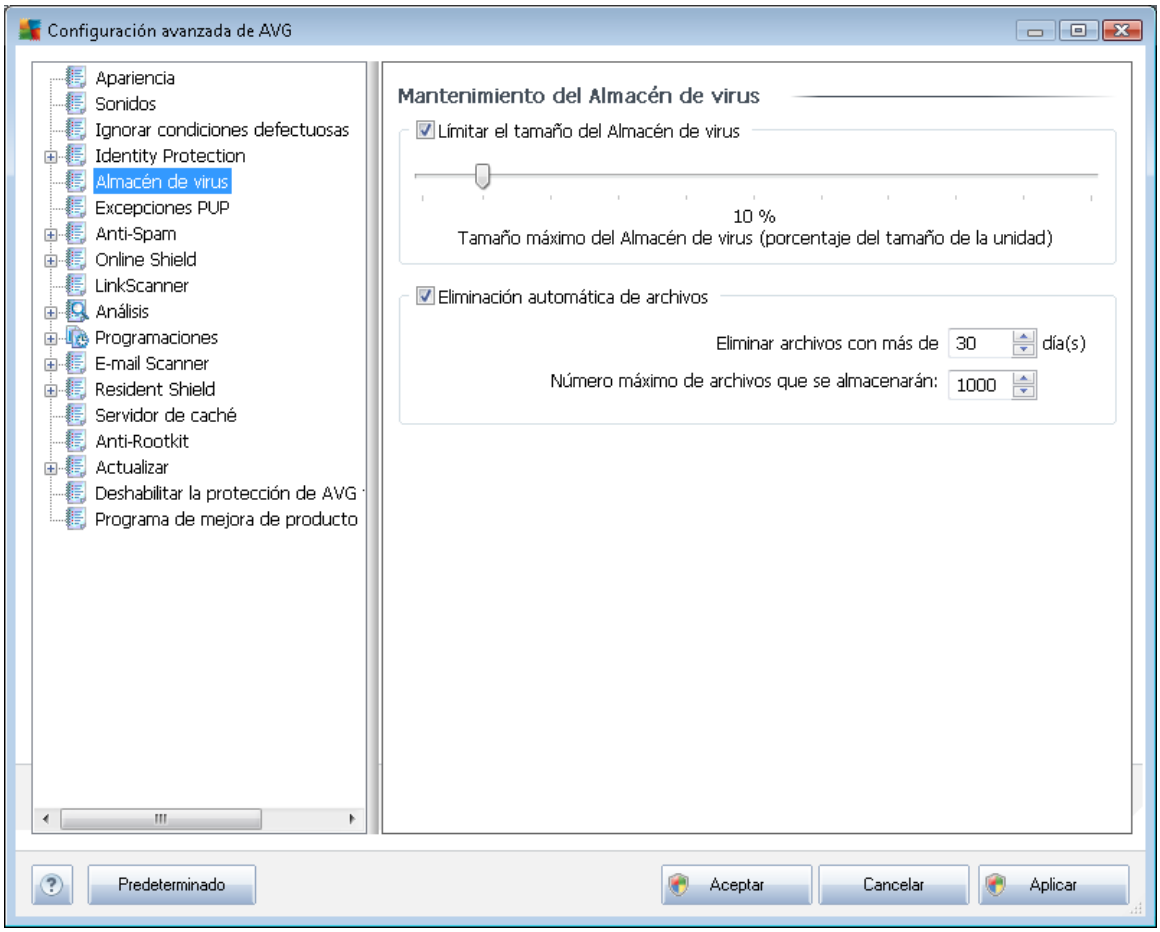
- ***Agregar***: pulse este botón para agregar una nueva aplicación a la lista de permitidos. Se abre el siguiente cuadro de diálogo:



- o ***Archivo***: escriba la ruta completa del archivo (*aplicación*) que desea marcar como una excepción
- o ***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.
- o ***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

9.5. 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***:

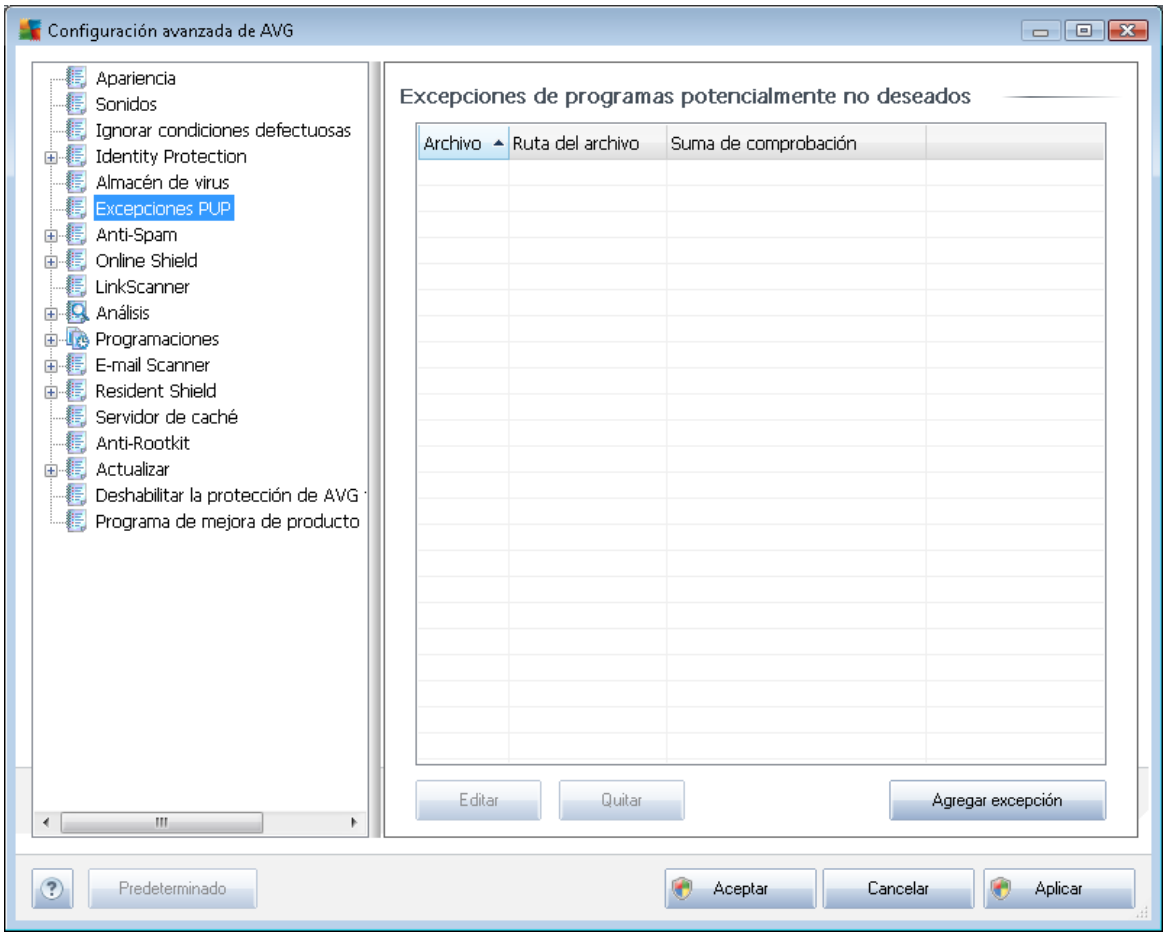
- ***Limitar el tamaño del Almacén de virus***: utilice el control deslizante para configurar el tamaño máximo del ***Almacén de virus***. El tamaño se especifica en proporción al tamaño del disco duro local.

- ***Eliminación automática de archivos***: defina en esta sección 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***)

9.6. Excepciones PUP

AVG Internet Security 2011 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. Tal adware podría ser detectado y notificado por AVG 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:

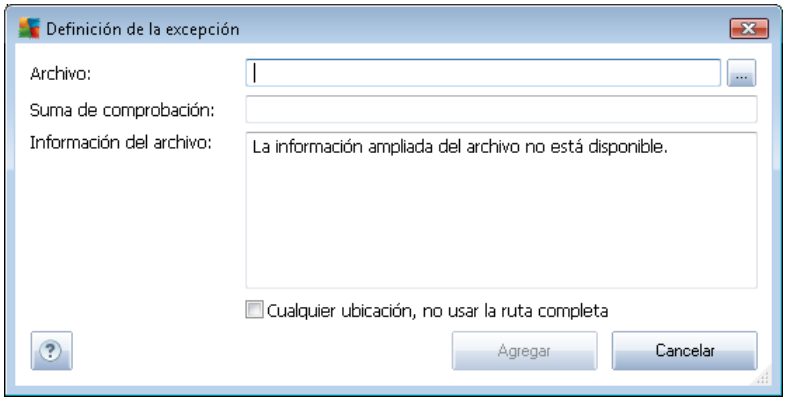
- ***Archivo***: proporciona el nombre de la aplicación respectiva
- ***Ruta del archivo***: muestra la ruta a la ubicación de la aplicación
- ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generada automáticamente que permite 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:



o ***Archivo***: escriba la ruta completa del archivo que desea marcar como excepción

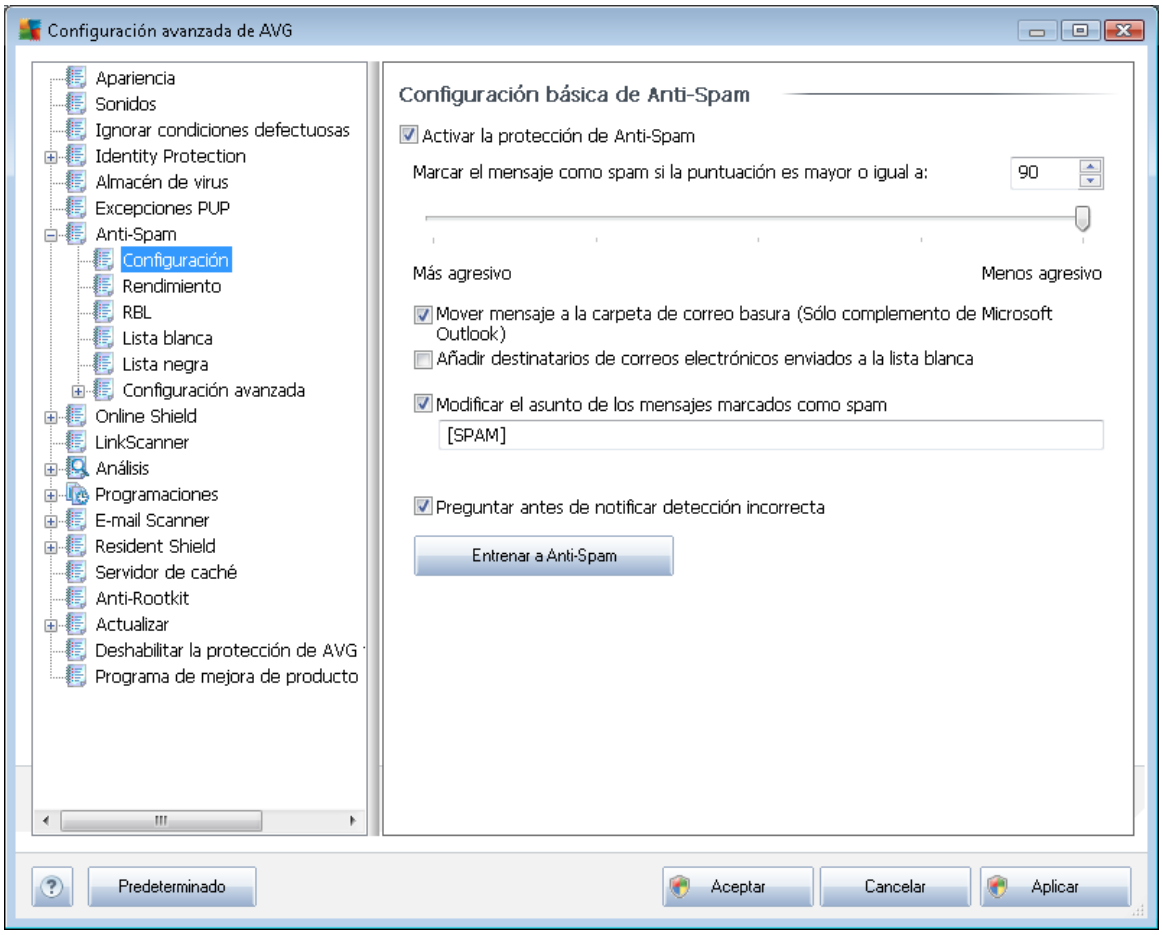
o ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generada automáticamente que permite a AVG distinguir de forma inequívoca el archivo elegido de otros archivos. La suma de comprobación se genera y muestra después de agregar correctamente el archivo.

o ***Información del archivo***: muestra cualquier información adicional que esté disponible sobre el archivo (*licencia/información de la versión, etc.*)

o ***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*).

9.7. Anti-Spam

9.7.1. Configuración



En el cuadro de diálogo ***Configuración básica de Anti-Spam***, puede seleccionar o dejar en blanco la casilla de verificación ***Activar la protección de Anti-Spam*** para permitir o prohibir 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 básica de Anti-Spam***, puede definir la forma en que deben tratarse los mensajes de correo electrónico de spam detectados:

- ***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;

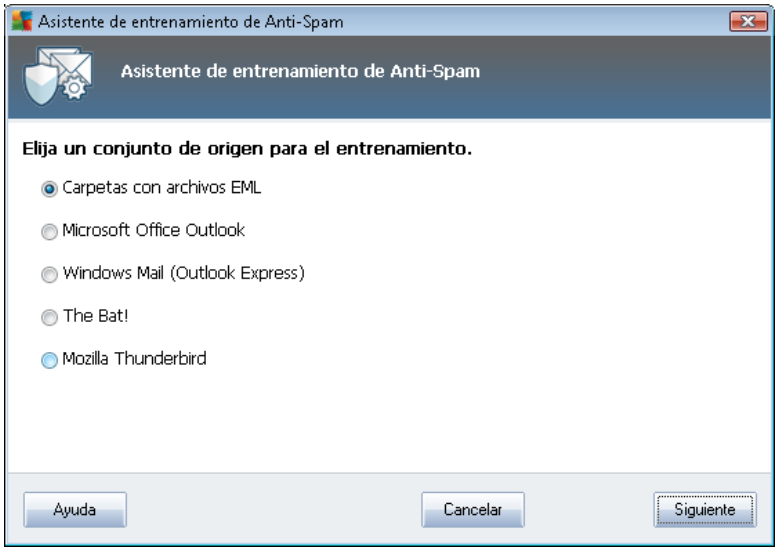
- ***Modificar el asunto de los mensajes marcados como spam***: marque esta casilla de verificación si desea que todos los mensajes detectados como spam se marquen con una palabra o un carácter concreto en el campo de asunto del correo electrónico; el texto deseado se puede escribir el campo de texto activo.

- ***Preguntar antes de notificar detección incorrecta***: suponiendo que durante el proceso de instalación indicara su disposición a 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:

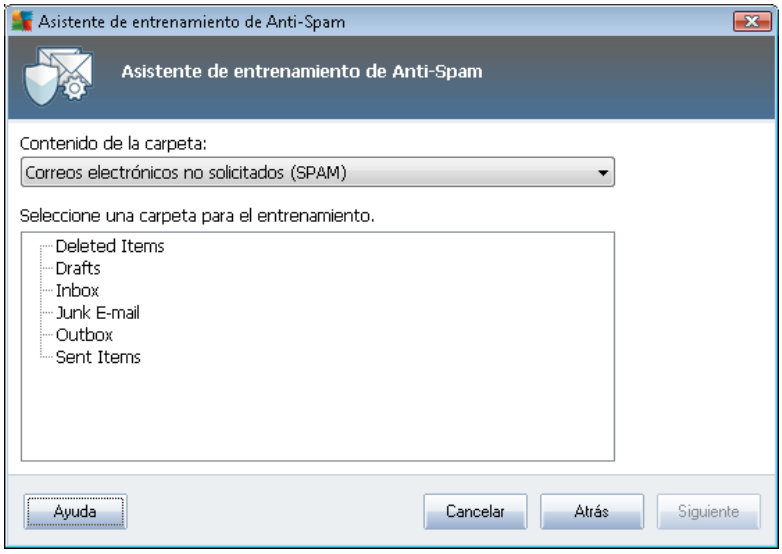
- ***Un cliente específico de correo electrónico***: si utiliza uno de los clientes de correo electrónico enumerados (*MS Outlook, Outlook Express, The Bat!*), simplemente seleccione la opción correspondiente
- ***Carpeta con archivos EML***: si utiliza cualquier otro programa de correo electrónico,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



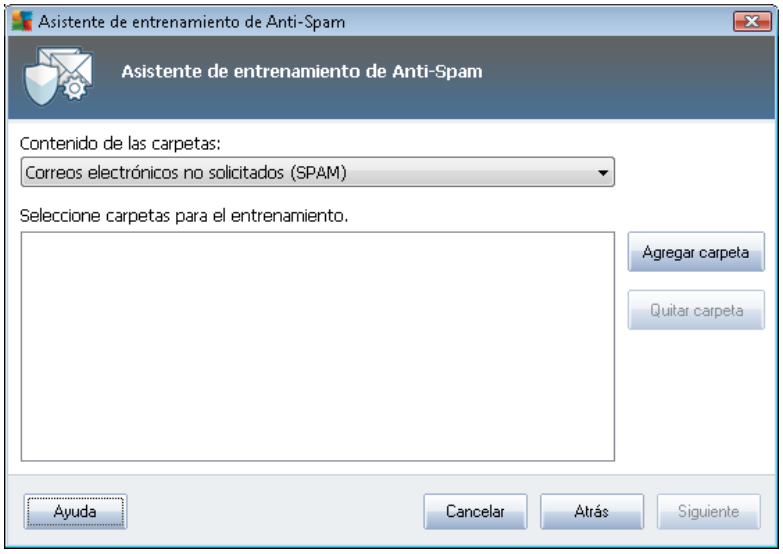
En este cuadro de diálogo, seleccione la carpeta con los mensajes que desea utilizar para el entrenamiento. Pulse el botón ***Agregar carpeta*** para localizar la carpeta con los archivos .eml (*mensajes de correo electrónico guardados*). A continuación, la carpeta seleccionada aparecerá en el cuadro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

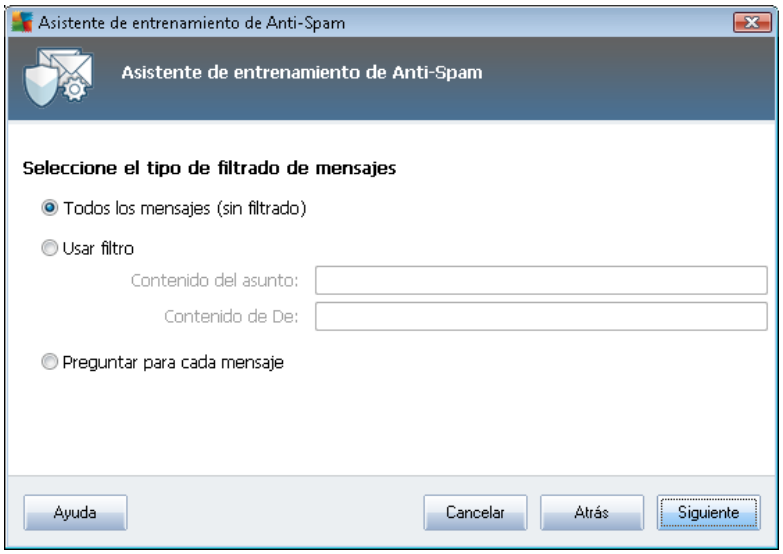
Cuando haya confirmado una de las opciones, aparecerá un nuevo cuadro de diálogo.



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.

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)***.

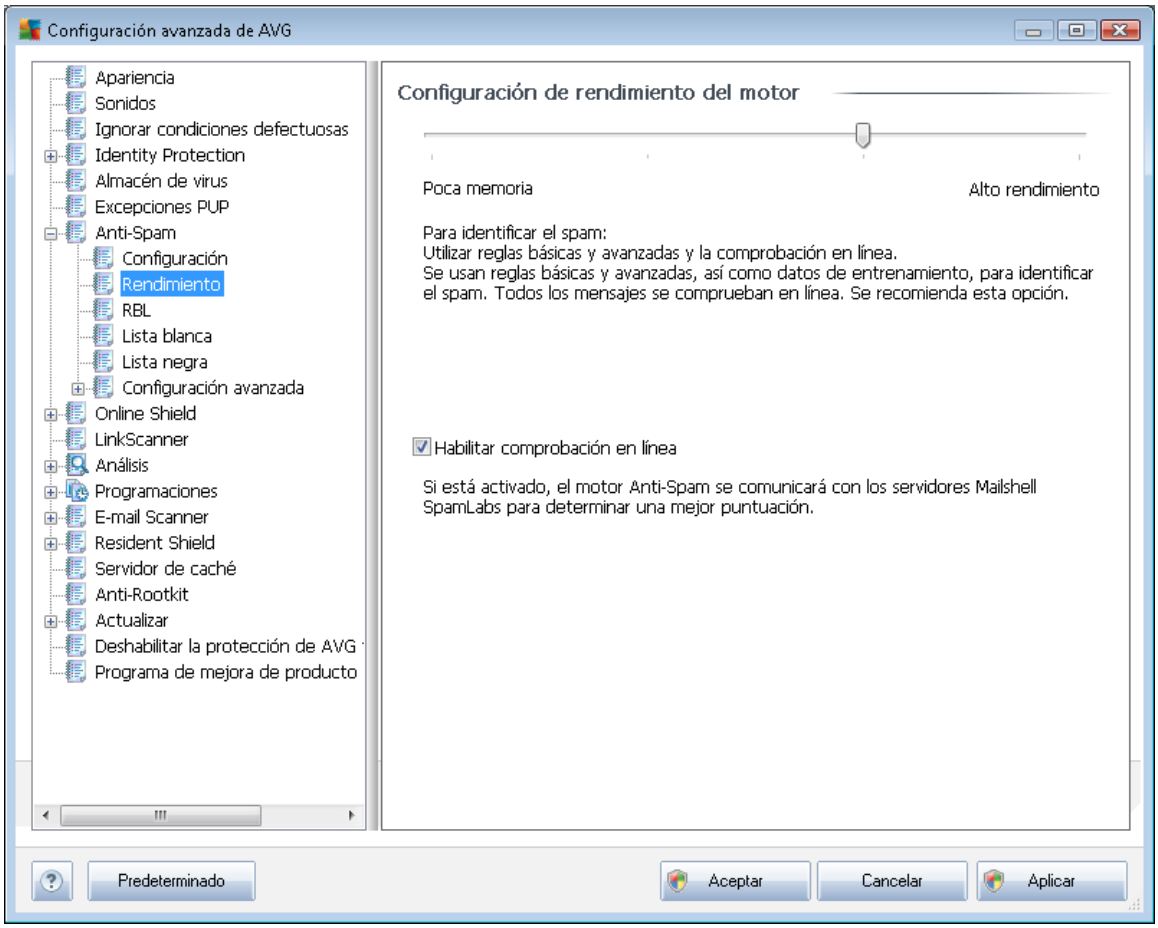
Si tiene dudas acerca de los mensajes que contiene la carpeta y desea que el asistente le pregunte sobre cada mensaje (para que pueda indicar si desea utilizarlo para el entrenamiento o no), seleccione la opción ***Preguntar para cada mensaje***.

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.

Atención: *si rellena los dos campos de texto, también se usarán las direcciones que coincidan solamente con una de las dos condiciones.*

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.

9.7.2. Rendimiento



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 realizado para detectar spam, no se utilizarán reglas. 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.

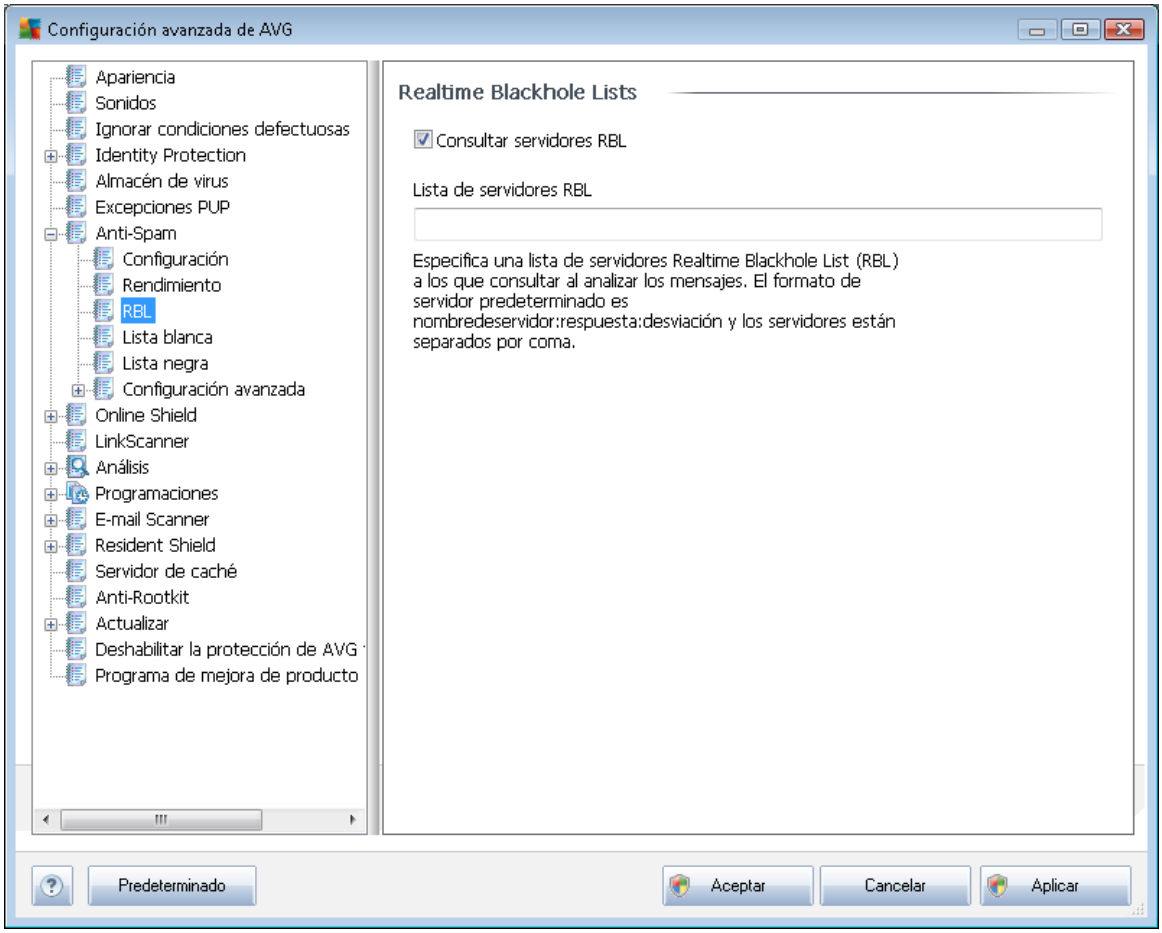
- ***Alto rendimiento***: este modo consumirá una gran cantidad de memoria. Durante el proceso de análisis realizado para detectar spam, se emplearán las siguientes características: reglas y caché de base de datos de spam, reglas básicas y avanzadas, direcciones IP de remitentes que envían spam y bases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

9.7.3. RBL

El elemento ***RBL*** abre un cuadro de diálogo de edición llamado ***Realtime Blackhole Lists***:



En este cuadro de diálogo 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.

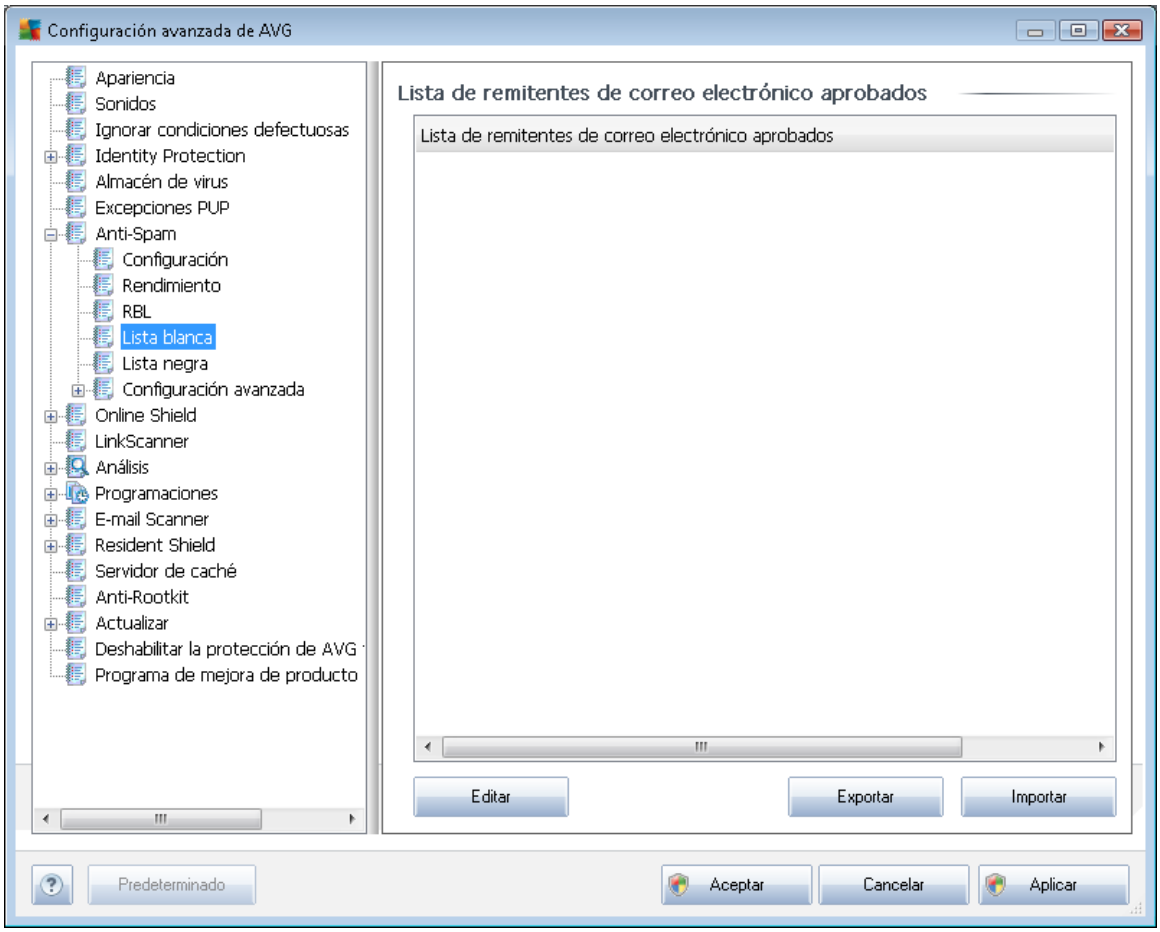
La ***lista de servidores RBL*** le permite definir ubicaciones específicas de los servidores RBL.

Nota: *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 del servidor RBL.*

No se envía ningún dato personal al servidor.

9.7.4. Lista blanca

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.

