



# AVG Internet Security 2011

## Manual del usuario

### Revisión del documento 2011.01 (10.9.2010)

Copyright AVG Technologies CZ, s.r.o. Todos los derechos reservados.  
Todas las demás marcas comerciales pertenecen a sus respectivos propietarios.

Este producto emplea el MD5 Message-Digest Algorithm de RSA Data Security, Inc., Copyright (C) 1991-2 de RSA Data Security, Inc. Creado en 1991.

Este producto emplea código de la biblioteca C-SaCzech, Copyright (c) 1996-2001 de Jaromir Dolecek (dolecek@ics.muni.cz).

Este producto emplea la biblioteca de compresión zlib, Copyright (C) 1995-2002 de Jean-loup Gailly y Mark Adler.

Este producto emplea la biblioteca de compresión libbzip2, Copyright (C) 1996-2002 de Julian R. Seward.



## Contenido

|  |           |
|--|-----------|
| <b>1. Introducción</b>                             | <b>8</b>  |
| <b>2. Requisitos de instalación de AVG</b>         | <b>9</b>  |
| 2.1 Sistemas operativos compatibles                | 9         |
| 2.2 Requisitos mínimos y recomendados de hardware  | 9         |
| <b>3. Opciones de instalación de AVG</b>           | <b>10</b> |
| <b>4. Proceso de instalación de AVG</b>            | <b>11</b> |
| 4.1 Bienvenido                                     | 11        |
| 4.2 Activar su licencia AVG                        | 12        |
| 4.3 Seleccionar el tipo de instalación             | 13        |
| 4.4 Opciones personalizadas                        | 14        |
| 4.5 Instalar la Barra de herramientas AVG Security | 15        |
| 4.6 Cerrar las aplicaciones en ejecución           | 16        |
| 4.7 Progreso de la instalación                     | 17        |
| 4.8 La instalación se ha realizado correctamente   | 18        |
| <b>5. Después de la instalación</b>                | <b>20</b> |
| 5.1 Registro del producto                          | 20        |
| 5.2 Acceso a la interfaz del usuario               | 20        |
| 5.3 Análisis de todo el equipo                     | 20        |
| 5.4 Análisis Eicar                                 | 20        |
| 5.5 Configuración predeterminada de AVG            | 21        |
| <b>6. Interfaz del usuario de AVG</b>              | <b>22</b> |
| 6.1 Menú del sistema                               | 23        |
| 6.1.1 Archivo                                      | 23        |
| 6.1.2 Componentes                                  | 23        |
| 6.1.3 Historial                                    | 23        |
| 6.1.4 Herramientas                                 | 23        |
| 6.1.5 Ayuda  | 23        |
| 6.2 Información del estado de seguridad            | 26        |
| 6.3 Vínculos rápidos                               | 27        |
| 6.4 Descripción general de los componentes         | 28        |
| 6.5 Estadísticas                                   | 29        |
| 6.6 Icono en la bandeja de sistema                 | 29        |



|  |           |
|--|-----------|
| 6.7 Gadget de AVG .....  | 31        |
| <b>7. Componentes de AVG .....</b>                                   | <b>33</b> |
| 7.1 Anti-Virus .....   | 33        |
| 7.1.1 Principios de Anti-Virus .....                                 | 33        |
| 7.1.2 Interfaz de Anti-Virus .....                                   | 33        |
| 7.2 Anti-Spyware .....   | 34        |
| 7.2.1 Principios de Anti-Spyware .....                               | 34        |
| 7.2.2 Interfaz de Anti-Spyware .....                                 | 34        |
| 7.3 Anti-Spam .....  | 36        |
| 7.3.1 Principios de Anti-Spam .....                                  | 36        |
| 7.3.2 Interfaz de Anti-Spam .....                                    | 36        |
| 7.4 Firewall .....   | 38        |
| 7.4.1 Principios de Firewall .....                                   | 38        |
| 7.4.2 Perfiles de Firewall .....                                     | 38        |
| 7.4.3 Interfaz de Firewall .....                                     | 38        |
| 7.5 Link Scanner .....   | 42        |
| 7.5.1 Principios de Link Scanner .....                               | 42        |
| 7.5.2 Interfaz de Link Scanner .....                                 | 42        |
| 7.5.3 Search-Shield .....  | 42        |
| 7.5.4 Surf-Shield .....  | 42        |
| 7.6 Protección residente .....                                       | 45        |
| 7.6.1 Principios de la Protección residente .....                    | 45        |
| 7.6.2 Interfaz de la protección residente .....                      | 45        |
| 7.6.3 Detección de la protección residente .....                     | 45        |
| 7.7 Analizador de correos electrónicos .....                         | 50        |
| 7.7.1 Principios del analizador de correos electrónicos .....        | 50        |
| 7.7.2 Interfaz del analizador de correos electrónicos .....          | 50        |
| 7.7.3 Detección mediante el analizador de correos electrónicos ..... | 50        |
| 7.8 Administrador de actualización .....                             | 54        |
| 7.8.1 Principios del administrador de actualización .....            | 54        |
| 7.8.2 Interfaz del administrador de actualización .....              | 54        |
| 7.9 Licencia .....   | 56        |
| 7.10 Remote administration .....                                     | 57        |
| 7.11 Online Shield .....   | 58        |
| 7.11.1 Principios de Online Shield .....                             | 58        |
| 7.11.2 Interfaz de Online Shield .....                               | 58        |
| 7.11.3 Detección de Online Shield .....                              | 58        |



|   |           |
|---|-----------|
| 7.12 Anti-Rootkit .....                                     | 61        |
| 7.12.1 Principios de Anti-Rootkit .....                     | 61        |
| 7.12.2 Interfaz de Anti-Rootkit .....                       | 61        |
| 7.13 Herramientas del sistema .....                         | 63        |
| 7.13.1 Procesos .....                                       | 63        |
| 7.13.2 Conexiones de red .....                              | 63        |
| 7.13.3 Inicio automático .....                              | 63        |
| 7.13.4 Extensiones del explorador .....                     | 63        |
| 7.13.5 Visor de LSP .....                                   | 63        |
| 7.14 PC Analyzer .....                                      | 68        |
| 7.15 Identity Protection .....                              | 70        |
| 7.15.1 Principios de Identity Protection .....              | 70        |
| 7.15.2 Interfaz de Identity Protection .....                | 70        |
| <b>8. Barra de herramientas AVG Security .....</b>          | <b>73</b> |
| 8.1 Interfaz de la barra de herramientas AVG Security ..... | 73        |
| 8.1.1 Botón del logotipo de AVG .....                       | 73        |
| 8.1.2 Cuadro de búsqueda de Yahoo! .....                    | 73        |
| 8.1.3 Nivel de protección .....                             | 73        |
| 8.1.4 Estado de la página .....                             | 73        |
| 8.1.5 Noticias de AVG .....                                 | 73        |
| 8.1.6 Noticias .....  | 73        |
| 8.1.7 Eliminar historial .....                              | 73        |
| 8.1.8 Notificador de correo electrónico .....               | 73        |
| 8.1.9 Información meteorológica .....                       | 73        |
| 8.1.10 Facebook .....                                       | 73        |
| 8.2 Opciones de la Barra de herramientas AVG Security ..... | 81        |
| 8.2.1 Pestaña General .....                                 | 81        |
| 8.2.2 Pestaña Botones útiles .....                          | 81        |
| 8.2.3 Pestaña Seguridad .....                               | 81        |
| 8.2.4 Pestaña Opciones avanzadas .....                      | 81        |
| <b>9. Configuración avanzada de AVG .....</b>               | <b>85</b> |
| 9.1 Apariencia .....  | 85        |
| 9.2 Sonidos .....   | 87        |
| 9.3 Ignorar condiciones de falla .....                      | 89        |
| 9.4 Identity Protection .....                               | 90        |
| 9.4.1 Configuración de Identity Protection .....            | 90        |
| 9.4.2 Lista Permitidos .....                                | 90        |



|        |  |     |
|--------|--|-----|
| 9.5    | Bóveda de Virus  | 94  |
| 9.6    | Excepciones de PUP   | 94  |
| 9.7    | Anti-Spam  | 96  |
| 9.7.1  | Configuración  | 96  |
| 9.7.2  | Rendimiento  | 96  |
| 9.7.3  | RBL  | 96  |
| 9.7.4  | Lista blanca   | 96  |
| 9.7.5  | Lista negra  | 96  |
| 9.7.6  | Configuración avanzada                                     | 96  |
| 9.8    | Online Shield  | 107 |
| 9.8.1  | Protección web   | 107 |
| 9.8.2  | Mensajería instantánea                                     | 107 |
| 9.9    | Link Scanner   | 111 |
| 9.10   | Análisis   | 111 |
| 9.10.1 | Análisis de todo el equipo                                 | 111 |
| 9.10.2 | Análisis de la extensión de la shell                       | 111 |
| 9.10.3 | Análisis de carpetas o archivos específicos                | 111 |
| 9.10.4 | Análisis de dispositivos extraíbles                        | 111 |
| 9.11   | Programaciones   | 117 |
| 9.11.1 | Análisis programado  | 117 |
| 9.11.2 | Programación de actualización de la base de datos de virus | 117 |
| 9.11.3 | Programación de actualización del programa                 | 117 |
| 9.11.4 | Programación de actualización de Anti-Spam                 | 117 |
| 9.12   | Analizador de correos electrónicos                         | 128 |
| 9.12.1 | Certificación  | 128 |
| 9.12.2 | Filtros de correos electrónicos                            | 128 |
| 9.12.3 | Servidores   | 128 |
| 9.13   | Protección residente                                       | 137 |
| 9.13.1 | Configuración avanzada                                     | 137 |
| 9.13.2 | Elementos excluidos  | 137 |
| 9.14   | Servidor de caché  | 141 |
| 9.15   | Anti-Rootkit   | 142 |
| 9.16   | Actualización  | 143 |
| 9.16.1 | Proxy  | 143 |
| 9.16.2 | Conexión telefónica  | 143 |
| 9.16.3 | URL  | 143 |
| 9.16.4 | Administrar  | 143 |
| 9.17   | Remote administration                                      | 149 |



|   |            |
|---|------------|
| 9.18 Desactivar temporalmente la protección de AVG .....      | 150        |
| 9.19 Programa de mejora de productos .....                    | 150        |
| 9.20 Barra de herramientas AVG Security .....                 | 153        |
| <b>10. Configuración del Firewall .....</b>                   | <b>154</b> |
| 10.1 General .....  | 154        |
| 10.2 Seguridad .....  | 155        |
| 10.3 Perfiles de áreas y adaptadores .....                    | 156        |
| 10.4 IDS .....  | 157        |
| 10.5 Registros .....  | 159        |
| 10.6 Perfiles .....   | 160        |
| 10.6.1 Información del perfil .....                           | 160        |
| 10.6.2 Redes definidas .....                                  | 160        |
| 10.6.3 Aplicaciones .....                                     | 160        |
| 10.6.4 Servicios del sistema .....                            | 160        |
| <b>11. Análisis de AVG .....</b>                              | <b>172</b> |
| 11.1 Interfaz de análisis .....                               | 172        |
| 11.2 Análisis predefinidos .....                              | 173        |
| 11.2.1 Análisis de todo el equipo .....                       | 173        |
| 11.2.2 Análisis de carpetas o archivos específicos .....      | 173        |
| 11.2.3 Análisis Anti-Rootkit .....                            | 173        |
| 11.3 Análisis en el Explorador de Windows .....               | 184        |
| 11.4 Análisis desde línea de comandos .....                   | 185        |
| 11.4.1 Parámetros del análisis desde CMD .....                | 185        |
| 11.5 Programación de análisis .....                           | 187        |
| 11.5.1 Configuración de programación .....                    | 187        |
| 11.5.2 Cómo analizar .....                                    | 187        |
| 11.5.3 Qué analizar .....                                     | 187        |
| 11.6 Descripción general de los resultados del análisis ..... | 197        |
| 11.7 Detalles de los resultados del análisis .....            | 198        |
| 11.7.1 Pestaña Descripción general de los resultados .....    | 198        |
| 11.7.2 Pestaña Infecciones .....                              | 198        |
| 11.7.3 Pestaña Spyware .....                                  | 198        |
| 11.7.4 Pestaña Advertencias .....                             | 198        |
| 11.7.5 Pestaña Rootkits .....                                 | 198        |
| 11.7.6 Pestaña Información .....                              | 198        |
| 11.8 Bóveda de virus .....                                    | 206        |



|   |            |
|---|------------|
| <b>12. Actualizaciones de AVG</b> .....                 | <b>209</b> |
| 12.1 Niveles de actualización .....                     | 209        |
| 12.2 Tipos de actualización .....                       | 209        |
| 12.3 Proceso de actualización .....                     | 209        |
| <b>13. Historial de eventos</b> .....                   | <b>211</b> |
| <b>14. Preguntas frecuentes y soporte técnico</b> ..... | <b>213</b> |



## 1. Introducción

Este manual del usuario proporciona documentación exhaustiva para **AVG Internet Security 2011**.

### **Felicidades por la compra de AVG Internet Security 2011.**

**AVG Internet Security 2011** es uno de los productos de una gama de productos galardonados de AVG, diseñados para proporcionarle tranquilidad y total seguridad para su equipo. Al igual que todos los productos de AVG, **AVG Internet Security 2011** ha sido completamente rediseñado desde la base, para proporcionar la protección de seguridad renombrada y acreditada de AVG de una forma nueva, más agradable y eficiente para el usuario. El nuevo producto **AVG Internet Security 2011** tiene una interfaz simplificada combinada con un análisis más agresivo y rápido. Para su conveniencia se han automatizado más funciones de seguridad y se han incluido nuevas opciones inteligentes para el usuario, de manera que pueda adaptar las funciones de seguridad a su estilo de vida. No anteponga más la facilidad de uso a la seguridad.

AVG se ha diseñado y desarrollado para proteger sus actividades de uso de equipos informáticos y de conexión en red. Disfrute la experiencia de la protección completa de AVG.

### **Todas las ofertas de los productos de AVG**

- Protección relevante para la forma en que utiliza su equipo e Internet: compras y operaciones bancarias, navegación y búsquedas, chat y correo electrónico, o descarga de archivos y redes sociales; AVG cuenta con un producto de protección adecuado para usted
- Protección sin complicaciones en la que confían más de 110 millones de personas en todo el mundo y que está impulsada por una red mundial de investigadores con gran experiencia
- Protección respaldada por soporte experto a cualquier hora





## 2. Requisitos de instalación de AVG

### 2.1. Sistemas operativos compatibles

**AVG Internet Security 2011** tiene como propósito proteger las estaciones de trabajo con los siguientes sistemas operativos:

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

(y posiblemente Service Packs superiores para determinados sistemas operativos)

**Nota:** El componente [Identity Protection](#) no es compatible con Windows XP x64. En este sistema operativo, puede instalar AVG Internet Security 2011, pero sólo sin el componente IDP.

### 2.2. Requisitos mínimos y recomendados de hardware

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

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

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

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



### 3. Opciones de instalación de AVG

AVG se puede instalar desde el archivo de instalación que incorpora el CD de instalación, o puede descargar el archivo de instalación más reciente del sitio web de AVG (<http://www.avg.com/>).

**Antes de comenzar a instalar AVG, le recomendamos que visite el sitio web de AVG (<http://www.avg.com/>) para comprobar si existe algún archivo de instalación nuevo. Así, puede asegurarse de instalar la última versión disponible de AVG Internet Security 2011.**

Durante el proceso de instalación, se le solicitará su número de venta o número de licencia. Por favor, téngalo a mano antes de comenzar con la instalación. El número de venta se encuentra en el paquete del CD. Si ha adquirido su copia de AVG en línea, se le ha enviado el número de licencia por correo electrónico.



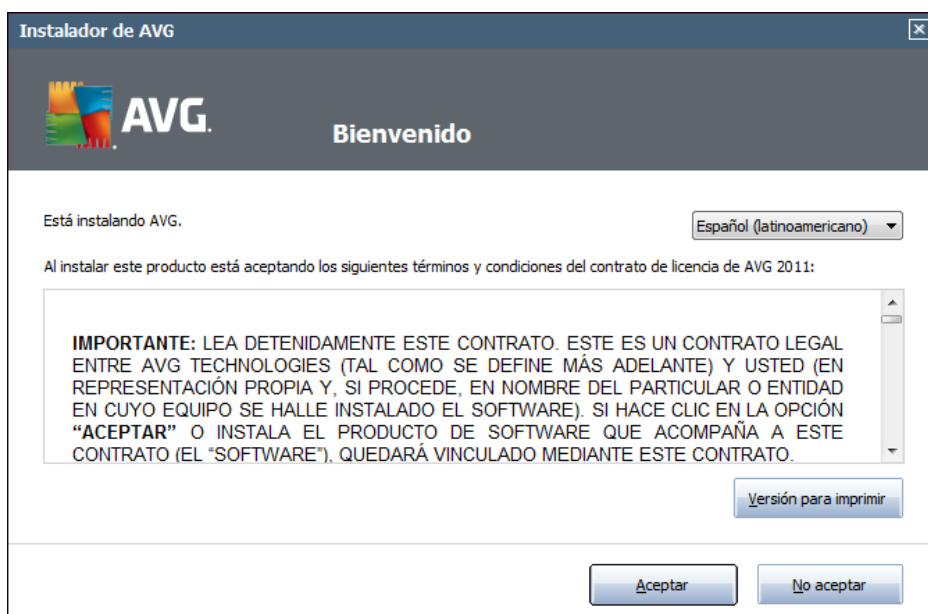
## 4. Proceso de instalación de AVG

Para instalar **AVG Internet Security 2011** en su equipo debe obtener el archivo de instalación más reciente. Puede utilizar el CD de instalación que forma parte de su edición en caja, pero este archivo puede no estar actualizado. Por lo tanto, recomendamos obtener el archivo de instalación más reciente en línea. Puede descargar el archivo desde el sitio Web de AVG (<http://www.avg.com/>), en la sección [Centro de soporte/Descarga](#).

La instalación consta de una secuencia de ventanas de diálogo que contienen una breve descripción de lo que se debe hacer en cada paso. A continuación, ofrecemos una explicación para cada ventana de diálogo:

### 4.1. Bienvenido

El proceso de instalación comienza con la ventana del cuadro de diálogo **Bienvenido**. Aquí selecciona el idioma empleado para el proceso de instalación y el idioma predeterminado de la interfaz del usuario de AVG. En la sección superior de la ventana del cuadro de diálogo se encuentra el menú desplegable con la lista de los idiomas que puede seleccionar:



**Atención:** Aquí se selecciona el idioma del proceso de instalación. El idioma que seleccione se instalará como idioma predeterminado de la interfaz del usuario de AVG, junto con el inglés, que se instala automáticamente. Si desea instalar otros idiomas adicionales para la interfaz del usuario, defínalos en el cuadro de diálogo de configuración [Opciones personalizadas](#).

Además, el cuadro de diálogo muestra íntegramente el contrato de licencia de AVG. Léalo con detenimiento. Para confirmar que lo leyó, lo entendió y acepta el contrato, presione el botón **Aceptar**. Si no está conforme con el contrato de licencia, presione el botón **No acepto** y el proceso de instalación se terminará de inmediato.



## 4.2. Activar su licencia AVG

En el cuadro de diálogo **Active su licencia** se le invita a introducir su número de licencia en el campo de texto incluido.

El número de venta se puede encontrar en el paquete del CD en la caja de **AVG Internet Security 2011**. El número de licencia se encuentra en el correo electrónico de confirmación que recibió después de la compra en línea de **AVG Internet Security 2011**. Debe escribir el número exactamente como se muestra. Si está disponible el número de licencia en formato digital (*en el correo electrónico*), se recomienda utilizar el método de copiar y pegar para insertarlo.

Instalador de AVG

**AVG** Active la licencia

Número de licencia:

Ejemplo: 9FULL-NSDR5-KUL4L-UKSFR-L96M9-B2ALT-XWMX3

Si compró el software AVG 2011 en línea, se le enviará el número de licencia por correo electrónico. Para evitar errores de escritura, recomendamos cortar y pegar el número del mensaje de correo a esta pantalla.

Si compró el software en una tienda, encontrará el número de licencia en la tarjeta de registro de producto incluida con el paquete. Asegúrese de copiar el número correctamente.

< Atrás    Siguiete >    Cancelar

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



### 4.3. Seleccionar el tipo de instalación



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

Para la mayoría de los usuarios, se recomienda mantener la **Instalación rápida** estándar, que instala el programa AVG en modo totalmente automático con la configuración predefinida por el proveedor del programa. Esta configuración proporciona la máxima seguridad combinada con el uso óptimo de los recursos. En el futuro, si es necesario cambiar la configuración, siempre podrá hacerlo directamente en la aplicación AVG. Si ha seleccionado la opción **Instalación rápida**, presione el botón **Siguiete** para proceder al siguiente cuadro de diálogo **Instalar la Barra de herramientas AVG Security**.

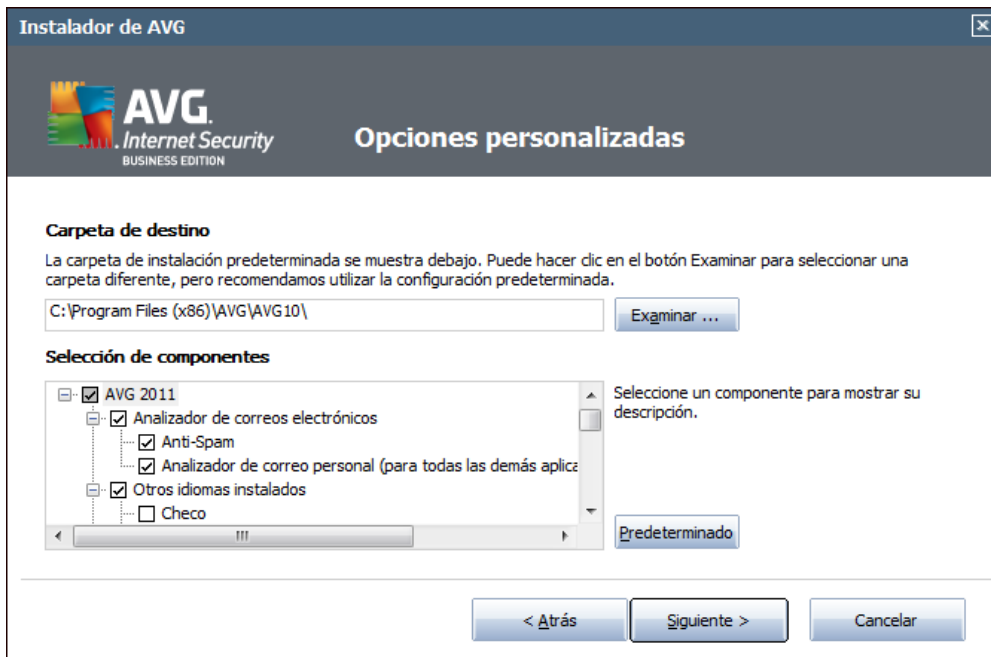
La **Instalación personalizada** sólo debería ser utilizada por usuarios con experiencia que tienen un motivo importante para instalar AVG con una configuración distinta de la estándar (por ejemplo, para ajustarse a necesidades específicas del sistema). Una vez seleccionada esta opción, presione el botón **Siguiete** para proceder al cuadro de diálogo **Opciones personalizadas**.