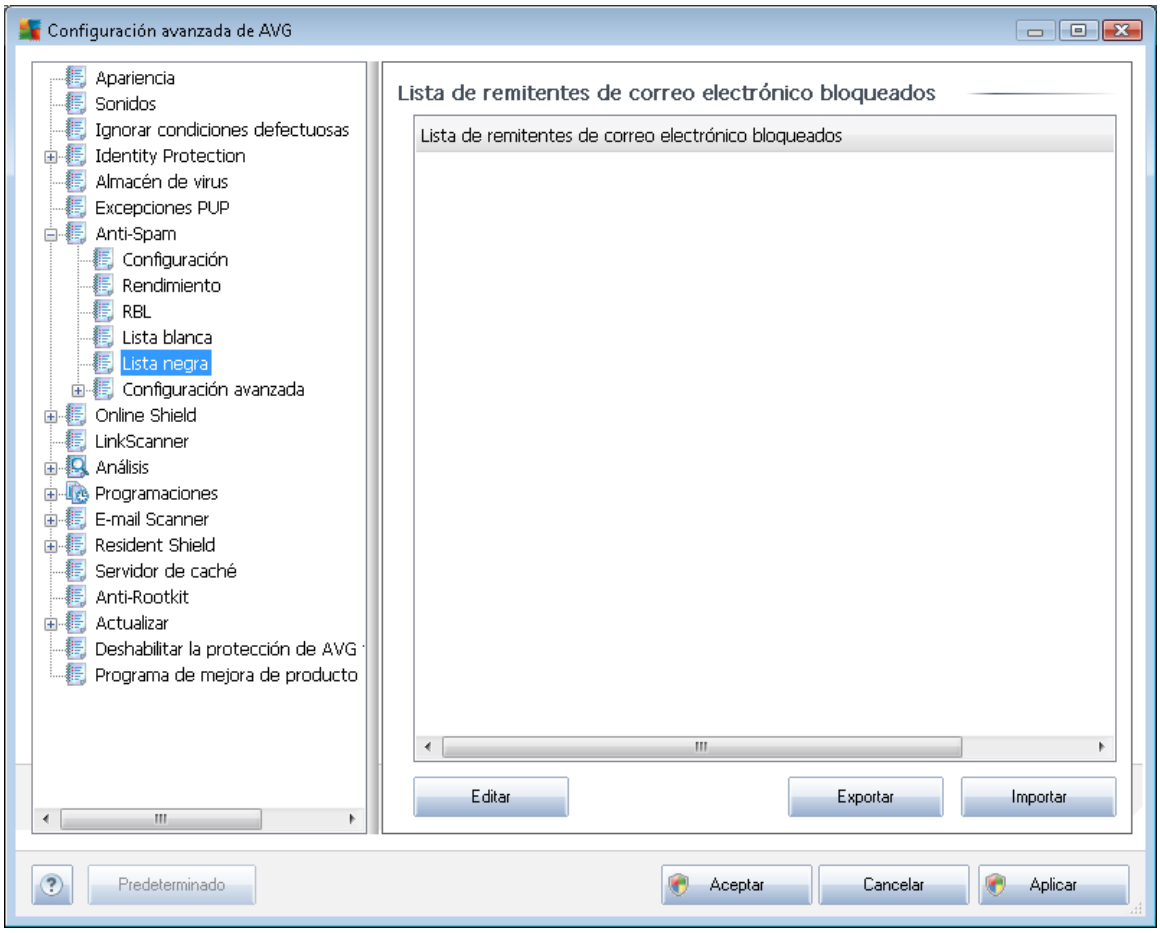
Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo. Los botones de control disponibles son los siguientes:

- ***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.

9.7.5. Lista negra

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.



En la interfaz de edición puede compilar una lista de remitentes de los que espera recibir mensajes no deseados (spam). 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. 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.

9.7.6. Configuración avanzada

La rama Configuración avanzada contiene numerosas opciones de configuración para el componente Anti-Spam. Estas opciones están destinadas a usuarios experimentados, generalmente administradores de red que necesitan configurar la protección anti-spam de manera sumamente específica para obtener la mejor protección de los 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

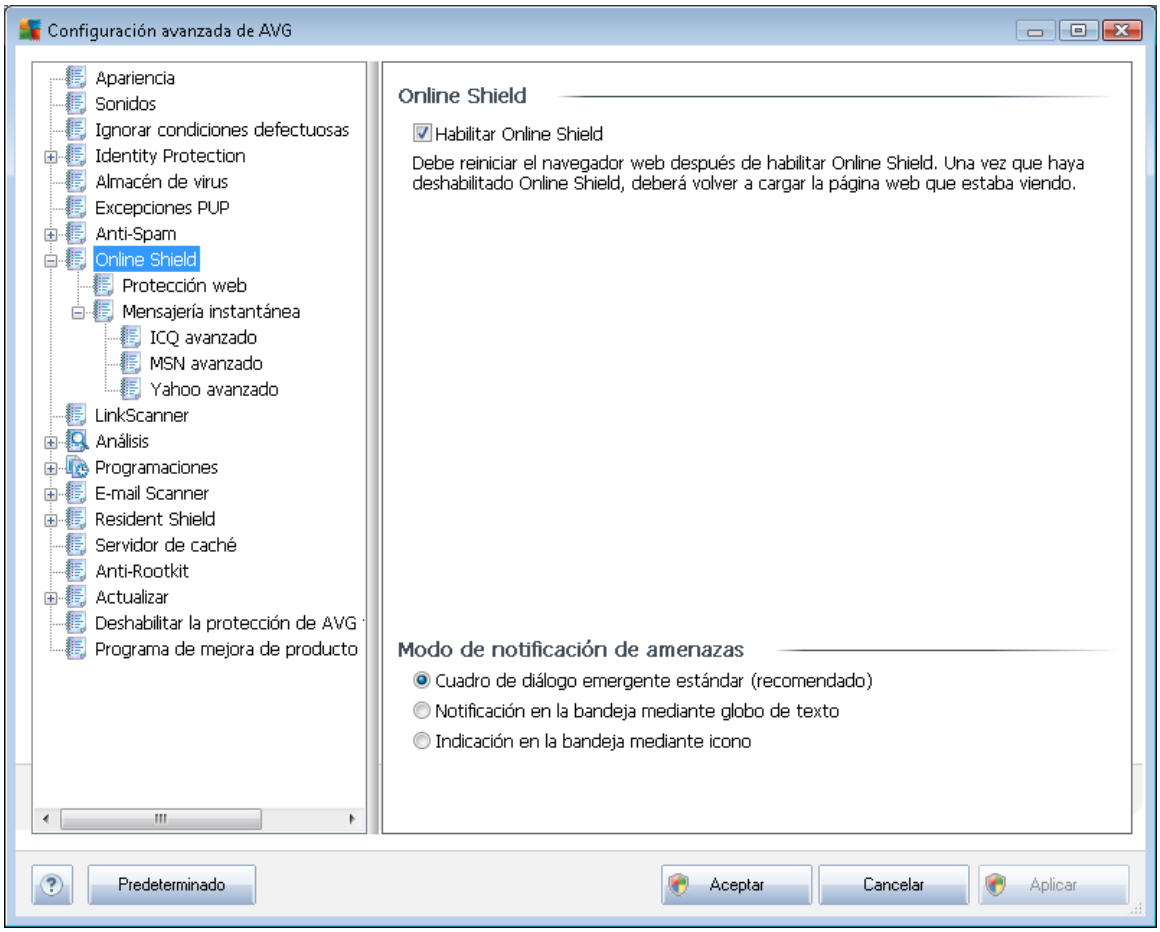
- ***Entrenamiento***: máximo de palabras, umbral de autoentrenamiento, relevancia

- ***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

9.8. Online Shield



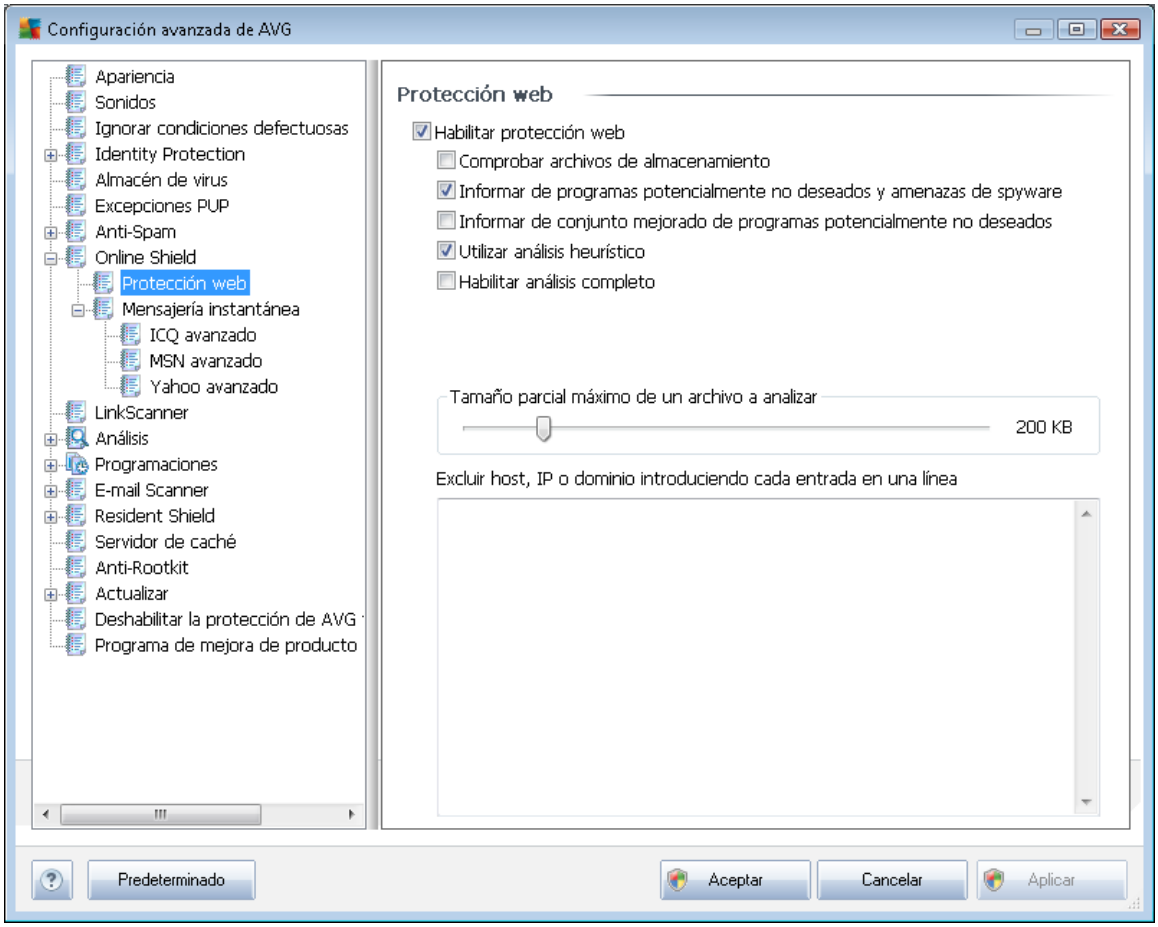
El cuadro de diálogo ***Online Shield*** permite activar o desactivar el componente ***Online Shield*** al completo a través de la opción ***Habilitar Online Shield*** (*activada de forma predeterminada*). Para continuar con la configuración avanzada de este componente, vaya a los siguientes cuadros de dialogo según se incluyen en el árbol de navegación:

- ***Protección web***
- ***Mensajería instantánea***

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.

9.8.1. Protección web



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 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 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.

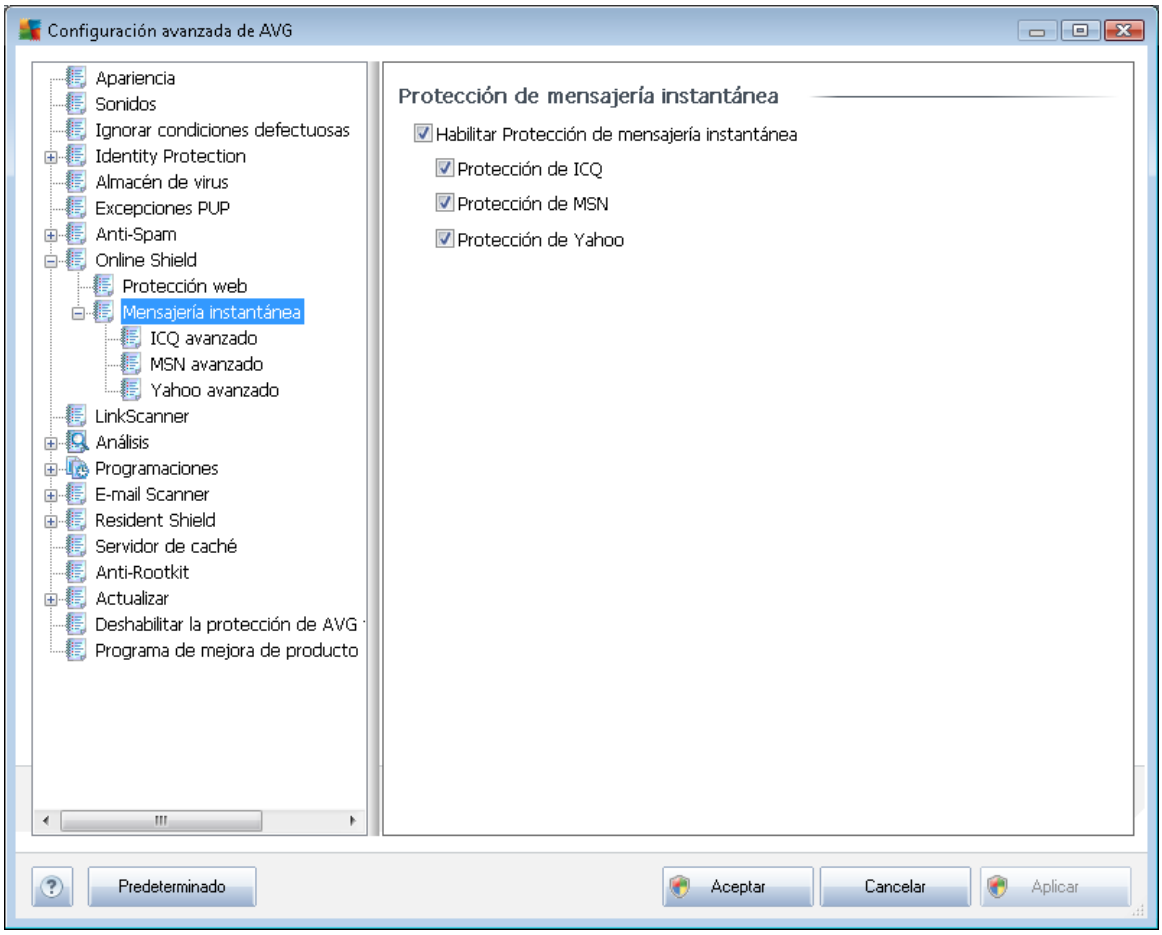
- ***Utilizar análisis heurístico*** (*activada de forma predeterminada*): al marcar esta opción, se analiza el contenido de la página que se va a mostrar utilizando el método de análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en el entorno de un equipo virtual*).

- ***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.

9.8.2. Mensajería instantánea

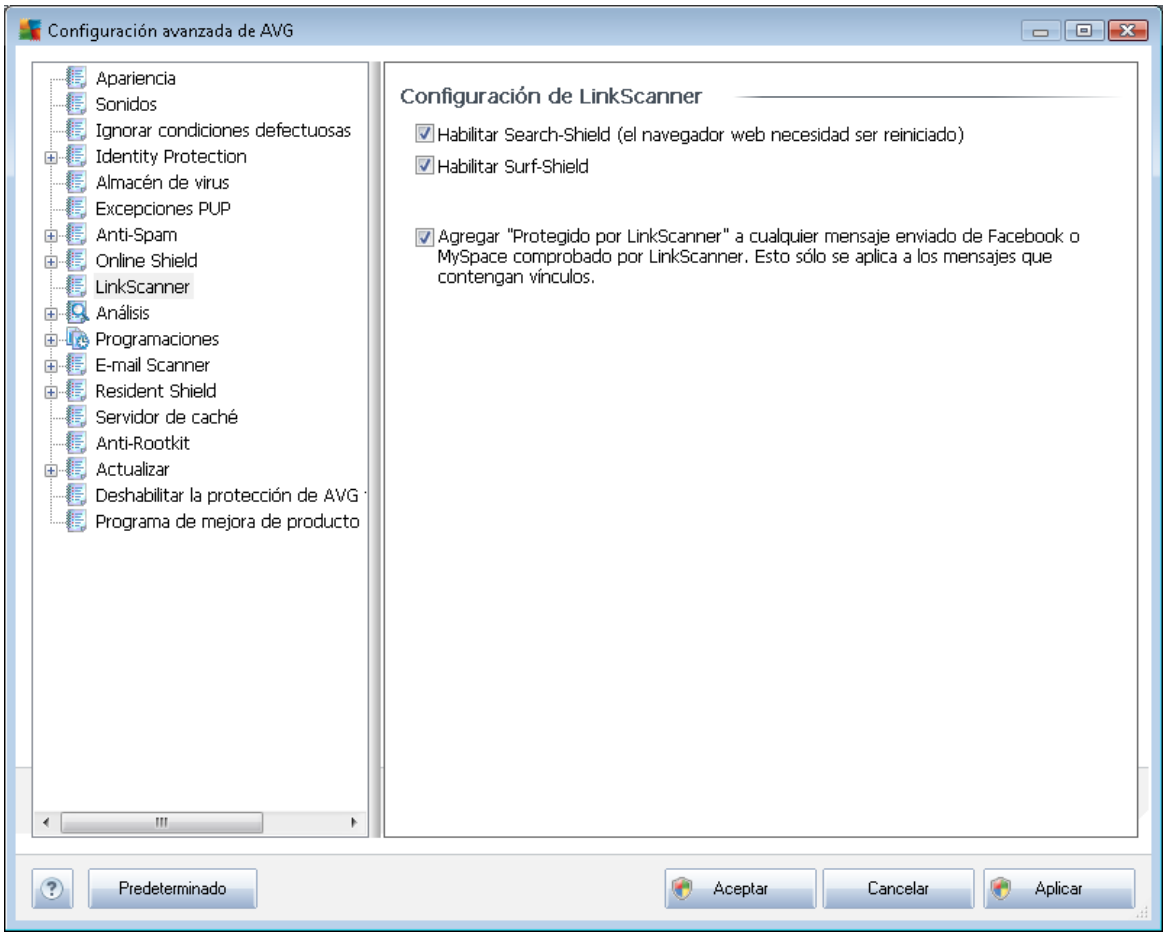


En el cuadro de diálogo ***Protección de mensajería instantánea***, puede editar la configuración de los componentes de ***Online Shield*** relativa al análisis de mensajería instantánea. Actualmente son compatibles los siguientes tres programas de mensajería instantánea: ***ICQ***, ***MSN*** y ***Yahoo***; marque el elemento correspondiente a cada uno de ellos si desea que ***Online Shield*** compruebe que la comunicación en línea está libre de virus.

Para indicar los usuarios permitidos o bloqueados, puede visualizar y editar el correspondiente cuadro de diálogo (***ICQ avanzado***, ***MSN avanzado, Yahoo avanzado***) y especificar la ***Lista blanca*** (*lista de usuarios autorizados para comunicarse con usted*) y la ***Lista negra*** (*usuarios que se deben bloquear*).

9.9. 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'...***: marque este elemento para confirmar que desea agregar el aviso que certifica que se ha comprobado con *LinkScanner* a todos los mensajes con hipervínculos que se envíen desde las redes sociales Facebook y MySpace.

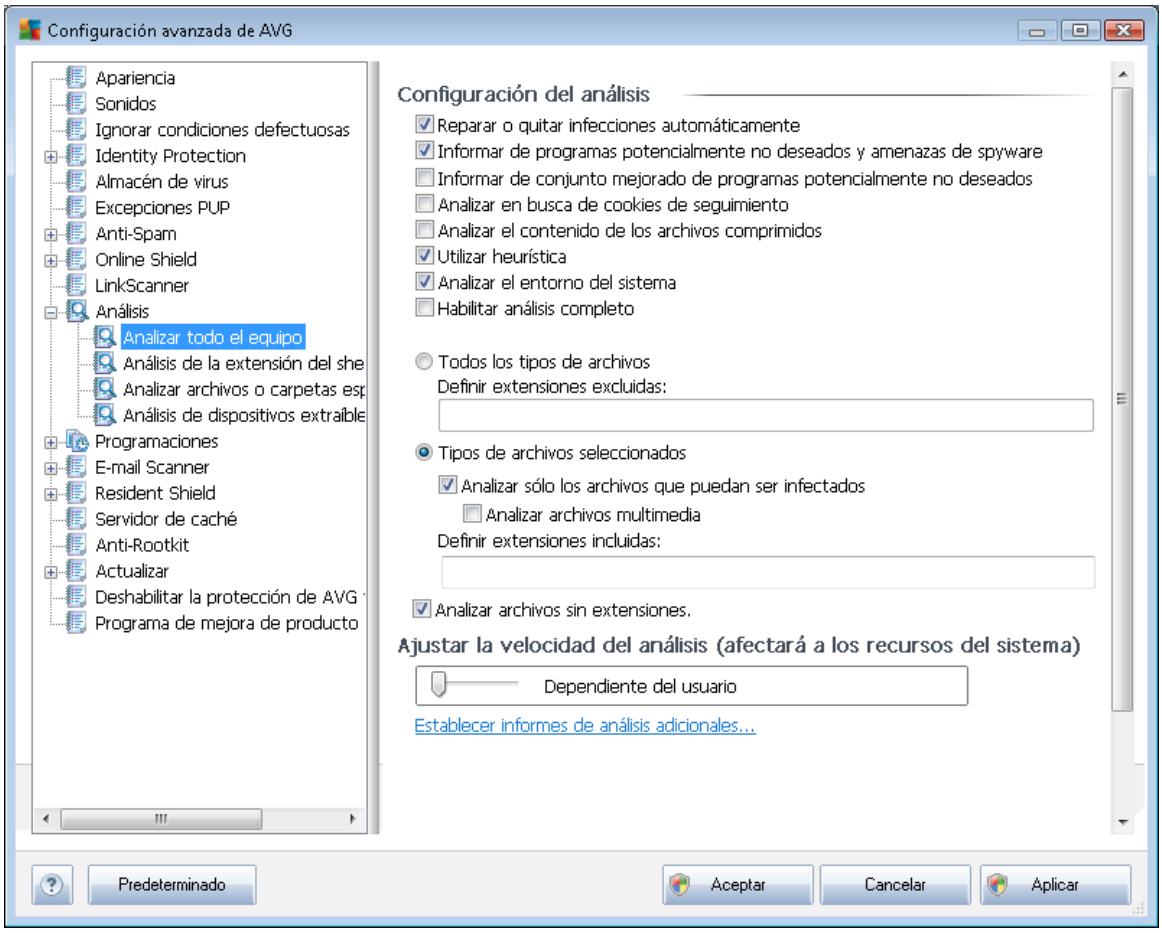
9.10. Análisis

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
- ***Analizar 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

9.10.1. Analizar todo el equipo

La opción ***Análisis del equipo completo*** permite editar los parámetros de uno de los análisis predefinidos por el proveedor 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.

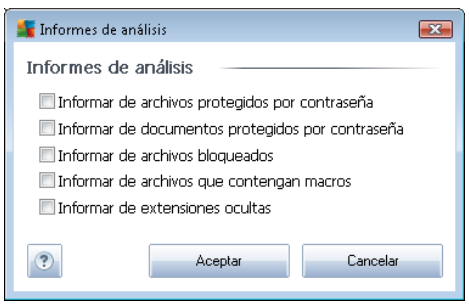
- Opcionalmente, puede indicar que desea ***Analizar archivos sin extensiones***: esta opción está activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

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.

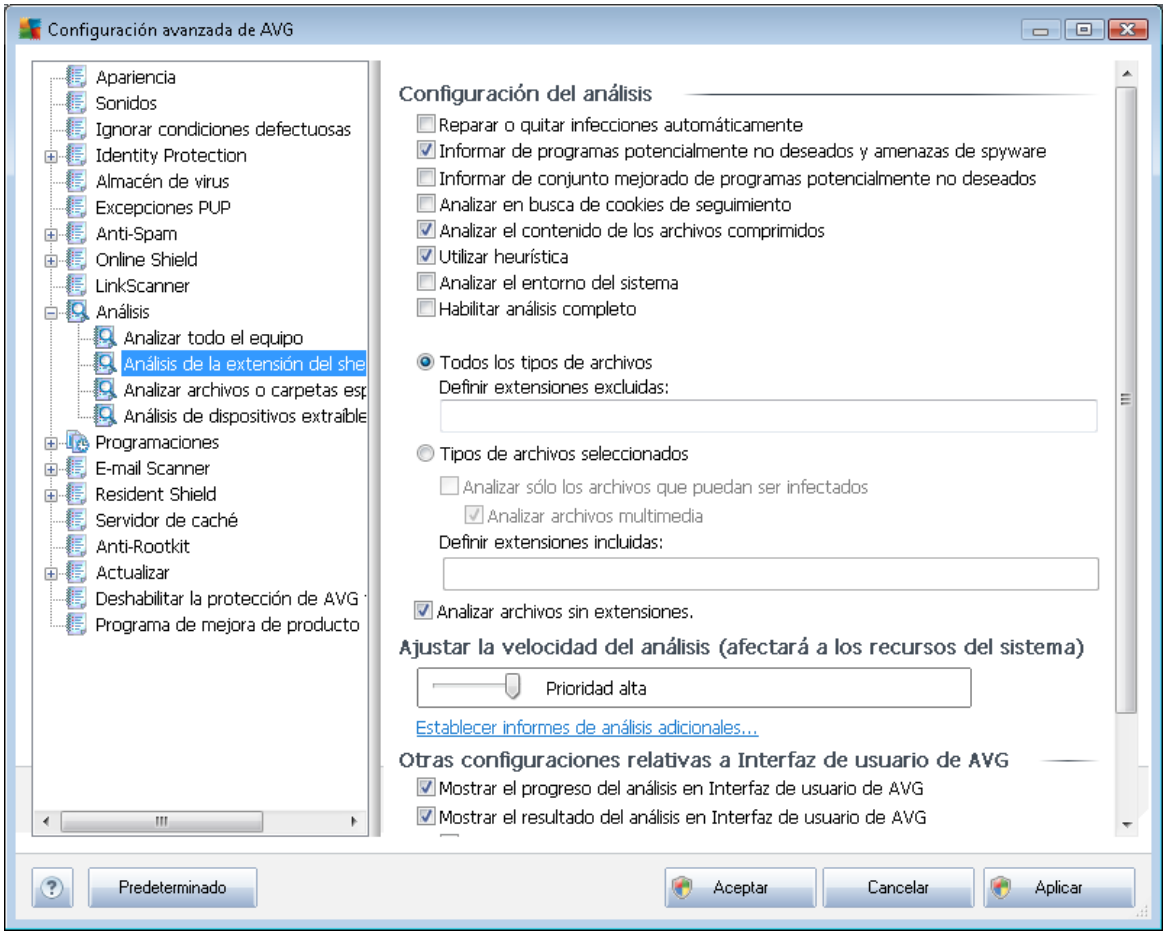
Establecer informes de análisis adicionales...

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:



9.10.2. 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***:



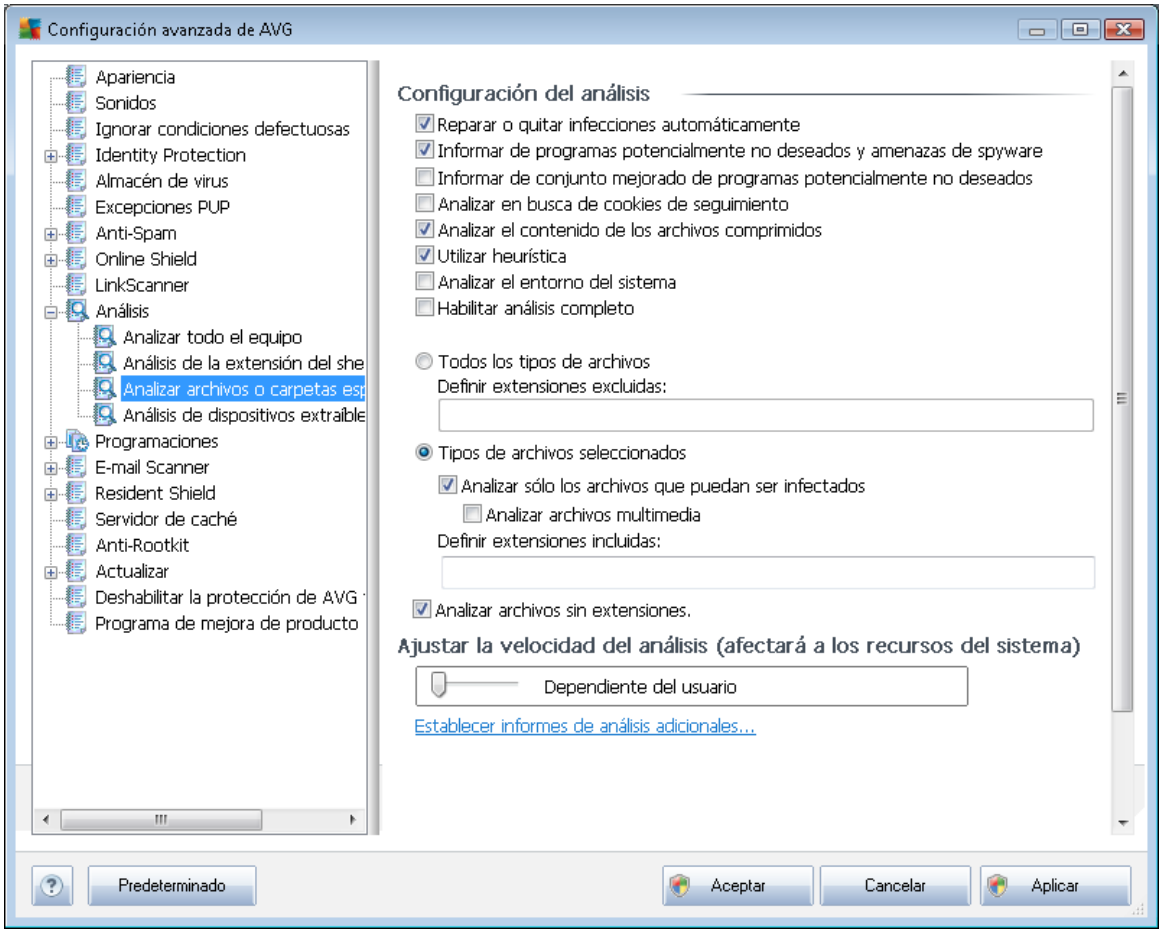
La lista de parámetros es idéntica a la que incluye el ***Análisis del equipo completo***. Sin embargo, la configuración predeterminada es distinta (*por ejemplo, el Análisis del equipo completo no comprueba los archivos comprimidos de manera predeterminada, pero sí que analiza el entorno del sistema,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

A diferencia del cuadro de diálogo ***Análisis del equipo completo*****, el** cuadro de diálogo ***Análisis de la extensión del shell*** también incluye la sección llamada ***Otras configuraciones relativas a Interfaz de usuario de AVG***, en la que puede especificar si desea que se puedan consultar el progreso y 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.