En la sección de la derecha del cuadro de diálogo encontrará la casilla de verificación relacionada con el **gadget AVG** (*admitido en Windows Vista/Windows 7*). Si desea tener instalado este gadget, marque la casilla de verificación correspondiente. **El gadget AVG** aparecerá en la barra lateral de Windows para proporcionarle acceso inmediato a las funciones más importantes de **AVG Internet Security 2011**, es decir, **análisis** y **actualización**.



#### 4.4. Opciones personalizadas

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



##### Carpeta de destino

En la sección **Carpeta de destino** del cuadro de diálogo debe especificar la ubicación en la que se instalará **AVG Internet Security 2011**. De modo predeterminado, AVG se instalará en la carpeta de archivos de programa de la unidad C:. Si la carpeta no existe, un nuevo cuadro de diálogo le pedirá que confirme que está de acuerdo en que AVG cree esta carpeta en este momento. Si desea cambiar esta ubicación, utilice el botón **Examinar** para ver la estructura de la unidad y seleccione la carpeta correspondiente.

##### Selección de componentes

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

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

Resalte cualquier elemento de la lista **Selección de componentes**, y aparecerá una breve descripción del componente correspondiente en la parte derecha de esta



sección. Para obtener información detallada sobre las funciones de cada componente, consulte el capítulo [Descripción general de los componentes](#) de esta documentación. Para volver a la configuración predeterminada predefinida por el proveedor de software, utilice el botón **Predeterminado**.

Presione el botón **Siguiente** para continuar.

#### 4.5. Instalar la Barra de herramientas AVG Security

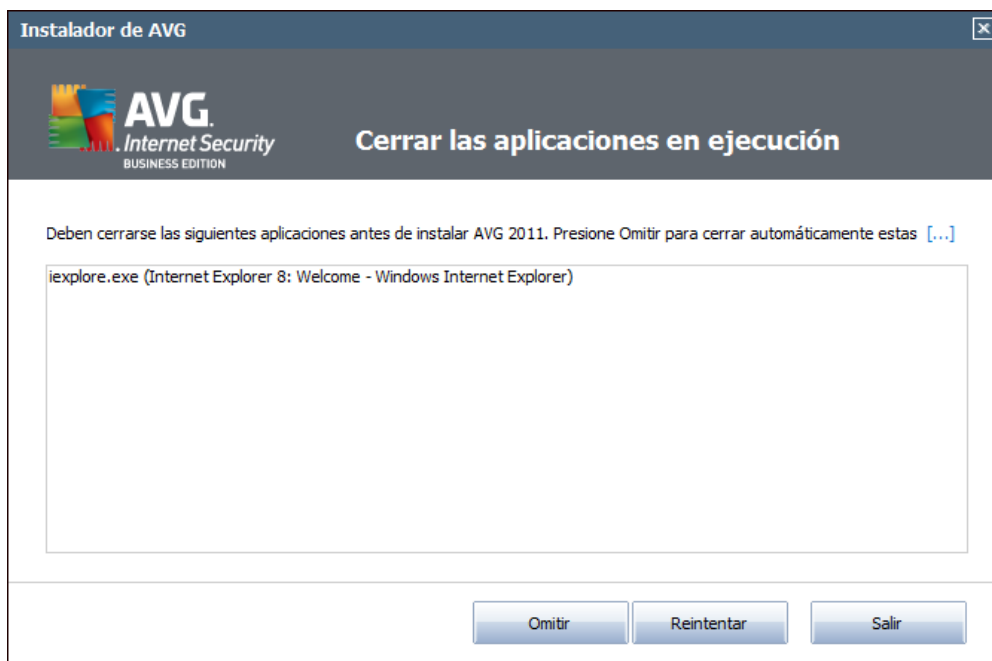


En el cuadro de diálogo **Instalar la Barra de herramientas AVG Security**, decida si desea instalar la [Barra de herramientas AVG Security](#). Si no cambia la configuración predeterminada, este componente se instalará automáticamente en el navegador de Internet (los navegadores compatibles actualmente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

Asimismo, puede decidir si desea utilizar Yahoo! como su proveedor de búsqueda predeterminado. De ser así, mantenga marcada la casilla de verificación correspondiente.



#### 4.6. Cerrar las aplicaciones en ejecución



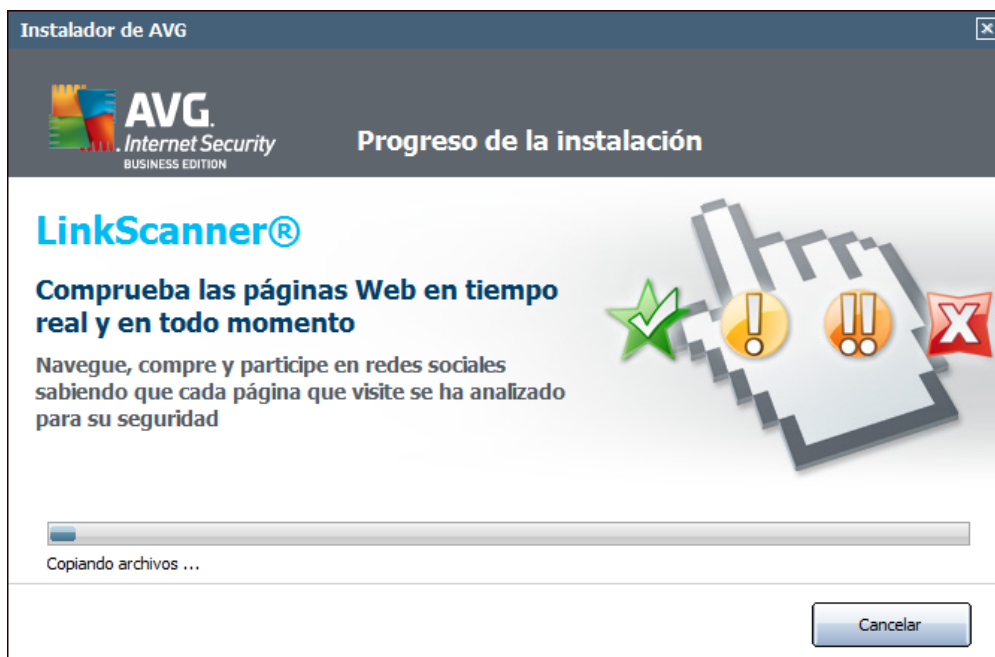
El cuadro de diálogo **Cerrar las aplicaciones en ejecución** sólo aparecerá durante el proceso de instalación si en su equipo se produjera un conflicto con otros programas en ejecución. A continuación, se proporcionará una lista de los programas que deben cerrarse para finalizar correctamente el proceso de instalación. Presione el botón **Salir** sobre un elemento seleccionado en la lista para terminar la aplicación correspondiente o presione el botón **Reintentar** para confirmar que está de acuerdo en cerrar las aplicaciones correspondientes y continuar con el paso siguiente.





#### 4.7. Progreso de la instalación

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



Cuando el proceso de instalación haya terminado, el programa y la base de datos de virus se actualizarán automáticamente. Luego será redirigido al cuadro de diálogo siguiente.



#### 4.8. La instalación se ha realizado correctamente



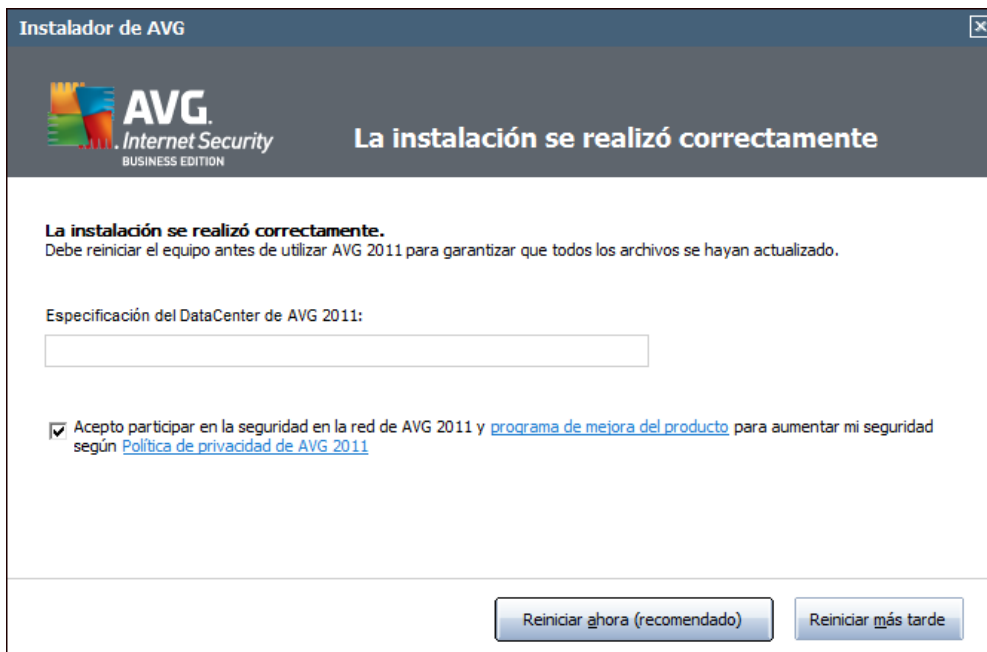
El cuadro de diálogo **La instalación se ha realizado correctamente** confirma que **AVG Internet Security 2011** se ha instalado y configurado por completo.

En este cuadro de diálogo proporcione su información de contacto para que pueda recibir toda la información y las noticias relativas a los productos. Debajo del formulario de registro verá las dos opciones siguientes:

- **Sí, quiero recibir información sobre las noticias de seguridad y las ofertas especiales de AVG 2011 por correo electrónico:** seleccione esta casilla de verificación para confirmar que desea recibir información sobre las novedades en la esfera de la seguridad de Internet y que desea recibir información sobre ofertas especiales, mejoras, actualizaciones, etc., de los productos de AVG.
- **Acepto participar en el programa de seguridad en la red y mejora de productos de AVG 2011...:** seleccione esta casilla de verificación para aceptar que desea participar en el programa de mejora de productos (*para obtener más detalles, consulte el capítulo [Configuración avanzada de AVG/ Programa de mejora de productos](#)*) que recopila información anónima sobre las amenazas detectadas para aumentar el nivel general de seguridad en Internet.

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

**Nota:** Si utiliza cualquier licencia de AVG para empresas y en caso de que haya seleccionado anteriormente que se instalara el elemento Remote Administration (consulte [Opciones personalizadas](#)), aparecerá el cuadro de diálogo La instalación se ha realizado correctamente, con la interfaz siguiente:



*Debe especificar los parámetros de AVG DataCenter; proporcione la cadena de conexión a AVG DataCenter con el formato servidor:puerto. Si esta información no está disponible por el momento, deje el campo en blanco; más tarde, puede proporcionar la configuración en el cuadro de diálogo [Configuración avanzada/Remote Administration](#). Para obtener información detallada acerca de AVG Remote Administration, consulte el manual del usuario de AVG Network Edition, que puede descargar del sitio web de AVG (<http://www.avg.com/>).*



## 5. Después de la instalación

### 5.1. Registro del producto

Al terminar la instalación de **AVG Internet Security 2011**, registre su producto en línea en el sitio web de AVG (<http://www.avg.com/>), en la página **Registro** ( *siga las instrucciones indicadas directamente en la página*). Tras el registro, dispondrá de pleno acceso a la cuenta de usuario AVG, el boletín de actualizaciones de AVG y otros servicios que se ofrecen exclusivamente para los usuarios registrados.

### 5.2. Acceso a la interfaz del usuario

Se puede obtener acceso a la [Interfaz del usuario de AVG](#) de varios modos:

- Haga doble clic en el [icono de la bandeja del sistema AVG](#).
- haga doble clic en el icono AVG del escritorio
- Haga doble clic en la línea de estado situada en la sección inferior del [gadget AVG](#) (*si está instalado; compatible con Windows Vista/Windows 7*).
- desde el menú **Inicio/Programas/AVG 2011/Interfaz del usuario de AVG**
- Desde la [Barra de herramientas AVG Security](#) , a través de la opción **Ejecutar AVG**

### 5.3. Análisis de todo el equipo

Existe el riesgo potencial de que un virus informático se transmitiera a su equipo antes de la instalación de **AVG Internet Security 2011**. Por esta razón debe ejecutar un [Análisis de todo el equipo](#) para estar seguro de que no hay infecciones en su equipo.

Para obtener instrucciones sobre la ejecución de un [Análisis de todo el equipo](#) consulte el capítulo [Análisis de AVG](#).

### 5.4. Análisis Eicar

Para confirmar que **AVG Internet Security 2011** se ha instalado correctamente, puede realizar el análisis EICAR.

El Análisis EICAR es un método estándar y absolutamente seguro que se utiliza para comprobar el funcionamiento de un sistema anti-virus. Es seguro emplearlo porque no se trata de un virus real y no incluye ningún fragmento de código viral. La mayoría de los productos reaccionan ante él como si fuera un virus (*aunque suelen notificarlo con un nombre obvio, tal como "EICAR-AV-Test" [análisis anti-virus EICAR]*). Puede descargar el virus EICAR del sitio web [www.eicar.com](http://www.eicar.com). Allí también encontrará toda la información necesaria relacionada con el análisis EICAR.



Intente descargar el archivo ***eicar.com*** y guárdelo en el disco local. Inmediatamente después de que confirme que desea descargar el archivo de análisis, ***Online Shield*** reaccionará con una advertencia. Esta notificación demuestra que AVG se ha instalado correctamente en su equipo.



Desde el sitio web <http://www.eicar.com> también puede descargar la versión comprimida del "virus" EICAR (por ejemplo, con el formato *eicar\_com.zip*). ***Online Shield*** permite descargar este archivo y guardarlo en el disco local, pero la ***Protección residente*** detectará el "virus" cuando intente descomprimirlo. **Si AVG no identifica el archivo de análisis EICAR como un virus, deberá comprobar nuevamente la configuración del programa.**

## 5.5. Configuración predeterminada de AVG

La configuración predeterminada (es decir, la configuración de la aplicación inmediatamente después de la instalación) de **AVG Internet Security 2011** está definida por el proveedor de software para que todos los componentes y funciones proporcionen un rendimiento óptimo.

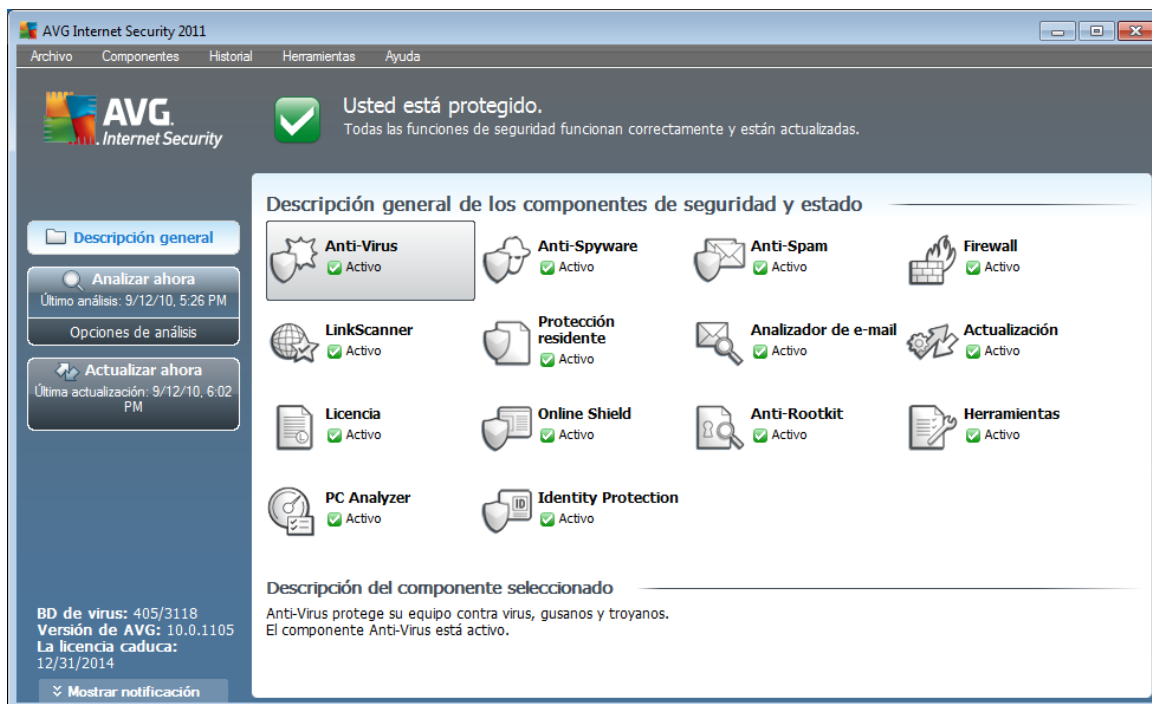
**No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración.**

Se pueden efectuar pequeñas modificaciones de la configuración de los ***componentes de AVG*** directamente desde la interfaz del usuario del componente concreto. Si considera que debe cambiar la configuración de AVG para adaptarla mejor a sus necesidades, vaya a ***Configuración avanzada de AVG***, seleccione el elemento del menú del sistema ***Herramientas/Configuración avanzada*** y modifique la configuración de AVG en el cuadro de diálogo ***Configuración avanzada de AVG*** que se abre.



## 6. Interfaz del usuario de AVG

AVG Internet Security 2011 se abre con la ventana principal:



La ventana principal se divide en varias secciones:

- **Menú del sistema** (línea del sistema superior en la ventana) es la navegación estándar que le permite tener acceso a todos los componentes, servicios y funciones de AVG. [Detalles >>](#)
- **Información del estado de seguridad** (sección superior de la ventana) le proporciona información acerca del estado actual de su programa AVG. [Detalles >>](#)
- **Vínculos rápidos** (sección izquierda de la ventana) le permite tener acceso rápidamente a las tareas de AVG más importantes y que se utilizan con mayor frecuencia. [Detalles >>](#)
- **Vista general de componentes** (sección central de la ventana) ofrece una descripción general de todos los componentes de AVG instalados. [Detalles >>](#)
- **Estadísticas** (sección inferior izquierda de la ventana) le proporciona todos los datos estadísticos relacionados con la operación de los programas. [Detalles >>](#)
- **Icono de la bandeja del sistema** (esquina inferior derecha del monitor, en la bandeja del sistema) indica el estado actual del AVG. [Detalles >>](#)
- **El gadget de AVG** (barra lateral de Windows, compatible con Windows Vista/7) permite un acceso rápido al análisis y la actualización de AVG. [Detalles >>](#)



## 6.1. Menú del sistema

El **menú del sistema** es el método de navegación estándar que se utiliza en todas las aplicaciones Windows. Está situado horizontalmente en la parte superior de la ventana principal de **AVG Internet Security 2011**. Utilice el menú del sistema para acceder a componentes, funciones y servicios específicos de AVG.

El menú del sistema está dividido en cinco secciones principales:

### 6.1.1. Archivo

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

### 6.1.2. Componentes

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

- **Descripción general del sistema**: permite ir al cuadro de diálogo predeterminado de la interfaz del usuario con la [descripción general de todos los componentes instalados y su estado](#).
- **Anti-Virus** garantiza la protección del equipo frente a los virus que intenten introducirse en él. [Detalles >>](#)
- **Anti-Spyware** garantiza que el equipo está protegido contra spyware y adware. [Detalles >>](#)
- **Anti-Spam** analiza todos los mensajes de correo electrónico y marca los no deseados como SPAM. [Detalles >>](#)
- **Firewall** controla cómo el equipo intercambia datos con otros equipos en Internet o la red local. [Detalles >>](#)
- **Link Scanner** verifica los resultados de búsqueda visualizados en el navegador de Internet. [Detalles >>](#)
- **Analizador de correos electrónicos** analiza todo el correo entrante y saliente para ver si contiene virus. [Detalles >>](#)
- **Protección residente** se ejecuta en segundo plano y analiza los archivos mientras éstos se copian, abren o guardan. [Detalles >>](#)
- **Administrador de actualización** controla todas las actualizaciones de AVG. [Detalles >>](#)
- **Licencia** muestra el número de licencia, el tipo de licencia y la fecha de vencimiento. [Detalles >>](#)



- **Online Shield** analiza todos los datos que se descargan mediante un navegador web. [Detalles >>](#)
- **Anti-Rootkit** detecta los programas y las tecnologías que intentan ocultar malware. [Detalles >>](#)
- **Herramientas del sistema** ofrece un resumen detallado del entorno de AVG e información del sistema operativo. [Detalles >>](#)
- **PC Analyzer** es un analizador que proporciona información sobre el estado del equipo. [Detalles >>](#)
- **Identity Protection**: componente anti-malware que se centra en evitar los robos de identidad utilizando su valiosa información digital personal. [Detalles >>](#)
- **Remote Administration** sólo se muestra en AVG Network Edition si especificó durante el [proceso de instalación](#) que desea tener este componente instalado

### 6.1.3. Historial

- **Resultados del análisis**: cambia a la interfaz de análisis de AVG, específicamente al diálogo de [Descripción general de los resultados del análisis](#)
- **Detección de protección residente**: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por la [Protección residente](#)
- **Detección del Analizador de correos electrónicos**: abre un cuadro de diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente [Analizador de correos electrónicos](#)
- **Hallazgos de Online Shield**: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por [Online Shield](#)
- **Bóveda de Virus**: abre la interfaz del espacio de cuarentena ([Bóveda de Virus](#)) en el cual AVG elimina todas las infecciones detectadas que no pueden repararse automáticamente por alguna razón. Los archivos infectados se aíslan dentro de esta cuarentena, garantizando la seguridad de su equipo, y al mismo tiempo se guardan los archivos infectados para repararlos en el futuro si existe la posibilidad.
- **Registro de historial de eventos**: abre la interfaz del registro de historial de todas las acciones **AVG Internet Security 2011** registradas.
- **Firewall**: abre la interfaz de configuración del Firewall en la pestaña [Registros](#) con una descripción general detallada de todas las acciones del Firewall.





#### 6.1.4. Herramientas

- **Analizar el equipo:** cambia a la [interfaz de análisis de AVG](#) y ejecuta un análisis del equipo completo
- **Analizar la carpeta seleccionada:** cambia a la [interfaz de análisis de AVG](#) y permite definir qué archivos y carpetas se analizarán dentro de la estructura de árbol de su equipo
- **Analizar archivo:** permite ejecutar un análisis bajo petición en un archivo seleccionado de la estructura de árbol de su disco
- **Actualizar:** ejecuta automáticamente el proceso de actualización de **AVG Internet Security 2011**
- **Actualizar desde el directorio:** ejecuta el proceso de actualización desde los archivos de actualización ubicados en una carpeta específica en el disco local. Sin embargo, esta opción sólo se recomienda en casos de emergencia, por ejemplo, en situaciones en que no existe una conexión a Internet disponible *por ejemplo, su equipo se encuentra infectado y está desconectado de Internet, su equipo está conectado a una red sin acceso a Internet, etc.*). En la nueva ventana abierta, seleccione la carpeta donde guardó el archivo de actualización anteriormente, y ejecute el proceso de actualización.
- **Configuración avanzada:** abre el cuadro de diálogo [Configuración avanzada de AVG](#) en el cual es posible editar la configuración de **AVG Internet Security 2011**. Generalmente, se recomienda mantener la configuración predeterminada de la aplicación como se encuentra definida por el distribuidor del software.
- **Configuración del Firewall:** abre un cuadro de diálogo independiente para la configuración avanzada del componente [Firewall](#)

#### 6.1.5. Ayuda

- **Contenido:** abre los archivos de ayuda AVG
- **Obtener ayuda en línea:** abre el sitio Web de AVG (<http://www.avg.com/>) en la página del centro de soporte al cliente
- **Su Web AVG:** abre el sitio Web de AVG (<http://www.avg.com/>)
- **Acerca de virus y amenazas:** abre la [Enciclopedia de virus](#) en línea donde puede buscar información detallada acerca del virus identificado
- **Reactivar:** abre el cuadro de diálogo **Activar AVG** con la información introducida en el cuadro de diálogo [Personalizar AVG](#) del [proceso de instalación](#). Dentro de este cuadro de diálogo puede introducir el número de licencia para reemplazar el número de venta (*el número con el que instaló AVG*) o el número de licencia antiguo (*como al actualizar a un nuevo producto AVG*).
- **Registrar ahora:** permite conectarse a la página de registro del sitio Web de AVG (<http://www.avg.com/>). Introduzca su información de registro; sólo los



clientes con productos AVG registrados pueden recibir soporte técnico gratuito.

**Nota:** si utiliza la versión de prueba de **AVG Internet Security 2011**, los dos últimos elementos aparecen como **Comprar ahora** y **Activar**, con lo que puede comprar la versión completa del programa inmediatamente. Para **AVG Internet Security 2011** instalado con un número de venta, los elementos aparecen como **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 pestañas que proporcionan información acerca del nombre del programa, la versión del programa y la base de datos de virus, información del sistema, el contrato de licencia e información de contacto de **AVG Technologies CZ**.

## 6.2. Información del estado de seguridad

La sección **Información del estado de seguridad** está situada en la parte superior de la ventana principal de AVG. En esta sección siempre encontrará información sobre el estado de seguridad actual de su **AVG Internet Security 2011**. Consulte la descripción general de los iconos que posiblemente se muestran en esta sección, y su significado:



- El icono verde indica que AVG funciona completamente. Su equipo está totalmente protegido, actualizado y todos los componentes instalados funcionan correctamente.



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

Este icono también aparece si por alguna razón ha decidido [ignorar el estado de error de un componente](#) (la opción "Ignorar el estado del componente" está disponible desde el menú contextual haciendo clic con el botón secundario sobre el icono del componente respectivo en la descripción general del componente de la ventana principal de AVG). Puede ser necesario utilizar esta opción en una situación específica, pero es muy recomendable desactivar la opción "**Ignorar el estado del componente**" a la mayor brevedad.



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



[técnico de AVG.](#)

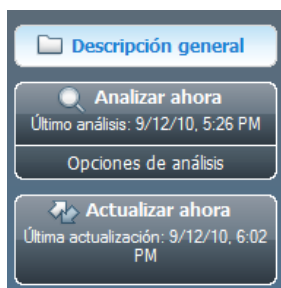
En caso de que AVG no esté configurado para un rendimiento óptimo, aparece un nuevo botón llamado Reparar (de forma alternativa, Reparar todo si el problema concierne a más de un componente) junto a la información de estado de seguridad. Presione el botón para iniciar un proceso automático de confirmación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

Se recomienda encarecidamente que preste atención a la **información del estado de seguridad** y en caso de que el informe indique algún problema, siga adelante y trate de solucionarlo de inmediato. De otra manera, su equipo estará en peligro.

**Nota:** la información de estado de AVG también se puede obtener en cualquier momento del [icono de la bandeja del sistema](#).

### 6.3. Vínculos rápidos

Los **vínculos rápidos** (en la sección izquierda de la [Interfaz del usuario de AVG](#)) le permiten el acceso inmediato a las funciones más importantes y de uso más frecuente de AVG:



- **Descripción general** : utilice este vínculo para cambiar de cualquier interfaz de AVG abierta actualmente a la interfaz predeterminada con una descripción general de todos los componentes instalados (consulte el capítulo [Descripción general de los componentes >>](#))
- **Analizar ahora**: de manera predeterminada, el botón proporciona información (tipo de análisis, fecha de último lanzamiento) de este último análisis iniciado. Puede ejecutar el comando **Analizar ahora** para volver a iniciar el mismo análisis, o siga el vínculo **Analizador de equipo** para abrir la interfaz del usuario de AVG, donde podrá ejecutar análisis, programar análisis o editar sus parámetros. Consulte el capítulo [Análisis de AVG >>](#)
- **Actualizar ahora**: el vínculo proporciona la fecha en que se inició el proceso de actualización la última vez. Presione el botón para abrir la interfaz de actualización, y ejecute el proceso de actualización de AVG inmediatamente. Consulte el capítulo [Actualizaciones de AVG >>](#)

Estos vínculos están disponibles desde la interfaz del usuario en todo momento. Una



vez que emplea un vínculo rápido para ejecutar un proceso específico, la interfaz gráfica del usuario (GUI) cambiará a un nuevo cuadro de diálogo pero los vínculos rápidos aún están disponibles. Más aún, el proceso de ejecución se ve más gráficamente.

#### 6.4. Descripción general de los componentes

La sección **descripción general de los componentes** se encuentra en la parte central de la [Interfaz del usuario de AVG](#). La sección se divide en dos partes:

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

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

- **Anti-Virus** garantiza la protección del equipo frente a los virus que intenten introducirse en él. [Detalles >>](#)
- **Anti-Spyware** garantiza que el equipo está protegido contra spyware y adware. [Detalles >>](#)
- **Anti-Spam** analiza todos los mensajes de correo electrónico y marca los no deseados como SPAM. [Detalles >>](#)
- **Firewall** controla cómo el equipo intercambia datos con otros equipos en Internet o la red local. [Detalles >>](#)
- **Link Scanner** verifica los resultados de búsqueda visualizados en el navegador de Internet. [Detalles >>](#)
- **Analizador de correos electrónicos** analiza todo el correo entrante y saliente para ver si contiene virus. [Detalles >>](#)
- **Protección residente** se ejecuta en segundo plano y analiza los archivos mientras éstos se copian, abren o guardan. [Detalles >>](#)
- **Administrador de actualización** controla todas las actualizaciones de AVG. [Detalles >>](#)
- **Licencia** muestra el número de licencia, el tipo de licencia y la fecha de vencimiento. [Detalles >>](#)
- **Online Shield** analiza todos los datos que se descargan mediante un navegador web. [Detalles >>](#)
- **Anti-Rootkit** detecta los programas y las tecnologías que intentan ocultar malware. [Detalles >>](#)



- **Herramientas del sistema** ofrece un resumen detallado del entorno de AVG e información del sistema operativo. [Detalles >>](#)
- **PC Analyzer** proporciona información sobre el estado del equipo. [Detalles >>](#)
- **Identity Protection**: componente anti-malware que se centra en evitar los robos de identidad utilizando su valiosa información digital personal. [Detalles >>](#)
- **Remote Administration** sólo se muestra en AVG Network Edition si especificó durante el [proceso de instalación](#) que desea tener este componente instalado

Haga un solo clic en el icono de cualquier componente para resaltarlo en la vista general de componentes. Simultáneamente aparece una descripción de las funciones básicas del componente en la parte inferior de la interfaz del usuario. Haga doble clic en el icono para abrir la interfaz propia del componente con una lista de datos estadísticos básicos.

Haga clic con el botón secundario del mouse sobre el icono de un componente para expandir un menú de contexto; además, al abrir la interfaz gráfica del componente también puede seleccionar **Ignorar el estado del componente**. Seleccione esta opción para expresar que es consciente del [estado de error del componente](#) pero que por alguna razón desea conservar su AVG de esta manera y no desea que se le advierta mediante el [icono en la bandeja de sistema](#).

## 6.5. Estadísticas

La sección **Estadísticas** se encuentra en la parte inferior izquierda de la [Interfaz del usuario de AVG](#). Ofrece una lista de información acerca del funcionamiento del programa:

- **Base de datos de virus**: informa de la versión de la base de datos de virus instalada en este momento.
- **Versión AVG**: informa de la versión instalada del programa AVG (*el número tiene el formato 10.0.xxxx, donde 10.0 es la versión de la línea de producto y xxxx es el número de compilación*)
- **La licencia caduca**: indica la fecha de vencimiento de la licencia de AVG.


## 6.6. Icono en la bandeja de sistema

El **Icono en la bandeja de sistema** (en la barra de tareas de Windows) indica el estado actual de **AVG Internet Security 2011**. Está visible en todo momento en la bandeja del sistema, tanto si la ventana principal de AVG está abierta como si está cerrada:

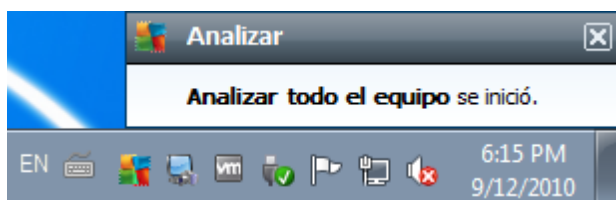


Si aparece a todo color , el **icono de la bandeja del sistema** indica que todos los



componentes de AVG están activos y completamente operativos. También, el icono en la bandeja de sistema AVG se puede mostrar en color completo si AVG está en estado de error pero usted está totalmente consciente de esta situación y ha decidido de manera deliberada **Ignorar el estado del componente**. Un icono con un signo de exclamación  indica un problema (*componente inactivo, estado de error, etc.*). Haga doble clic en el **icono en la bandeja del sistema** para abrir la ventana principal y editar un componente.

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



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

- **Abrir Interfaz del usuario de AVG:** haga clic para abrir la [Interfaz del usuario de AVG](#).
- **Análisis:** haga clic aquí para abrir el menú contextual de [análisis predefinidos](#) ([Análisis de todo el equipo](#), [Análisis de carpetas/archivos específicos](#), [Análisis Anti-Rootkit](#)) y seleccione el análisis que corresponda, se iniciará inmediatamente
- **Firewall:** haga clic aquí para abrir el menú contextual de opciones de configuración del [Firewall](#), donde podrá editar los parámetros más importantes: [Estado del Firewall](#) (*Firewall activado/Firewall desactivado/Modo de emergencia*), [cambio al modo de juego](#) y [perfiles de Firewall](#)
- **Análisis en ejecución:** este elemento se muestra sólo si se está ejecutando un análisis en ese momento en el equipo. Para este análisis puede establecer la prioridad, o detener o pausar el análisis que se está ejecutando. Además, se pueden realizar las siguientes acciones: *Establecer prioridad para todos los análisis, Pausar todos los análisis o Detener todos los análisis.*
- **Actualizar ahora:** inicia inmediatamente una [actualización](#)
- **Ayuda:** abre el archivo de ayuda de la página de inicio





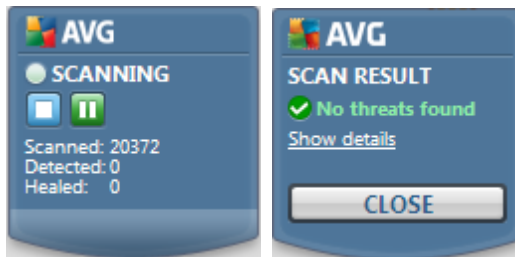
## 6.7. Gadget de AVG

**El gadget de AVG** se muestra en el escritorio de Windows (*barra lateral de Windows*). Esta aplicación sólo es compatible con los sistemas operativos Windows Vista y Windows 7. **El gadget de AVG** ofrece un acceso inmediato a las funciones más importantes de **AVG Internet Security 2011**, por ejemplo, [análisis](#) y [actualización](#):




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

- **Analizar ahora:** haga clic en el vínculo **Analizar ahora** para iniciar el [análisis de todo el equipo](#) directamente. Puede ver el progreso del proceso de análisis en la interfaz del usuario alternativa del gadget. Una breve descripción general de las estadísticas proporciona información sobre el número de objetos analizados, las amenazas detectadas y las amenazas reparadas. Durante el análisis, siempre puede pausar  o detener  el proceso de análisis. Para obtener información detallada sobre los resultados del análisis, consulte el cuadro de diálogo estándar [Descripción general de los resultados del análisis](#); el elemento correspondiente aparecerá como **análisis de gadgets de la barra lateral**.





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



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



- **Vínculo a Facebook** : abre el navegador de Internet con el sitio web de Facebook, en concreto en la página de la **comunidad de AVG**
- **PC Analyzer** : abre la interfaz del usuario en el componente **[PC Analyzer](#)**





## 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 archivos (abrir y cerrar archivos, etc.) en busca de virus conocidos. Se bloquearán los virus detectados para que no puedan realizar ninguna acción y después se limpiarán o pondrán en cuarentena. La mayoría del software antivirus también utiliza el análisis heurístico; en este análisis se analizan los archivos para detectar características típicas de los virus, denominadas firmas virales. Esto significa que el analizador antivirus puede detectar un virus nuevo y desconocido si éste contiene algunas características típicas de los virus ya existentes.

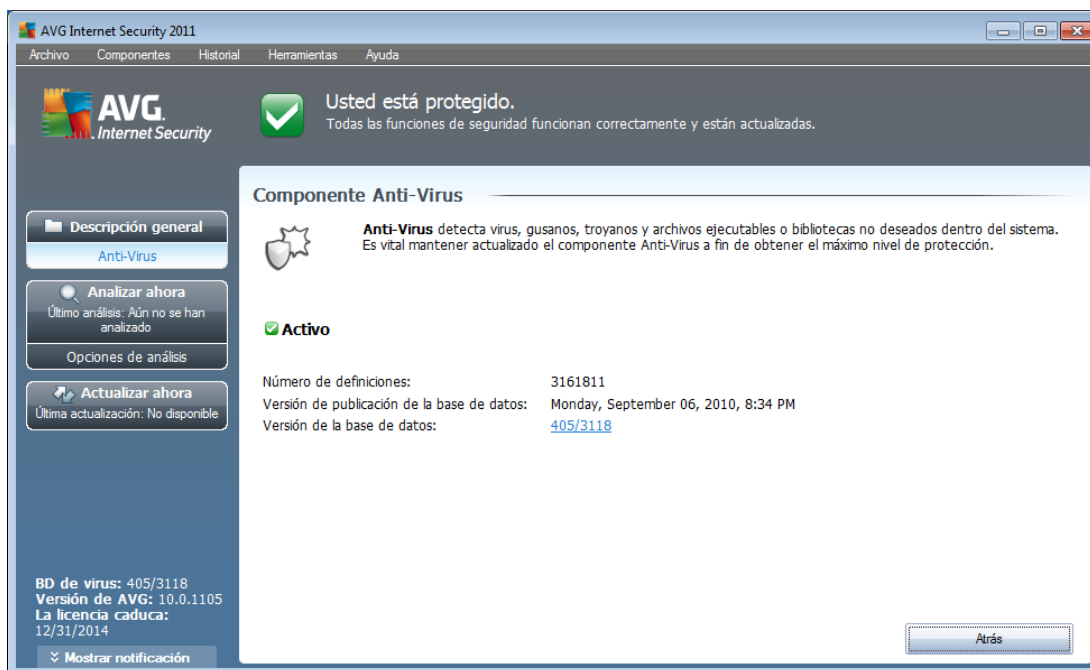
***La función esencial de la protección antivirus es que ningún virus conocido pueda ejecutarse en el equipo.***

Dado que hay casos en que una tecnología por si sola podría no llegar a detectar o identificar un virus, el **Anti-Virus** combina varias tecnologías para garantizar que su equipo esté protegido frente a los virus:

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

AVG también puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas dentro del sistema. Llamamos a estas amenazas programas potencialmente no deseados (diversos tipos de spyware, adware etc.). Además, AVG analiza el registro de su sistema para comprobar si posee entradas sospechosas, archivos temporales de Internet y cookies de rastreo, y le permite tratar todos esos elementos potencialmente dañinos de la misma manera que trata cualquier otra infección.

## 7.1.2. Interfaz de Anti-Virus



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

- **Número de definiciones:** número que proporciona el recuento de los virus definidos en la versión actualizada de la base de datos de virus
- **Versión de publicación de la base de datos:** especifica la fecha y la hora en que se actualizó la base de datos de virus por última vez
- **Versión de la base de datos:** define el número de la versión de la base de datos de virus instalada en este momento; y este número aumenta con cada actualización de la base de datos de virus

Sólo hay un botón de operación disponible dentro de la interfaz de este componente (**Atrás**): presione el botón para regresar a la [interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

## 7.2. Anti-Spyware



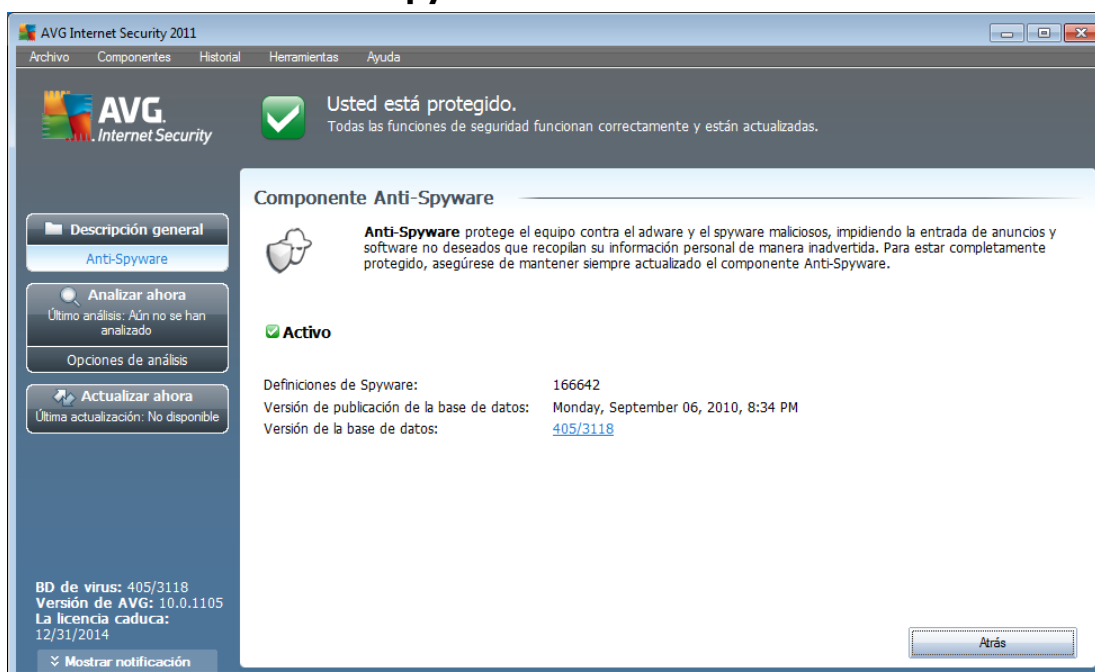
### 7.2.1. Principios de Anti-Spyware

El spyware generalmente se define como un tipo de malware, esto es, un software que recopila información del equipo del usuario sin el conocimiento ni el consentimiento del usuario. Algunas aplicaciones de spyware también pueden instalarse intencionalmente y, con frecuencia, incluyen algunos avisos, ventanas emergentes o diferentes tipos de software desagradable.

Actualmente, el origen más común de la infección suele estar en los sitios web con contenido potencialmente peligroso. Hay otros métodos de transmisión; por ejemplo, a través del correo electrónico infectado con gusanos y virus, lo que también es frecuente. La protección más importante que se debe utilizar es un analizador que se ejecute permanentemente en segundo plano, **Anti-Spyware**, que actúe como protección residente y analice las aplicaciones en segundo plano mientras el usuario las ejecuta.

También existe el riesgo de que se haya transmitido malware a su equipo antes de que AVG estuviera instalado, o de que usted no haya mantenido su **AVG Internet Security 2011** actualizado con las últimas [actualizaciones de la base de datos y del programa](#). Por ello, AVG le permite analizar su equipo en busca de malware/spyware por medio de la función de análisis. También detecta malware inactivo y no peligroso, esto es, malware que se ha descargado pero que no se ha activado aún.