9.10.3. Analizar 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***:

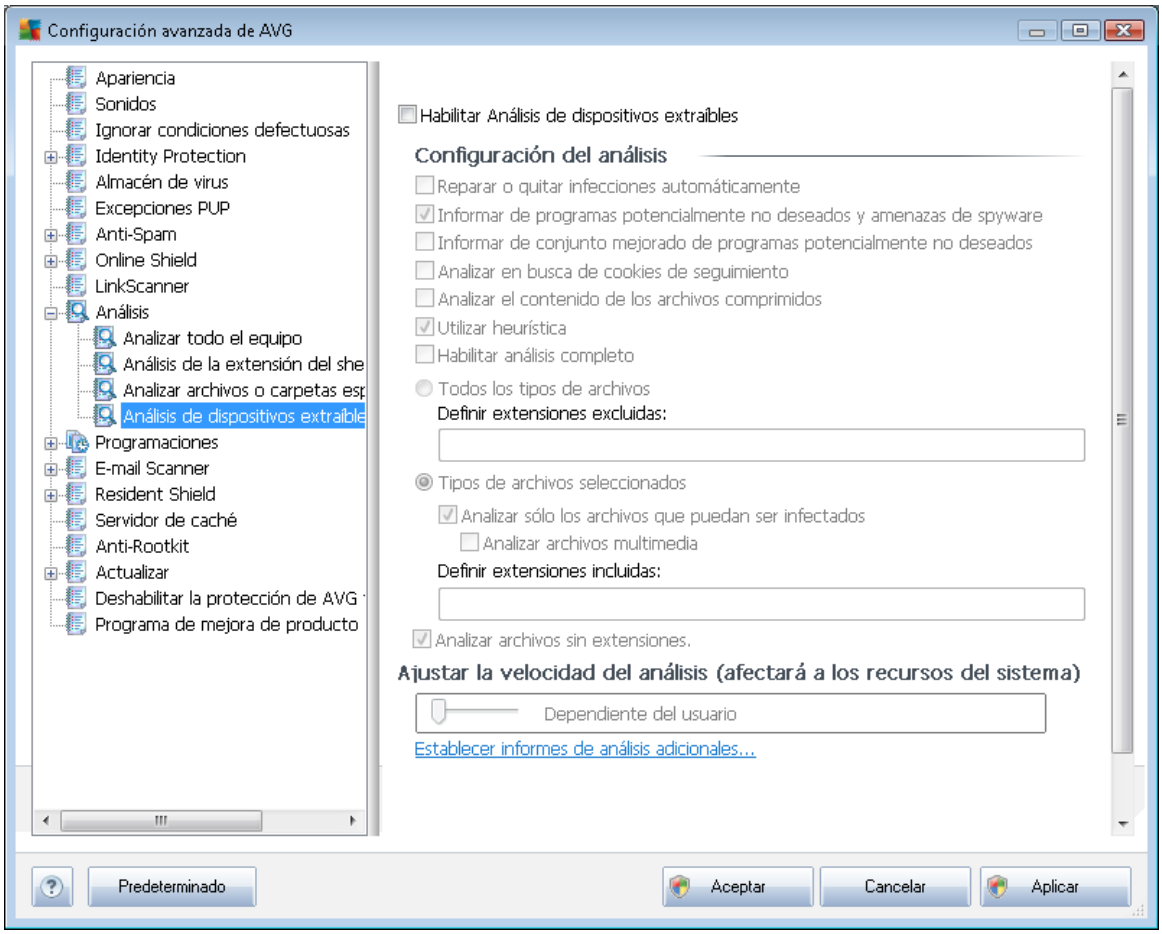


Todos los parámetros definidos en este cuadro de diálogo de configuración se aplican únicamente a las áreas seleccionadas para ser analizadas mediante la opción ***Analizar archivos o carpetas específicos***.

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

9.10.4. 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****.*

9.11. Programaciones

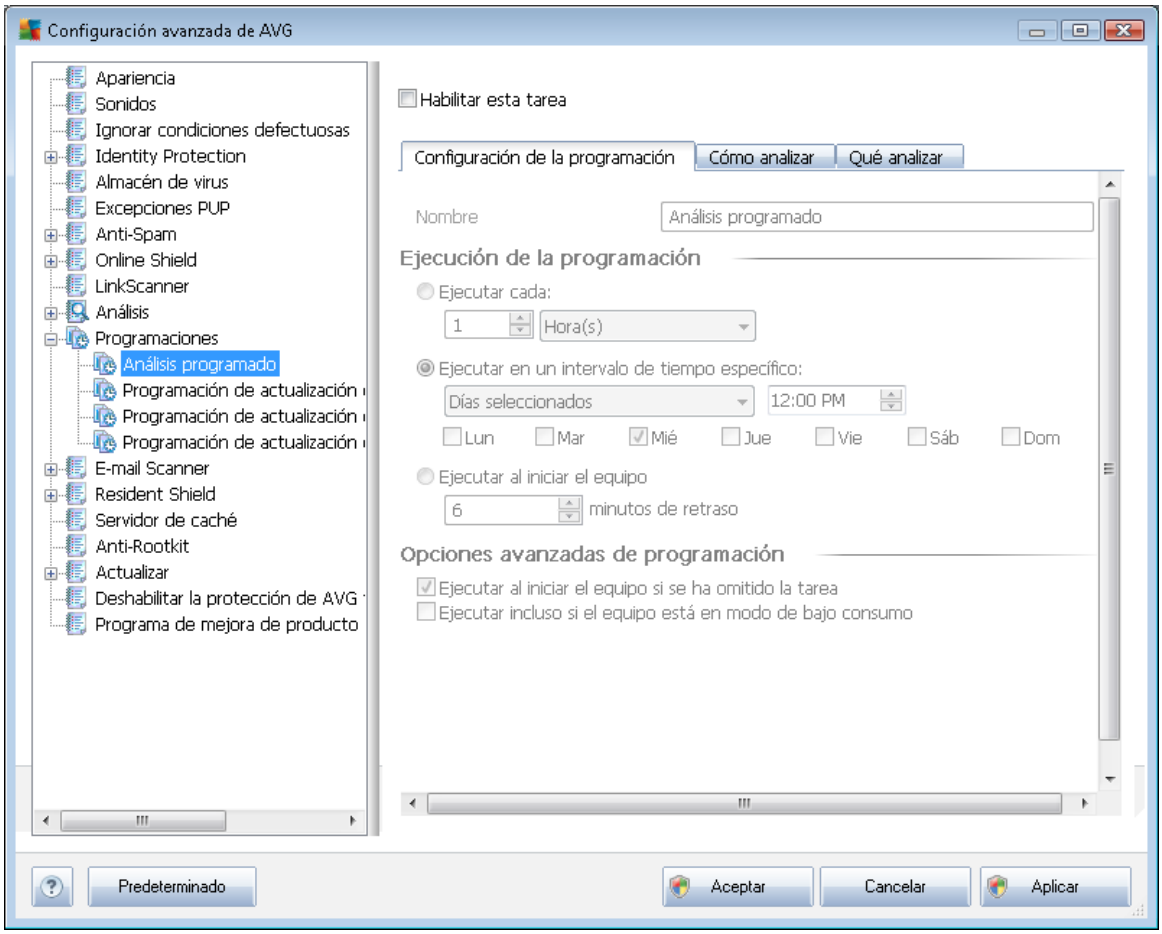
En la sección ***Programaciones*** puede editar la configuración predeterminada de:

- Análisis programado

- Programación de actualización de la base de datos de virus
- Programación de actualización del programa
- Programación de actualización de Anti-Spam

9.11.1. Análisis programado

Es posible editar los parámetros del análisis programado (*o configurar una nueva programación*) en tres fichas. En cada ficha puede primero marcar o no 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:

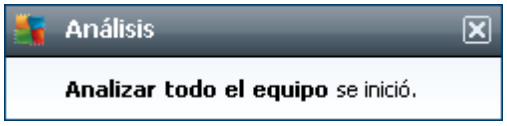
Ejecución de la programación

En esta sección puede especificar los intervalos de tiempo para el inicio del análisis que acaba de programar. Los intervalos 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***.

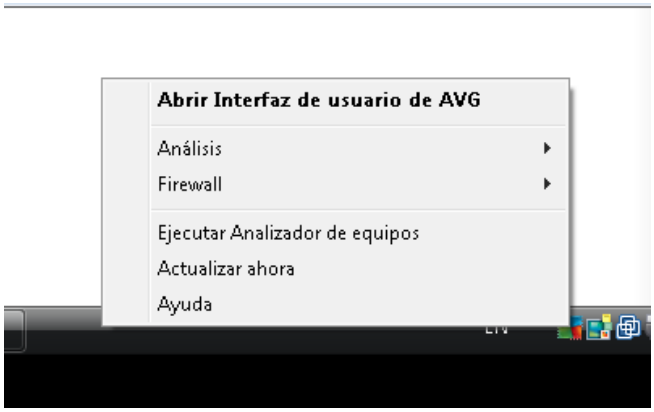
Opciones avanzadas de programación

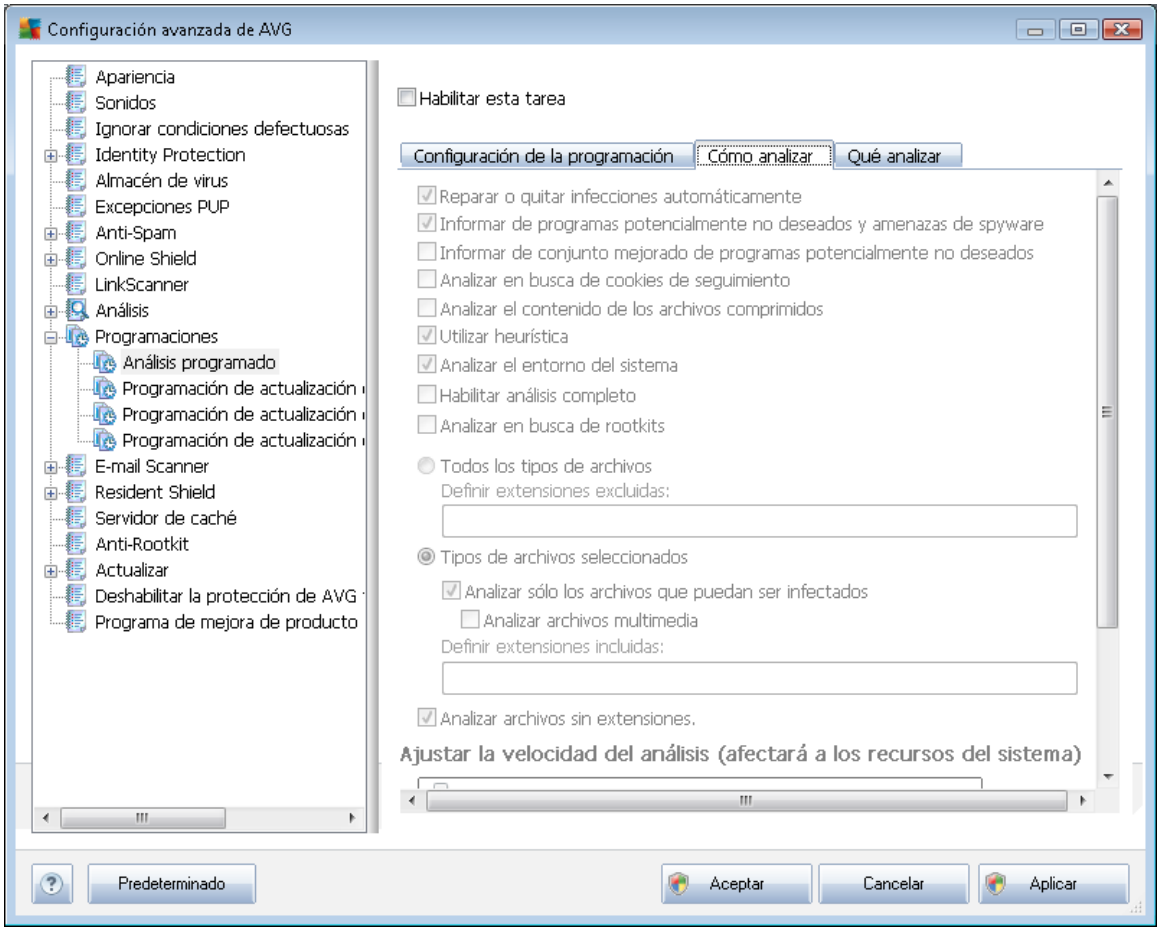
Esta sección permite definir bajo qué condiciones deberá iniciarse o no el análisis si el equipo está en modo de bajo consumo o apagado completamente.

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

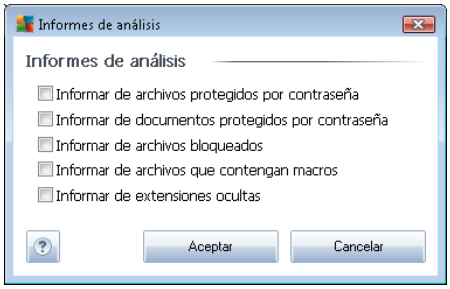
deberían analizarse siempre.

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.

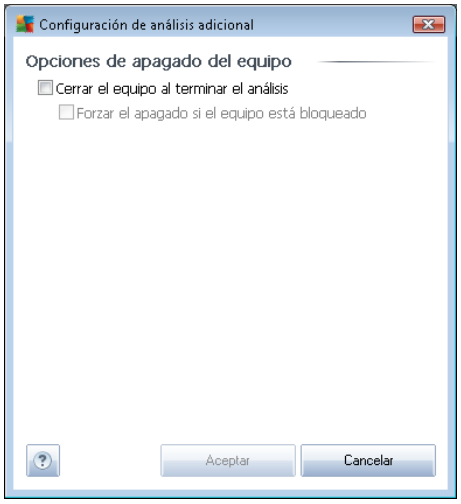
Establecer informes de análisis adicionales

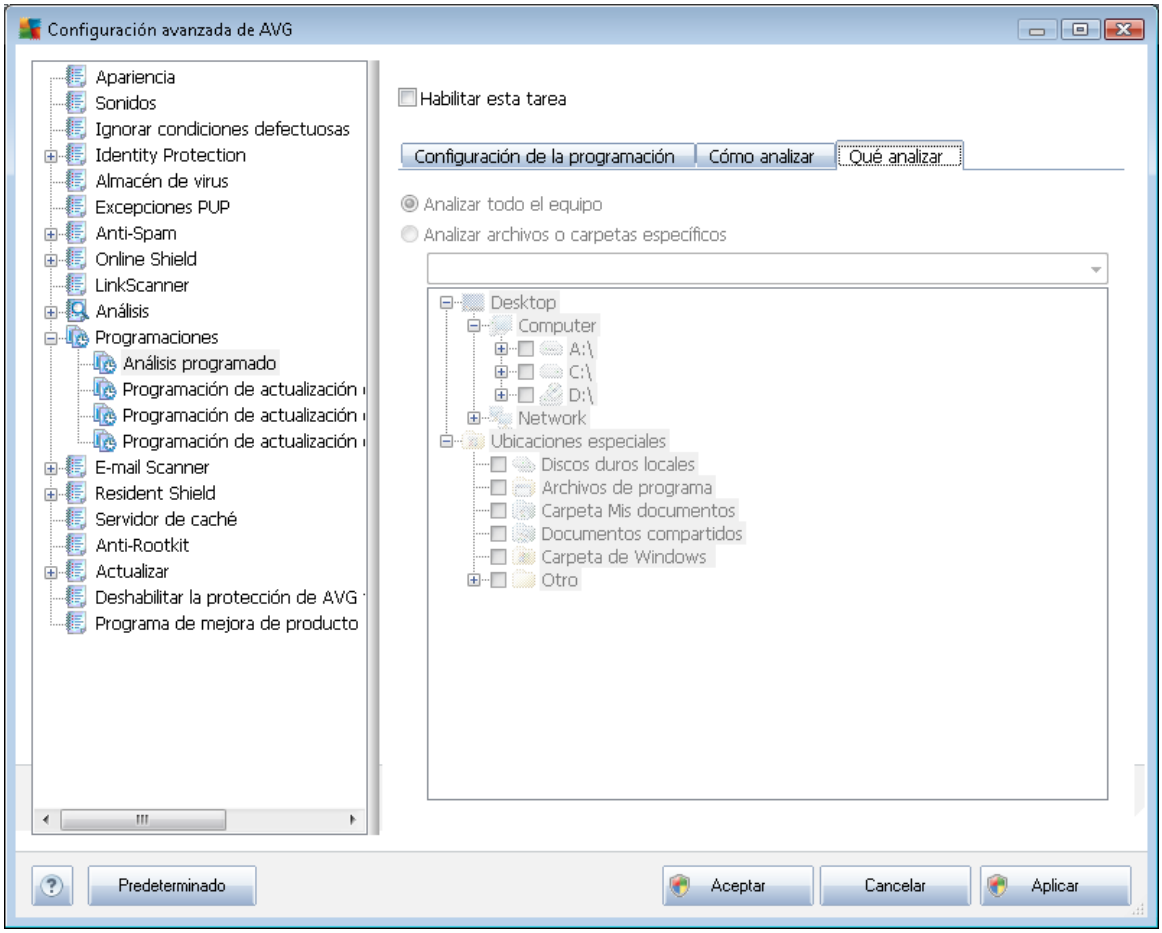
Haga clic en el vínculo ***Establecer informes de análisis adicionales...*** para abrir una nueva ventana de cuadro de diálogo independiente llamada ***Informes de análisis*** en la que puede marcar diferentes elementos para definir qué resultados del análisis deben incluirse en el informe:



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***).



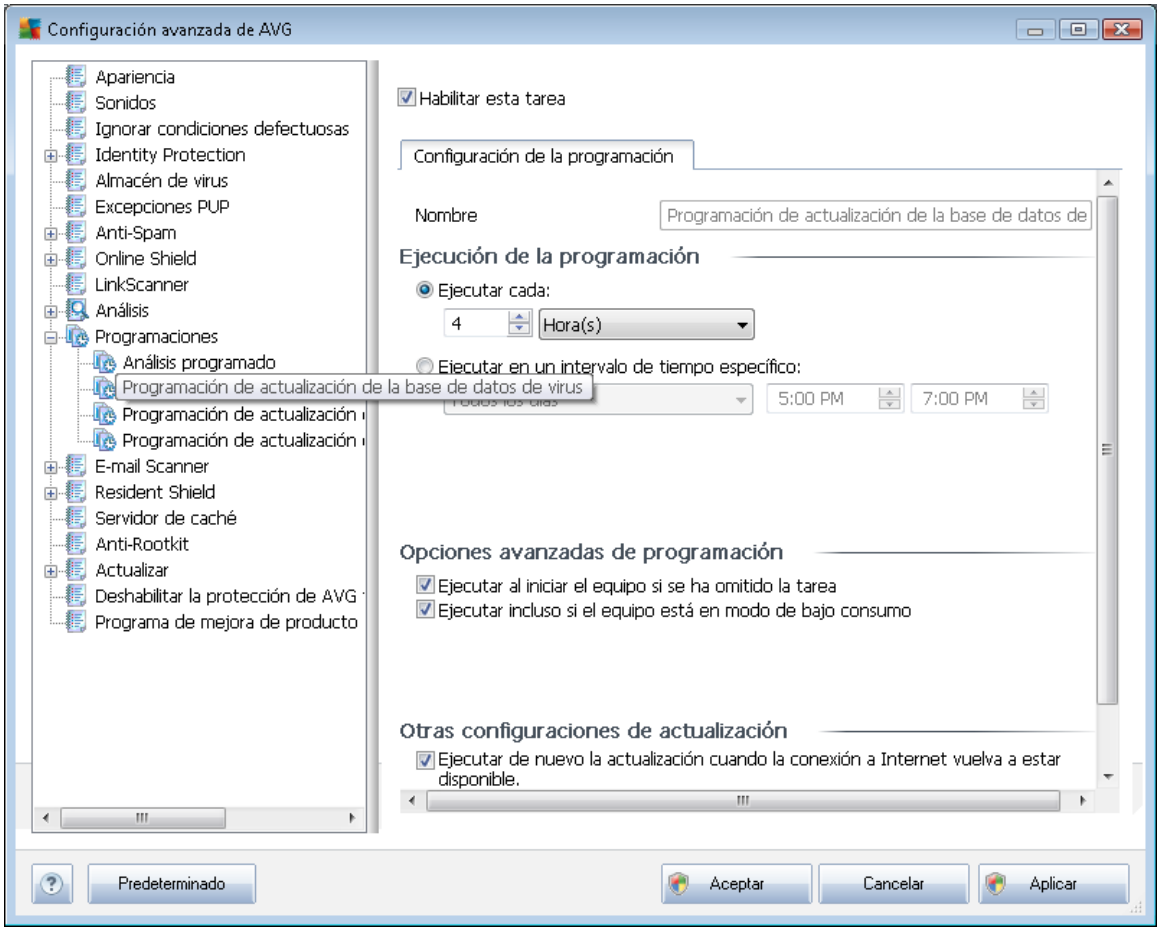


En la ficha ***Qué analizar*** se puede definir si se desea programar el análisis del equipo completo o el análisis de archivos o carpetas específicos. En caso de que se seleccione el análisis de archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activa la estructura de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

mostrada, pudiéndose especificar las carpetas a analizar.

9.11.2. Programación de actualización de la base de datos de virus

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



La programación de actualización básica de la base de datos de virus se incluye dentro del componente ***Administrador de actualizaciones***. En este cuadro de diálogo se pueden configurar algunos parámetros detallados de la programación de actualización de la base de datos de virus. 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 la base de datos de virus 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 permite definir bajo qué condiciones deberá iniciarse o no la actualización de la base de datos de virus si el equipo está en modo de bajo consumo o apagado completamente.

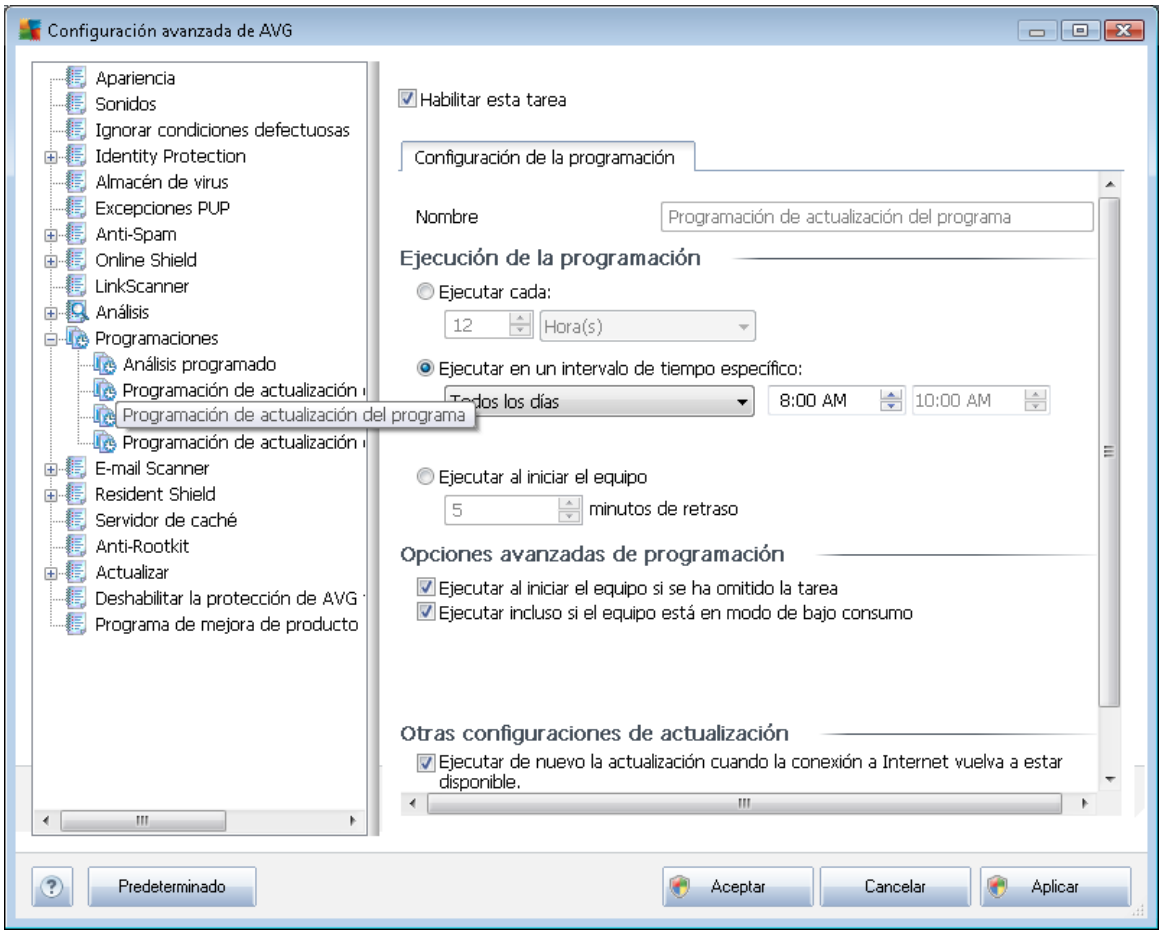
Otras configuraciones de actualización

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***).

9.11.3. 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

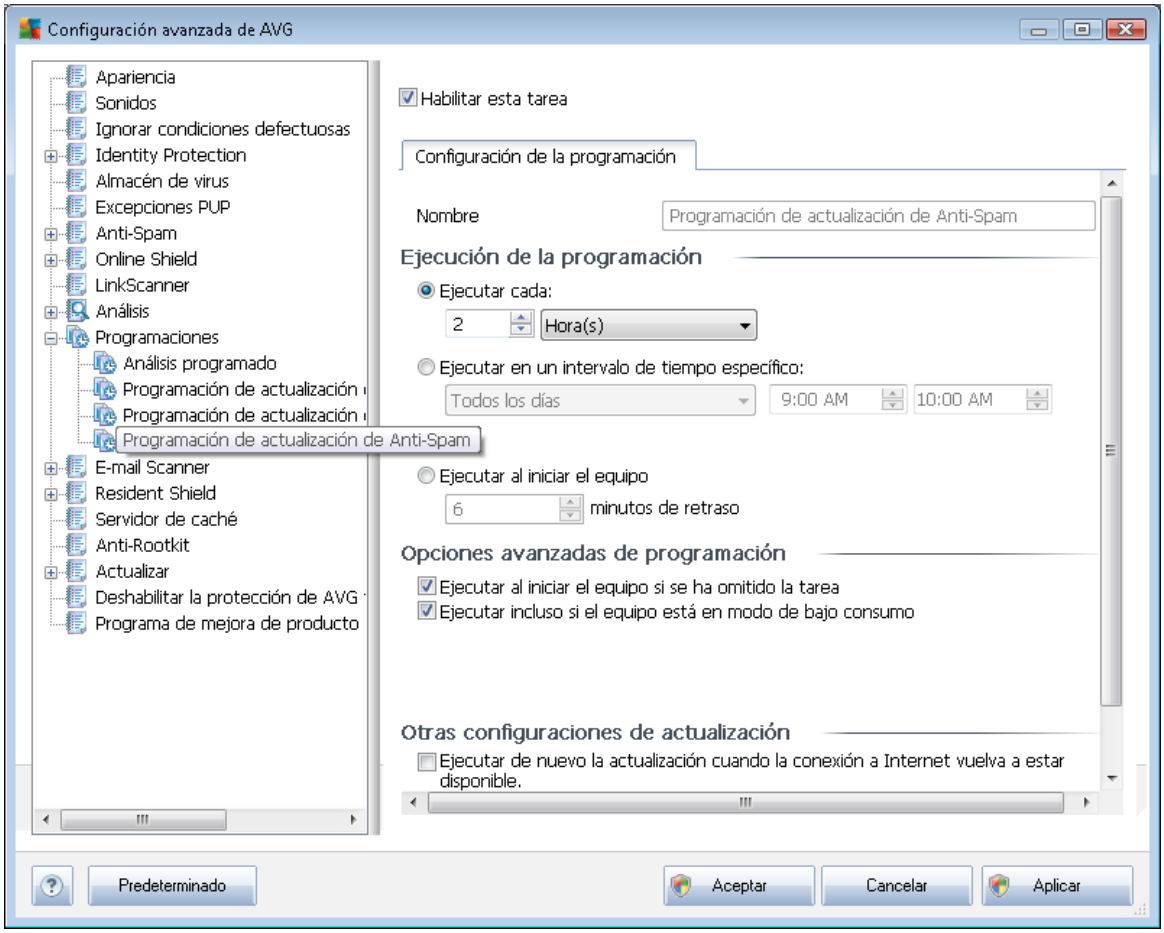
Marque la opción ***Ejecutar de nuevo la actualización cuando la conexión a Internet vuelva a estar disponible*** para asegurarse de que si la conexión a Internet se interrumpe y falla el proceso de actualización, se iniciará automáticamente de nuevo cuando la conexión de Internet se restablezca.

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 AVG en la bandeja del sistema (*siempre que haya mantenido la configuración predeterminada en el 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.*

9.11.4. Programación de actualización de Anti-Spam

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



La programación de actualización básica ***de Anti-Spam*** se incluye dentro del componente ***Administrador de actualizaciones***. 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

En esta sección, 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 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 de ***Anti-Spam*** si el equipo está en modo de bajo consumo o apagado completamente.