### 7.2.2. Interfaz de Anti-Spyware



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

- **Definiciones de Spyware**: número que proporciona el recuento de muestras



de spyware definido en la última versión de la base de datos de spyware

- **Versión de publicación de la base de datos:** especifica la fecha y la hora en que se actualizó la base de datos de spyware
- **Versión de la base de datos :** define el número de la última versión de la base de datos de spyware; y este número aumenta con cada actualización de la base de virus

Sólo hay un botón de operación disponible dentro de la interfaz de este componente (**Atrás**): presione el botón para regresar a la [interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

### 7.3. Anti-Spam

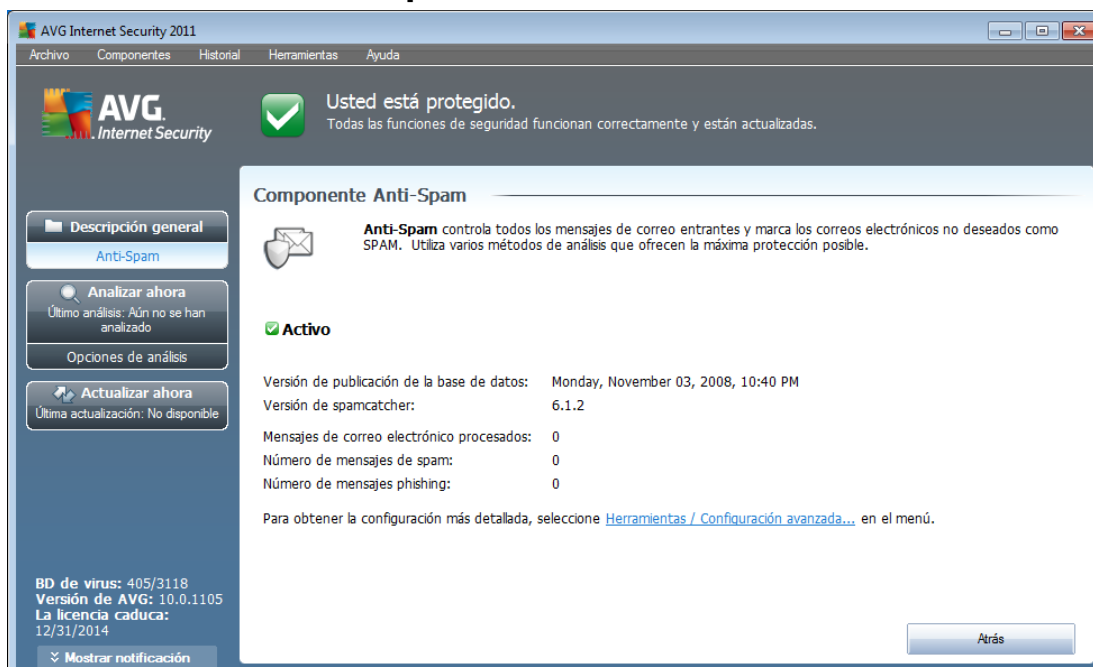
El término spam hace referencia al correo electrónico no solicitado, la mayoría publicitando un producto o servicio, que se envía de forma masiva a un gran número de direcciones de correo al mismo tiempo, lo que llena los buzones de correo de los destinatarios. Los correos Spam no son correos comerciales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

#### 7.3.1. Principios de Anti-Spam

**AVG Anti-Spam** comprueba todos los mensajes de correo electrónico entrantes y marca los no deseados como spam. **AVG Anti-Spam** puede modificar el asunto del correo electrónico (*identificado como spam*) agregando una cadena de texto especial. A continuación, 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 y ofrece la mayor protección posible contra mensajes de correo electrónico no deseados. **AVG Anti-Spam** utiliza una base de datos que se actualiza regularmente para la detección del spam. También es posible usar [servidores RBL](#) (*bases de datos públicas con direcciones de correo electrónico de "spammer conocidos"*), así como agregar manualmente direcciones de correo electrónico a la [Lista de remitentes autorizados](#) (*nunca marcar como spam*) y a la [Lista de remitentes no autorizados](#) (*marcar siempre como spam*).

### 7.3.2. Interfaz de Anti-Spam



En el cuadro de diálogo del componente **Anti-Spam** encontrará un texto breve con una descripción de las funciones del componente, información sobre el estado actual y las estadísticas siguientes:

- **Versión de la base de datos:** especifica la fecha y la hora en que se actualizó y publicó la base de datos de spam.
- **Versión de Spamcatcher:** define el número de la versión más reciente del motor anti-spam.
- **Número de mensajes de correo electrónico procesados:** especifica cuántos mensajes de correo electrónico se analizaron desde la última ejecución del motor Anti-Spam
- **Número de mensajes de spam:** de todos los correos electrónicos analizados, especifica cuántos mensajes se marcaron como spam
- **Número de mensajes phishing:** de todos los correos electrónicos analizados, especifica cuántos mensajes se asignaron como intentos de phishing

El cuadro de diálogo de **Anti-Spam** también proporciona el vínculo [Herramientas/Configuración avanzada](#). Utilice el vínculo para ir al entorno de configuración avanzada de todos los componentes de **AVG Internet Security 2011**.

**Observe que:** *El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado*



*puede llevar a cabo cambios en la configuración.*

Sólo hay un botón de operación disponible dentro de la interfaz de este componente (**Atrás**): presione el botón para regresar a la [interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

## **7.4. Firewall**

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

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

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

**Recomendación:** *normalmente no se recomienda usar más de un firewall en un solo equipo. El equipo no será más seguro si se instalan más firewalls. Es más probable que se produzcan algunos conflictos entre estas dos aplicaciones. Por lo tanto le recomendamos que sólo utilice un firewall en su equipo y desactive los demás; así se elimina el riesgo de posibles conflictos y cualquier problema relacionado con esto.*

### **7.4.1. Principios de Firewall**

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

**Nota:** *el Firewall AVG no está diseñado para plataformas de servidor.*

#### **El Firewall AVG puede:**

- Permitir o bloquear intentos de comunicación de [aplicaciones](#) conocidas de



forma automática, o solicitarle una confirmación.

- Utilizar [perfiles](#) completos con reglas predefinidas, de acuerdo con sus necesidades
- [Cambiar el perfil](#) de forma automática al conectarse a diferentes redes, o utilizar diferentes adaptadores de red

#### 7.4.2. Perfiles de Firewall

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

#### Perfiles disponibles

- **Permitir todo:** un perfil de sistema de [Firewall](#) que ha preestablecido el fabricante y siempre se encuentra presente. Al activar este perfil, se permite toda la comunicación a través de la red y no se aplican reglas de políticas de seguridad, como si la protección del [Firewall](#) estuviera desactivada (*todas las aplicaciones se permiten, pero los paquetes continúan siendo analizados; para desactivar por completo cualquier filtrado necesita deshabilitar el Firewall*). El perfil de sistema no puede duplicarse, eliminarse, y su configuración no puede ser cambiada.
- **Bloquear todo:** un perfil de sistema de [Firewall](#) que ha preestablecido el fabricante y siempre se encuentra presente. Cuando este perfil está activado, se bloquea toda la comunicación de red, y el equipo no estará disponible para las redes externas y tampoco podrá comunicarse con ellas. El perfil de sistema no puede duplicarse, eliminarse, y su configuración no puede ser cambiada.
- **Perfiles personalizados:**
  - **Conectado directamente a Internet:** adecuado para equipos domésticos de escritorio comunes conectados directamente a Internet o equipos portátiles que se conectan a Internet fuera de la red segura de la compañía. Seleccione esta opción si se conecta desde su casa o se encuentra en la red de una empresa pequeña sin control central. Asimismo, seleccione esta opción si va a viajar y se va a conectar mediante un equipo portátil desde diferentes lugares desconocidos y posiblemente peligrosos (*cafés Internet, habitaciones de hotel, etc.*). Se crearán reglas más restrictivas, ya que se supone que estos equipos no tienen protección adicional y, por lo tanto, necesitan la protección máxima.
  - **Equipo en un dominio:** adecuada para los equipos dentro de una red local, por ejemplo, corporativa o escolar. Se asume que la red está



protegida por algunas medidas adicionales, por lo que el nivel de seguridad puede ser menor que para un equipo independiente.

- **Red doméstica pequeña o de oficina pequeña:** adecuada para equipos en redes pequeñas, por ejemplo, en casa o en una oficina pequeña, que funcionan sólo como varios equipos conectados entre sí, sin un administrador central.

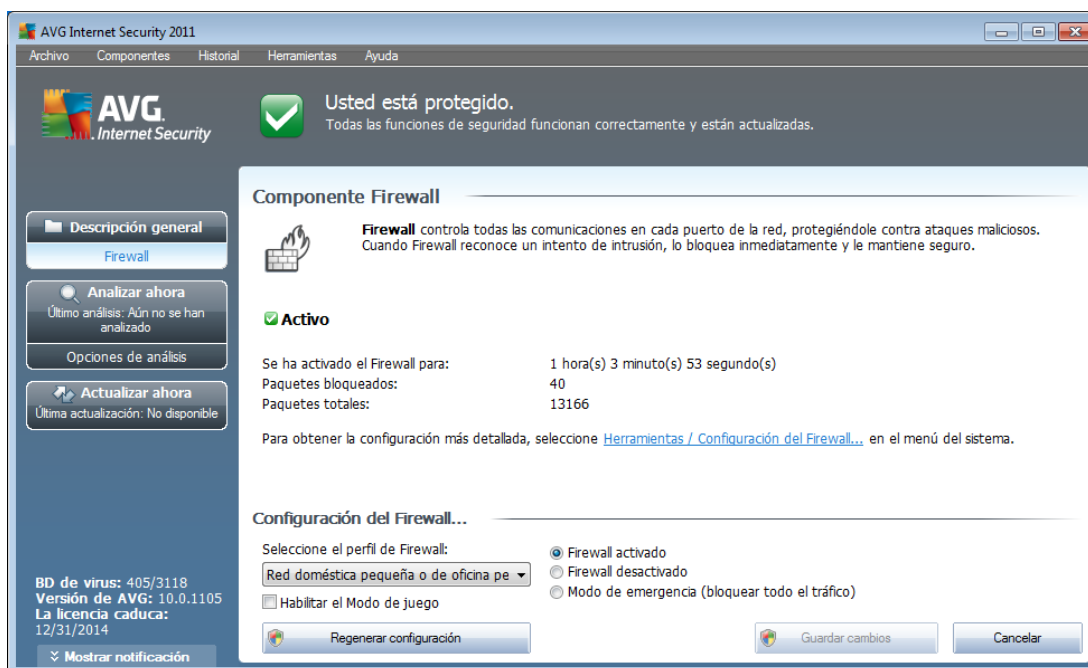
## Cambio de perfiles

La función de cambio de perfil permite al **Firewall** cambiar automáticamente al perfil definido al utilizar un adaptador de red determinado o al conectarse a un cierto tipo de red. Si aún no se ha asignado un perfil al área de red, hasta la siguiente conexión a esa área, el **Firewall** mostrará un cuadro de diálogo que solicitará asignar un perfil.

Puede asignar los perfiles a todas las áreas o interfaces de redes locales y especificar la configuración más detalladamente en el cuadro de diálogo **Perfiles de áreas y adaptadores**, donde también puede desactivar la característica si no desea utilizarla (*posteriormente, para cualquier tipo de conexión, se utilizará el perfil predeterminado*).

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

### 7.4.3. Interfaz de Firewall



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





### **Firewall:**

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

### **Configuración del Firewall**

- **Seleccionar el perfil de Firewall:** en el menú desplegable, seleccione uno de los perfiles definidos: existen dos perfiles disponibles en todo momento (los *perfiles predeterminados llamados Permitir todo y Bloquear todo*); otros perfiles se agregaron manualmente mediante la edición de perfiles en el cuadro de diálogo [Perfiles](#) en [Configuración del Firewall](#).
- **Habilitar el modo de juego:** marque esta opción para asegurarse de que al ejecutar aplicaciones de pantalla completa (juegos, presentaciones de PowerPoint, etc.), el [Firewall](#) no muestre cuadros de diálogo de confirmación para permitir o bloquear la comunicación para las aplicaciones desconocidas. Si en ese momento una aplicación desconocida intenta comunicarse mediante la red, el [Firewall](#) permitirá o bloqueará automáticamente el intento de acuerdo a la configuración que existe en el perfil actual. Cuando está activado el modo de juego, todas las tareas programadas (*análisis y actualizaciones*) se posponen hasta que la aplicación se cierra.
- **Estado del Firewall:**
  - **Firewall activado:** seleccione esta opción para permitir la comunicación con aquellas aplicaciones que tienen la asignación de 'permitido' en el conjunto de reglas definido dentro del perfil de [Firewall](#) seleccionado
  - **Firewall desactivado:** esta opción desactiva el [Firewall](#) por completo, se permite todo el tráfico pero no se analiza
  - **Modo de emergencia (bloquear todo el tráfico de Internet):** seleccione esta opción para bloquear todo el tráfico en todos los puertos de red; el [Firewall](#) aún estará en ejecución, pero se detendrá todo el tráfico de red

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



## Botones de control

- **Regenerar configuración:** presione este botón para sobrescribir la configuración actual del **Firewall** y para volver a la configuración predeterminada según la detección automática.
- **Guardar cambios:** presione este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo.
- **Cancelar:** presione este botón para volver a la [interfaz del usuario de AVG](#) predeterminada (*descripción general de componentes*)

## 7.5. Link Scanner

### 7.5.1. Principios de Link Scanner

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

La tecnología de **LinkScanner** consta de dos funciones, [Search-Shield](#) y [Surf-Shield](#):

- [Search-Shield](#) contiene una lista de los sitios web (*direcciones URL*) que se sabe que son peligrosos. Al realizar búsquedas con Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot, todos los resultados de la búsqueda se comprueban según esta lista y aparece un icono de veredicto (*para los resultados de búsqueda de Yahoo! sólo se muestran iconos de veredicto del tipo "sitio web vulnerable"*).
- [Surf-Shield](#) analiza el contenido de los sitios web que visita, independientemente de la dirección del sitio web. Aunque [Search-Shield](#) no detecte alguno de estos sitios web (*p. ej., un sitio web malicioso que se haya creado recientemente o un sitio web que antes estaba limpio pero que ahora contiene malware*), [Surf-Shield](#) lo detectará y lo bloqueará cuando intente visitarlo.

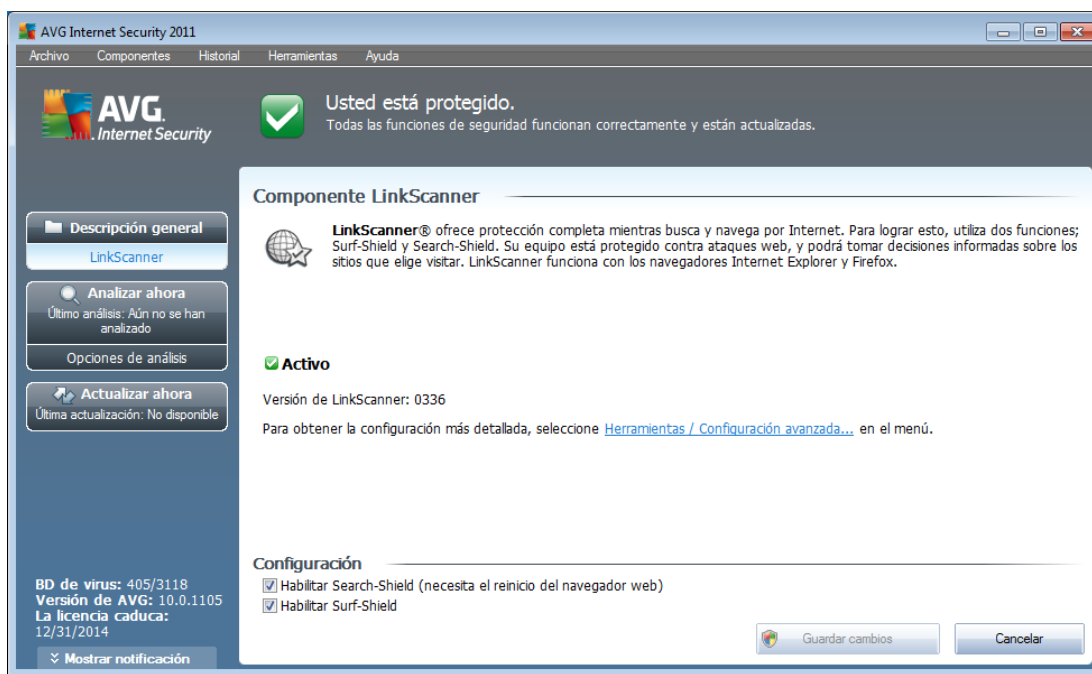
**Nota:** *LinkScanner no está diseñado para plataformas de servidor.*

### 7.5.2. Interfaz de Link Scanner

La interfaz del componente [LinkScanner](#) proporciona una breve descripción de las funciones del componente e información sobre su estado actual. Además, puede encontrar la información acerca del número de versión de la base de datos más



reciente de [LinkScanner](#) (Versión de LinkScanner).



## Configuración de LinkScanner

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






- **Habilitar [Search-Shield](#)** (activado de forma predeterminada): iconos asesores de notificación sobre las búsquedas realizadas con Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot que comprueban por adelantado el contenido de los sitios devueltos por el motor de búsqueda.
- **Habilitar [Surf-Shield](#)** (activado de forma predeterminada): protección activa (en tiempo real) contra sitios de explotación cuando se obtiene acceso a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario obtiene acceso a ellos a través de un navegador web (o cualquier otra aplicación que utilice HTTP).

### 7.5.3. Search-Shield

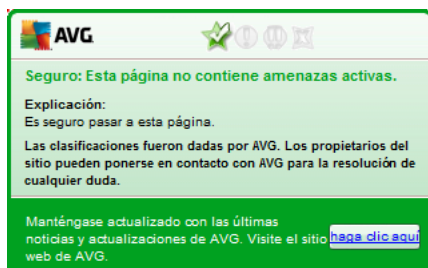
Al realizar búsquedas en Internet con **Search-Shield** activado, todos los resultados de búsqueda que devuelven los motores de búsqueda más populares (Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg y SlashDot) se analizan para buscar vínculos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



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

-  La página vinculada es segura (con el motor de búsqueda de Yahoo! en la [barra de herramientas AVG Security](#) (este icono no se mostrará).).
-  La página vinculada no contiene amenazas pero es algo sospechosa (origen o motivos cuestionables, por lo tanto no recomendable para realizar compras por Internet, etc.).
-  La página vinculada puede ser segura por sí misma pero contiene vínculos a páginas definitivamente peligrosas, o contener un código sospechoso, aunque no emplee ninguna amenaza directa en ese momento.
-  La página vinculada contiene amenazas activas! Por su seguridad, no se le permitirá visitar esta página.
-  La página vinculada no es accesible, y por ello no puede analizarse.

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



#### 7.5.4. Surf-Shield

Esta poderosa protección bloqueará el contenido malicioso de cualquier página que intente abrir, y evitará que se descargue en su equipo. Con esta característica activada, al hacer clic en un vínculo o escribir la URL de un sitio peligroso se evitará que se abra la página Web, y le protegerá por lo tanto de infecciones inadvertidas. Es importante recordar que las páginas Web con vulnerabilidades pueden infectar su equipo por el mero hecho de visitar el sitio afectado; por esta razón, cuando solicita una página peligrosa que contiene vulnerabilidades u otras amenazas serias, [AVG Link Scanner](#) no permitirá que su navegador la muestre.

Si encuentra un sitio web malicioso, [AVG Link Scanner](#) del navegador web le advertirá con un mensaje similar al siguiente:



haga clic aquí web de AVG.'"/&gt;

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

## **7.6. Protección residente**

### **7.6.1. Principios de la Protección residente**

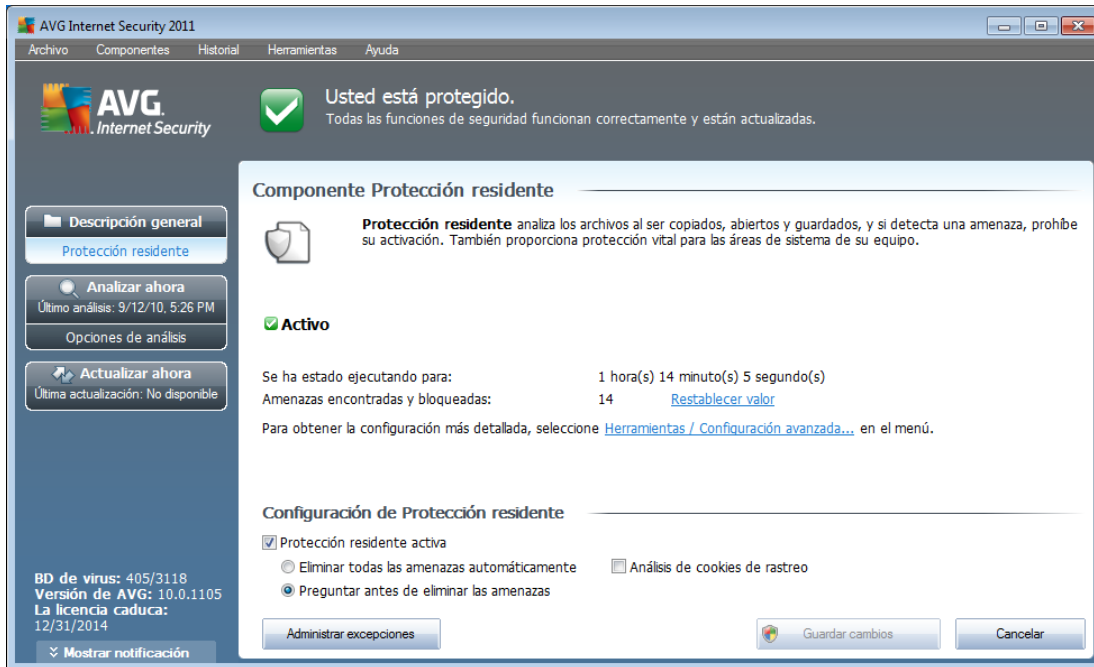
El componente ***Protección residente*** brinda protección continua a su equipo. Analiza cada archivo abierto, guardado o copiado, y protege las áreas de sistema del equipo. Cuando la ***Protección residente*** descubre un virus en un archivo al que se está teniendo acceso, detiene la operación que se está realizando y no permite que el virus se active. Normalmente no se advierte su presencia, ya que se ejecuta "en segundo plano", y usted sólo recibe notificaciones cuando se encuentran amenazas; al mismo tiempo, la ***Protección residente*** bloquea la activación de la amenaza y la elimina. La ***Protección residente*** se carga en la memoria del equipo durante el inicio del sistema.

La ***Protección residente*** puede:

- Analizar en busca de amenazas específicas
- Analizar medios extraíbles (*unidad flash, etc.*)
- Analizar archivos con extensiones específicas o sin extensiones
- Permitir excepciones durante el análisis al especificar archivos o carpetas que nunca deben analizarse

***Advertencia: la Protección residente se carga en la memoria del equipo durante el inicio del sistema, y es vital que la mantenga activada todo el tiempo.***

## 7.6.2. Interfaz de la protección residente



Además de una descripción general de la función **Protección residente** y la información sobre el estado del componente, la interfaz de la **Protección residente** ofrece también algunos datos estadísticos:

- **Protección residente se ha estado ejecutando:** indica el tiempo desde la última ejecución del componente
- **Amenazas detectadas y bloqueadas:** número de infecciones detectadas cuya ejecución o apertura se evitó (*si es necesario, este valor puede ser restablecido, por ejemplo, por cuestiones estadísticas: Restablecer valor*)

### Configuración de la Protección residente

En la parte inferior de la ventana de diálogo encontrará la sección **Configuración de la protección residente**, donde puede editar algunas configuraciones básicas de funcionamiento del componente (*la configuración detallada, como con todos los demás componentes, está disponible a través de Herramientas/Configuración avanzada del menú del sistema*).

La opción **La Protección residente está activa** le permite activar o desactivar fácilmente la protección residente. De manera predeterminada, la función está activada. Con la protección residente activada puede decidir de manera adicional como se deben tratar (eliminar) las posibles infecciones detectadas:

- automáticamente (**Eliminar todas las amenazas automáticamente**)



- o o sólo después de la aprobación del usuario (***Preguntarme antes de eliminar las amenazas***)

Esta opción no tiene impacto sobre el nivel de seguridad, y sólo refleja sus preferencias.

En ambos casos, puede seleccionar si desea **Analizar cookies de rastreo**. En algunos casos específicos puede activar esta opción para alcanzar los máximos niveles de seguridad, sin embargo, esta opción está desactivada de manera predeterminada. ( *cookies = paquetes de texto enviados por un servidor a un navegador web y después enviados de regreso sin cambios por el explorador cada vez que tiene acceso a ese servidor. Las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico*).

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

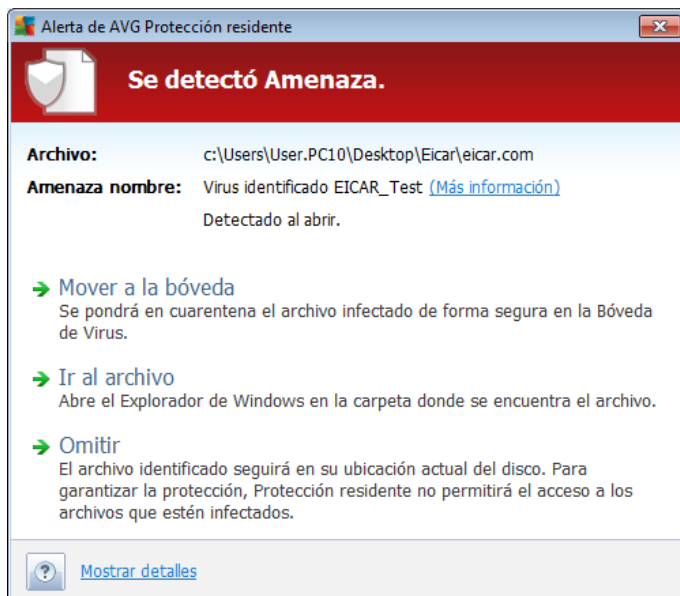
### **Botones de control**

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

- **Administrar excepciones** : abre el cuadro de diálogo [Protección residente: Elementos excluidos](#), donde podrá definir carpetas y archivos que deberían excluirse del análisis de la [Protección residente](#)
- **Guardar cambios**: presione este botón para guardar y aplicar los cambios efectuados en este cuadro de diálogo.
- **Cancelar**: presione este botón para volver a la [Interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

### **7.6.3. Detección de la protección residente**

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



Con este cuadro de diálogo de advertencia, buscará datos en el archivo que se detectó y se designó como infectado (*Nombre del archivo*), el nombre de la infección reconocida (*Nombre de la amenaza*) y un vínculo a la [Enciclopedia de Virus](#), donde podrá encontrar información detallada sobre la infección detectada, si se conoce ([Más información](#)).

Además, tendrá que decidir qué acción se debe emprender. Están disponibles las siguientes opciones:

**Tenga en cuenta que, en determinadas condiciones (el tipo de archivo infectado y dónde se encuentra), no todas las opciones están siempre disponibles.**

- **Eliminar la amenaza como usuario avanzado:** seleccione la casilla si supone que no tiene suficientes derechos para eliminar la amenaza como un usuario común. El usuario avanzado tiene derechos de acceso extensos y, si la amenaza se localiza en una cierta carpeta del sistema, puede ser necesario utilizar esta casilla de selección para eliminarla con éxito.
- **Reparar:** este botón sólo aparece si se puede reparar la infección detectada. A continuación se elimina del archivo y restaura el archivo al estado original. Si el propio archivo es un virus, utilice esta función para eliminarlo (*es decir, enviarlo a la [Bóveda de Virus](#)*)
- **Mover a la Bóveda:** el virus será movido a la Bóveda de virus [AVG](#).
- **Ir al archivo:** esta opción lo redirige a la ubicación del objeto sospechoso (*abre una ventana nueva del Explorador de Windows*)
- **Ignorar:** recomendamos encarecidamente NO utilizar esta opción, a menos que tenga una muy buena razón para hacerlo.

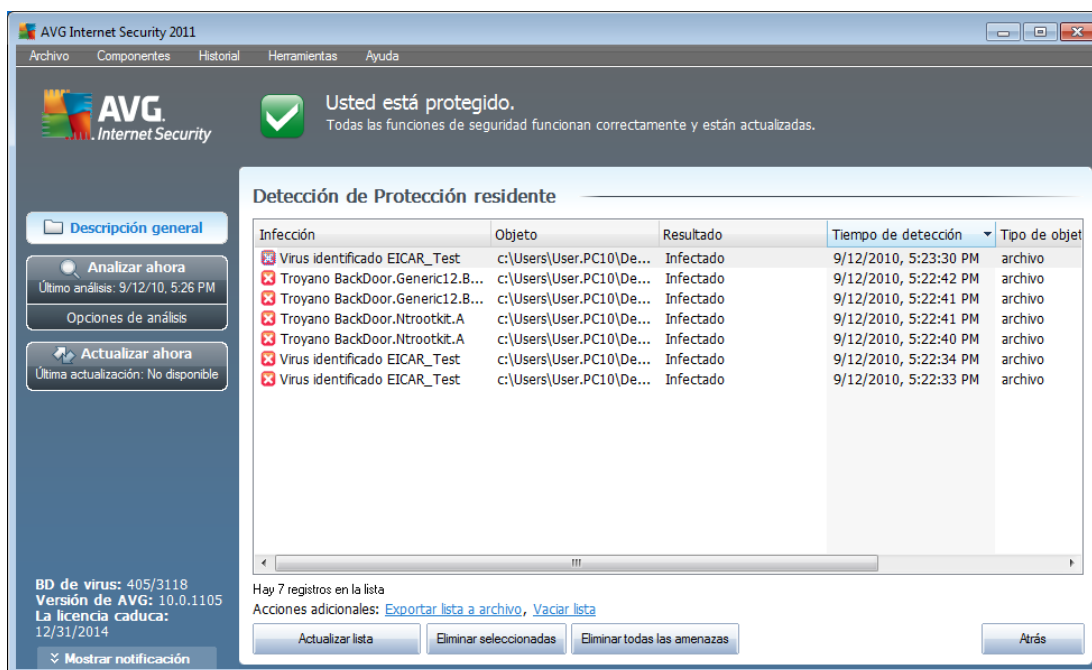
En la sección inferior del cuadro de diálogo encontrará el vínculo **Mostrar detalles** :





haga clic sobre él para abrir una ventana emergente con información detallada sobre el proceso que se estaba ejecutando cuando se detectó la infección, y la identificación del proceso.

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



La **Detección de protección residente** ofrece una descripción general de los objetos que detectó la **Protección residente**, evaluados como peligrosos y reparados o movidos a la **Bóveda de virus**. Para cada objeto detectado se proporciona la siguiente información:

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

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



**archivo**) y eliminar todas las entradas en los objetos detectados (**Vaciar lista**). El botón **Actualizar lista** actualizará la lista de hallazgos detectados por la **Protección residente**. Con el botón **Atrás** regresará a la [Interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

## 7.7. Analizador de correos electrónicos

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

### 7.7.1. Principios del analizador de correos electrónicos

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

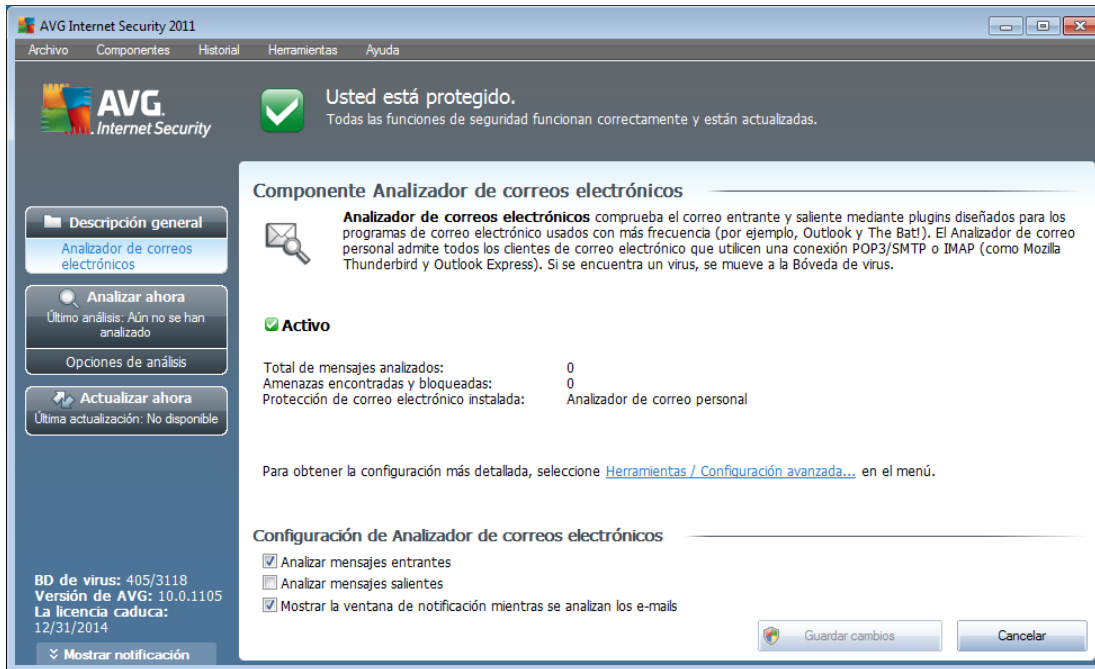
Durante la [instalación de AVG](#) hay dos servidores automáticos de AVG creados para controlar el correo electrónico: uno para comprobar los correos electrónicos entrantes y el otro para comprobar los correos electrónicos salientes. Utilizando estos dos servidores, los correos electrónicos se analizan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

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

- **Correo entrante:** al recibir un mensaje del servidor, el componente **Analizador de correos electrónicos** lo analiza en busca de virus, elimina los archivos adjuntos infectados y agrega una certificación. Si se detectan virus, éstos se pondrán en cuarentena en la [Bóveda de virus](#) de forma inmediata. Después pasa el mensaje al cliente de correo.
- **Correo saliente:** el mensaje se envía desde el cliente de correo electrónico al Analizador de correos electrónicos, el cual analiza el mensaje y los archivos adjuntos en busca de virus y después envía el mensaje al servidor SMTP (*el análisis de los correos electrónicos salientes está desactivado de forma predeterminada y se puede configurar manualmente*).

**Nota:** El analizador de correos electrónicos AVG no está diseñado para plataformas de servidor.

## 7.7.2. Interfaz del analizador de correos electrónicos



En el cuadro de diálogo del componente **Analizador de correos electrónicos** encontrará un texto breve con una descripción de las funciones del componente, información sobre el estado actual y las estadísticas siguientes:

- **Número total de mensajes de correo electrónico analizados:** indica cuántos mensajes de correo electrónico se han analizado desde la última ejecución del **Analizador de correos electrónicos** (si es necesario, este valor puede ser restablecido, por ejemplo, por cuestiones estadísticas: Restablecer valor)
- **Amenazas encontradas y bloqueadas:** indica el número de infecciones detectadas en mensajes de correo electrónico desde la última ejecución del **Analizador de correos electrónicos**.
- **Protección de correo electrónico instalada:** información acerca de algún complemento para protección del correo electrónico instalado, específico para su cliente de correo instalado.

### Configuración del Analizador de correos electrónicos

En la parte inferior del cuadro de diálogo puede encontrar la sección denominada **Configuración del Analizador de correos electrónicos** donde puede editar algunas funciones básicas del componente:

- **Analizar mensajes entrantes:** seleccione este elemento para especificar que todos los correos electrónicos entregados en la cuenta deben analizarse en



busca de virus. De manera predeterminada, este elemento está activado, y se recomienda no cambiar esta configuración.

- **Analizar mensajes salientes:** seleccione este elemento para confirmar que se deben analizar en busca de virus todos los correos enviados desde la cuenta. De forma predeterminada, este elemento se encuentra desactivado.
- **Mostrar ventana de notificación cuando se estén analizando correos electrónicos:** marque este elemento para confirmar que desea utilizar el cuadro de notificación que aparece sobre el icono de AVG en la bandeja del sistema durante el análisis del correo con el componente [Analizador de correos electrónicos](#). De manera predeterminada, este elemento está activado, y se recomienda no cambiar esta configuración.

Se puede obtener acceso a la configuración avanzada del componente **Analizador de correos electrónicos** mediante el elemento **Herramientas/Configuración avanzada** del menú del sistema; no obstante, la configuración avanzada sólo se recomienda para los usuarios con experiencia.

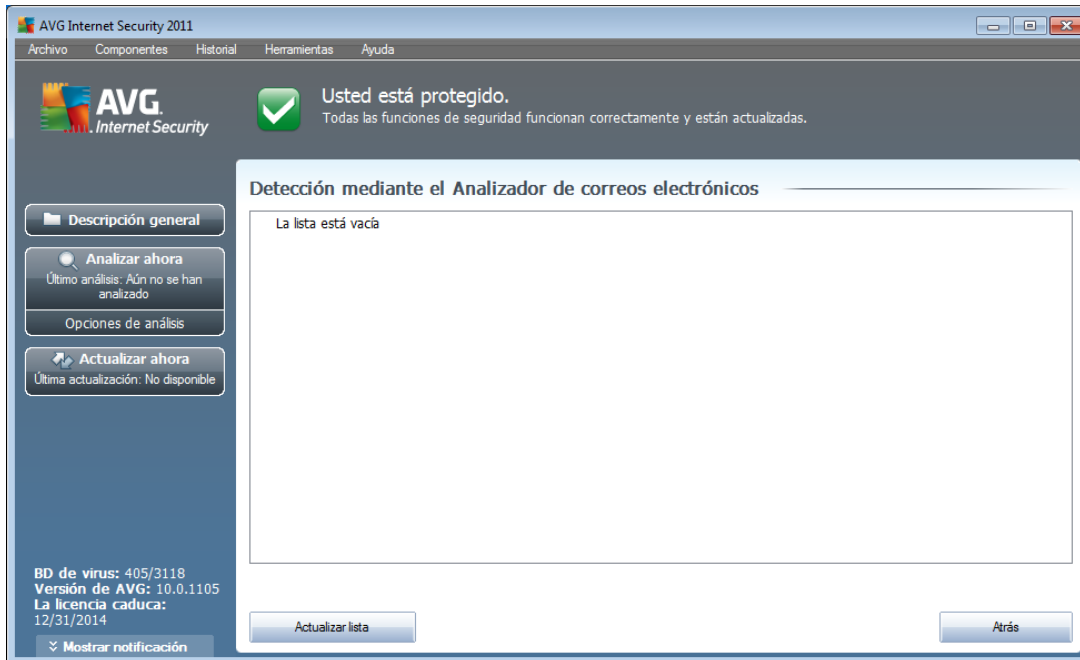
**Observe que:** *El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración. Si necesita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

## Botones de control

Los botones de control disponibles en la interfaz del **Analizador de correos electrónicos** son:

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

### 7.7.3. Detección mediante el analizador de correos electrónicos



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

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

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

#### Botones de control

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

- **Actualizar lista:** actualiza la lista de amenazas detectadas



- **Atrás:** le lleva al cuadro de diálogo mostrado anteriormente

## 7.8. Administrador de actualización

### 7.8.1. Principios del administrador de actualización

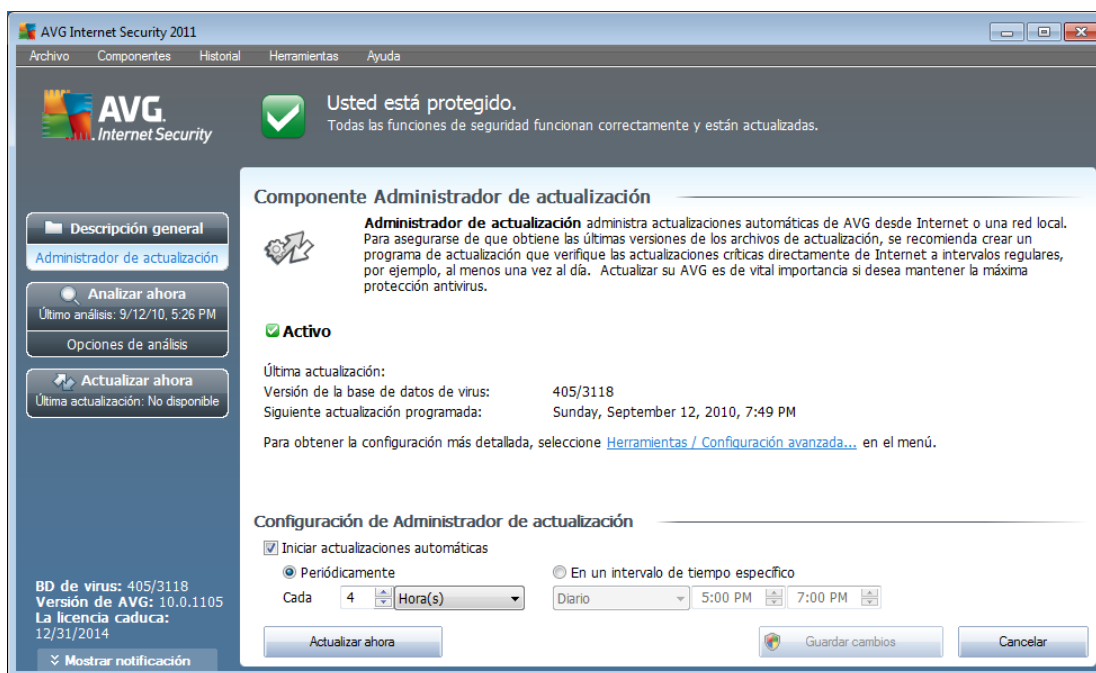
Ningún software de seguridad puede garantizar una verdadera protección ante los diversos tipos de amenazas si no se actualiza periódicamente. Los desarrolladores de virus siempre buscan nuevas fallas que explotar en el software y el sistema operativo. Diariamente aparecen nuevos virus, nuevo malware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

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

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

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

### 7.8.2. Interfaz del administrador de actualización



La interfaz del **Administrador de actualización** muestra información sobre la función



del componente y su estado actual, y proporciona los datos estadísticos correspondientes:

- **Actualización más reciente:** especifica la fecha y la hora en que se ha actualizado la base de datos.
- **Versión de la base de datos de virus:** define el número de la versión de la base de datos de virus instalada en este momento; y este número aumenta con cada actualización de la base de datos de virus
- **Siguiente actualización programada:** especifica cuándo y a qué hora está programada la siguiente actualización de la base de datos

### Configuración del Administrador de actualización

En la parte inferior del cuadro de diálogo puede encontrar la sección **Configuración del Administrador de actualización** donde puede efectuar algunos cambios en las reglas de ejecución del proceso de actualización. Puede definir si desea descargar los archivos de actualización automáticamente (**Iniciar actualizaciones automáticas**) o sólo a pedido. De modo predeterminado, la opción **Iniciar actualizaciones automáticas** está seleccionada, y recomendamos dejarla así. Descargar periódicamente los últimos archivos de actualizaciones es fundamental para el correcto funcionamiento de cualquier software de seguridad.

De modo adicional, puede definir cuándo debe ejecutarse la actualización:

- **Periódicamente:** defina el intervalo de tiempo.
- **A un intervalo específico de tiempo:** define el momento del día exacto en que se debería iniciar la actualización

De modo predeterminado, el valor de actualización configurado es cada 4 horas. Se recomienda encarecidamente que no modifique esta configuración salvo que tenga un motivo real para hacerlo.