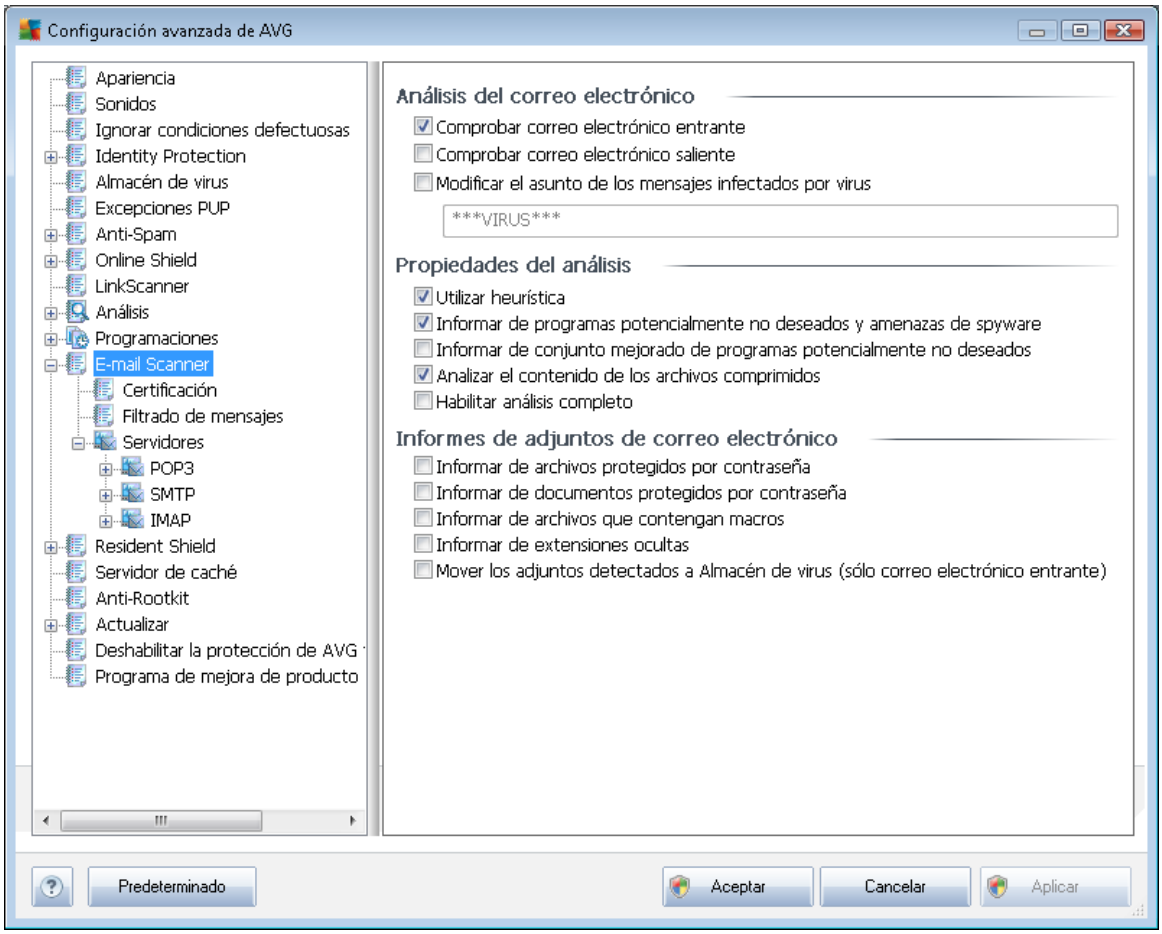
Otras configuraciones de actualización

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 AVG en la bandeja del sistema (*siempre que haya mantenido la configuración predeterminada del cuadro de diálogo **Configuración avanzada/Apariencia***).

9.12. 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.

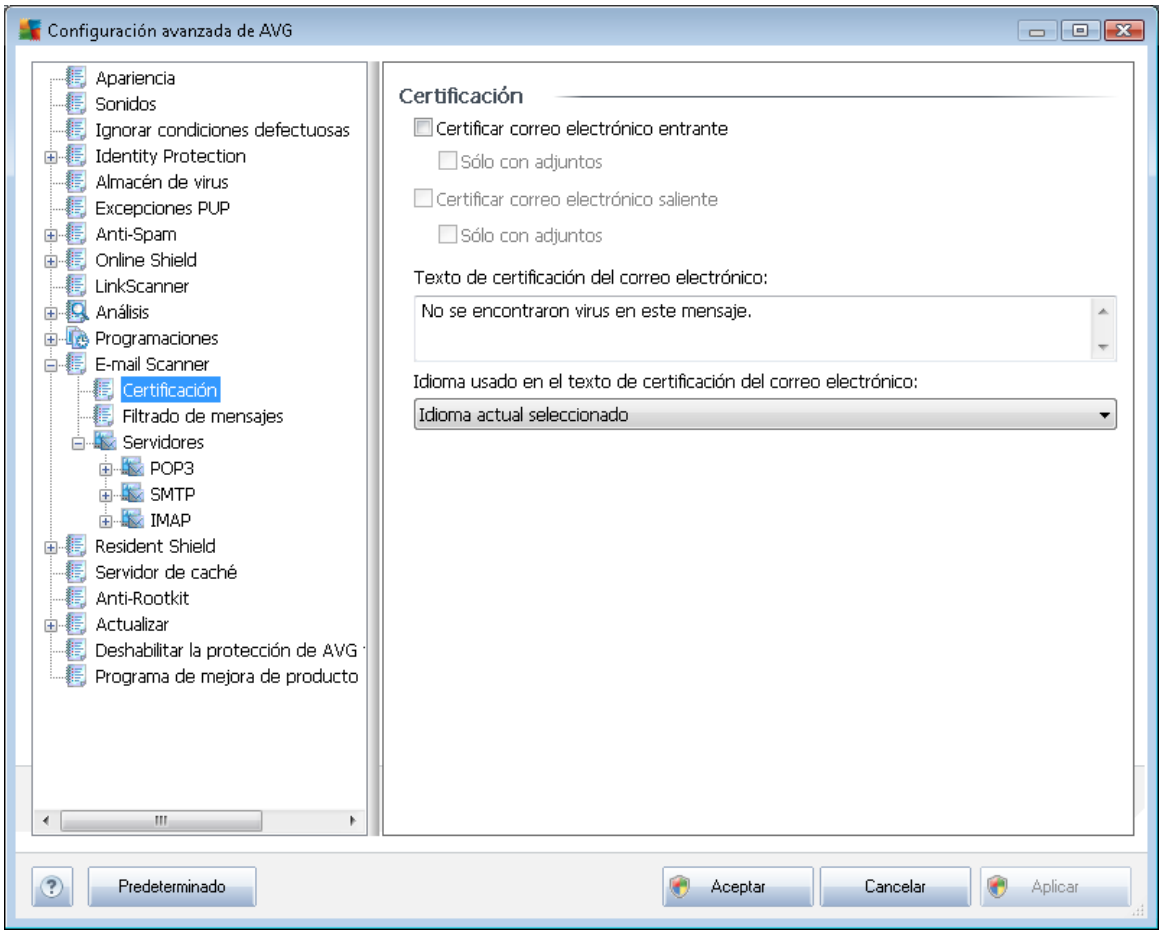
Informes de adjuntos de correo electrónico

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***.

9.12.1. Certificación

En el cuadro de diálogo ***Certificación*** puede especificar el texto y el idioma de certificación tanto para el correo entrante como para el correo saliente:



El texto de certificación consta de dos partes, la parte del usuario y la parte del sistema; en el siguiente ejemplo, la primera línea representa la parte del usuario y el resto se genera automáticamente:

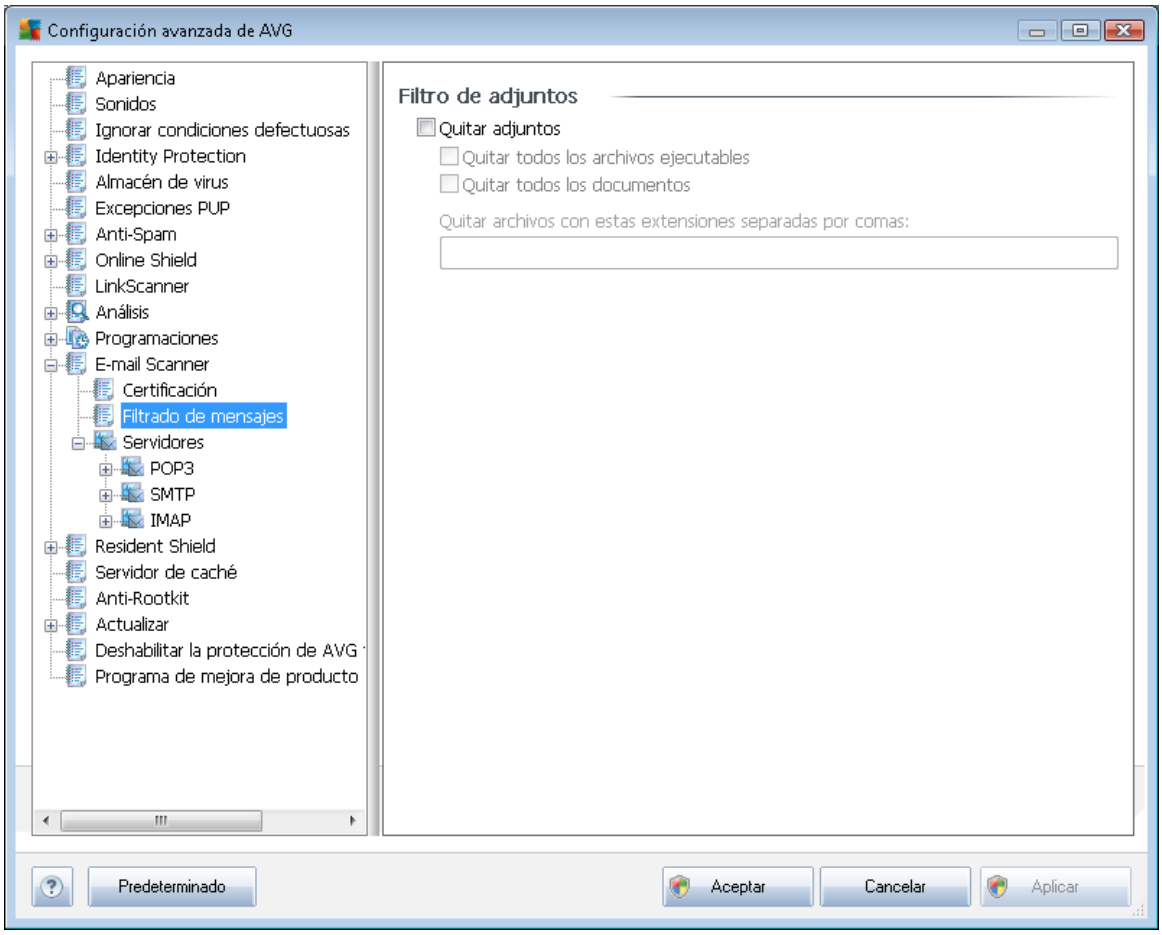
No se encontraron virus en este mensaje.

Comprobado por AVG.

Versión: x.y.zz / Base de datos de virus: xx.y.z - Fecha de publicación: 12/9/2010

Si decide utilizar la certificación de los mensajes de correo electrónico entrantes o salientes, en este cuadro de diálogo puede especificar las palabras exactas de la parte del usuario del texto de certificación (***Texto de certificación del correo electrónico***) y elegir el idioma a utilizar para la parte de la certificación correspondiente al sistema que se genera automáticamente (***Idioma usado en el texto de certificación del correo electrónico***).

9.12.2. Filtrado de mensajes

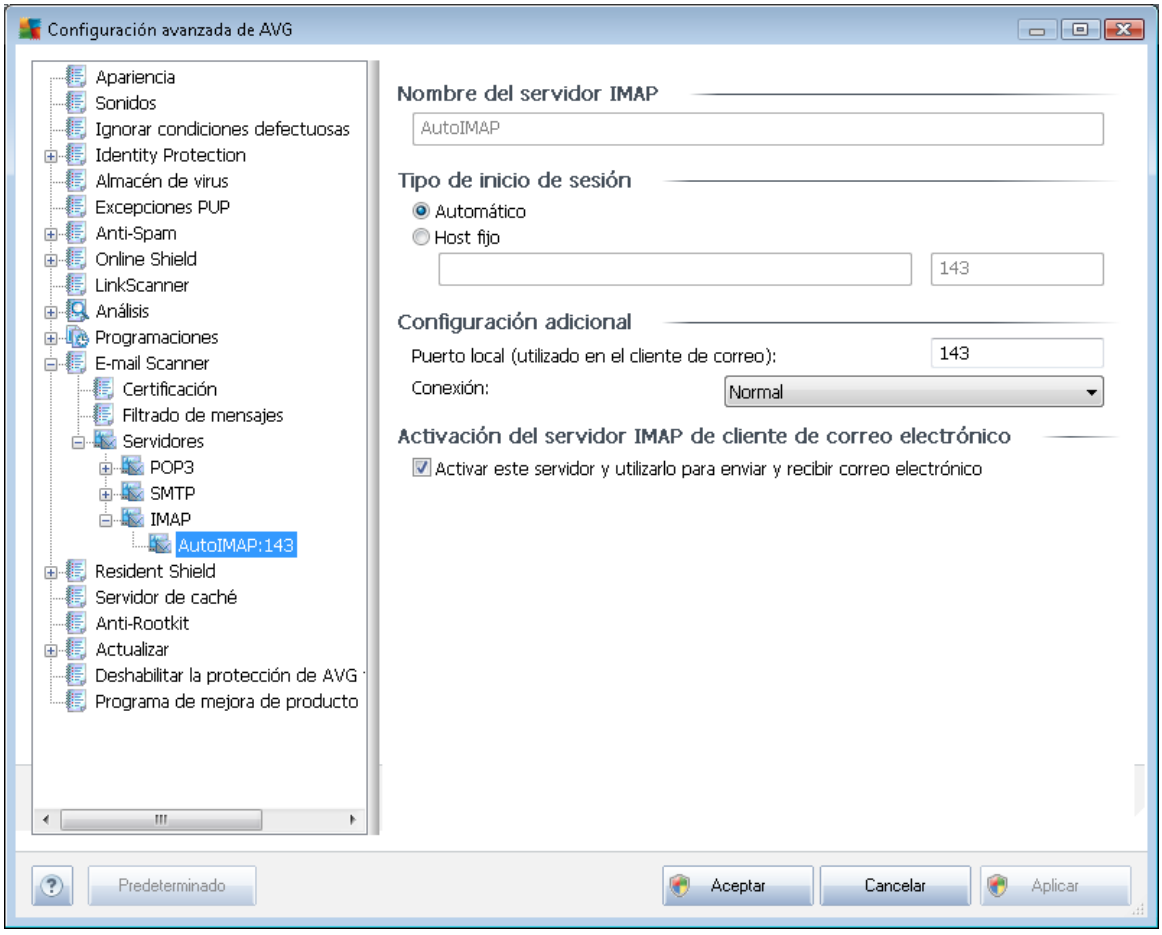


En el cuadro de diálogo ***Filtro de adjuntos***, puede configurar parámetros que se utilizarán para analizar los adjuntos a los mensajes de correo electrónico. De manera predeterminada, la opción ***Quitar adjuntos*** se encuentra desactivada. Si decide activarla, todos los adjuntos a los mensajes de 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

9.12.3. Servidores

En la sección ***Servidores***, puede editar parámetros de los servidores del componente ***Analizador de correo electrónico*** o configurar un nuevo servidor utilizando el 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

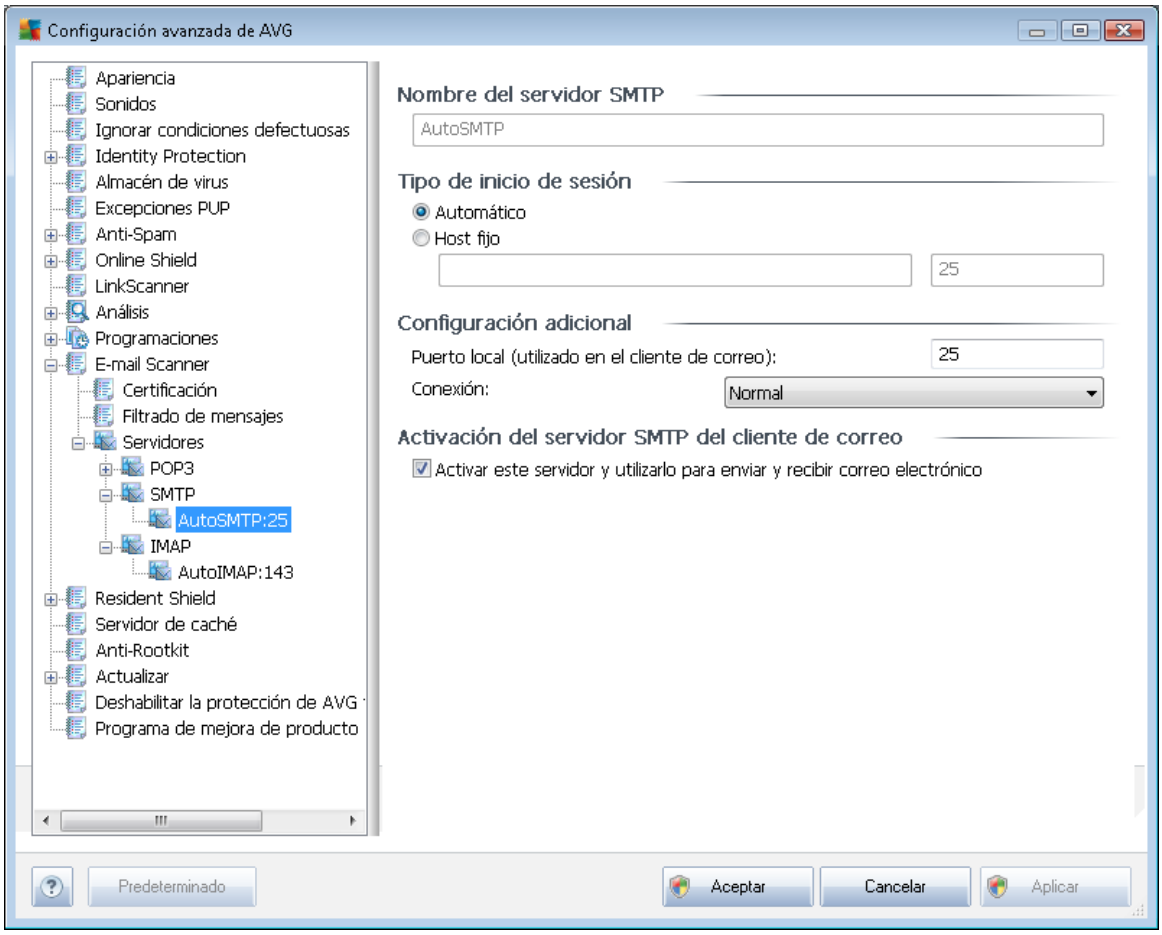
después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, pop.acme.com:8200*). El puerto estándar para las comunicaciones POP3 es el 110.

- ***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

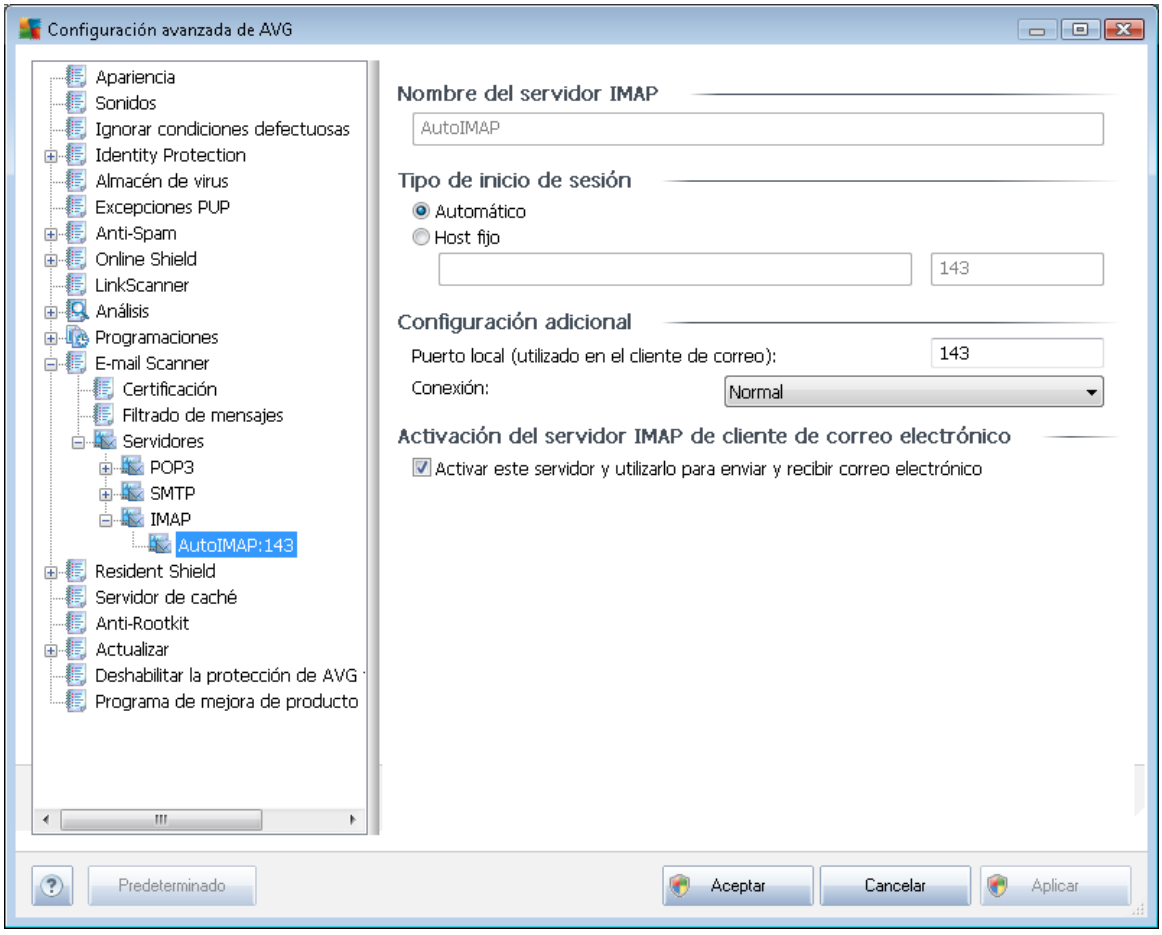
    - ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. Como nombre puede usar un nombre de dominio (*por ejemplo, smtp.acme.com*) o una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo 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

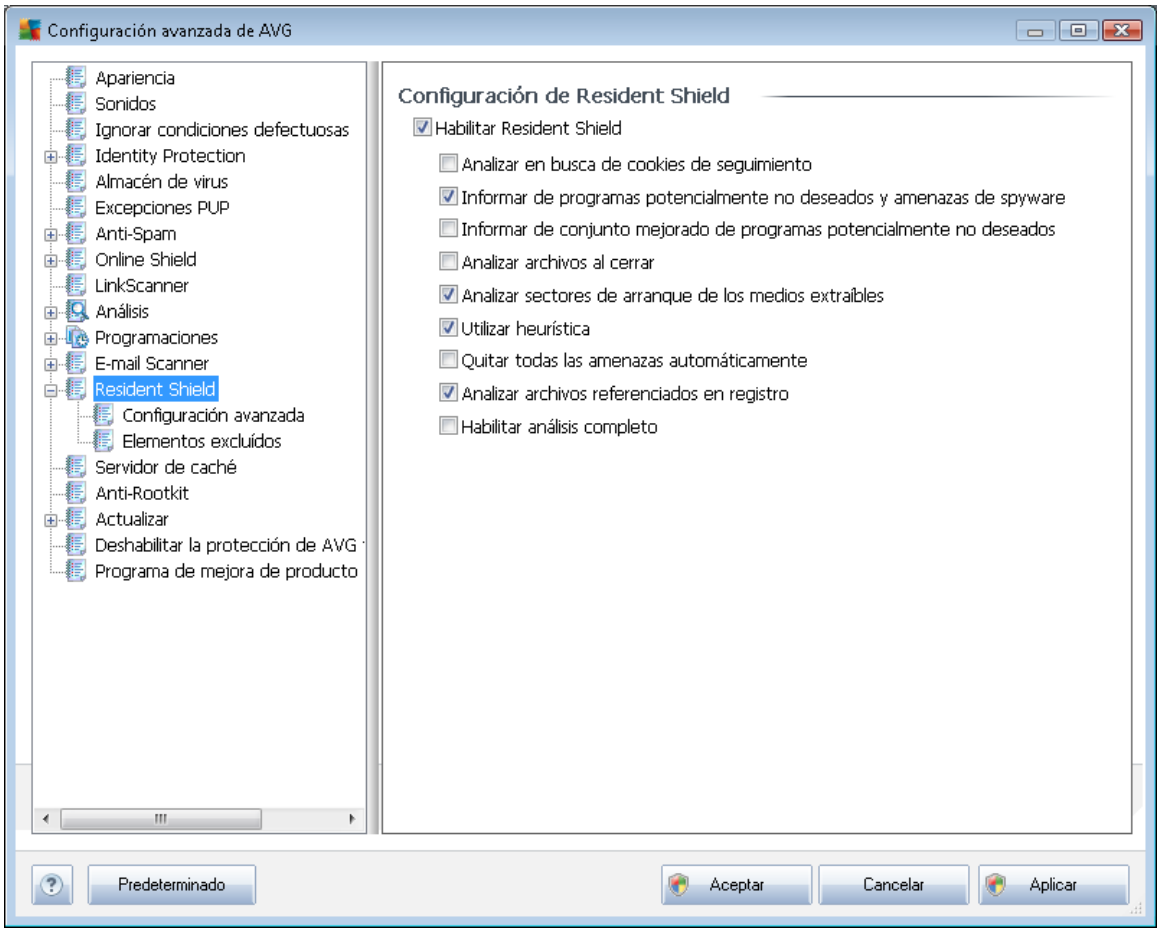
    - ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. Como nombre puede usar un nombre de dominio (*por ejemplo, smtp.acme.com*) o una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo 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:
  - o ***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.
  - o ***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

9.13. Protección residente

El componente ***Protección residente*** protege en tiempo real los archivos y carpetas contra virus, spyware y otro software malicioso.



En el cuadro de diálogo ***Configuración de Protección residente***, puede activar o desactivar

completamente la ***Protección residente*** marcando o dejando en blanco el elemento ***Habilitar Protección residente*** (*esta opción se encuentra activada de manera predeterminada*). Además puede seleccionar las características de ***Protección residente*** que deben activarse:

- ***Analizar en busca de cookies de seguimiento*** (*desactivado de forma predeterminada*): este parámetro establece que el análisis debe detectar las cookies. (*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 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 archivos al cerrar*** (*desactivado de forma predeterminada*): realizar un análisis al cerrar garantiza que AVG analizará los objetos activos (por ejemplo, aplicaciones, documentos, etc.) cuando se abran y también cuando se cierren. Esta característica ayuda a proteger el equipo contra ciertos tipos de virus sofisticados

- ***Analizar sectores de arranque de los medios extraíbles*** (*activado de forma predeterminada*)

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

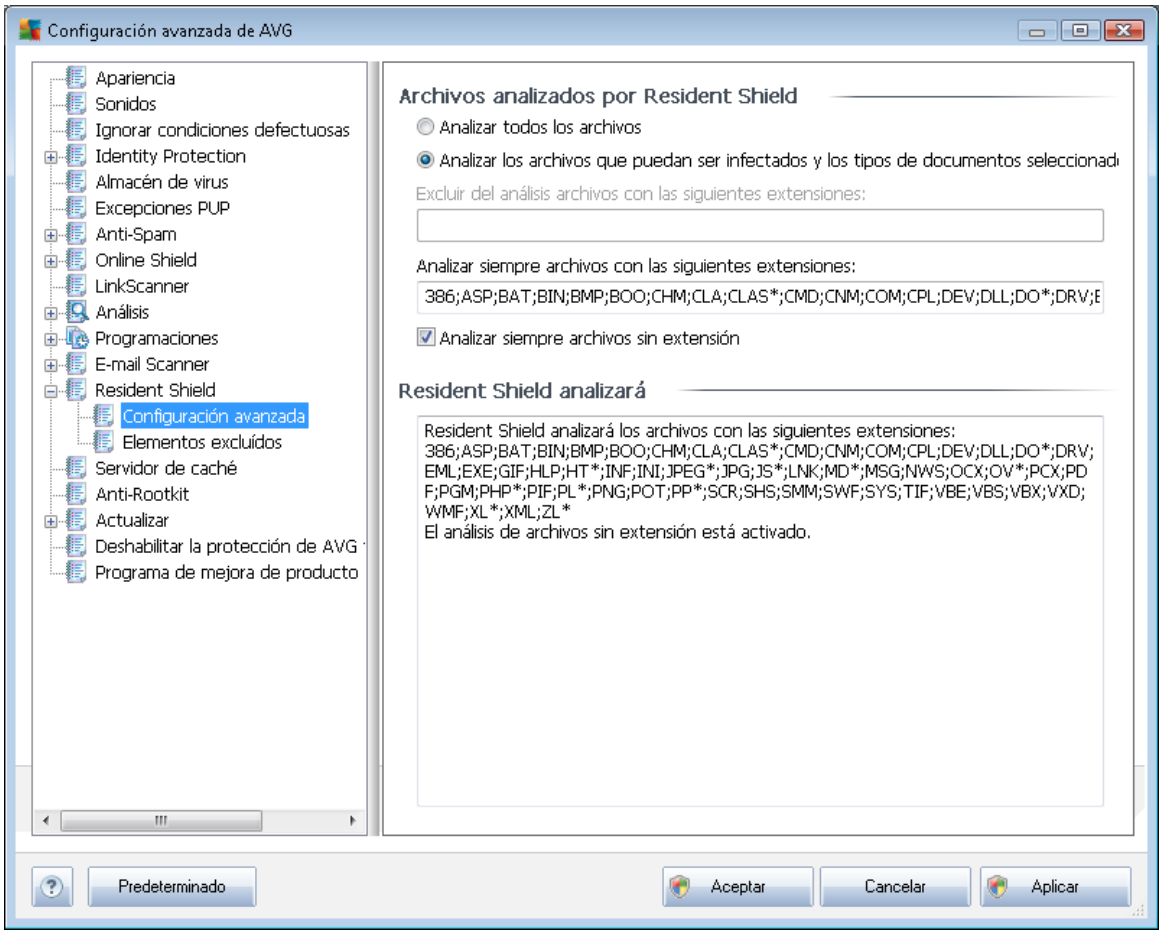
- ***Quitar todas las amenazas automáticamente*** (*desactivado de forma predeterminada*): toda infección detectada se reparará automáticamente si es posible hacerlo o, si no se puede reparar, se eliminará.

- ***Analizar archivos referenciados en el Registro*** (*activado de forma 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*** (*desactivado de forma predeterminada*): en situaciones específicas (*en un estado de emergencia extrema*), puede marcar esta opción para que se activen los algoritmos más detallados que analizarán en profundidad todos los objetos que suponen una posible amenaza. Recuerde, sin embargo, que este método tiene una duración considerable.