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

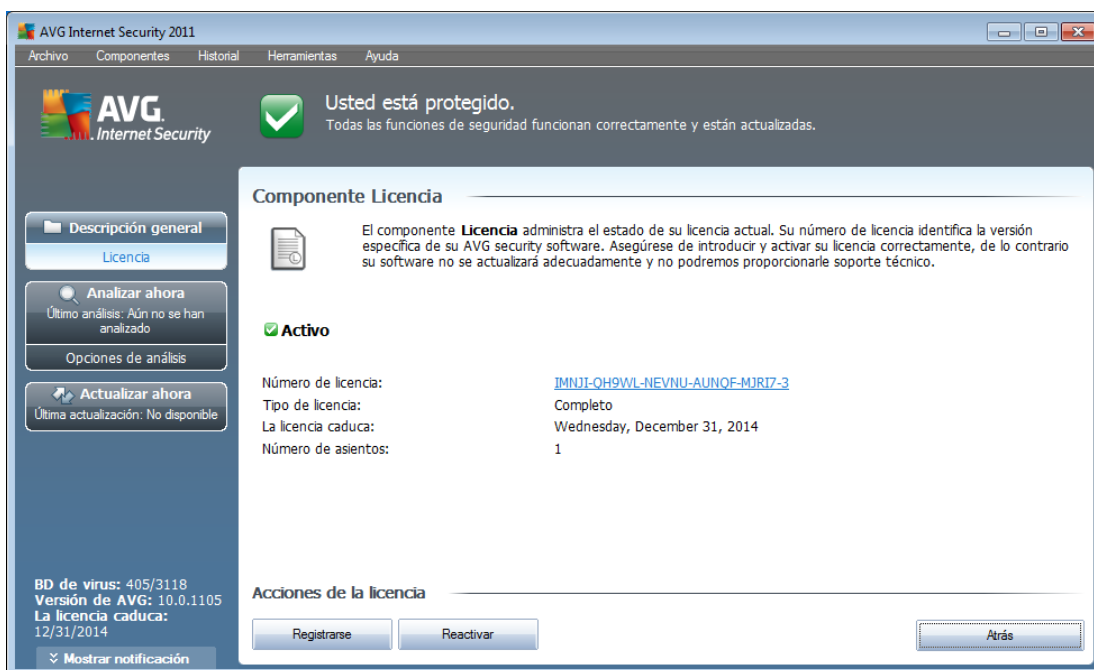
### Botones de control

Los botones de control disponibles en la interfaz del **Administrador de actualización** son:

- **Actualizar ahora:** ejecuta una [actualización inmediata](#) a pedido.

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

## 7.9. Licencia



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

- **Número de licencia:** proporciona la forma abreviada del número de licencia (*por motivos de seguridad, faltan los cuatro últimos símbolos*). Al especificar el número de licencia, debe ser totalmente preciso y escribirlo exactamente como aparece. Por lo tanto, recomendamos utilizar siempre el método "copiar y pegar" para cualquier manipulación con el número de licencia.
- **Tipo de licencia:** especifica el tipo de producto instalado.
- **Caducidad de la licencia:** esta fecha determina el periodo de validez de la licencia. Si desea seguir utilizando **AVG Internet Security 2011** después de esta fecha, tendrá que renovar la licencia. La renovación de la licencia se puede efectuar en línea en [el sitio web de AVG](#).
- **Número de puestos:** indica en cuántas estaciones de trabajo puede instalar el programa **AVG Internet Security 2011**.





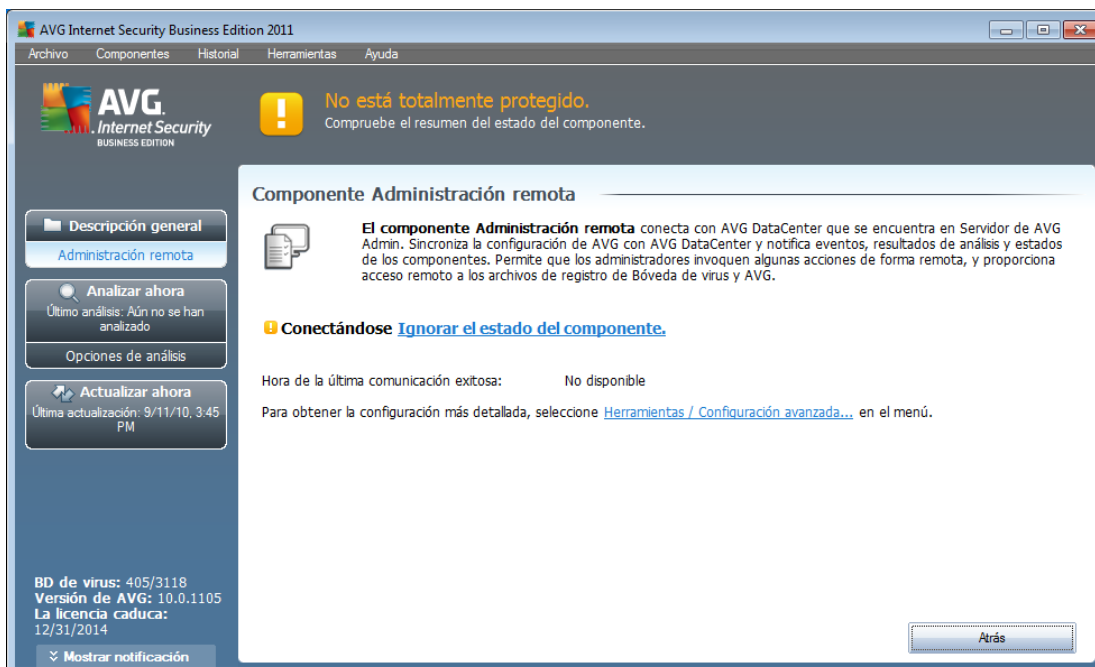
## Botones de control

- **Registrarse:** permite conectarse a la página de registro del sitio web de AVG (<http://www.avg.com/>). Introduzca su información de registro; sólo los clientes con productos AVG registrados pueden recibir soporte técnico gratuito.
- **Reactivar:** abre el cuadro de diálogo **Activar AVG** con la información introducida en el cuadro de diálogo **Personalizar AVG** del [proceso de instalación](#). Dentro de este cuadro de diálogo puede introducir el número de licencia para reemplazar el número de venta (*el número con el que instaló AVG*) o el número de licencia antiguo (*como al actualizar 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**, que le permiten comprar la versión completa del programa inmediatamente. Para **AVG Internet Security 2011** instalado con un número de venta, los botones aparecen como **Registrar** y **Activar**.

- **Atrás:** presione este botón para volver a la [interfaz del usuario de AVG](#) (*descripción general de los componentes*).

## 7.10. Remote administration



El componente **Remote Administration** sólo se muestra en la interfaz del usuario de **AVG Internet Security 2011** en caso de que haya instalado la edición para redes de su producto (*consulte el componente [Licencia](#)*). En el cuadro de diálogo **Remote administration** puede encontrar la información sobre si el componente está activo y conectado al servidor. Toda la configuración del componente **Remote**



**administration** debe realizarse en [Configuración avanzada/Remote administration](#).

Para obtener una descripción detallada de las opciones y funciones del componente en el sistema AVG Remote Administration, consulte la documentación específica dedicada a este tema exclusivamente. Esta documentación está disponible para su descarga en el [sitio web de AVG \(www.avg.com\)](http://www.avg.com), en la sección **Centro de soporte/Descargar/Documentación**.

### Botones de control

- **Atrás:** presione este botón para volver a la [interfaz del usuario de AVG](#) ( *descripción general de los componentes*).

## 7.11. Online Shield

### 7.11.1. 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 archivos que puedan contener*) incluso antes de que se visualicen en el navegador web o de que se descarguen en el equipo.

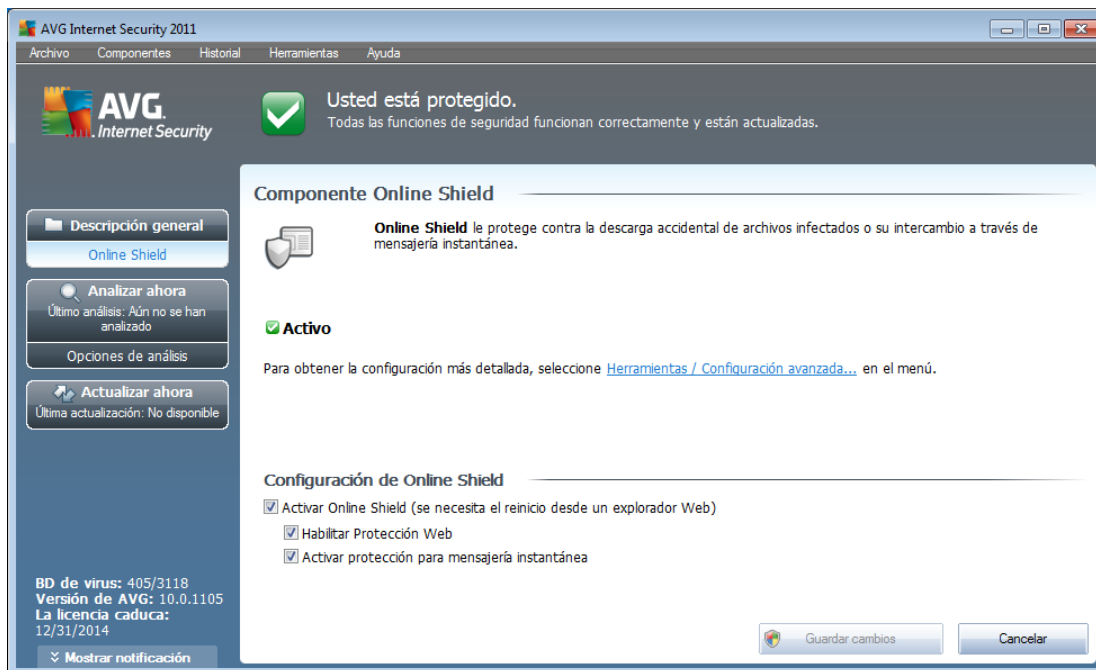
**Online Shield** detecta si la página que se va a visitar contiene algún javascript peligroso e impide que se visualice la página. Asimismo, reconoce el malware que contiene una página y detiene su descarga de inmediato para que nunca entre en el equipo.

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

### 7.11.2. Interfaz de Online Shield

La interfaz del componente **Online Shield** describe el comportamiento de este tipo de protección. Además, encontrará información sobre el estado actual del componente.

En parte inferior del cuadro de diálogo encontrará las opciones de edición básicas del funcionamiento de este componente:



## Configuración de Online Shield

Antes que nada, tiene la opción de activar o desactivar inmediatamente **Online Shield** haciendo clic en el elemento **Activar Online Shield**. Esta opción está habilitada de manera predeterminada y el componente **Online Shield** está activo. Sin embargo, si no tiene una buena razón para cambiar esta configuración, le recomendamos mantener el componente activo. Si el elemento está seleccionado y se está ejecutando **Online Shield**, se activan dos o más opciones de configuración:

- **Habilitar Protección Web:** esta opción confirma que **Online Shield** debe analizar el contenido de los sitios web.
- **Activar protección para mensajería instantánea:** compruebe este elemento si desea que **Online Shield** compruebe que la comunicación a través de mensajería instantánea (p. ej., ICQ, MSN Messenger, Yahoo,...) no contenga virus.

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

## Botones de control



Los botones de control disponibles dentro de la interfaz de **Online Shield** son:

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

### 7.11.3. Detección de Online Shield

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



Con este diálogo de advertencia, buscará datos en el archivo que se detectó y se designó como infectado (*Nombre del archivo*), el nombre de la infección reconocida (*Nombre de la amenaza*) y un vínculo a la [Enciclopedia de Virus](#), donde podrá encontrar información detallada sobre la infección detectada (*si se conoce*). El cuadro de diálogo proporciona los siguientes botones:

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

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



Para cada objeto detectado se proporciona la siguiente información:

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

En la parte inferior del cuadro de diálogo, debajo de la lista, encontrará información sobre el número total de los objetos detectados listados anteriormente. Adicionalmente puede exportar toda la lista de objetos detectados en un archivo (**Exportar lista a archivo**) y eliminar todas las entradas en los objetos detectados (**Vaciar lista**). El botón **Actualizar lista** actualizará la lista de hallazgos detectados por **Online Shield**. Con el botón **Atrás** regresará a la [Interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

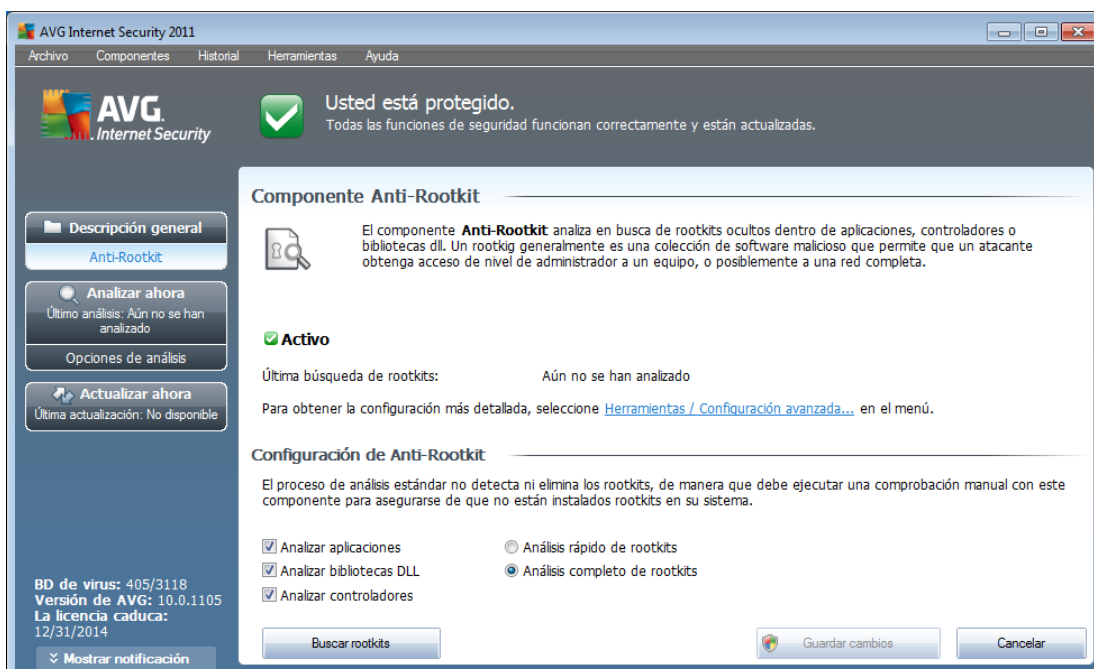
## 7.12. Anti-Rootkit

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

### 7.12.1. Principios de Anti-Rootkit

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

### 7.12.2. Interfaz de Anti-Rootkit



La interfaz del usuario de **Anti-Rootkit** proporciona una descripción breve de las funciones de los componentes, informa del estado actual de los componentes y proporciona información sobre la última vez que se ejecutó el análisis de **Anti-Rootkit** (**Última búsqueda de rootkits**). El cuadro de diálogo de **Anti-Rootkit** también proporciona el vínculo [Herramientas/Configuración avanzada](#). Utilice el vínculo para ir al entorno de configuración avanzada del componente **Anti-Rootkit**.

**Observe que:** El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración.

### Configuración de Anti-Rootkit

En la parte inferior del cuadro de diálogo, puede encontrar la sección **Configuración de Anti-Rootkit** donde puede configurar algunas funciones básicas del análisis de



detección de rootkits. En primer lugar, marque las casillas de verificación respectivas para especificar los objetos que deben analizarse:

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

También puede seleccionar el modo de análisis de rootkits:

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

### Botones de control

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

## 7.13. Herramientas del sistema

**Herramientas del sistema** hace referencia a las herramientas que ofrecen un resumen detallado del entorno **AVG Internet Security 2011** y el sistema operativo. El componente muestra una descripción general de:

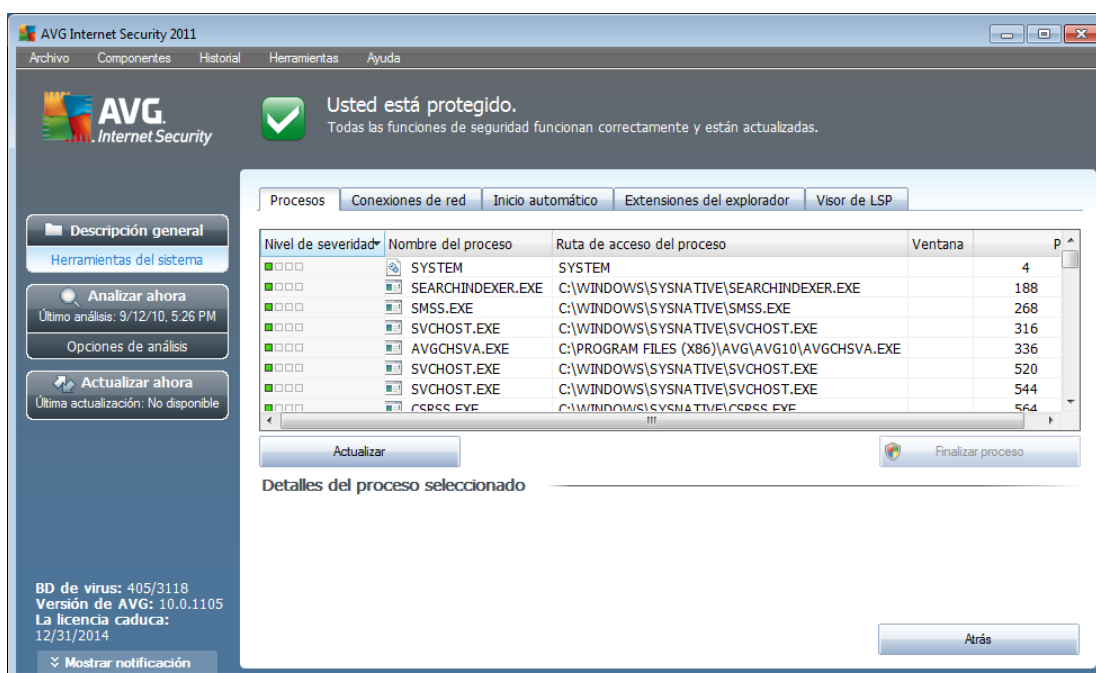
- [Procesos](#): lista de procesos (*(por ejemplo, aplicaciones en ejecución)*) que están activos actualmente en el equipo
- [Conexiones de red](#): lista de las conexiones de red activas actualmente
- [Inicio automático](#): lista de todas las aplicaciones que se ejecutan al iniciar el sistema Windows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



- [Visor de LSP](#): lista de los Proveedores de Servicio por Niveles (LSP)

**Las descripciones generales también pueden editarse, si bien esto sólo se recomienda para los usuarios con mucha experiencia.**

### 7.13.1. Procesos



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

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

### Botones de control

Los botones de control disponibles en la interfaz de **Herramientas del sistema** son:





- **Actualizar:** actualiza la lista de procesos de acuerdo con el estado actual
- **Finalizar proceso:** puede seleccionar una o más aplicaciones y después finalizarlas presionando este botón. **Le recomendamos encarecidamente que no finalice ninguna aplicación, a menos que tenga plena seguridad de que representa una amenaza verdadera.**
- **Atrás:** le lleva a la [Interfaz del usuario de AVG](#) predeterminada (descripción general de los componentes)

### 7.13.2. Conexiones de red

| Aplicación            | Protocolo | Dirección local         | Dirección remota    | Estado      |
|-----------------------|-----------|-------------------------|---------------------|-------------|
| [Proceso del sistema] | TCP       | SCR02:139               | SCR02:0             | Escuchando  |
| [Proceso del sistema] | UDP       | SCR02:137               |                     |             |
| [Proceso del sistema] | UDP       | SCR02:138               |                     |             |
| [Proceso del sistema] | TCP       | SCR02:445               | SCR02:0             | Escuchando  |
| [Proceso del sistema] | TCP6      | [0:0:0:0:0:0:0:0]:445   | [0:0:0:0:0:0:0:0]:0 | Desconocido |
| [Proceso del sistema] | TCP6      | [0:0:0:0:0:0:0:0]:5357  | [0:0:0:0:0:0:0:0]:0 | Desconocido |
| [Proceso del sistema] | TCP       | SCR02:5357              | SCR02:0             | Escuchando  |
| winit.exe             | TCP       | SCR02:49152             | SCR02:0             | Escuchando  |
| winit.exe             | TCP6      | [0:0:0:0:0:0:0:0]:49152 | [0:0:0:0:0:0:0:0]:0 | Desconocido |
| svchost.exe           | UDP6      | [0:0:0:0:0:0:0:0]:500   |                     |             |
| svchost.exe           | UDP6      | [0:0:0:0:0:0:0:0]:5355  |                     |             |
| svchost.exe           | TCP6      | [0:0:0:0:0:0:0:0]:49161 | [0:0:0:0:0:0:0:0]:0 | Desconocido |
| svchost.exe           | UDP6      | [0:0:0:0:0:0:0:0]:54698 |                     |             |
| svchost.exe           | UDP       | SCR02:1900              |                     |             |
| svchost.exe           | UDP       | SCR02:500               |                     |             |

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

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



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

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

### Botones de control

Los botones de control disponibles son:

- **Finalizar conexión:** cierra una o más conexiones seleccionadas en la lista
- **Finalizar proceso:** cierra una o más aplicaciones relacionadas con las conexiones seleccionadas en la lista
- **Atrás:** vuelve a la [Interfaz del usuario de AVG](#) predeterminada (descripción general de los componentes).

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

### 7.13.3. Inicio automático

| Nombre                           | Ubicación                            | Ruta de acceso                            |
|----------------------------------|--------------------------------------|---|
| Sidebar                          | \REGISTRY\USER\S-1-5-20\Software\... | %ProgramFiles%\Windows Sidebar\Side...    |
| mctadmin                         | \REGISTRY\USER\S-1-5-20\Software\... | C:\Windows\System32\mctadmin.exe          |
| Shell                            | \REGISTRY\MACHINE\SOFTWARE\Wo...     | explorer.exe                              |
| Shell                            | \REGISTRY\MACHINE\SOFTWARE\Mic...    | explorer.exe                              |
| Gadwin PrintScreen Pro           | \REGISTRY\USER\S-1-5-21-22073492...  | C:\Program Files (x86)\Gadwin Systems\... |
| mctadmin                         | \REGISTRY\USER\S-1-5-19\Software\... | C:\Windows\System32\mctadmin.exe          |
| vmware VMWare User Process       | \REGISTRY\MACHINE\SOFTWARE\Mic...    | "C:\Program Files\VMware\VMware Tool...   |
| C:\Windows\SysWOW64\mshta.exe... | \REGISTRY\MACHINE\SOFTWARE\Cla...    | C:\Windows\SysWOW64\mshta.exe "%...       |
| SHELL                            | \INI\system.ini\BOOT\SHELL           | SYS:Microsoft\Windows NT\CurrentVers...   |
| AVG_TRAY                         | \REGISTRY\MACHINE\SOFTWARE\Wo...     | C:\Program Files (x86)\AVG\AVG10\avg...   |
| vmware VMWare Tools              | \REGISTRY\MACHINE\SOFTWARE\Mic...    | "C:\Program Files\VMware\VMware Tool...   |
| Sidebar                          | \REGISTRY\USER\S-1-5-19\Software\... | %ProgramFiles%\Windows Sidebar\Side...    |

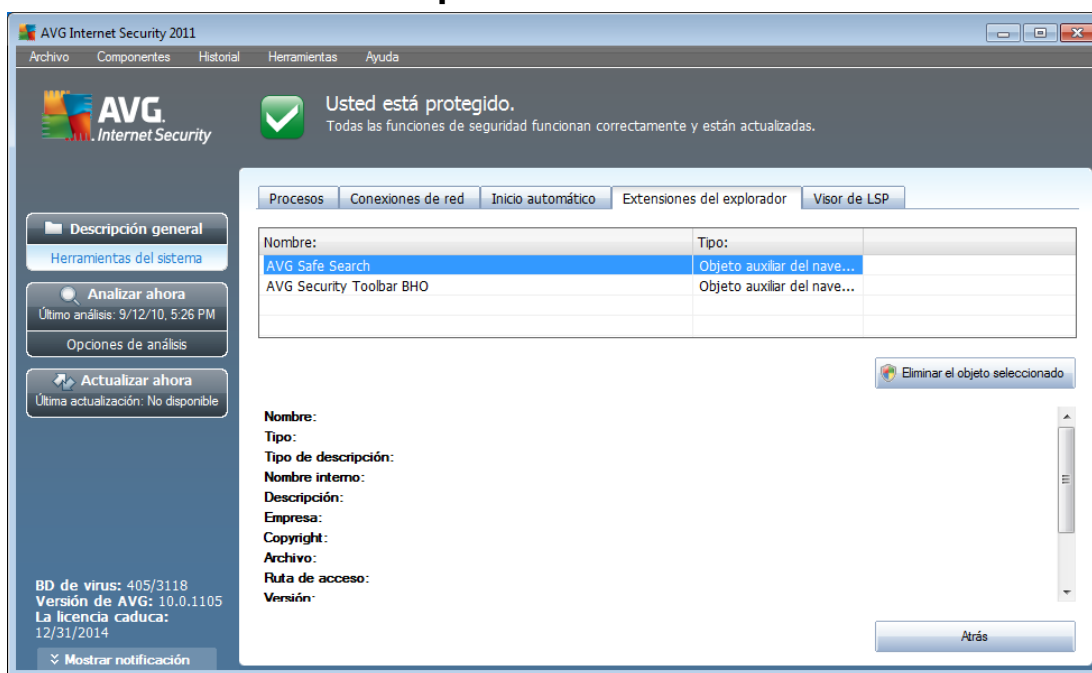
El diálogo **Inicio automático** muestra una lista de todas las aplicaciones que se ejecutan durante el inicio del sistema Windows. A menudo, muchas aplicaciones de malware se agregan automáticamente a sí mismas a la entrada del registro de inicio.



Se pueden eliminar una o más entradas seleccionándolas y presionando el botón **Eliminar seleccionados**. Con el botón **Atrás** regresará a la [Interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

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

#### 7.13.4. Extensiones del explorador



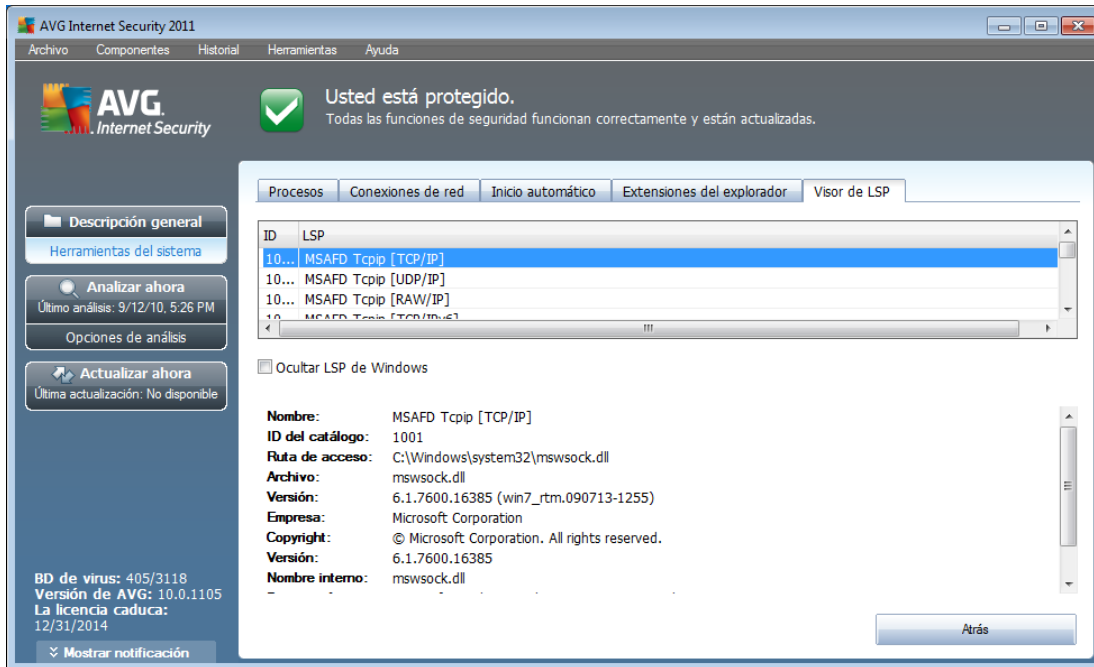
El cuadro de diálogo **Extensiones del navegador** contiene una lista de plugins (*por ejemplo, aplicaciones*) instalados dentro de su explorador de Internet. Esta lista puede contener tanto plugins comunes como programas que sean potencialmente maliciosos. Haga clic en un objeto de la lista para obtener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

#### Botones de control

Los botones de control de la pestaña **Extensión del navegador** son:

- **Eliminar el objeto seleccionado:** elimina el complemento resaltado de la lista. **Le recomendamos que no elimine ningún complemento de la lista, a menos que tenga plena seguridad de que representa una amenaza verdadera.**
- **Atrás:** le lleva a la [Interfaz del usuario de AVG](#) predeterminada (descripción general de los componentes)

### 7.13.5. Visor de LSP



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

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

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

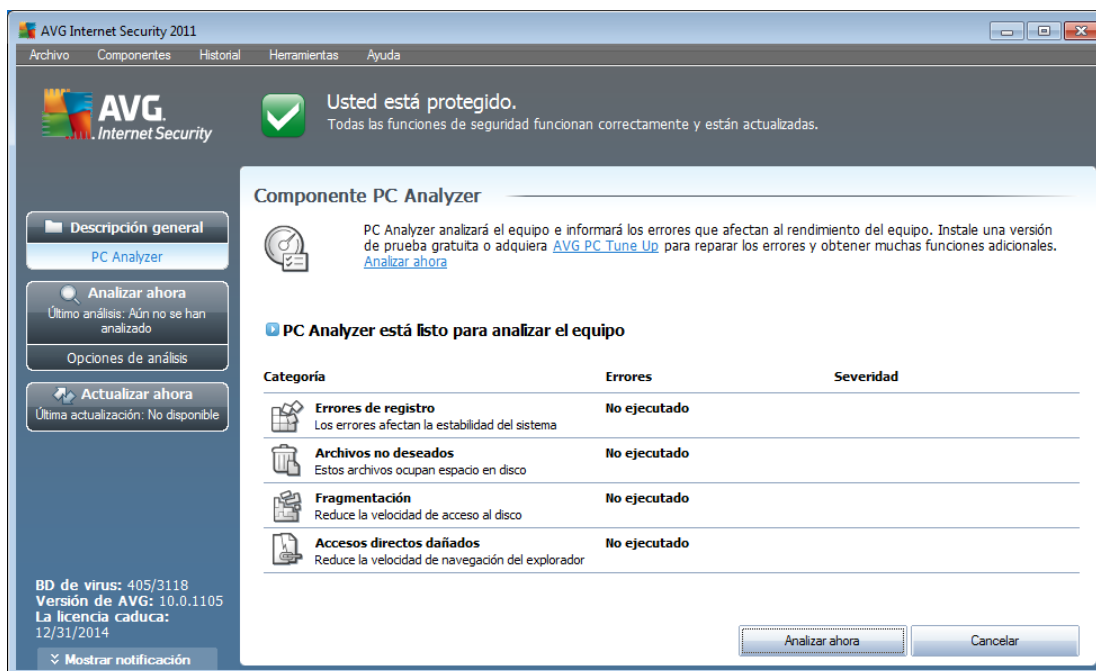
Para incluir los LSP de Windows en la lista, quite la marca de la casilla de verificación **Ocultar LSP de Windows**. Con el botón **Atrás** regresará a la [Interfaz del usuario de AVG](#) predeterminada (*descripción general de los componentes*).

### 7.14. PC Analyzer

El componente **PC Analyzer** puede analizar el equipo para detectar problemas del sistema y puede proporcionarle una descripción general clara de lo que podría estar afectando al rendimiento general de su equipo. En la interfaz del usuario del componente puede ver un gráfico dividido en cuatro líneas que hacen referencia a las

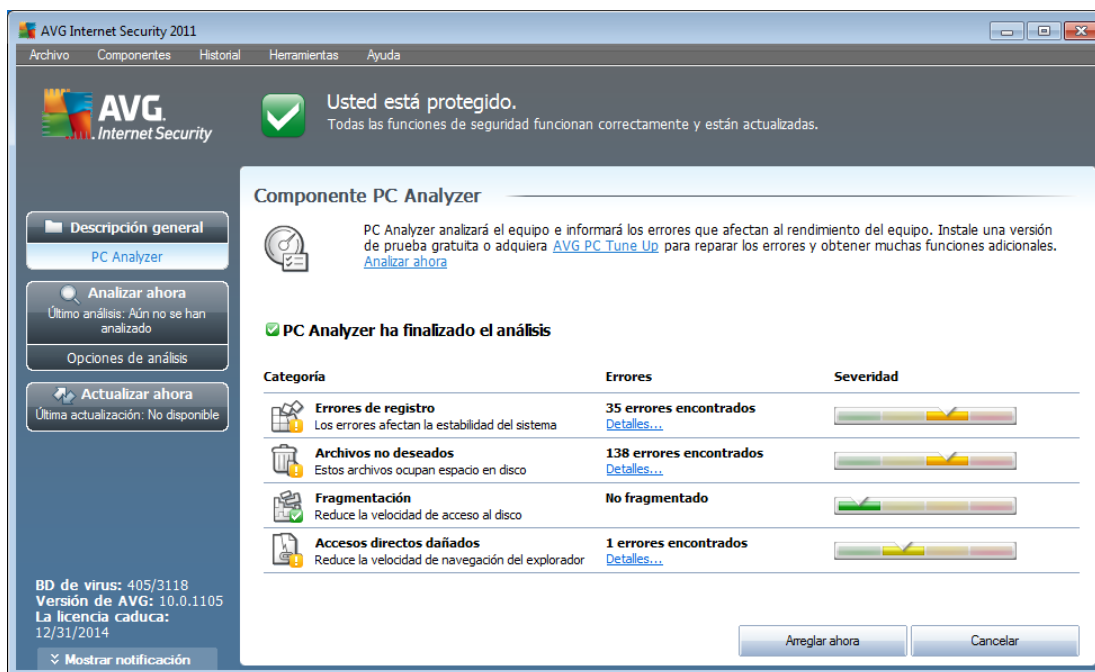


categorías correspondientes: errores de registro, archivos no deseados, fragmentación y accesos directos rotos:



- **Errores en el registro** mostrará el número de errores en el Registro de Windows. Debido a que corregir el Registro exige un conocimiento más profundo, no recomendamos que intente solucionar los errores usted mismo.
- **Archivos no deseados** proporcionará el número de archivos sin los que se puede trabajar perfectamente. Normalmente se tratará de varios tipos de archivos temporales, así como de archivos de la Papelera de reciclaje.
- **Fragmentación** calculará el porcentaje del disco duro que está fragmentado, es decir, que se ha utilizado durante mucho tiempo de forma que la mayoría de los archivos ahora están separados en distintas partes del disco físico. Puede utilizar alguna herramienta de desfragmentación para solucionarlo.
- **Accesos directos rotos** le notificará si hay accesos directos que ya no funcionan, que llevan a ubicaciones no existentes, etc.

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



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

### Botones de control

- **Más información:** presione el botón para ir al sitio web de AVG (<http://www.avg.com/>), en la página en la que se proporciona información detallada y actualizada relativa al componente **PC Analyzer**
- **Analizar ahora** (se muestra antes de que se inicie el análisis) : presione este botón para ejecutar el análisis del equipo inmediatamente
- **Arreglar ahora** (se muestra cuando el análisis ha terminado): presione el botón para ir al sitio web de AVG (<http://www.avg.com/>), en la página en la que se proporciona información detallada y actualizada sobre el componente **PC Analyzer**
- **Cancelar:** presione este botón para detener el análisis en ejecución o para volver a la **interfaz del usuario de AVG** predeterminada (*descripción general de los componentes*) cuando el análisis se haya completado

## 7.15. Identity Protection

**AVG Identity Protection** es un producto anti-malware dedicado a prevenir posibles robos de contraseñas, detalles de cuentas bancarias, números de tarjeta de crédito y otros datos digitales personales de valor mediante software malicioso (*malware*) en su equipo. Se asegura de que todos los programas que se ejecuten en su equipo



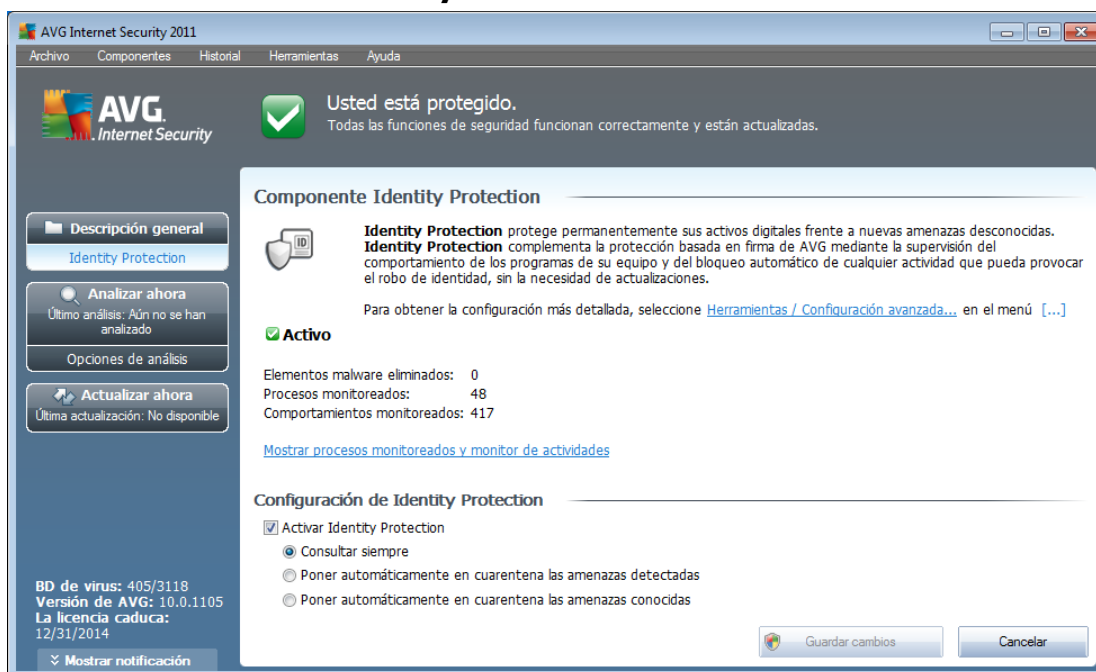
funcionen correctamente. **AVG Identity Protection** detecta y bloquea comportamientos sospechosos de forma continua, y protege su equipo de cualquier malware nuevo.

### 7.15.1. Principios de Identity Protection

**AVG Identity Protection** es un componente anti-malware que ofrece protección contra todo tipo de malware (*spyware, bots, robo de identidad, ...*) mediante tecnologías conductuales que proporcionan protección día cero frente a nuevos virus. El malware es cada vez más sofisticado y ya aparece como programas normales que pueden poner su equipo a disposición de ataques remotos de robo de identidad; por ello, **AVG Identity Protection** le protege de este nuevo malware basado en ejecución. Actúa como una protección complementaria a **AVG Anti-Virus** contra virus conocidos y basados en archivos mediante mecanismo de firmas y análisis.

**Se recomienda encarecidamente instalar ambos componentes, **AVG Anti-Virus** y **AVG Identity Protection**, a fin de proteger su equipo por completo.**

### 7.15.2. Interfaz de Identity Protection



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

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



ejecución dentro de las aplicaciones monitoreadas

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

### Configuración de Identity Protection

En la parte inferior del cuadro de diálogo, puede encontrar la sección **Configuración de Identity Protection** donde puede editar algunas funciones básicas del funcionamiento del componente:

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

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

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

### Botones de control

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

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





## 8. Barra de herramientas AVG Security

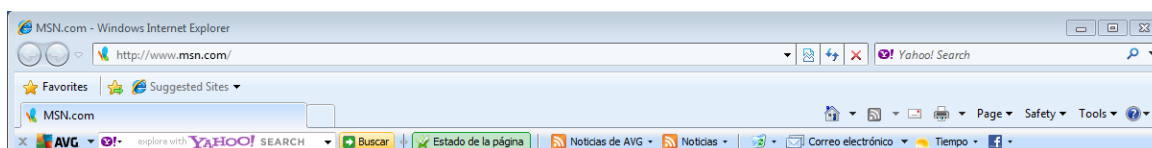
La **barra de herramientas AVG Security** es una nueva herramienta que funciona con el componente **LinkScanner**. La **Barra de herramientas AVG Security** se puede utilizar para controlar las funciones de **LinkScanner** y para ajustar su comportamiento.

Si elige instalar la barra de herramientas durante la instalación de **AVG Internet Security 2011**, ésta se agregará automáticamente a su navegador web (*Internet Explorer 6.0 o superior* y *Mozilla Firefox 3.0 o superior*). De momento no es compatible con ningún otro navegador de Internet.

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

### 8.1. Interfaz de la barra de herramientas AVG Security

La **Barra de herramientas AVG Security** está diseñada para trabajar con **MS Internet Explorer** (versión 6.0 o superior) y **Mozilla Firefox** (versión 3.0 o superior). Una vez que haya decidido instalar la **barra de herramientas Security** (durante el [proceso de instalación](#) de AVG se le solicita si desea instalar este componente), el componente se ubicará en el navegador web, justo debajo de la barra de direcciones:



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

#### 8.1.1. Botón del logotipo de AVG

Este botón proporciona acceso a los elementos de la barra de herramientas general. Haga clic en el botón del logotipo para ir al [sitio web de AVG](#). Al hacer clic con el puntero al lado del icono de AVG se abrirán las siguientes opciones:

- **Información de la barra de herramientas:** vínculo a la página de inicio de la **barra de herramientas AVG Security**, que contiene información detallada acerca de la protección que le ofrece la barra de herramientas.
- **Ejecutar AVG:** abre la **AVG Internet Security 2011 interfaz del usuario**
- **AVG Info:** abre un menú contextual con los vínculos siguientes que permiten ver información de seguridad importante sobre **AVG Internet Security 2011**:
  - *Acerca de las amenazas:* abre el [sitio web de AVG](#), en la página en la que se proporcionan los datos más importantes sobre las principales amenazas, recomendaciones de eliminación de virus, información sobre actualizaciones de AVG, acceso a la [base de datos de virus](#) y más información relevante



- *Noticias de AVG*: abre la página web que proporciona los comunicados de prensa relacionados con AVG más recientes
- *Nivel de amenaza actual*: abre la página web del laboratorio de virus con una visualización gráfica del nivel de amenaza actual en Internet
- *AVG Threat Labs*: abre el sitio web de [Reportes de sitios de AVG](#) donde puede buscar amenazas específicas por nombre y obtener información detallada sobre cada una de ellas
- **Opciones**: abre un cuadro de diálogo de configuración donde puede ajustar la configuración de la **barra de herramientas AVG Security** para adaptarla a sus necesidades. Consulte el siguiente capítulo: [Opciones de la barra de herramientas AVG Security](#)
- **Eliminar historial**: en la **barra de herramientas AVG Security** permite eliminar el historial completo o eliminar el historial de búsqueda, el historial del navegador, el historial de descarga y las cookies por separado.
- **Actualizar**: comprueba si existen nuevas actualizaciones para su **barra de herramientas AVG Security**
- **Ayuda**: proporciona opciones para abrir el archivo de ayuda, ponerse en contacto con el [soporte técnico de AVG](#), enviar comentarios sobre los productos o ver los detalles de la versión actual de la barra de herramientas

### 8.1.2. Cuadro de búsqueda de Yahoo!

El cuadro de búsqueda de Yahoo! : es una forma sencilla y segura de buscar en Internet utilizando la búsqueda de Yahoo!. Introduzca una palabra o una frase en el cuadro de búsqueda y presione el botón **Buscar** o la tecla **Intro** para iniciar la búsqueda en Yahoo! directamente, independientemente de la página que se muestra en estos momentos. El cuadro de búsqueda también muestra el historial de búsqueda. Las búsquedas hechas mediante el cuadro de búsqueda se analizan utilizando la protección [Search-Shield](#) .

De forma alternativa, dentro del campo de búsqueda puede cambiar a Wikipedia, o a algún otro servicio de búsqueda específico, consulte la imagen:



### 8.1.3. Nivel de protección

El botón **Protección total/Protección limitada/Sin protección** comprueba el estado de los componentes [Surf-Shield](#) y [Search-Shield](#). *Protección total* significa que ambos componentes están activos. *Protección limitada* se refiere al hecho de que sólo uno de estos componentes está activo, y *Sin protección* que ambos están desactivados. Cada botón abre la pestaña **Seguridad** en el cuadro de diálogo [Opciones de la barra de herramientas](#), que le permite asignar la función de **Barra de herramientas AVG Security** que desea utilizar.