9.13.1. Configuración avanzada

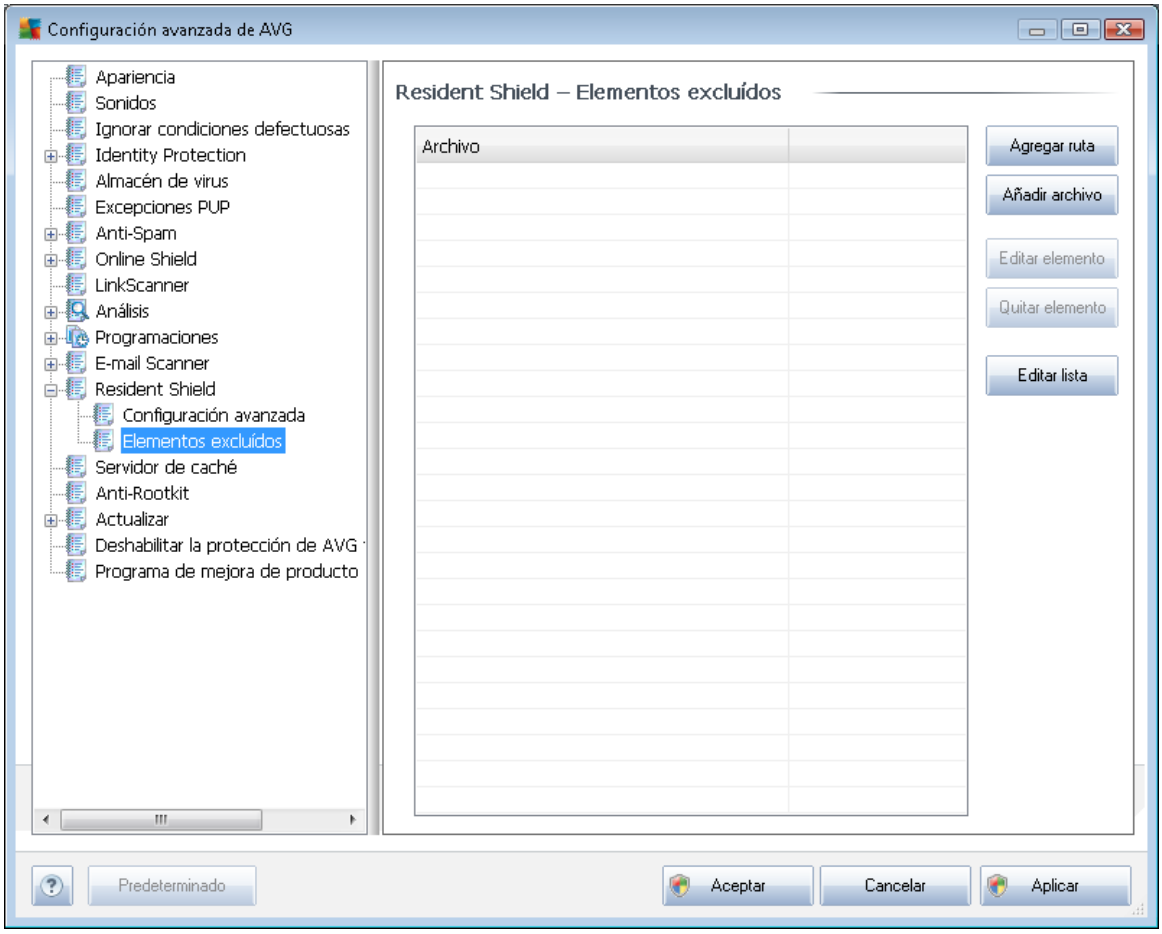
En el cuadro de diálogo ***Archivos analizados por Protección residente*** se pueden configurar los archivos a analizar (*por extensiones específicas*):



Decida si desea analizar todos los archivos o solamente los que puedan ser infectados; en tal caso, puede especificar una lista de extensiones que definan los archivos que deben excluirse del análisis y también una lista de extensiones de archivo que definan los archivos que deben analizarse 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.

9.13.2. Elementos excluidos



El cuadro de diálogo ***Protección residente - Elementos excluidos*** ofrece la posibilidad de definir los archivos y/o carpetas que deben excluirse del análisis de ***Protección residente***.

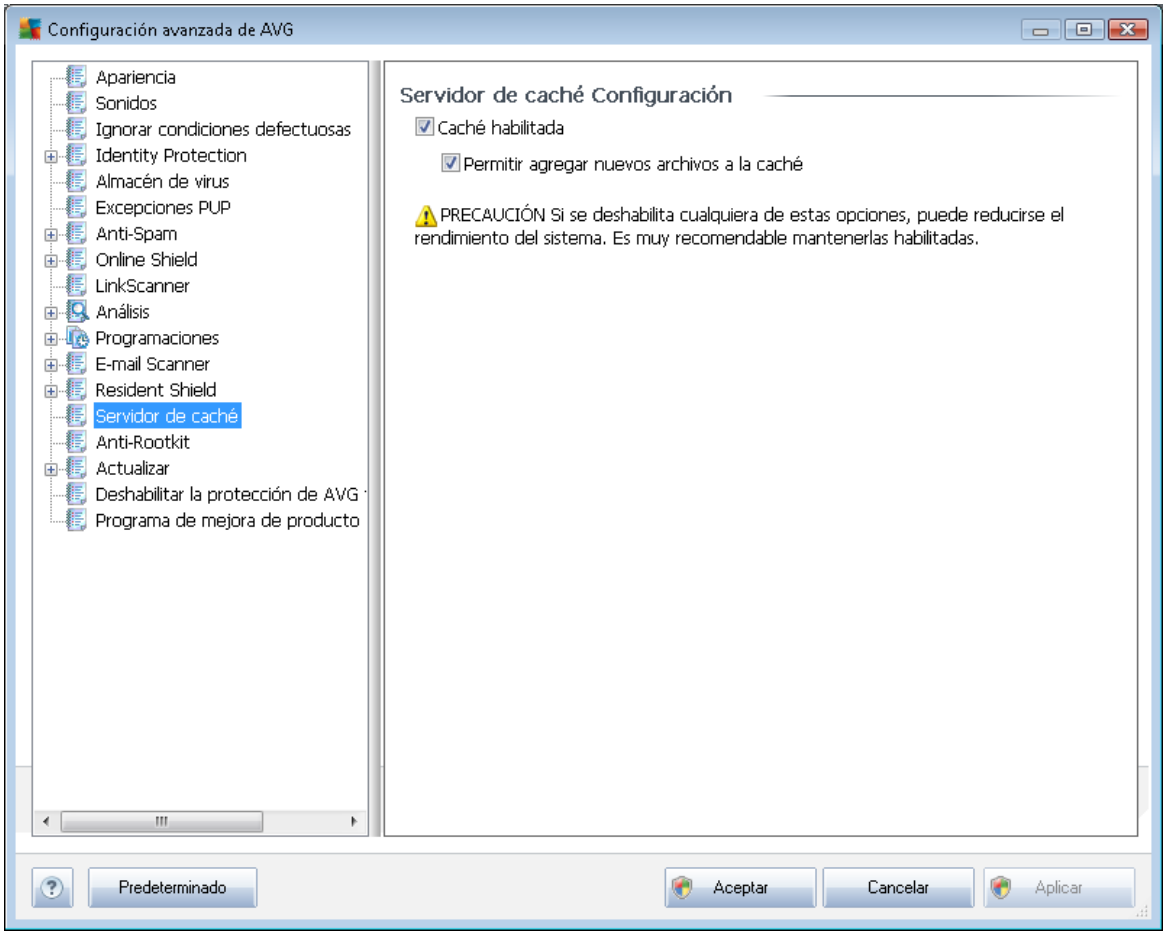
Si no es esencial, se recomienda encarecidamente no excluir ningún elemento.

El cuadro de diálogo incluye los siguientes botones de control:

- ***Agregar ruta***: especifique 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

9.14. Servidor de caché

El ***Servidor de caché*** es un proceso diseñado para acelerar cualquier tipo de análisis (*análisis bajo demanda, análisis programado de todo el equipo, análisis de Protección residente*). Recopila y guarda información sobre archivos fiables (*archivos del sistema con firma digital, etc.*): esos archivos se considerarán seguros y serán omitidos durante el análisis.



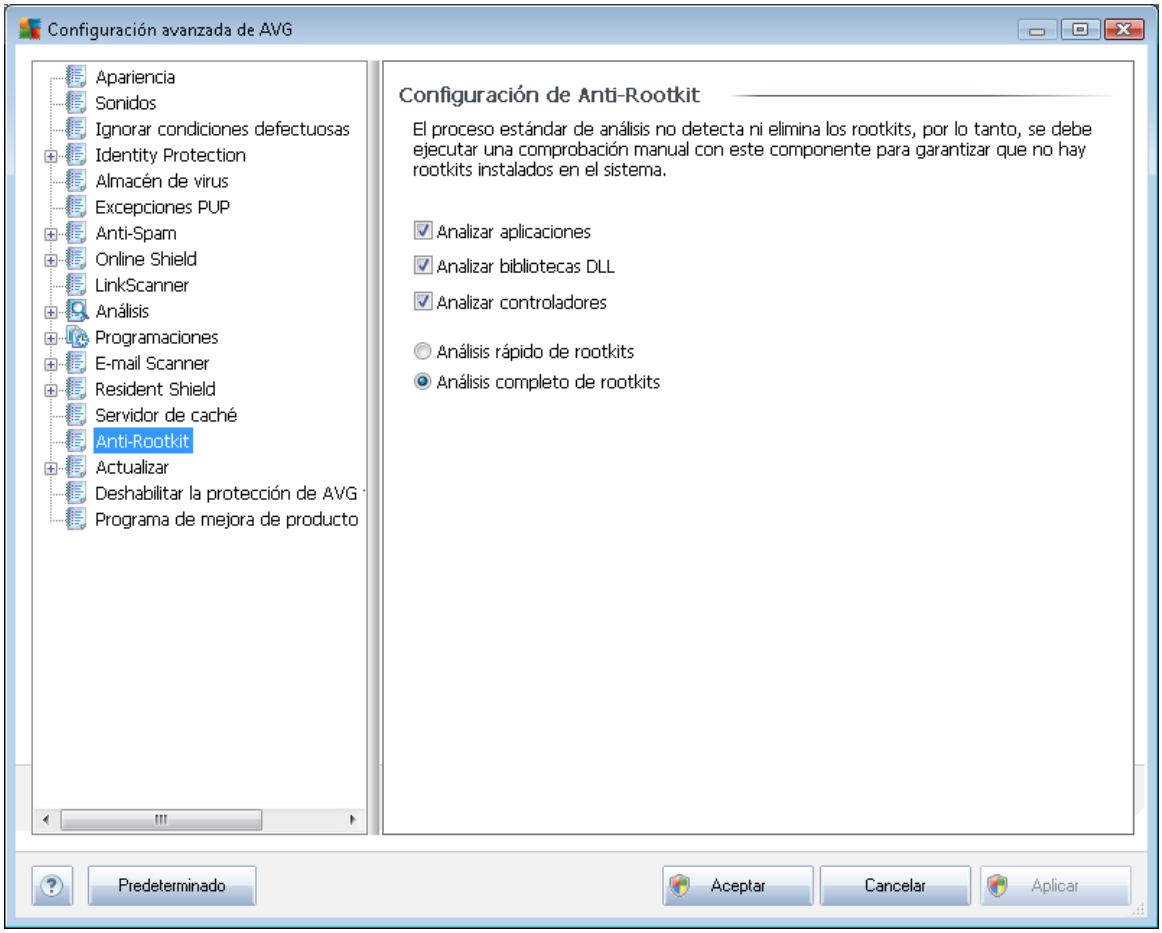
El cuadro de diálogo de configuración ofrece dos opciones:

- ***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.

9.15. Anti-Rootkit

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



Todas las funciones de edición del componente ***Anti-Rootkit*** incluidas en este cuadro de diálogo también están disponibles directamente desde la ***interfaz del componente Anti-Rootkit***.

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

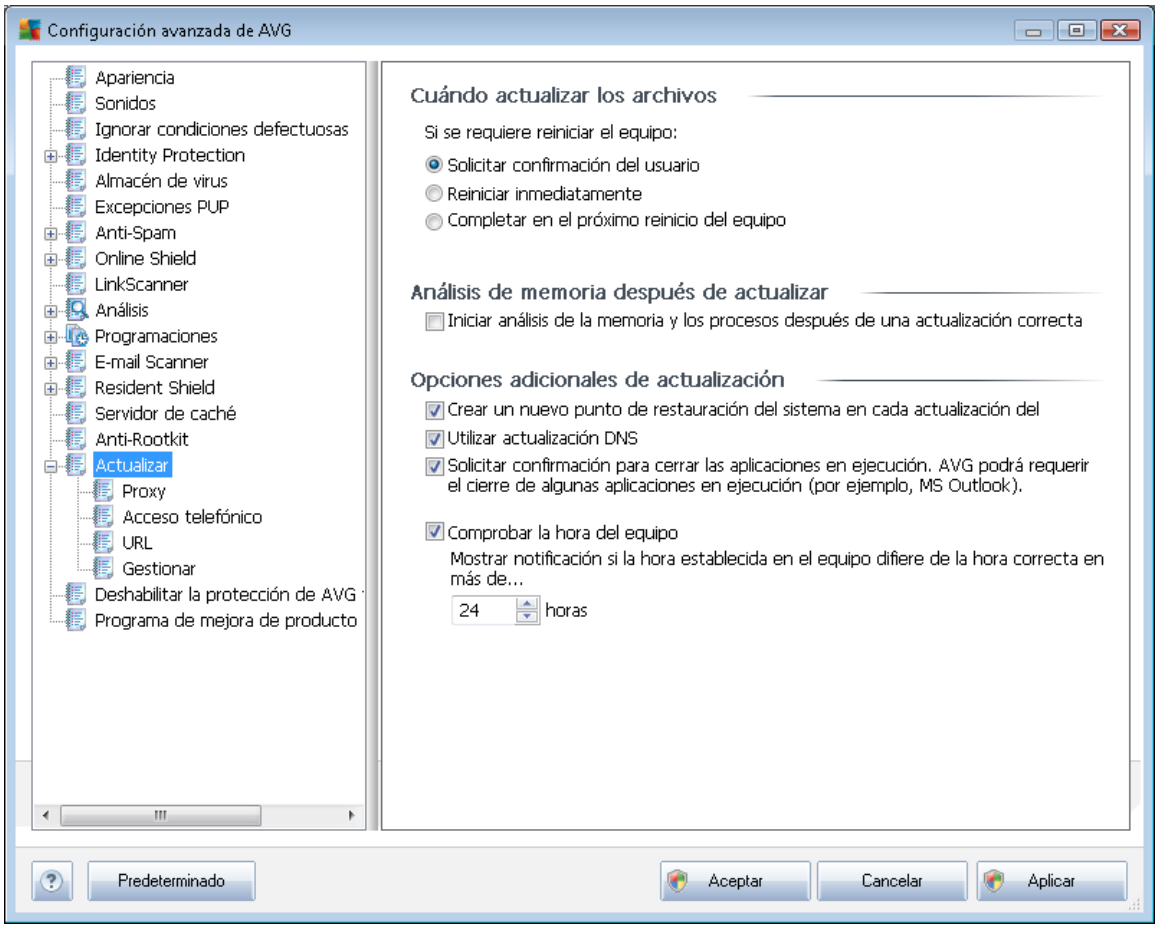
- ***Analizar aplicaciones***
- ***Analizar bibliotecas DLL***
- ***Analizar controladores***

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*)

9.16. 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. La finalización de la actualización se puede programar para el siguiente reinicio del equipo o bien reiniciar inmediatamente:

- ***Solicitar confirmación del usuario*** *(predeterminado*: se solicitará autorización para reiniciar el equipo, paso necesario para finalizar el proceso de actualización
- ***Reiniciar inmediatamente***: el equipo se reiniciará automáticamente nada más finalizar el proceso de actualización y no se solicitará autorización del usuario

- ***Completar en el próximo reinicio del equipo***: la finalización del proceso de actualización se pospondrá hasta en el próximo reinicio. 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

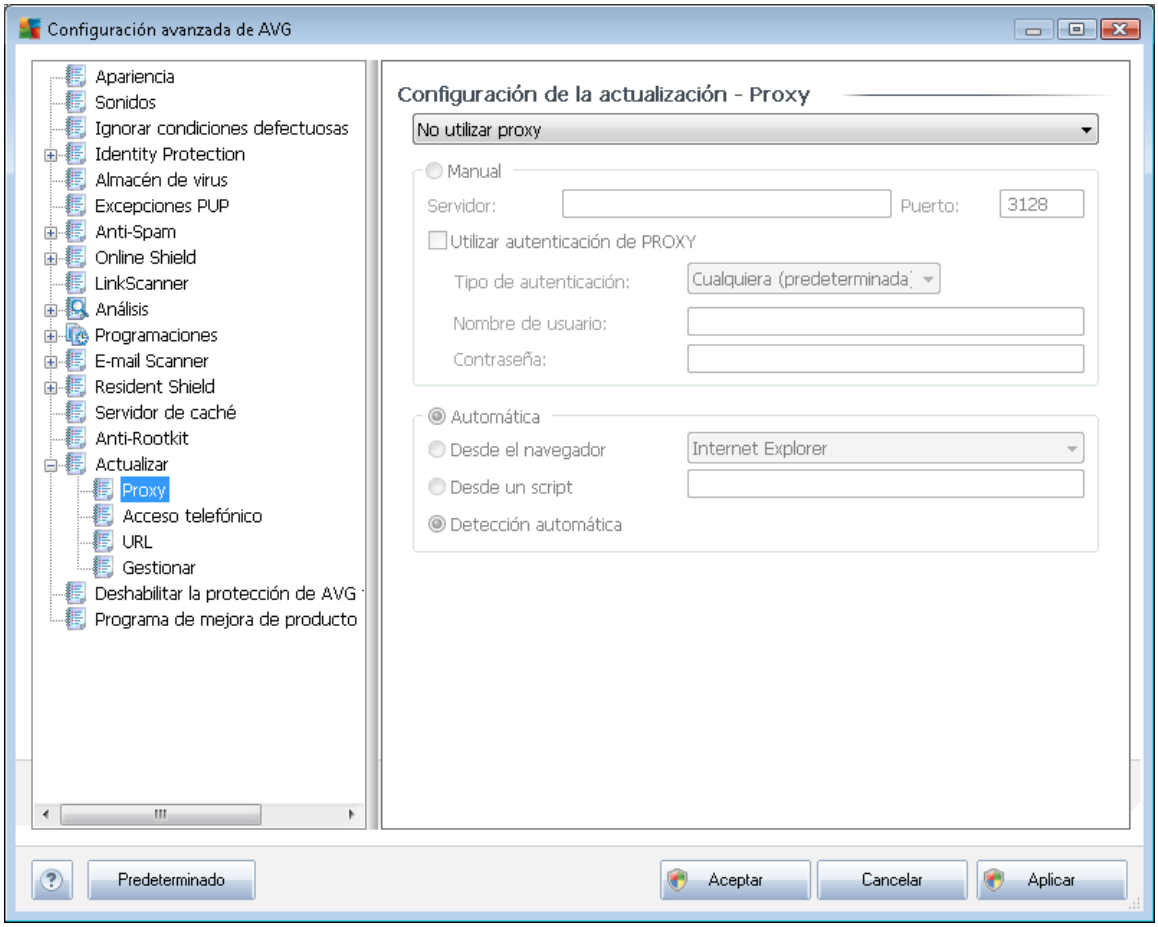
- ***Crear un nuevo punto de restauración del sistema en cada actualización del programa***: antes de iniciar cada actualización del programa AVG, se creará un punto de restauración del sistema. En caso de que falle el proceso de actualización y se bloquee el sistema operativo, este último siempre se 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 2011** 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.

9.16.1. 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*)

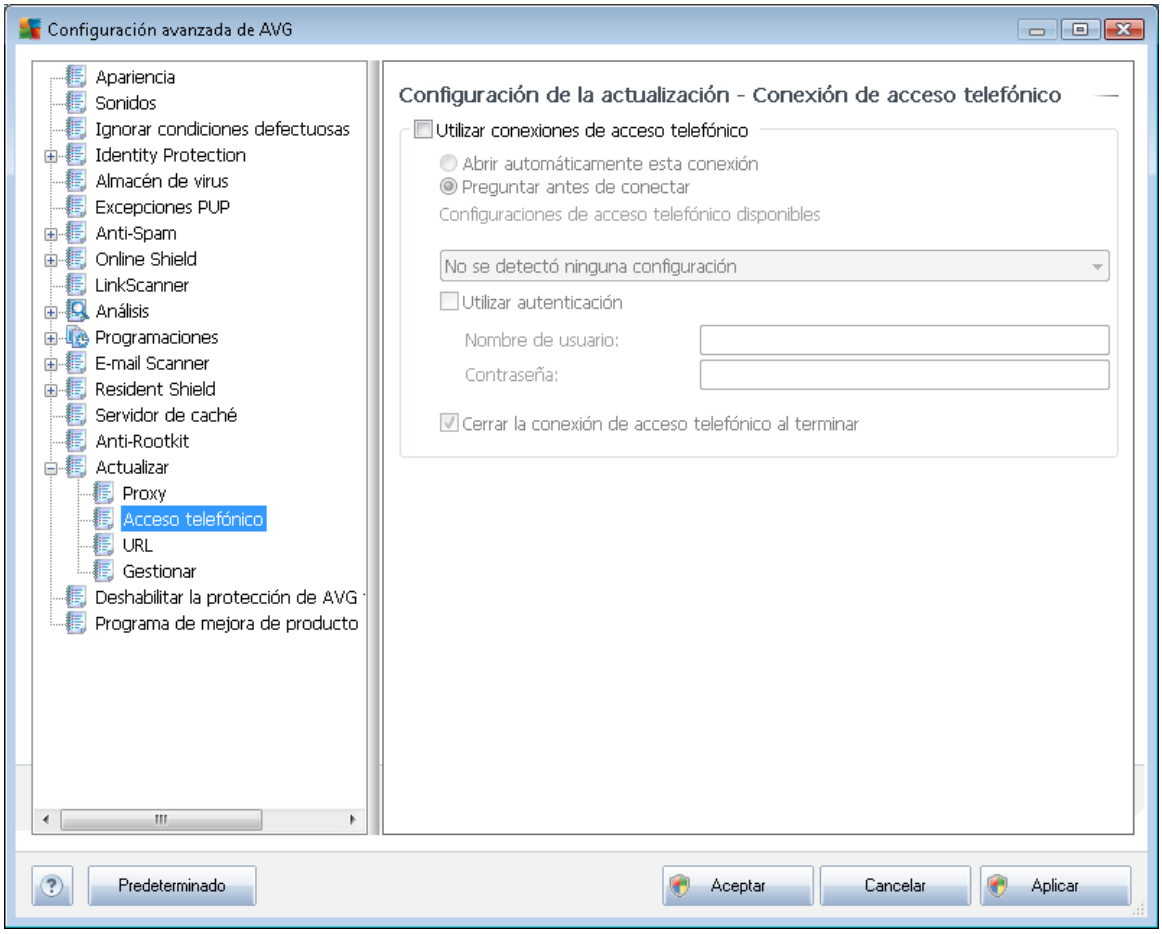
El servidor proxy también puede tener configuradas reglas específicas para cada usuario. Si el servidor proxy está configurado de esta manera, marque la opción ***Utilizar autenticación de PROXY*** para verificar que el nombre de usuario y la contraseña son válidos para la conexión a Internet a través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

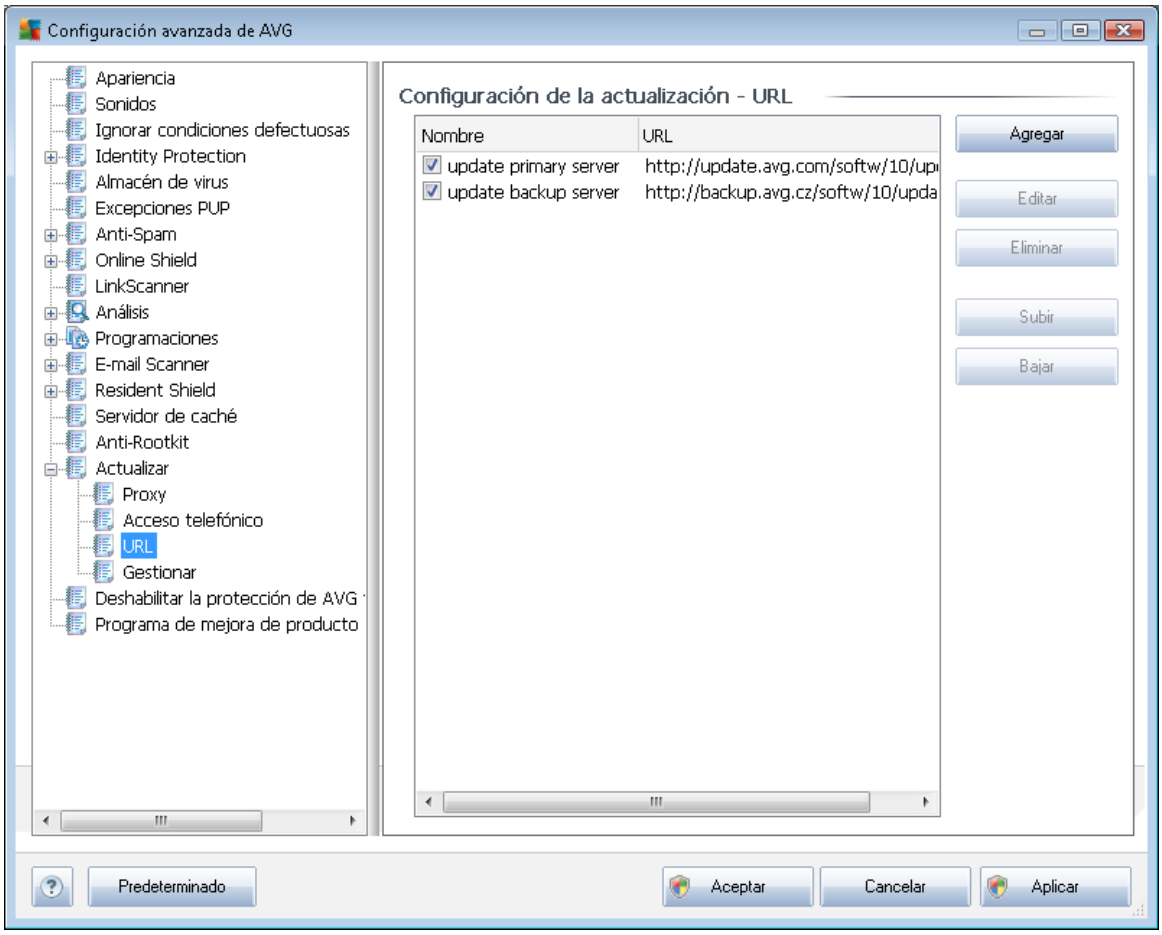
9.16.2. Acceso telefónico



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***).

9.16.3. URL

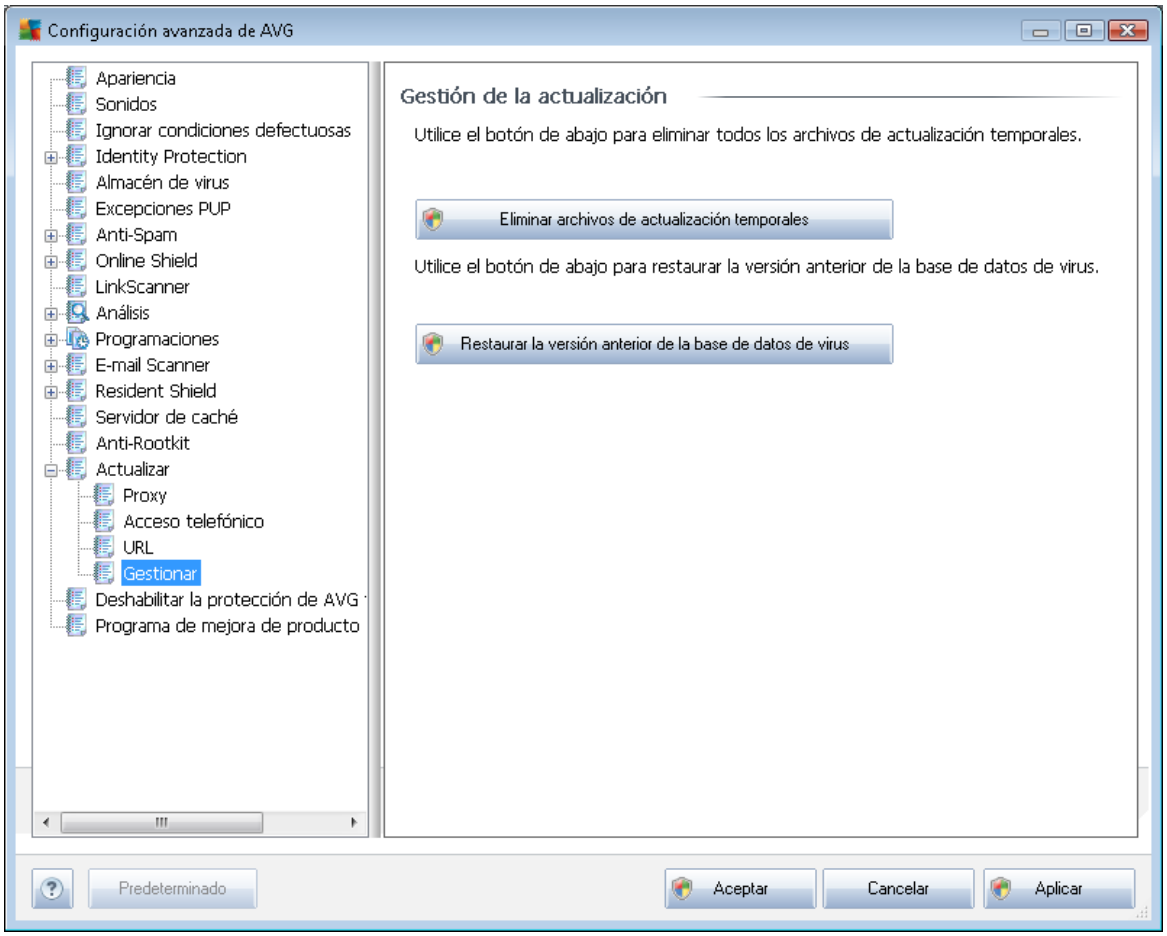


El cuadro de diálogo ***URL*** ofrece una lista de direcciones de Internet desde las cuales se pueden descargar los archivos de actualización. Puede modificar la lista y sus elementos empleando los siguientes botones de control:

- ***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

9.16.4. Gestionar

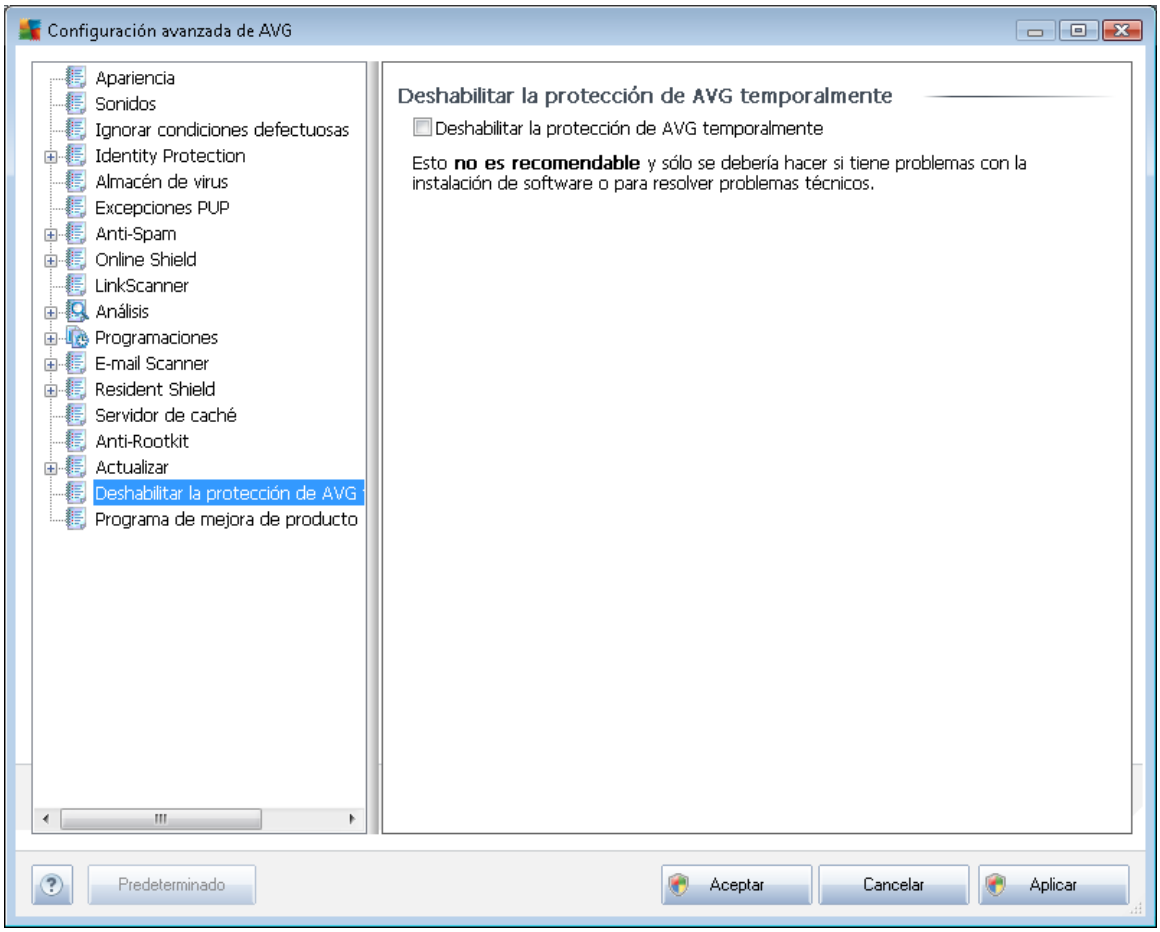
El cuadro de diálogo ***Gestionar*** ofrece dos opciones, a las que se puede acceder mediante dos botones:



- ***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*).

9.17. 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 2011**.

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

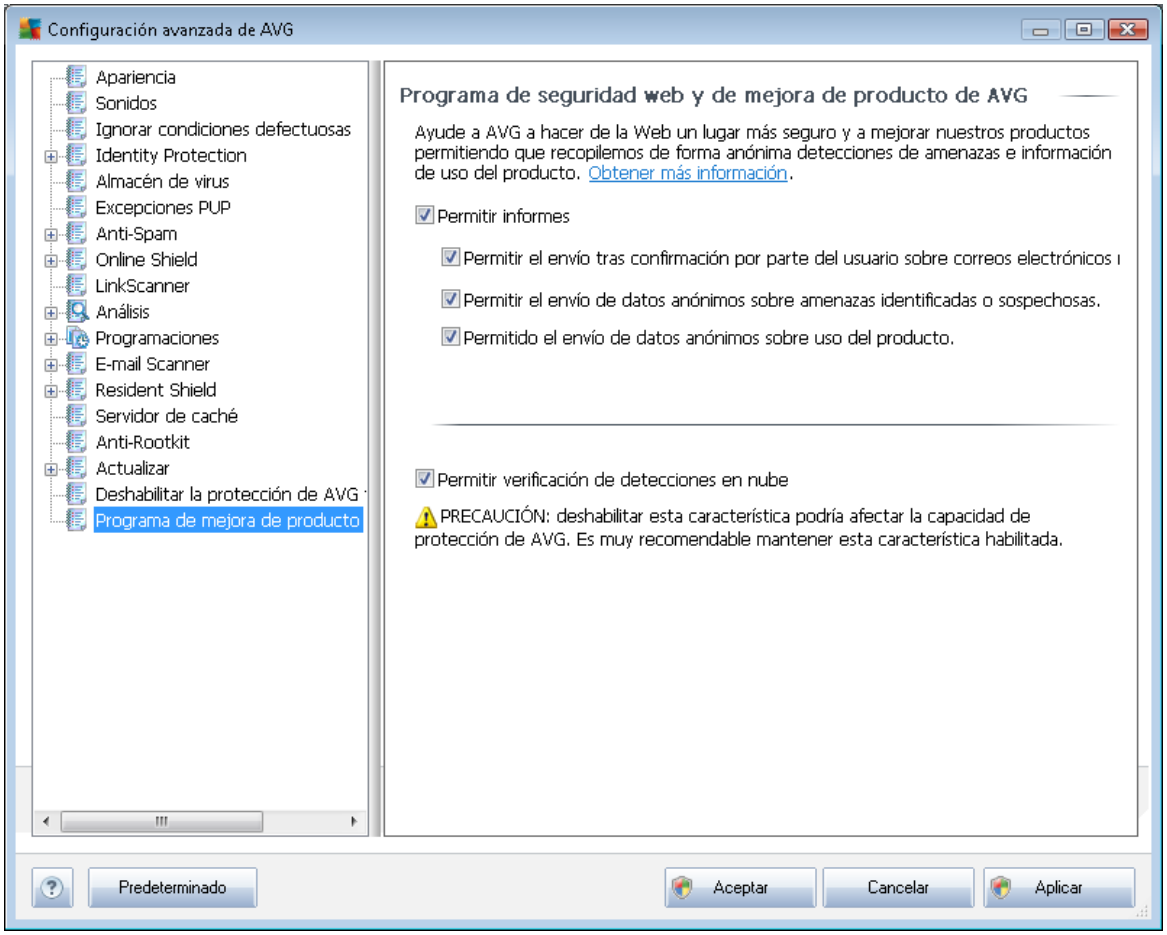
En la mayoría de los casos, ***no es necesario*** deshabilitar AVG antes de instalar un nuevo software o controladores, ni siquiera si el instalador o el asistente del software sugiere que se cierren los programas y aplicaciones en ejecución antes de empezar para asegurarse de que no ocurrirán interrupciones no deseadas durante el proceso de instalación. Si llegase a tener algún problema durante la instalación, intente desactivar primero el componente ***Protección residente***. Si tiene que deshabilitar AVG temporalmente, debería volverlo a habilitar tan pronto como sea posible. 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.

9.18. 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 sobre

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 procesa automáticamente, por lo que no le provocará ningún inconveniente. Los informes no incluyen datos personales. El envío de informes de amenazas detectadas es opcional, aunque recomendamos activar también esta característica, ya que 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 de todas estas clases diferentes de amenazas, AVG incluye los siguientes componentes especializados:

- ***Anti-Virus*** para proteger su equipo frente a los virus,

- ***Anti-Spyware*** para proteger su equipo frente al spyware,

- ***Online Shield*** para protegerle contra virus y spyware mientras navega por Internet,

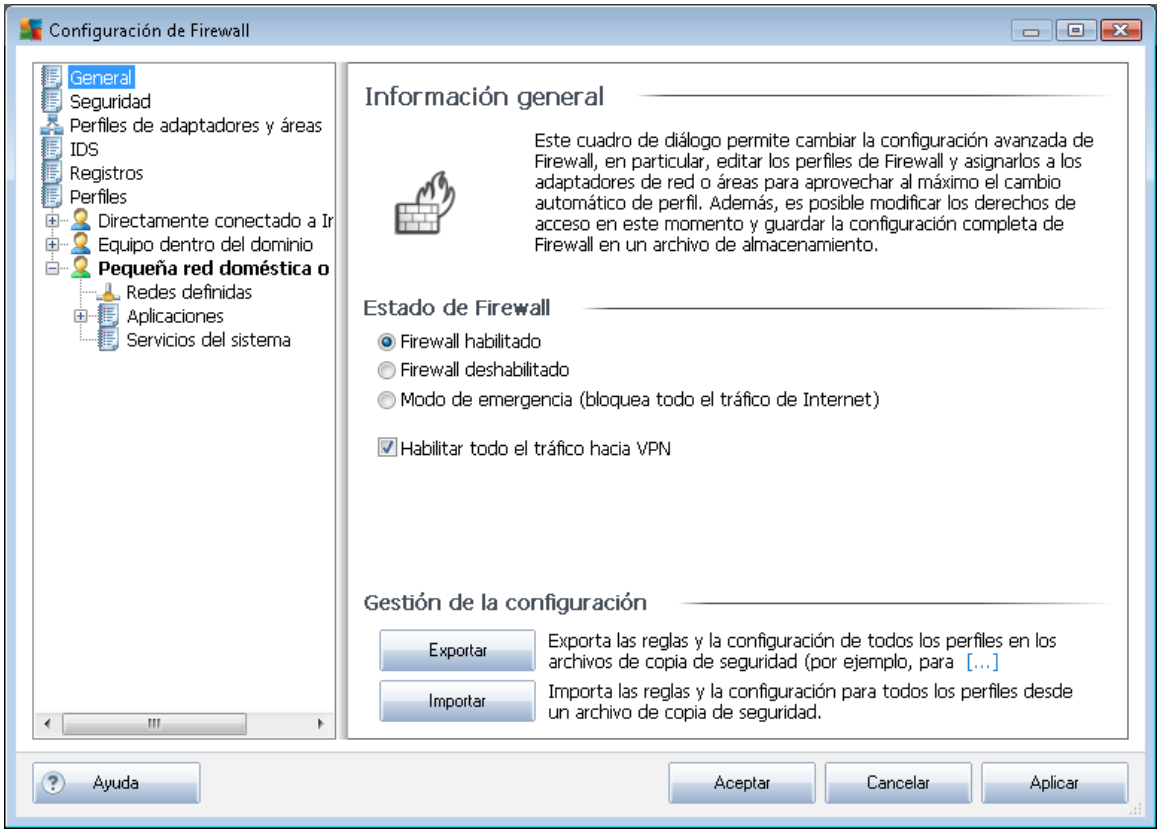
- ***LinkScanner*** para protegerle de otras amenazas en línea mencionadas en este capítulo.

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. ***No obstante, la modificación de la configuración avanzada sólo está destinada a expertos y usuarios experimentados.***

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

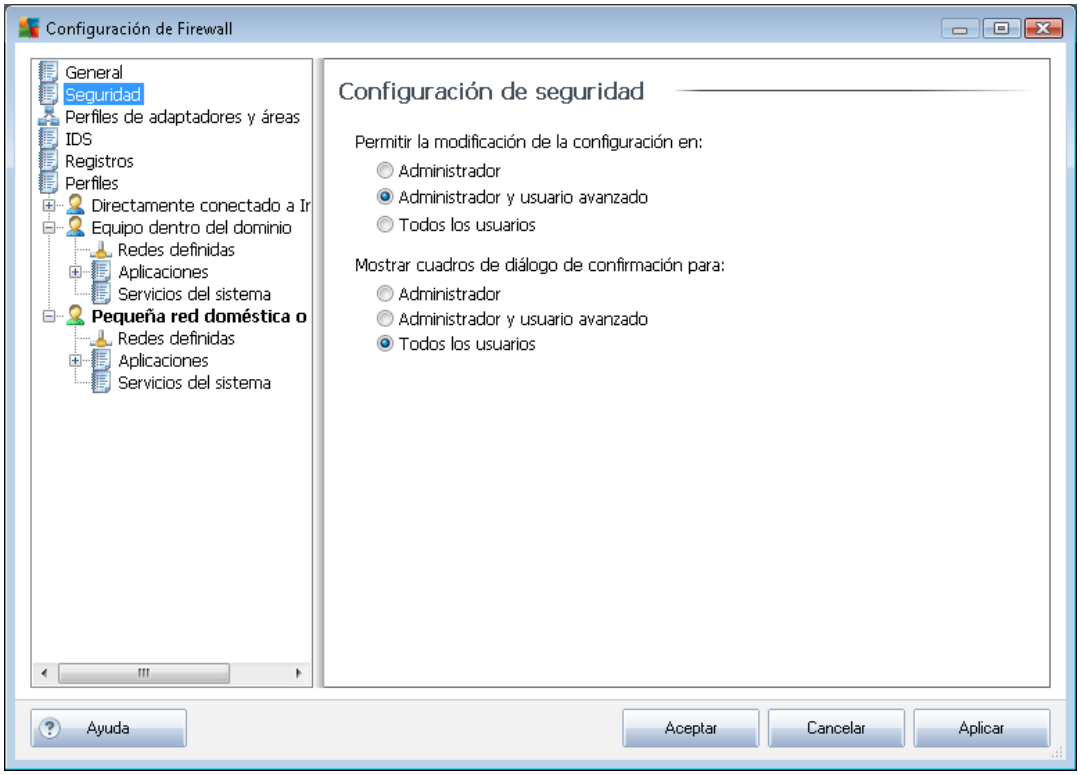
- ***Habilitar todo el tráfico hacia VPN***: si utiliza una conexión VPN *(Red privada virtual)*, por ejemplo, para conectarse con la oficina desde casa, se recomienda marcar esta casilla de verificación.***AVG Firewall*** buscará automáticamente entre los adaptadores de red para encontrar los que se utilizan para la conexión VPN y permitir 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 necesita 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*** / ***Importar*** la configuración del ***Firewall***; es decir, exportar las reglas y la configuración definida 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:

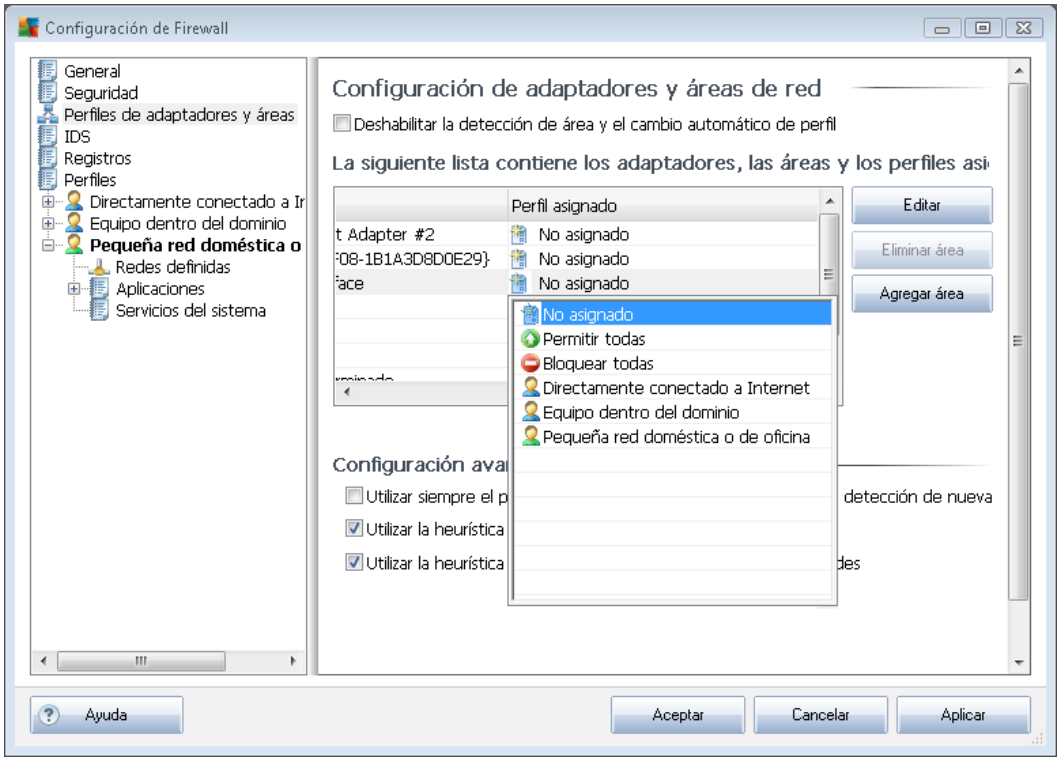
- ***Administrador***: controla el equipo completamente y tiene el derecho de asignar cada usuario a grupos con permisos específicamente definidos

- ***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***: se puede asignar

uno de los perfiles definidos 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 encontrará 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 en el elemento correspondiente en la lista de adaptadores y seleccione el perfil.

Configuración avanzada

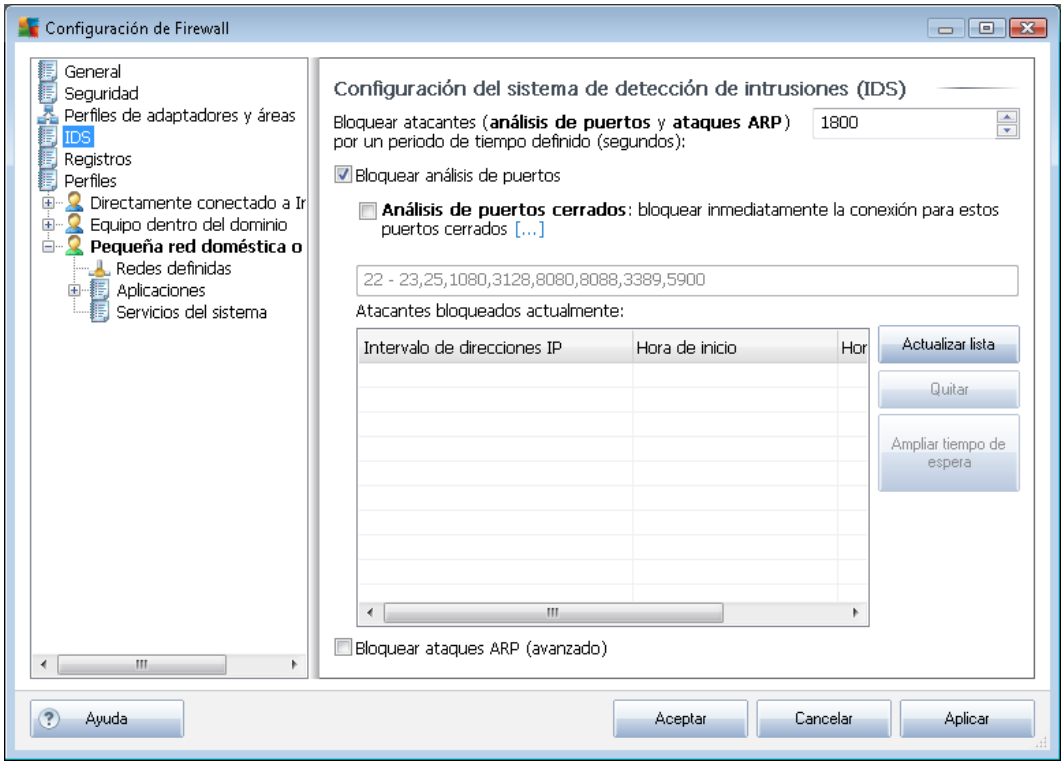
- ***Utilizar siempre el perfil predeterminado y no mostrar el cuadro de diálogo de detección de nueva red***: cada vez que el equipo se conecte a una nueva red, ***Firewall*** alertará y mostrará un cuadro de diálogo solicitando la selección de un tipo de conexión de red y su asignación a un ***Perfil 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***: habilita la adquisición de información sobre una nueva red detectada con los propios mecanismos AVG (*esta opción sólo está disponible en el sistema operativo Vista y posterior*

- ***Utilizar la heurística de Microsoft para la detección de nuevas redes***: habilita la adquisición de información sobre una nueva red detectada del servicio de Windows (*esta opción sólo está disponible en Windows Vista y posterior*).

10.4. IDS

El ***Sistema de detección de intrusiones*** o IDS, es una característica especial de análisis de comportamiento diseñada para identificar y bloquear intentos de comunicación sospechosos en determinados puertos del equipo. Puede configurar los parámetros de IDS en la siguiente interfaz:



El cuadro de diálogo ***Configuración del Sistema de detección de intrusiones (IDS)*** contiene las siguientes opciones de configuración:

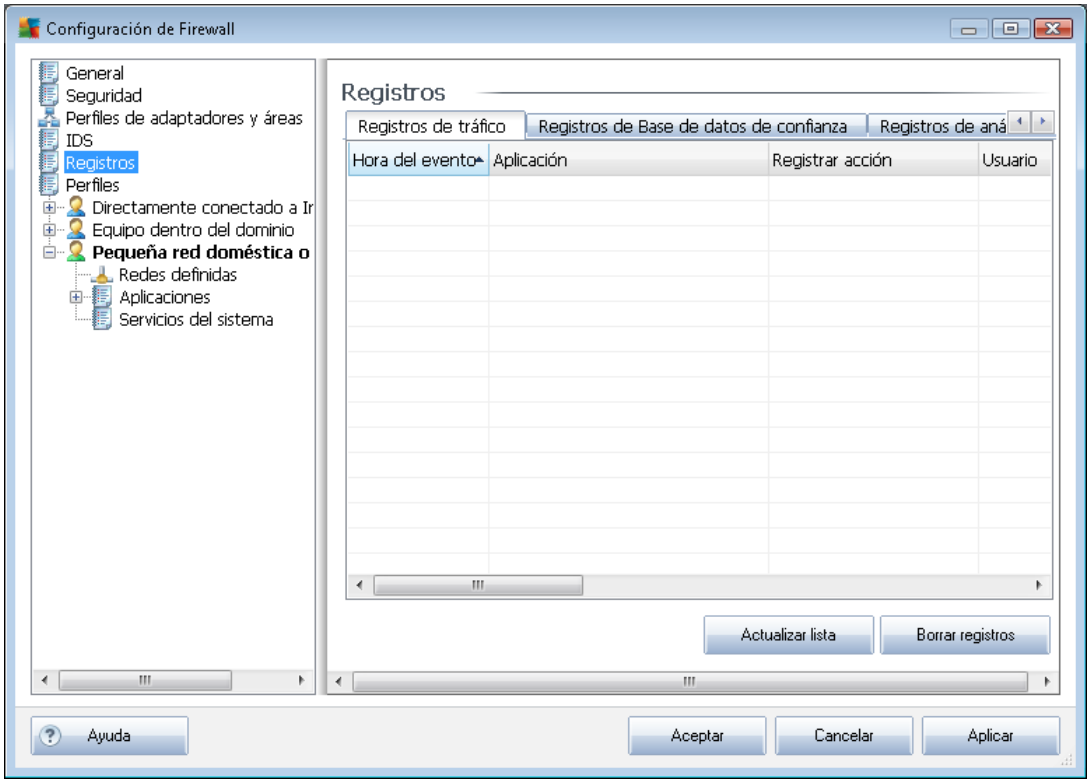
- ***Bloquear atacantes por un periodo de tiempo definido***: aquí puede especificar la cantidad de segundos que un puerto debe bloquearse cuando se detecte en él un intento de comunicación sospechoso. De manera predeterminada, el intervalo de tiempo está configurado como 1.800 segundos (*30 minutos*).
- ***Bloquear análisis de puertos***: marque la casilla para bloquear los intentos de comunicación desde el exterior hacia el equipo a través de los puertos TCP y UDP. Para cualquiera de estas conexiones se permiten cinco intentos, el sexto se bloquea.
    - ***Análisis de puertos cerrados***: marque la casilla para bloquear inmediatamente cualquier intento de comunicación a través de los puertos especificados en el campo de texto inferior. 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***: en esta sección se enumera cualquier intento de comunicación que en la actualidad está siendo bloqueado por el ***Firewall***. En el cuadro de diálogo ***Registros***, (*ficha Registros de análisis de puertos*), se puede visualizar un historial completo de los intentos que han sido bloqueados.
- ***Bloquear ataques ARP*** activa el bloqueo de tipos especiales de intentos de comunicación en el interior de una red local detectados por ***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.

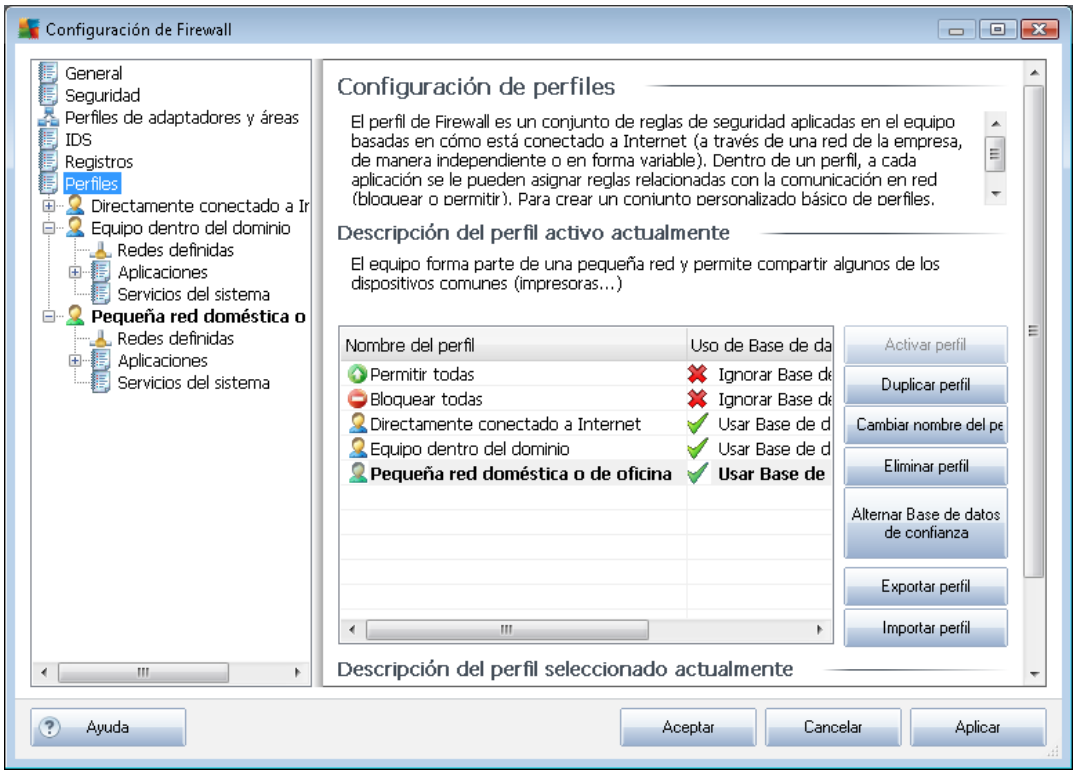
Botones de control

- ***Actualizar lista***: todos los parámetros registrados se pueden ordenar según el atributo seleccionado: orden cronológico (*fechas*) o alfabético (*otras columnas*), simplemente haciendo clic en el encabezado de columna correspondiente. Utilice el botón ***Actualizar lista*** para actualizar la información que aparece en este momento en pantalla.

- ***Vaciar lista***: borra 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.



Todos los perfiles que no sean del sistema se pueden editar directamente en este cuadro de diálogo, empleando los siguientes botones de control:

- ***Activar perfil***: este botón establece el perfil seleccionado como activo, lo que significa que la configuración del perfil seleccionado 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* (*que 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

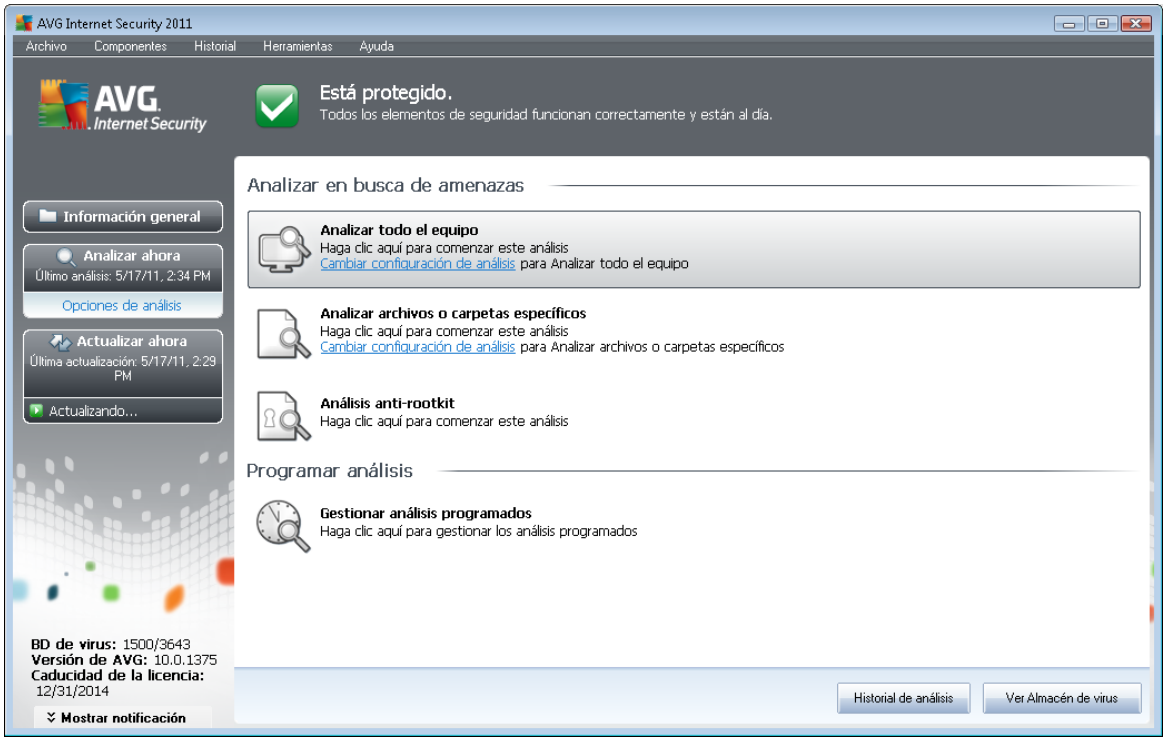
En la sección inferior del cuadro de diálogo puede encontrar la descripción del perfil actualmente seleccionado en la lista de arriba.

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*):

11. Análisis de AVG

El análisis es una parte crucial del funcionamiento de **AVG Internet Security 2011**. Puede ejecutar análisis bajo demanda o programarlos para que se ejecuten periódicamente a una hora que le resulte conveniente.

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 2011** 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.

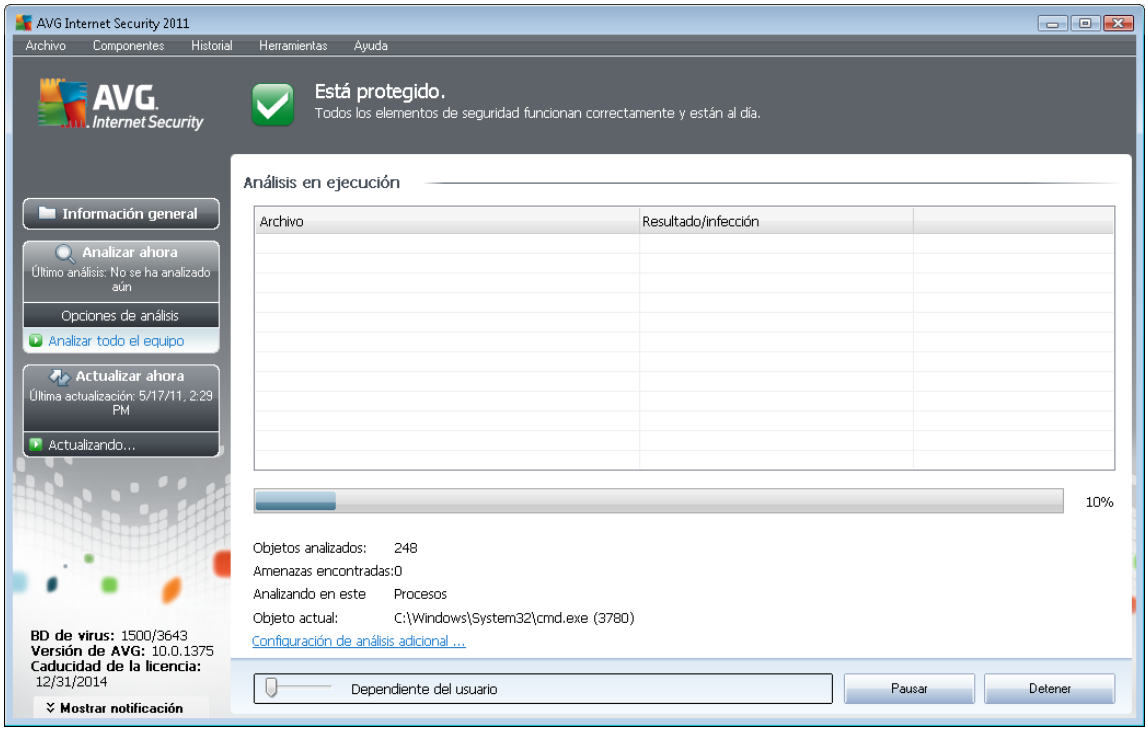
En **AVG Internet Security 2011**, encontrará los siguientes tipos de análisis predefinidos por el proveedor de software:

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.

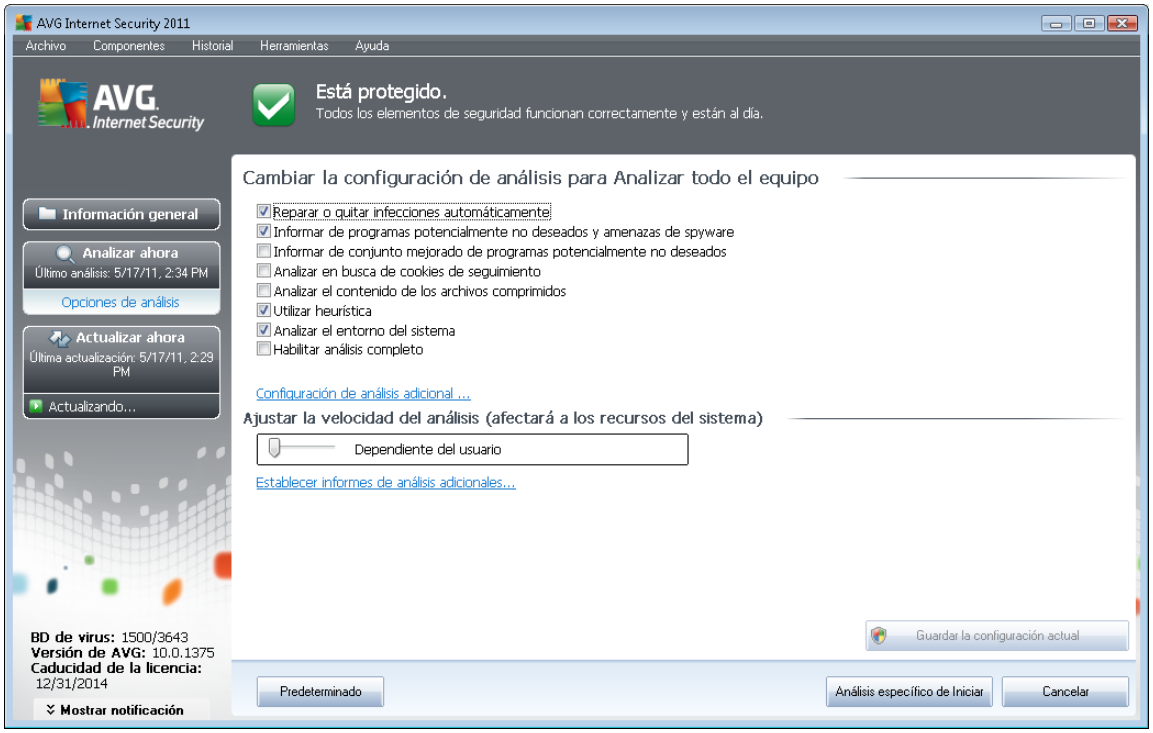
Inicio del análisis

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).

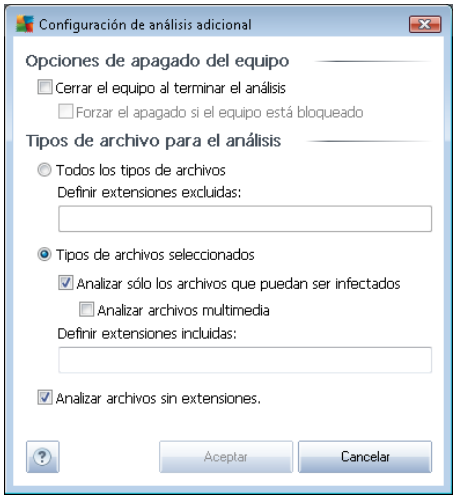
- **Analizar el contenido de los archivos comprimidos** (*desactivado de forma predeterminada*): este parámetro establece que el análisis debe comprobar todos los archivos que se encuentren dentro de archivos comprimidos, tales como ZIP, RAR, etc.

- **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***).

- **Definir los tipos de archivos para el análisis**: a continuación, debe indicar si desea que se analice lo siguiente:

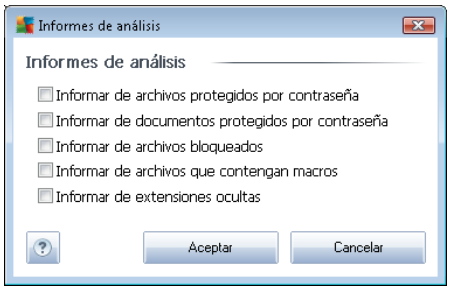
- ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis, proporcionando una lista de extensiones de archivo separadas por comas que no deben analizarse;

- ***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

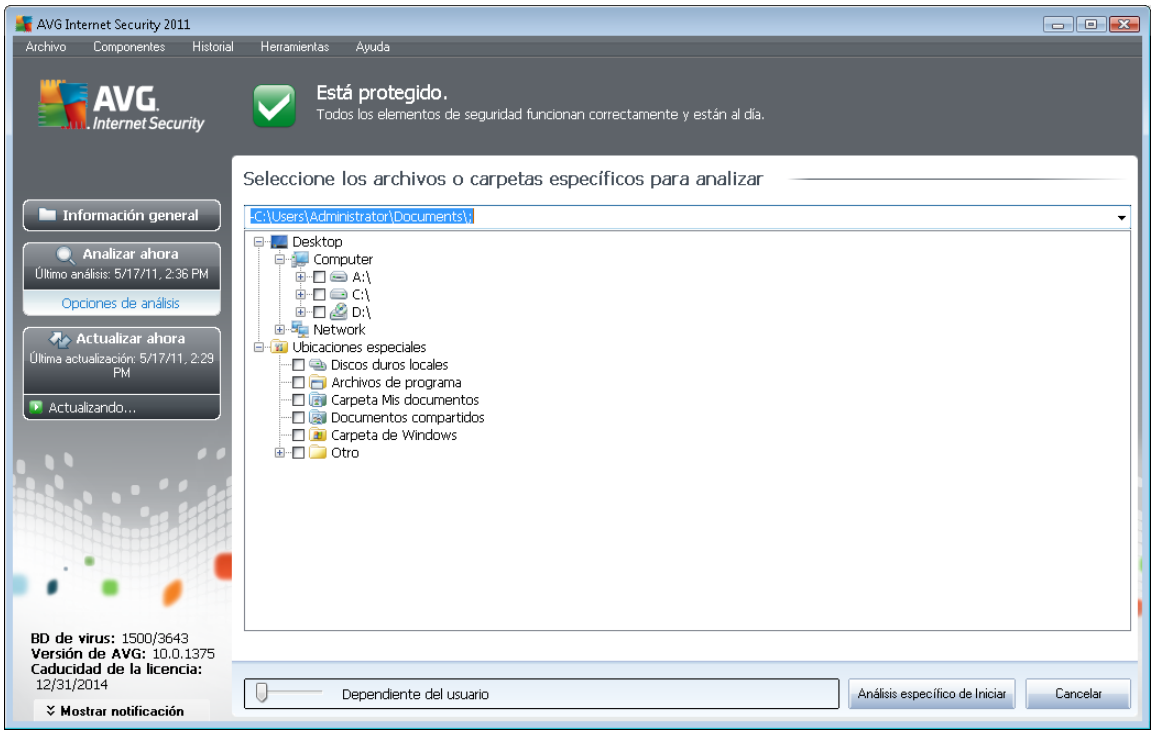
que en el análisis del equipo completo: todos los virus encontrados se reparan o se envían al ***Almacén de virus***. Puede utilizar el análisis de archivos o carpetas específicos para configurar análisis personalizados y programarlos según sus propias necesidades.

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 "!" .

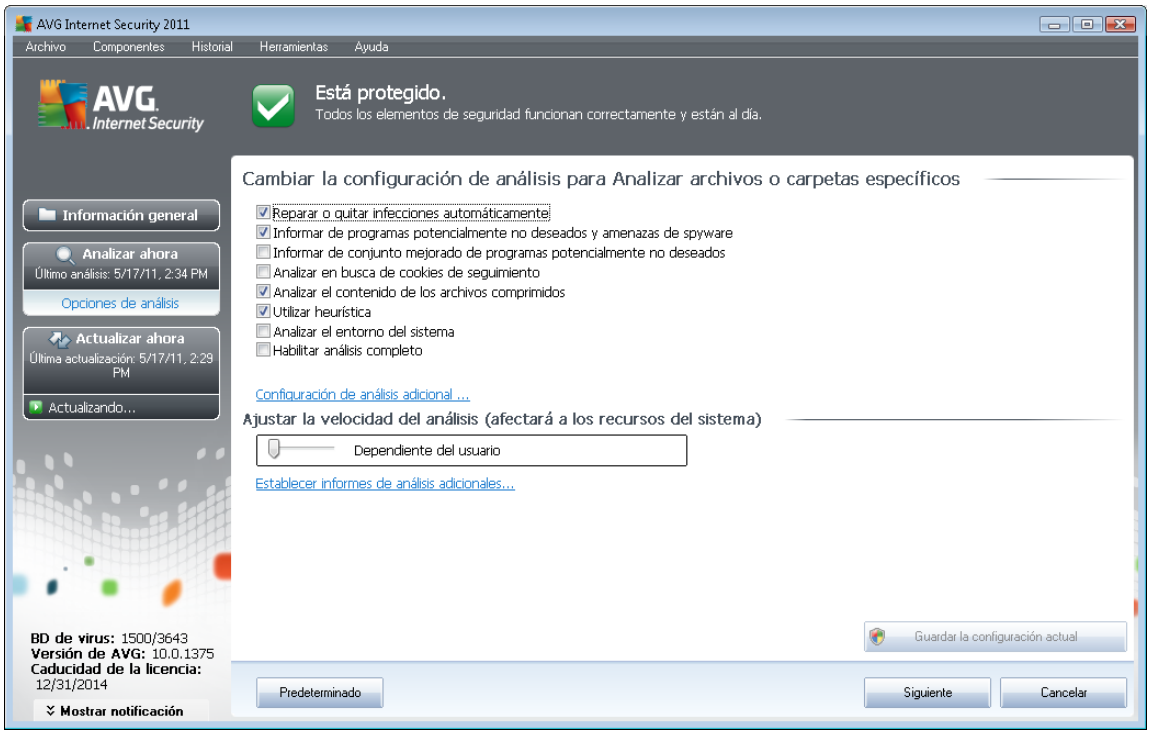
Por último, para iniciar el análisis, pulse el botón ***Iniciar análisis***; el proceso de análisis en sí es básicamente idéntico al Análisis del equipo completo.



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*).

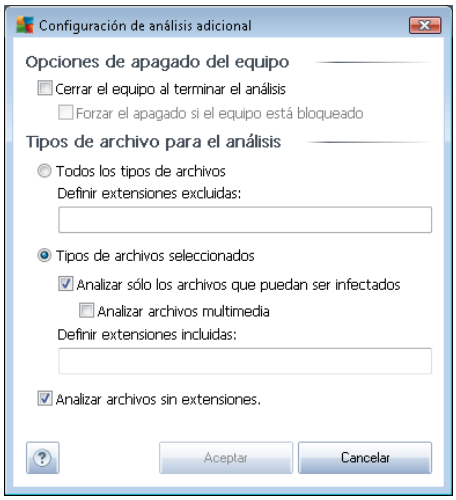
- ***Analizar el contenido de los archivos comprimidos*** (*activado de forma predeterminada*): este parámetro establece que el análisis debe comprobar todos los archivos que se encuentren dentro de archivos comprimidos, tales como ZIP, RAR, etc.

- ***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***).

- ***Definir los tipos de archivos para el análisis***: a continuación, debe indicar si desea

que se analice lo siguiente:

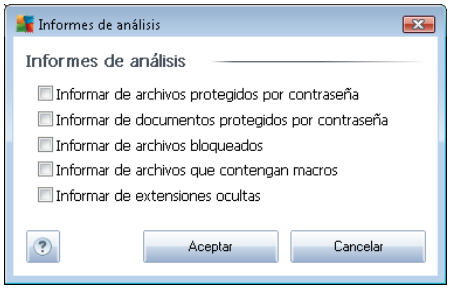
- ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis, proporcionando una lista de extensiones de archivo separadas por comas que no deben analizarse;

- ***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:



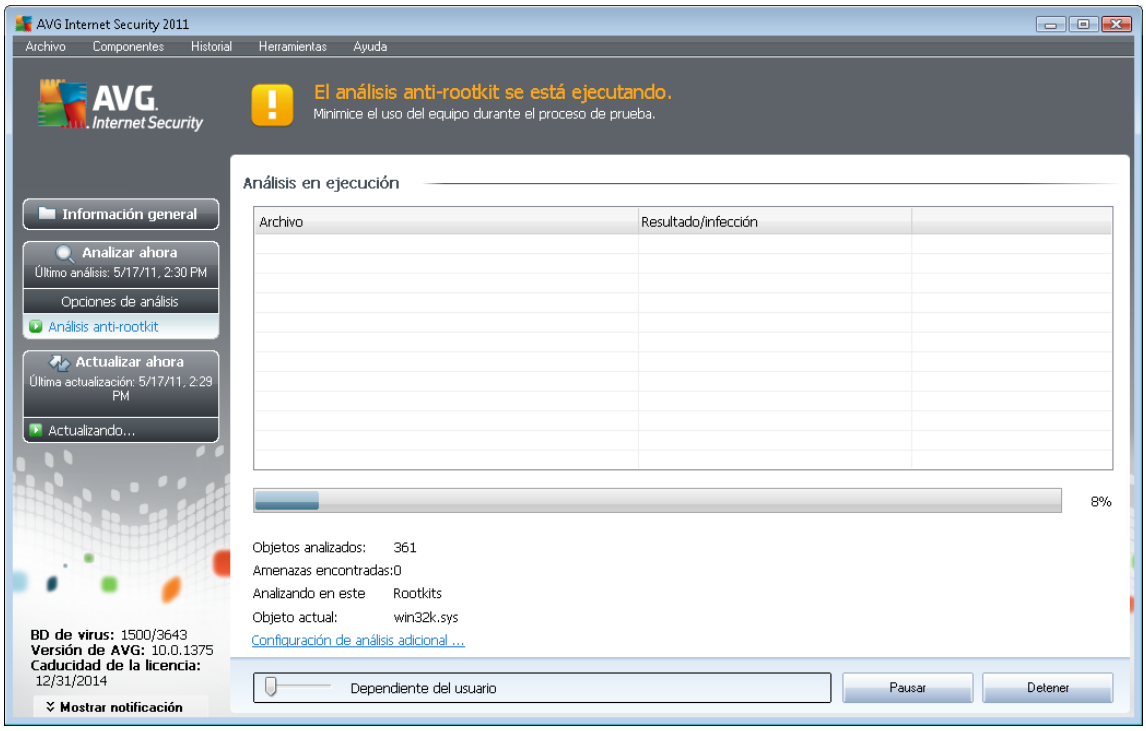
Advertencia: *esta configuración de análisis es idéntica a la que se emplea para un análisis recién definido, tal como se describe en el capítulo* ***Análisis de AVG / Programación de análisis / Cómo analizar****. Si decide cambiar la configuración predeterminada de la opción* ***Analizar archivos o 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***).



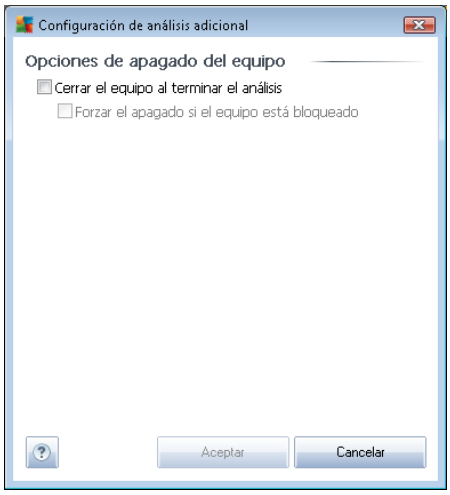
Edición de la configuración del análisis

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

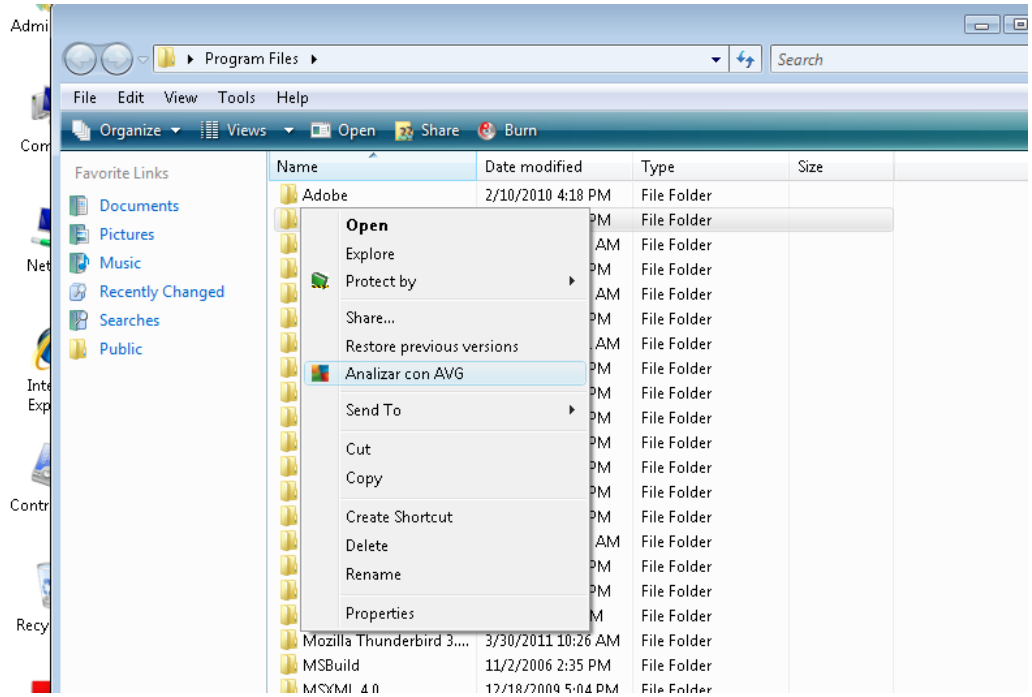
alternativa, puede ejecutar el proceso de análisis de forma más lenta, lo que significa que se minimiza la carga de los recursos del sistema (*resulta útil cuando necesita trabajar en el equipo pero no le importa tanto el tiempo que tarde el análisis*), o más rápida, con mayor exigencia de recursos del 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 2011** 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:



- En el Explorador de Windows, resalte el archivo (o carpeta) que desea analizar
- Haga clic con el botón secundario en el objeto para abrir el menú contextual
- Seleccione la opción ***Analizar con AVG*** para que AVG analice el archivo

11.4. Análisis desde la línea de comandos

En **AVG Internet Security 2011** 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/

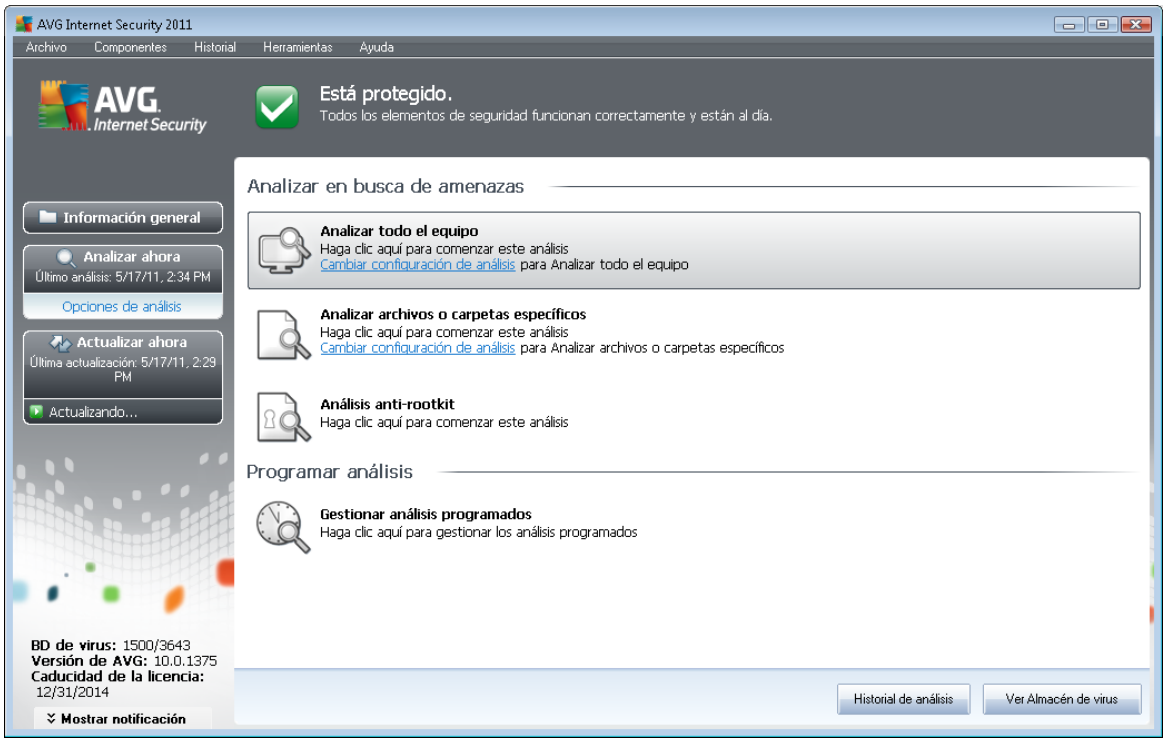
- ***/ARC*** Analizar archivos comprimidos
- ***/CLEAN*** Limpiar automáticamente
- ***/TRASH*** Mover archivos infectados a Almacén de virus
- ***/QT*** Análisis rápido
- ***/MACROW*** Informar de macros
- ***/PWDW*** Informar de archivos protegidos por contraseña
- ***/IGNLOCKED*** Ignorar archivos 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 2011**, 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.

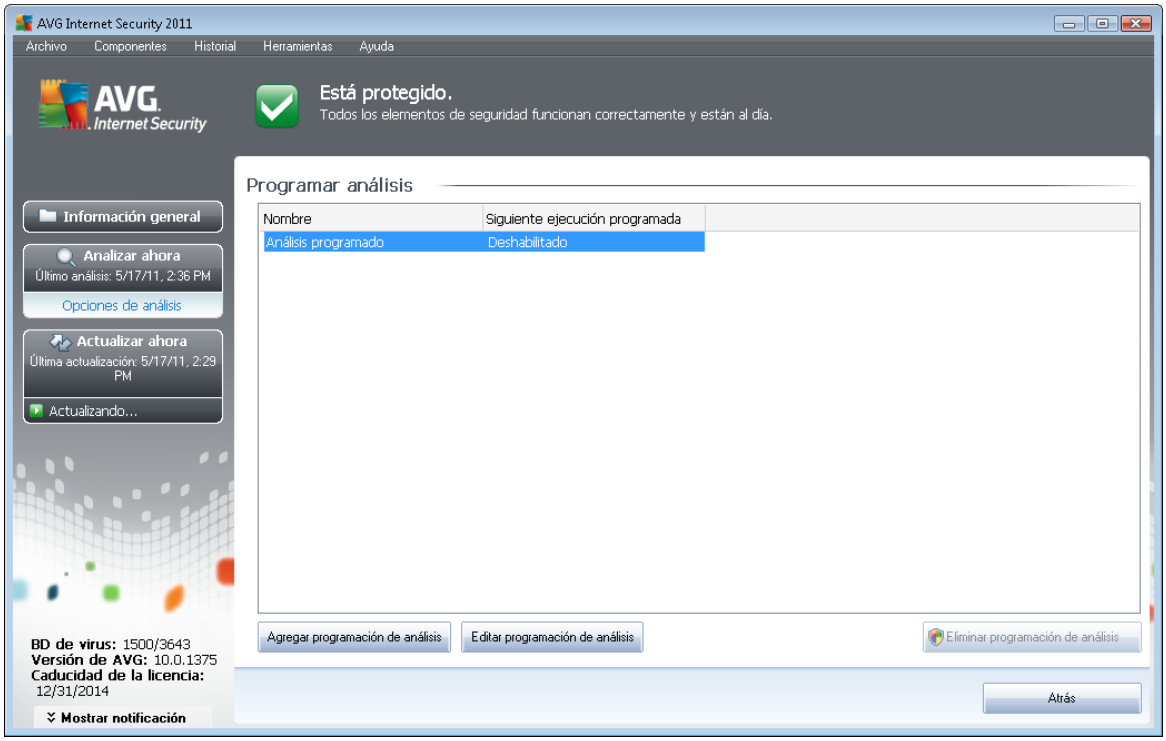
El ***Análisis del equipo completo*** debeía ejecutarse regularmente, al menos una vez por semana. Sin embargo, de ser posible, lo ideal es realizar el análisis del equipo completo a diario, tal como lo establece la configuración predeterminada de la programación de análisis. Si el equipo está continuamente 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 ubicado dentro 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.

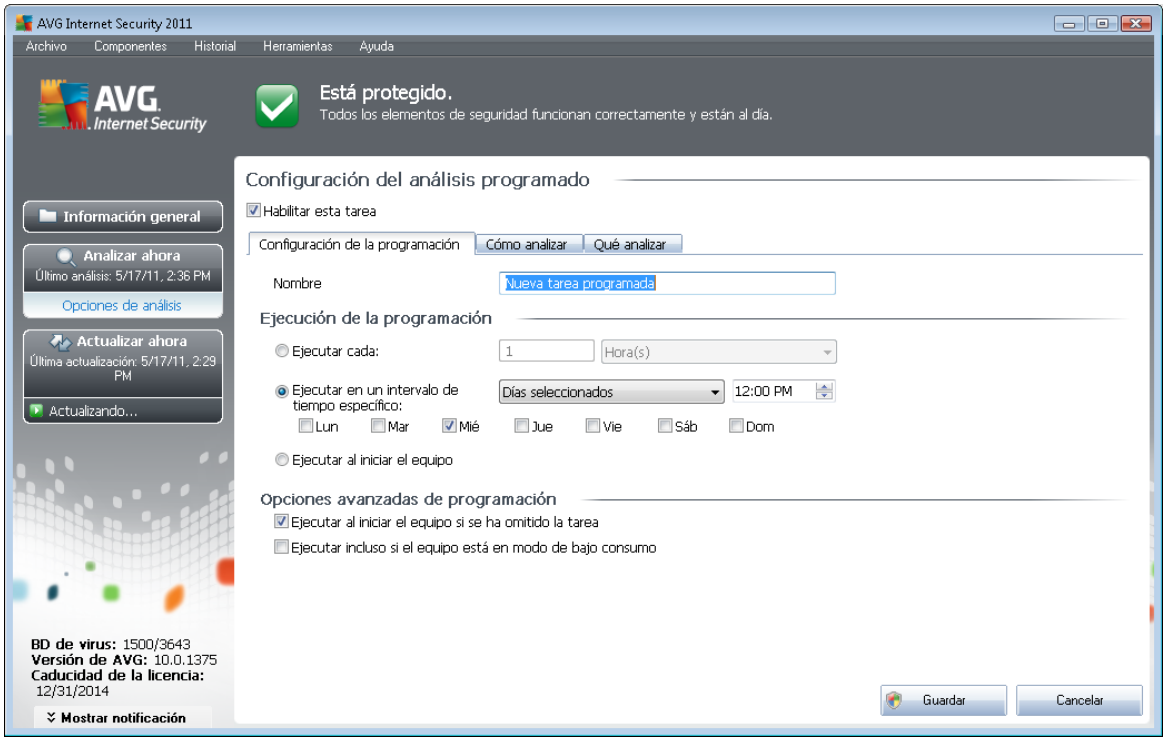
- ***Editar programación de análisis***: sólo puede utilizar este botón si ya seleccionó alguno de los análisis existentes en la lista de análisis programados. En ese caso, el botón se muestra activo y puede hacer clic en él para pasar al cuadro de diálogo ***Configuración del análisis programado***, 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***). Este cuadro de diálogo se divide en tres fichas: ***Configuración de la programación***; *consulte la imagen a continuación* (*la ficha predeterminada a la que se le redirigirá 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.

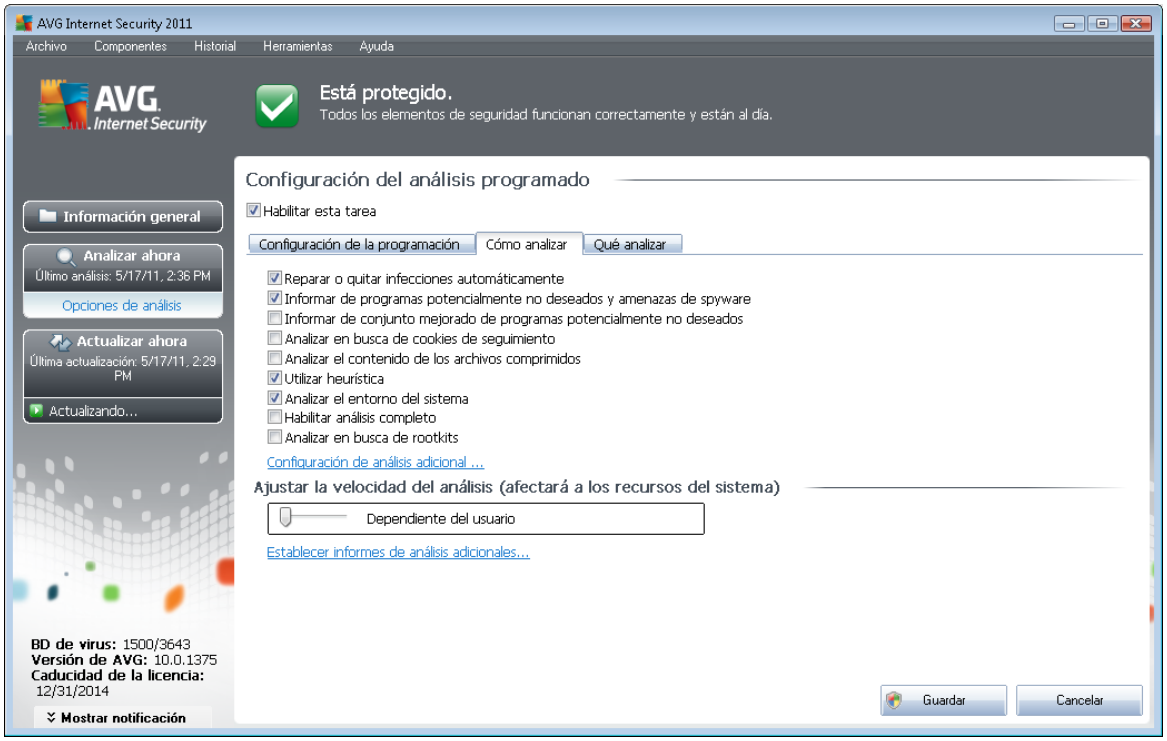
Botones de control del cuadro de diálogo Configuración del análisis programado

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, en todos los casos, cumplen las mismas funciones independientemente de la ficha en que se encuentre el usuario:

- ***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...

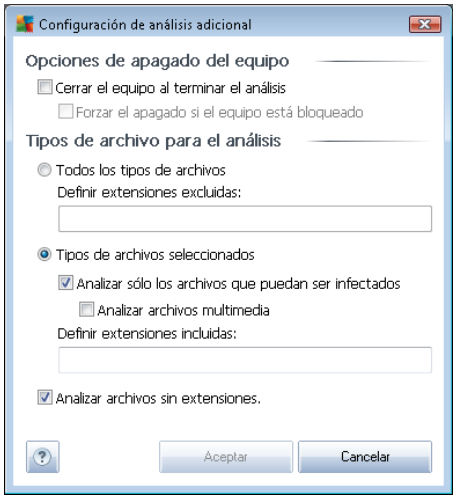
- ***Utilizar heurística*** (*activado de manera predeterminada*): el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos utilizados para detectar virus durante el análisis.

- ***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.

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***).

- ***Definir los tipos de archivos para el análisis***: a continuación, debe indicar si desea que se analice lo siguiente:

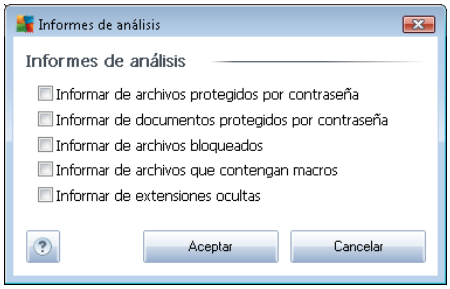
  - ***Todos los tipos de archivos*** con la opción de definir excepciones para el análisis, proporcionando una lista de extensiones de archivo separadas por comas que no deben analizarse;

  - ***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:



Nota: *de manera predeterminada, el análisis está configurado para ofrecer un rendimiento óptimo. A menos que tenga un buen motivo para modificar la configuración predeterminada del análisis, se recomienda mantenerla. Los cambios de configuración deben realizarlos únicamente los usuarios experimentados. Para conocer más opciones de configuración del análisis, consulte el cuadro de diálogo* ***Configuración avanzada****, al que puede acceder a través del elemento del menú del sistema* ***Archivo / Configuración avanzada****.*

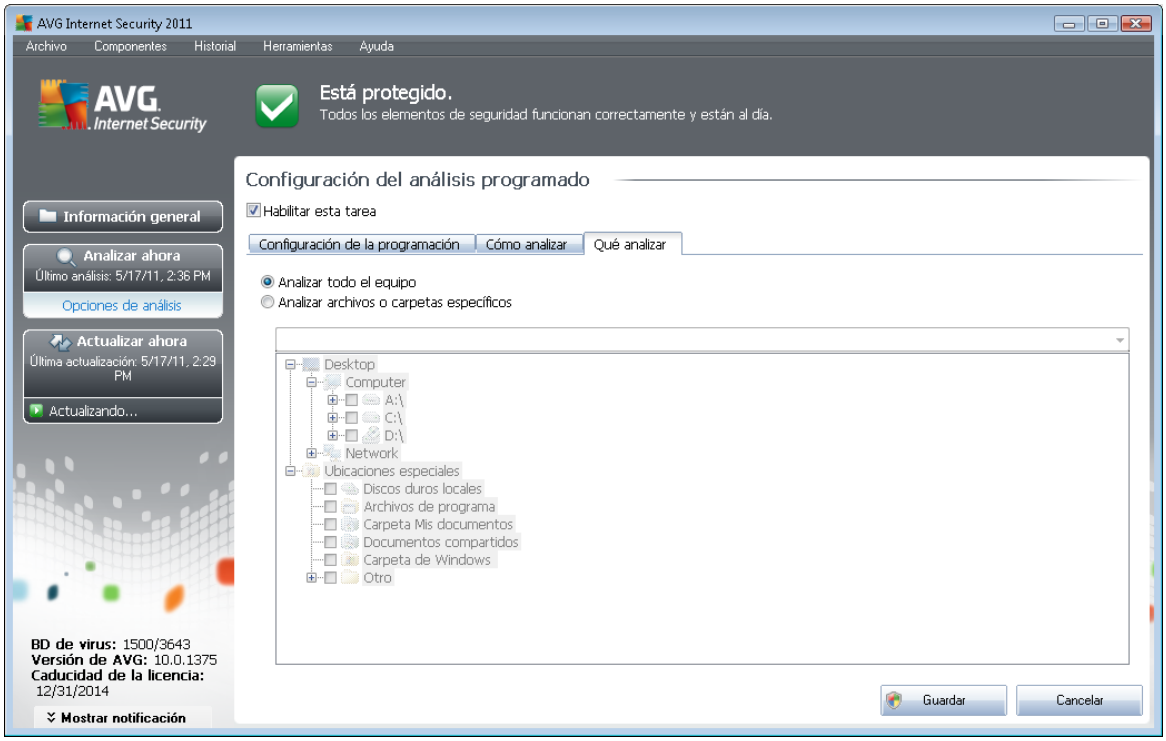
Botones de control

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\

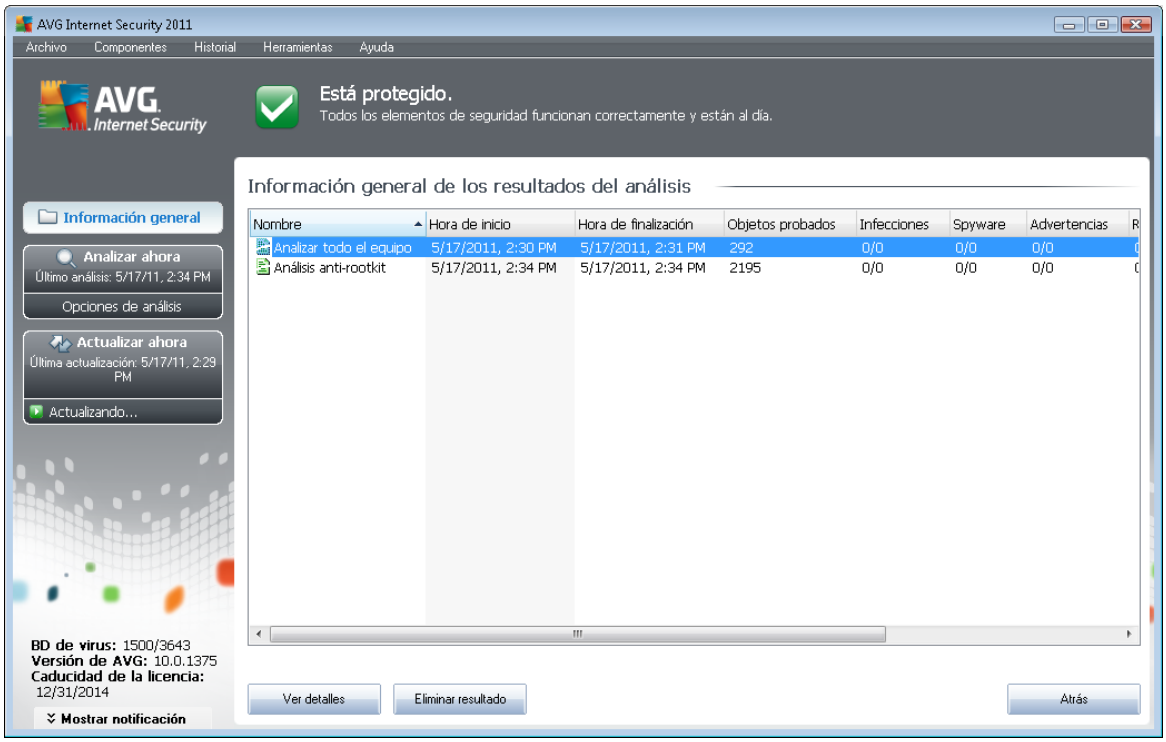
- ***Documentos compartidos***
  - *para Windows XP*: C:\Documents and Settings\All Users\Documentos compartidos\
  - *para Windows Vista/7*: C:\Usuarios\Acceso público\Documentos públicos\
- ***Carpeta de Windows*** - C:\Windows\
- ***Otras***
  - *Unidad del sistema*: la unidad de disco duro en la 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 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, en todos los casos, cumplen las mismas funciones independientemente de la ficha en que se encuentre el usuario:

- ***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

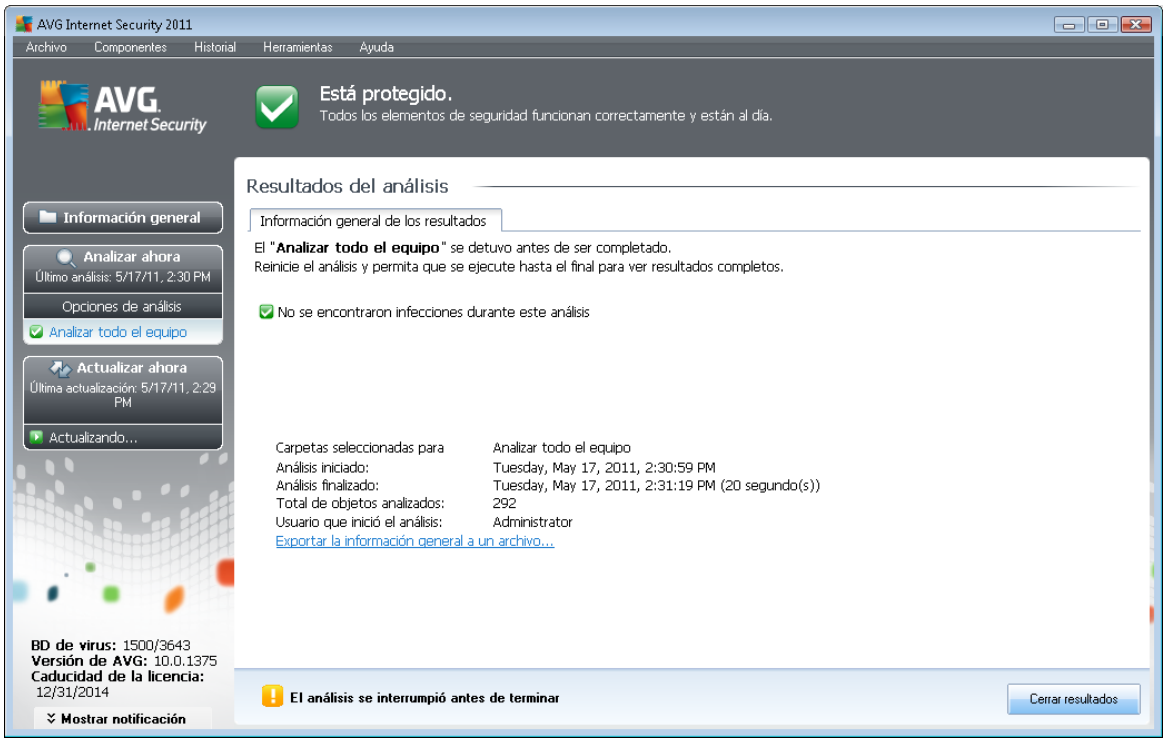
Si hay un análisis específico seleccionado en el cuadro de diálogo ***Información general de los resultados del análisis***, puede hacer clic en el botón ***Ver detalles*** para pasar al cuadro de diálogo ***Resultados del análisis***, que ofrece datos detallados sobre el transcurso y el resultado del 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. Asimismo, aquí encontrará información sobre objetos que no pudieron analizarse (por ejemplo, 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:

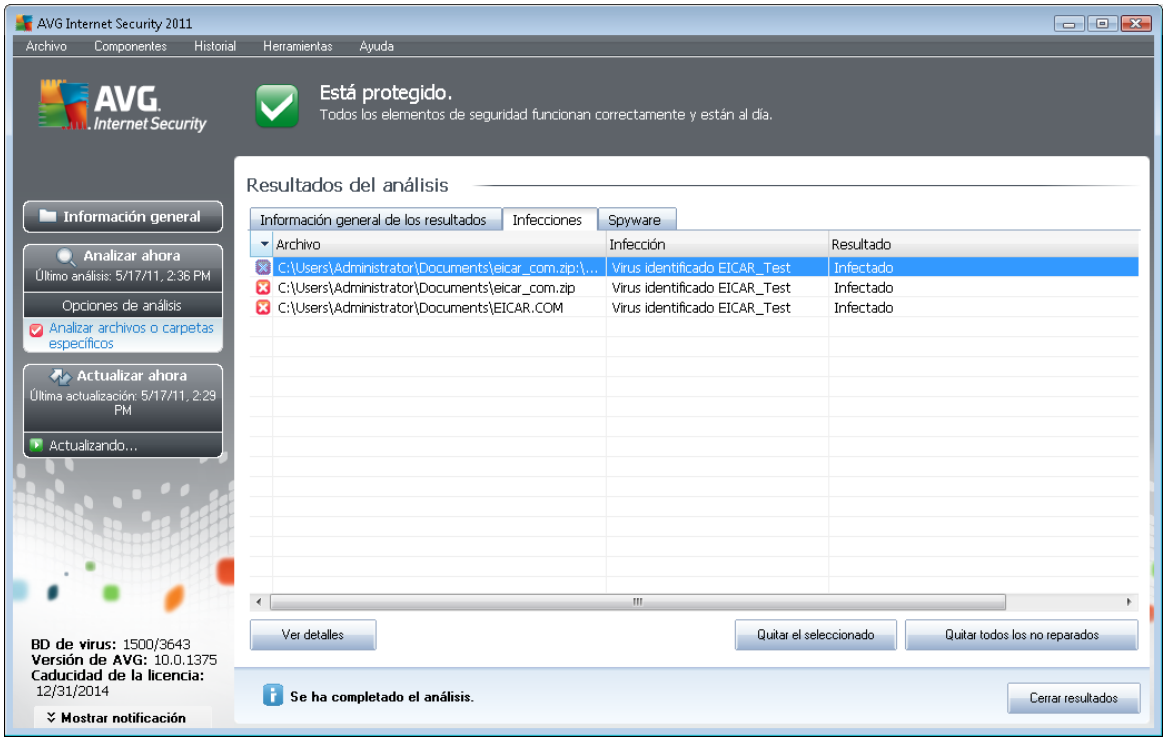
- infecciones de virus / spyware detectados
- infecciones de virus / spyware eliminados
- el número de infecciones de virus / spyware que no pudieron eliminarse ni repararse

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

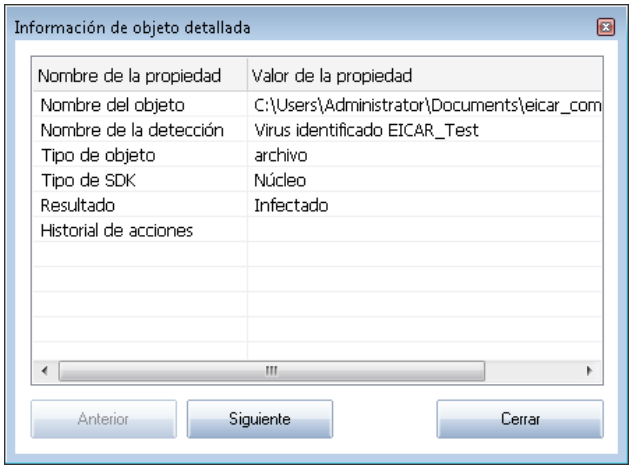
ha agregado a la lista de excepciones PUP (*configuradas en el cuadro de diálogo* ***Excepciones PUP*** *de la configuración avanzada*)

- ***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:

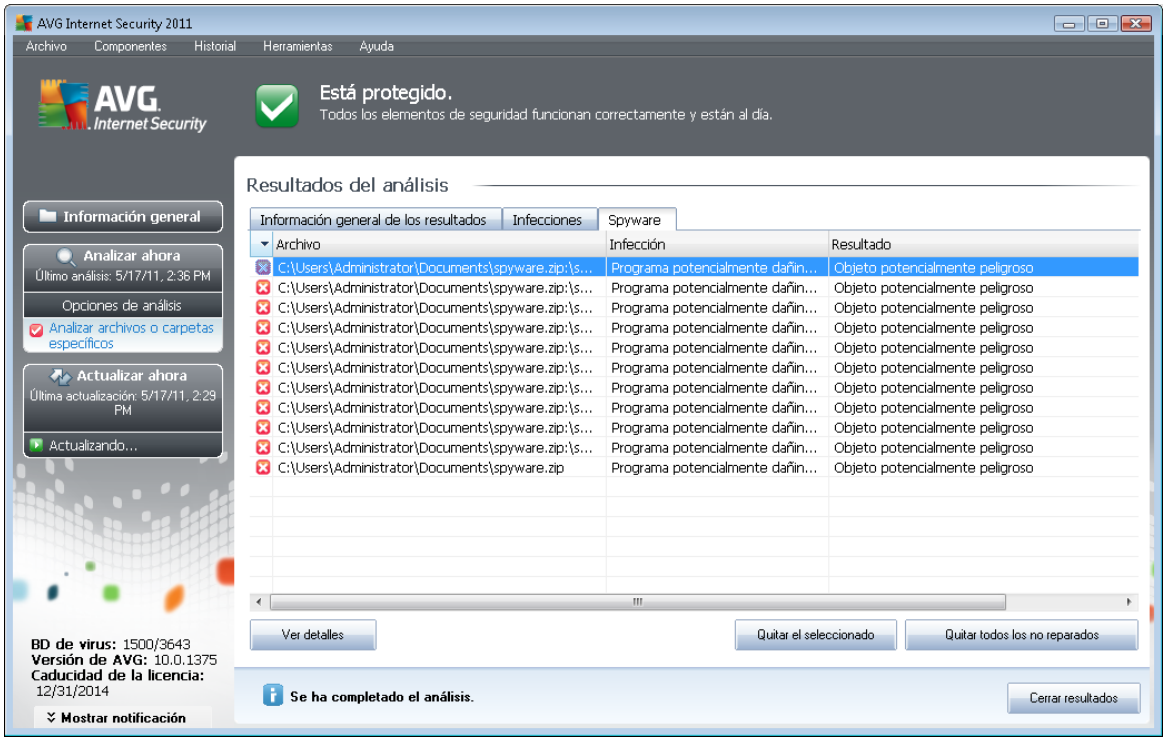
- ***Ver detalles***: el botón abre una nueva ventana de cuadro de diálogo denominada ***Información de objeto detallada***:



  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 detalles sobre virus específicos, consulte la **Enciclopedia de virus** en línea*)
- ***Resultado***: define el estado actual del objeto detectado durante el análisis:
    - ***Infectado***: el objeto infectado se ha detectado y se ha dejado en su ubicación original (por ejemplo, si 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 movió 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*

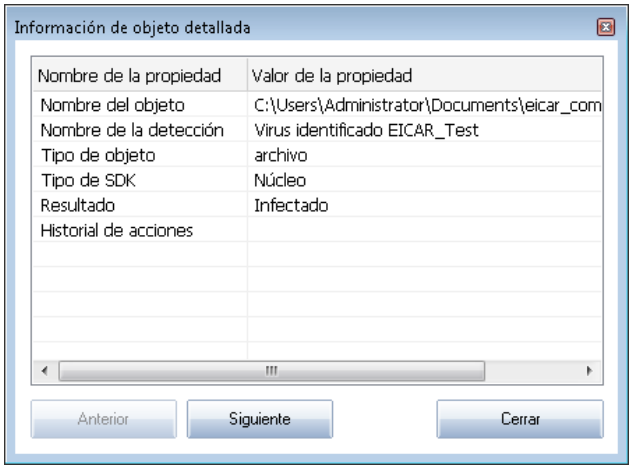
Excepciones PUP *de la configuración avanzada*)

- ***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 ***Almacén de virus de AVG***.***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 puede detectar archivos que quizás no estén infectados, pero que sean sospechosos. Estos archivos son notificados como ***Advertencia*** o como ***Información***.

Se puede notificar una gravedad del tipo ***Información*** por los siguientes motivos:

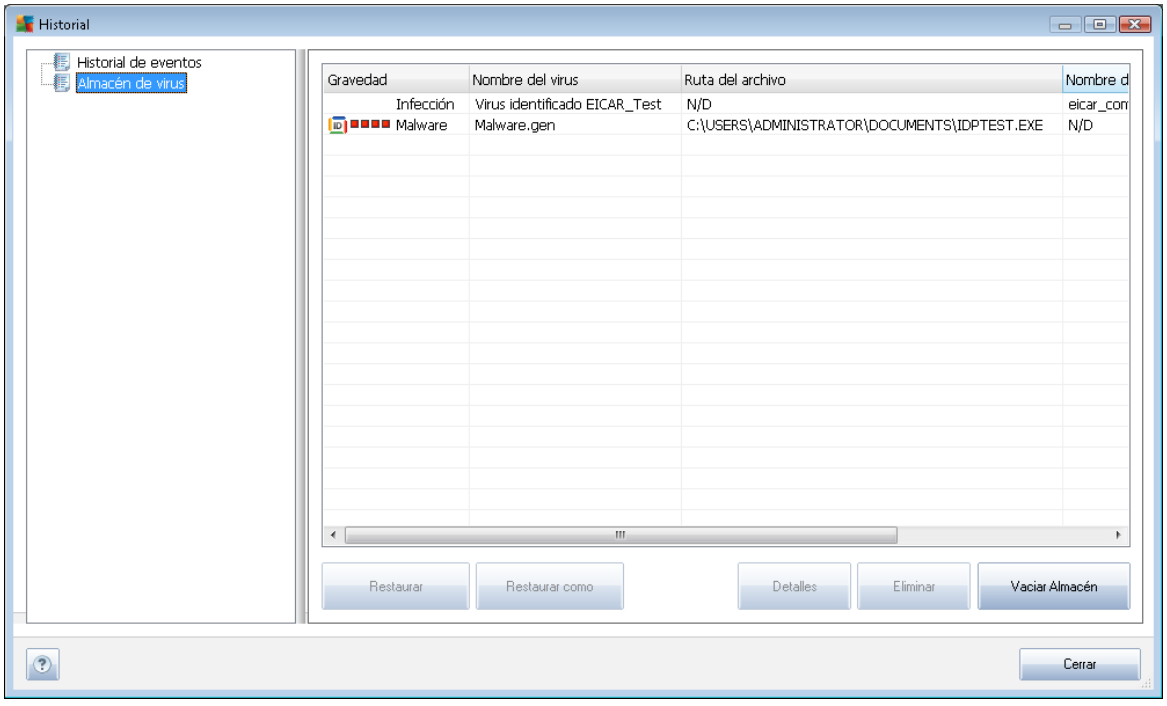
- ***Empaquetado en tiempo de ejecución***: el archivo se empaquetó con uno de los empaquetadores en tiempo de ejecución menos habituales, lo que puede indicar un intento de impedir el análisis de dicho archivo. Sin embargo, no todas las notificaciones sobre tales archivos indican un virus.
- ***Empaquetado 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***: AVG no puede analizar archivos protegidos por contraseña (*por lo general, ningún otro programa 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*). De manera predeterminada, la segunda extensión no es visible en Windows, por lo que AVG informa de este tipo de archivos para evitar que se abran accidentalmente.

- ***Ruta de archivo incorrecta***: si algún archivo importante del sistema se ejecuta desde una ruta diferente a la predeterminada (*por ejemplo, si se ejecuta winlogon.exe desde una ubicación diferente a la carpeta Windows*), AVG informa de 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, por lo que AVG no puede analizarlo. 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 2011**, 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***

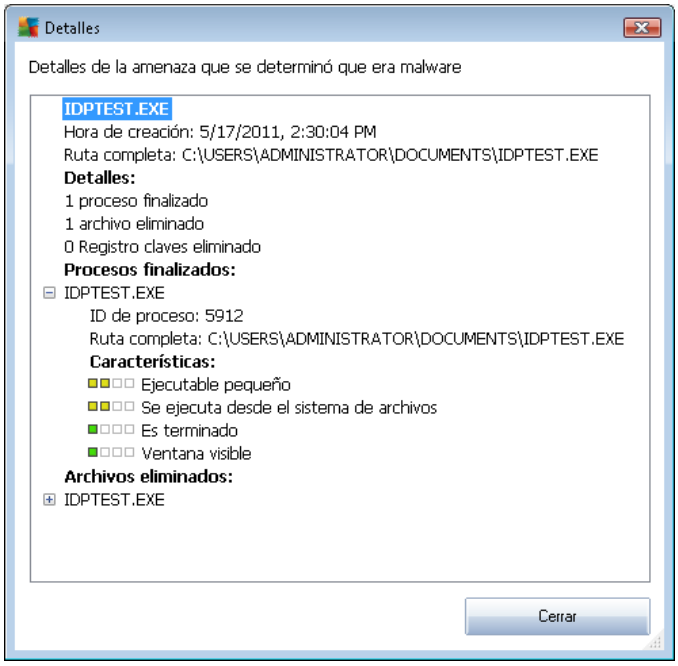
Botones de control

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

Mantener actualizado AVG es esencial para garantizar una detección lo más rápida posible de todos los virus descubiertos recientemente.

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, se recomienda comprobar la disponibilidad de nuevas actualizaciones al menos una vez al día o incluso con más frecuencia. Sólo así podrá estar seguro de que **AVG Internet Security 2011** se mantiene actualizado también durante el día.

12.1. Niveles de actualización

AVG ofrece dos niveles de actualización posibles:

- ***Actualización de definiciones*** contiene los cambios necesarios para una protección antivirus 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 seleccionar el nivel de prioridad que debe descargarse y aplicarse.

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.*

12.2. Tipos de actualización

Pueden distinguirse dos tipos de actualización:

- ***Actualización bajo demanda***: es una actualización de AVG inmediata que se puede ejecutar en cualquier momento que se necesite.

- ***Actualización programada***: en AVG también es posible preconfigurar un plan de actualización. En ese caso, la actualización planeada se lleva a cabo periódicamente según los parámetros de la configuración. Cuando existan nuevos archivos de actualización en la ubicación especificada, se descargarán directamente desde Internet o desde el directorio de la red. Si no hay disponibles actualizaciones más recientes, no se realiza ninguna acción.

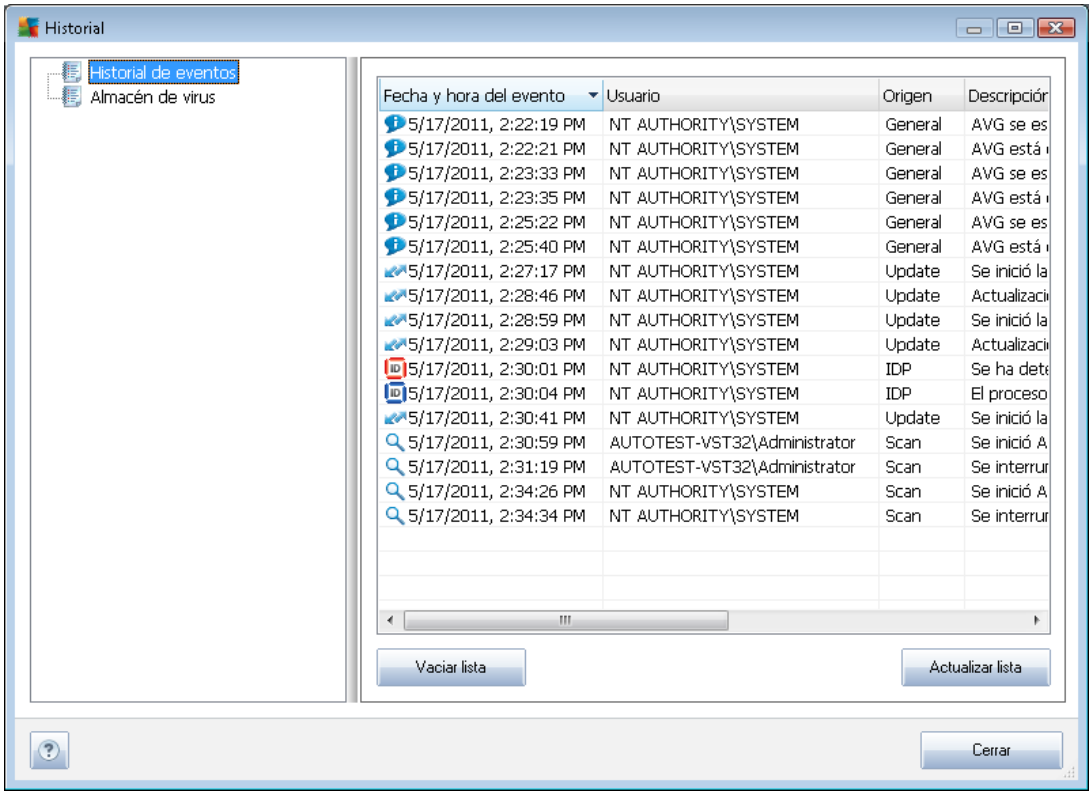
12.3. Proceso de actualización

El proceso de actualización puede iniciarse inmediatamente según sea necesario mediante el vínculo rápido ***Actualizar ahora***. Este vínculo está disponible en todo momento en cualquier cuadro de diálogo de la interfaz de usuario de AVG. Sin embargo, se recomienda encarecidamente realizar actualizaciones regulares como se especifica en la programación de la actualización que se puede editar desde el componente Administrador de actualizaciones.

Una vez iniciada la actualización, AVG verificará primero si hay disponibles nuevos archivos de actualización. Si es así, AVG comenzará la descarga e iniciará el propio proceso de actualización. Durante el proceso de actualización se le redirigirá a la interfaz de ***actualización***, donde podrá ver una representación gráfica del avance del proceso, así como una vista general de 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. Se puede acceder a esta opción a través de Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema. Recomendado sólo para usuarios expertos.*

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 2011**. ***Historial*** registra los siguientes tipos de eventos:

- Información sobre actualizaciones de la aplicación AVG
- Inicio, finalización o detención del análisis (*incluidas las pruebas realizadas automáticamente*)
- Eventos relacionados con la detección de virus (*realizada por la Protección residente o el análisis*) incluyendo 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 quién inició el evento
- ***Origen*** proporciona el componente de origen u otra parte del sistema AVG que generó el

evento

- ***Descripción del evento*** proporciona un breve resumen de lo que en realidad ha sucedido

Botones de control

- ***Vaciar lista***: elimina todas las entradas de la lista de eventos
- ***Actualizar lista***: actualiza todas las entradas de la lista de eventos

14. Preguntas más frecuentes (FAQ) y soporte técnico

En caso de que tenga algún problema con AVG, ya sea administrativo o técnico, consulte la sección ***Preguntas más frecuentes*** del sitio web de AVG (http://www.avg.com/).

Si no consigue encontrar la solución de esta manera, póngase en contacto con el departamento de soporte técnico por correo electrónico. Utilice para ello el formulario de contacto que encontrará en el menú del sistema a través de ***Ayuda / Obtener ayuda en línea***.