#### 8.1.4. Estado de la página

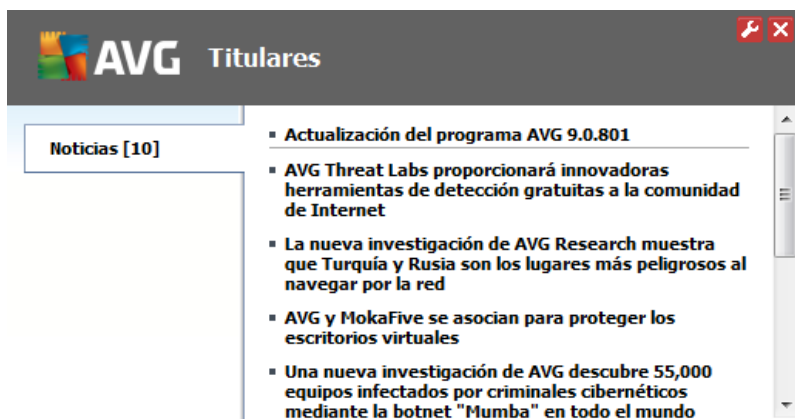
Directamente en la barra de herramientas, este botón muestra la evaluación de la página web mostrada en ese momento según los criterios del componente [Surf-Shield](#):

- - La página vinculada es segura
- : la página es algo sospechosa.
- : la página contiene vínculos a páginas definitivamente peligrosas.
- - La página vinculada contiene amenazas activas. Por su seguridad, no se le permitirá visitar esta página.
- : la página no es accesible, por lo tanto, no puede analizarse.

Haga clic en este botón para abrir un panel con información detallada sobre la página web específica.

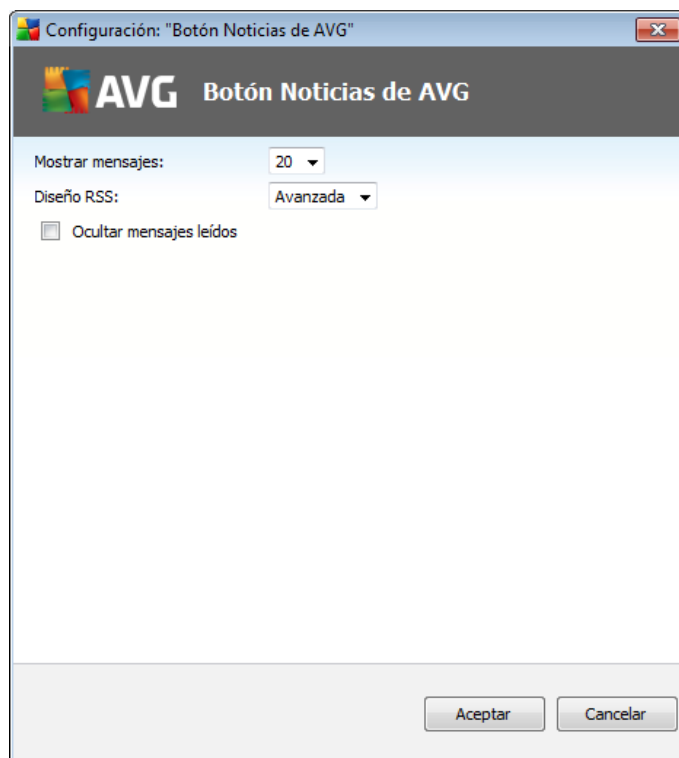
#### 8.1.5. Noticias de AVG


Directamente desde la **barra de herramientas AVG Security**, este botón abre un resumen de los **titulares** más recientes relativos a AVG, tanto noticias de la prensa como comunicados de prensa de la compañía:



En la esquina superior derecha puede ver dos botones de control rojos:

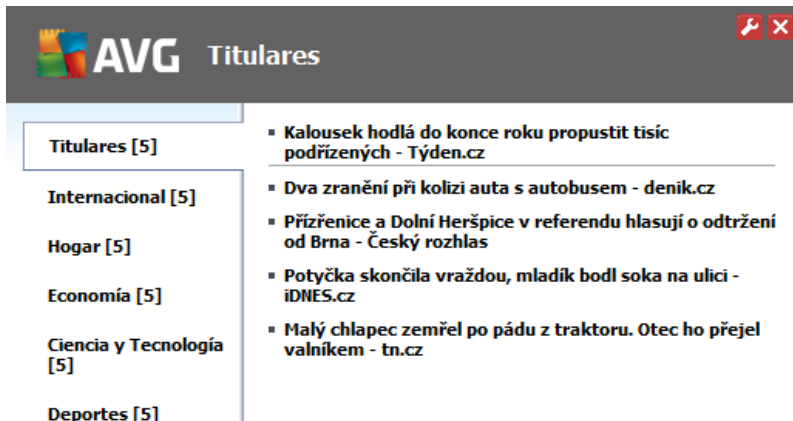
- : el botón abre el cuadro de diálogo de edición donde puede especificar los parámetros del botón **Noticias de AVG** que aparece en la **barra de herramientas AVG Security**:




- **Mostrar mensajes:** cambie el número de mensajes que desea que se muestren a la vez
- **Diseño RSS:** seleccione entre el modo avanzado o básico de la pantalla actual del resumen de noticias (*de forma predeterminada, el modo avanzado está seleccionado; consulte la imagen anterior*)
- **Ocultar mensajes leídos:** marque este elemento para confirmar que todos los mensajes leídos ya no se deben mostrar para que se puedan entregar mensajes nuevos
- : haga clic en este botón para cerrar el resumen de noticias abierto en este momento

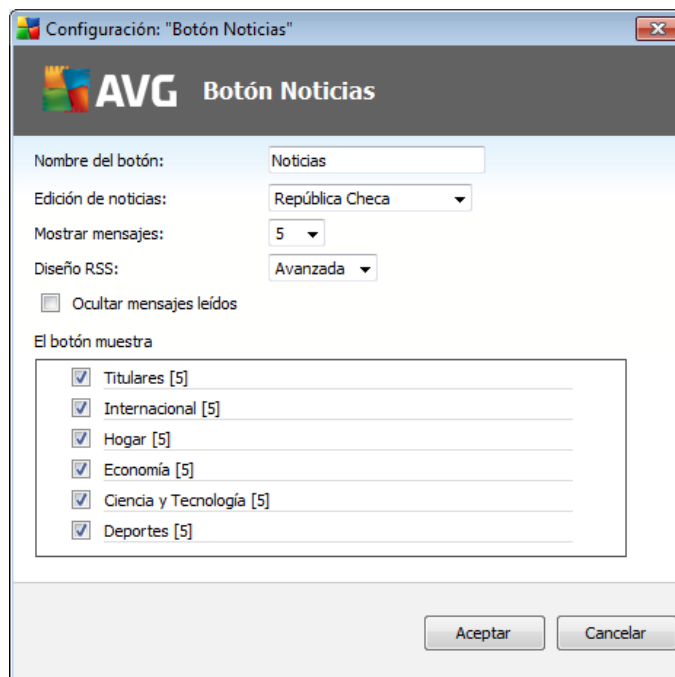
### 8.1.6. Noticias

De manera similar, directamente desde la **Barra de herramientas AVG Security**, este botón abre un resumen de las noticias más recientes de los medios de comunicación seleccionados divididas en varias secciones:




En la esquina superior derecha puede ver dos botones de control rojos:

- : este botón abre el cuadro de diálogo de edición donde puede especificar los parámetros del botón **Noticias** que aparece en la **Barra de herramientas AVG Security**:



- **Nombre del botón:** tiene la opción de cambiar el nombre del botón que se muestra en la **Barra de herramientas AVG Security**
- **Edición de noticias:** seleccione un país de la lista para que se muestren las noticias de la región seleccionada
- **Mostrar mensajes:** especifique el número de mensajes que desea que se muestren a la vez



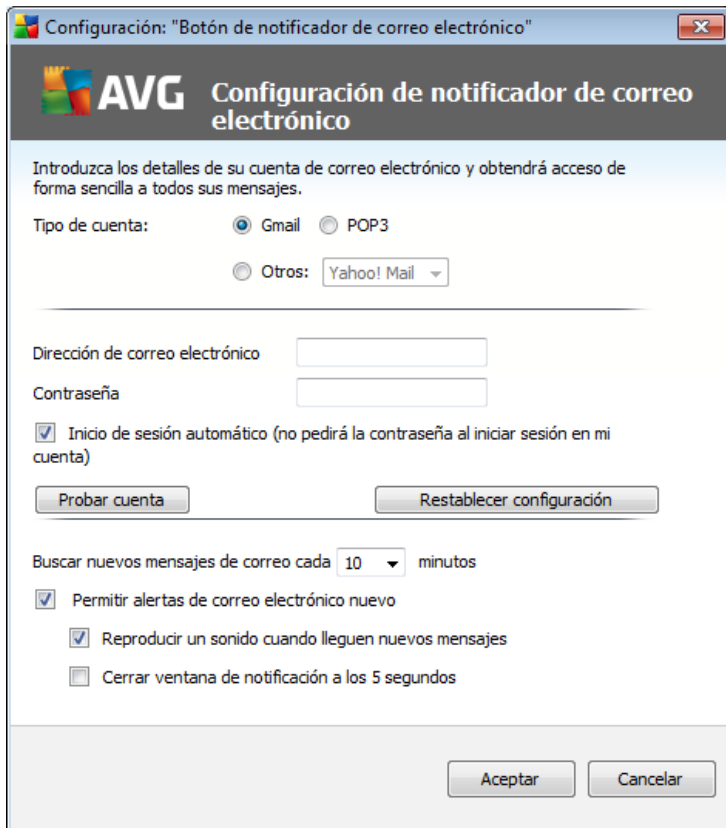
- **Diseño RSS:** cambie entre la opción básica y avanzada para seleccionar el diseño del resumen de noticias (**el diseño avanzado está definido de forma predeterminada; vea la imagen anterior**)
- **Ocultar mensajes leídos:** seleccione este elemento para confirmar que ya no deben mostrarse los mensajes leídos en el resumen de noticias y que deben reemplazarse con un titular nuevo
- **El botón muestra:** en este campo puede asignar el tipo de noticias que deben mostrarse en el resumen de noticias de la **Barra de herramientas AVG Security**
  - : haga clic en este botón para cerrar el resumen de noticias abierto en este momento

### 8.1.7. Eliminar historial

Mediante este botón puede eliminar el historial del navegador como a través de la opción **Logotipo de AVG -> Eliminar historial**.

### 8.1.8. Notificador de correo electrónico

El botón **Notificador de correo electrónico** permite activar la opción de estar informado de los mensajes de correo electrónico nuevos que llegan directamente en la interfaz de la **Barra de herramientas AVG Security**. El botón abre el cuadro de diálogo de edición siguiente, donde puede definir los parámetros de la cuenta de correo electrónico y las reglas de visualización de los correos electrónicos. Siga las instrucciones del cuadro de diálogo:



- **Tipo de cuenta:** especifique el tipo de protocolo que utiliza su cuenta de correo electrónico. Puede seleccionar entre las alternativas siguientes: *Gmail* o *POP3*, o seleccionar el nombre del servidor del menú desplegable incluido en el elemento *Otros* (actualmente puede utilizar esta opción si su cuenta es de Correo Yahoo! o Hotmail). Si no está seguro de qué tipo de servidor de correo electrónico utiliza su cuenta, intente obtener la información de su proveedor de correo electrónico o su proveedor de servicios de Internet.
- **Inicio de sesión:** en la sección de inicio de sesión escriba exactamente su *dirección de correo electrónico* y la *contraseña* correspondiente. Mantenga marcada la opción *Inicio de sesión automático* para que no tenga que escribir los datos continuamente.
- **Buscar nuevos mensajes de correo cada ... minutos:** defina el rango de tiempo que se utilizará para buscar mensajes de correo electrónico nuevos (entre 5 y 120 minutos) y especifique si desea que se le informe de la llegada de un mensaje nuevo y cómo desea que se le informe.

### 8.1.9. Información meteorológica

El botón **Tiempo** muestra la información sobre la temperatura actual (que se actualiza cada 3-6 horas) en el destino seleccionado directamente en la interfaz de la **Barra de herramientas AVG Security**. Haga clic en el botón para abrir un nuevo panel informativo con una descripción general del tiempo:



Brno, CZ °F °C ✕  
[ [Cambiar ubicación](#) ]

 **21° C** Velocidad del viento 16.09 km/h  
Salida del sol: 06:24  
Puesta del sol: 19:13

|  |  |
|--|--|
|  <b>Domingo</b><br><b>Máxima: 22 °C</b><br><b>Mínima: 11 °C</b> |  <b>Lunes</b><br><b>Máxima: 20 °C</b><br><b>Mínima: 12 °C</b> |
|--|--|

Actualizado 09/12/2010 15:17:42 **YAHOO! NEWS** [Previsión completa >](#)

A continuación se incluyen las opciones de edición:

- **Cambiar ubicación:** haga clic en el texto **Cambiar ubicación** para mostrar un nuevo cuadro de diálogo llamado **Busque su ubicación**. Rellene el nombre de la ubicación que desee en el campo de texto, y confírmelo haciendo clic en el botón **Buscar**. A continuación, dentro de la lista de todas las ubicaciones del mismo nombre, seleccione el destino que está buscando. Finalmente, se mostrará el panel de información de nuevo con la información del tiempo para la ubicación seleccionada.
- **Convertidor de Fahrenheit/Celsius:** en la esquina superior derecha del panel de información puede elegir entre las escalas de Fahrenheit y Celsius. Según su selección, se proporcionará la información de la temperatura también en la medida seleccionada.
- **Pronóstico completo:** si está interesado en un pronóstico completo y detallado, utilice el vínculo **Pronóstico completo** para obtener acceso al sitio web específico sobre el tiempo en <http://weather.yahoo.com/>

### 8.1.10. Facebook

El Botón **Facebook** le permite conectarse a la red social [Facebook](#) directamente desde la **Barra de herramientas AVG Security**. Haga clic en el botón y aparecerá la invitación de inicio de sesión; vuelva a hacer clic para abrir el cuadro de diálogo **Inicio de sesión en Facebook**. Especifique los datos de acceso y presione el botón **Conectar**. Si aún no tiene una cuenta en [Facebook](#), puede crear una directamente con el vínculo **Registrarse en Facebook**.

Cuando haya terminado el proceso de registro en [Facebook](#), se le invitará a permitir la aplicación **Extensión social de AVG**. Las funciones de esta aplicación son fundamentales para la conexión de la barra de herramientas y [Facebook](#), por lo que se recomienda permitir su funcionamiento; asegúrese de permitirlo. Luego se activará la conexión a [Facebook](#), y el botón **Facebook** de la **Barra de herramientas AVG**



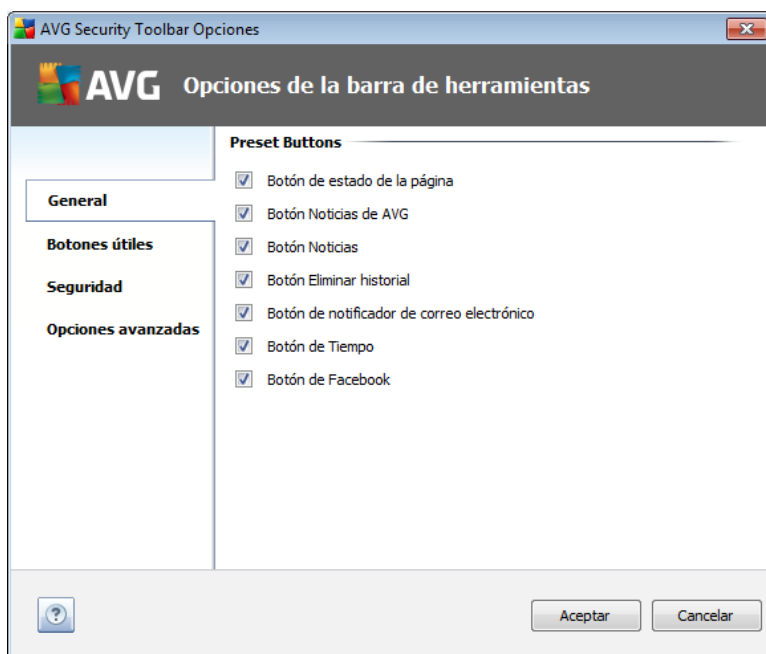


**Security** ahora ofrecerá las opciones estándar del menú de [Facebook](#).

## 8.2. Opciones de la Barra de herramientas AVG Security

Toda la configuración de los parámetros de la **barra de herramientas AVG Security** puede modificarse directamente en el panel de la **barra de herramientas AVG Security**. La interfaz de edición se abre mediante el elemento de menú de la barra de herramientas AVG / *Opciones* en un nuevo cuadro de diálogo denominado **Opciones de la barra de herramientas**, el cual se divide en cuatro secciones:

### 8.2.1. Pestaña General



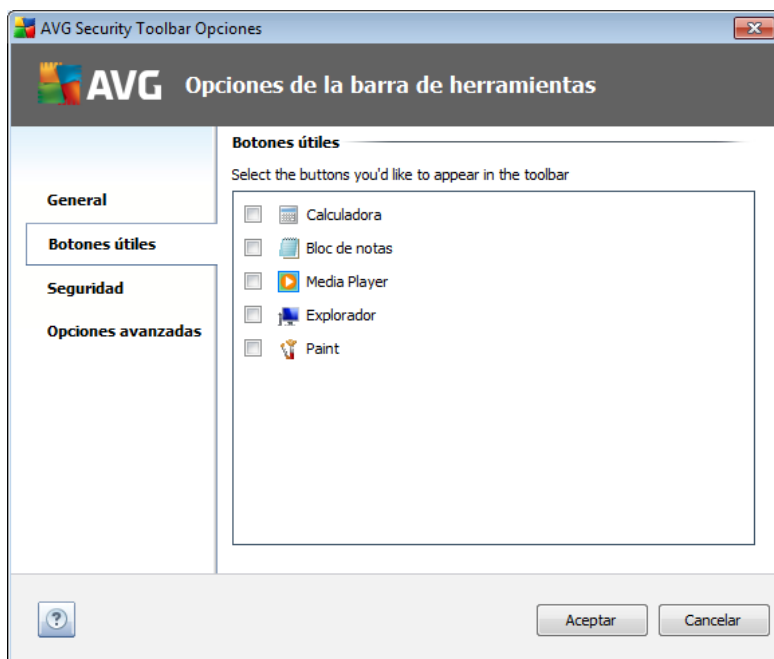
En esta pestaña puede especificar los botones de control de la barra de herramientas que deben mostrarse u ocultarse en el panel **Barra de herramientas AVG Security**. Marque las opciones para las cuales desea que se muestre el botón respectivo. A continuación encontrará una descripción de la función de los botones de la barra de herramientas:

- **Botón de estado de la página:** este botón ofrece la posibilidad de mostrar la información en el estado de seguridad de la página abierta en ese momento en la **Barra de herramientas AVG Security**
- **Botón Noticias de AVG:** abre una página web que proporciona los comunicados de prensa relacionados con AVG más recientes
- **Botón Noticias:** proporciona una descripción general estructurada de las noticias actuales de la prensa diaria
- **Botón Eliminar historial:** este botón permite eliminar el historial completo o eliminar el historial de búsqueda, eliminar el historial del navegador, eliminar el

historial de descargas o eliminar las cookies directamente desde el panel de la barra de herramientas de AVG Security

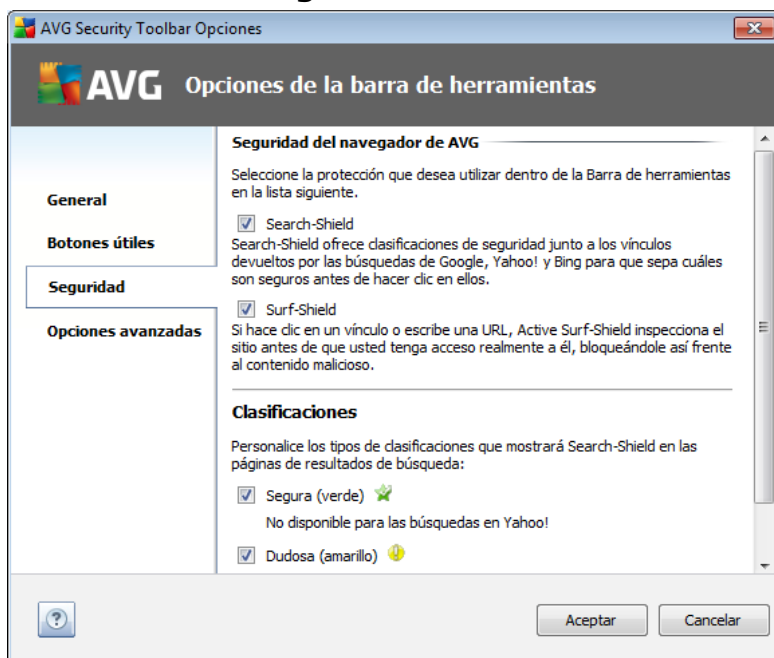
- **Botón de notificador de correo electrónico:** este botón permite mostrar los mensajes de correo nuevos en la interfaz de la **Barra de herramientas AVG Security**
- **Botón de Tiempo:** este botón ofrece información inmediata sobre la situación del tiempo en una ubicación determinada
- **Botón de Facebook:** este botón ofrece conexión directa con la red social [Facebook](#)

### 8.2.2. Pestaña Botones útiles








La pestaña **Botones útiles** permite seleccionar aplicaciones de una lista y visualizar su icono en la interfaz de la barra de herramientas. De esta manera, el icono sirve de vínculo rápido que permite iniciar inmediatamente la aplicación correspondiente.

### 8.2.3. Pestaña Seguridad



La pestaña **Seguridad** se divide en dos secciones, **Seguridad del navegador de AVG** y **Clasificaciones**, en donde puede seleccionar casillas de verificación específicas para asignar la funcionalidad de la **barra de herramientas AVG Security** que desee utilizar:

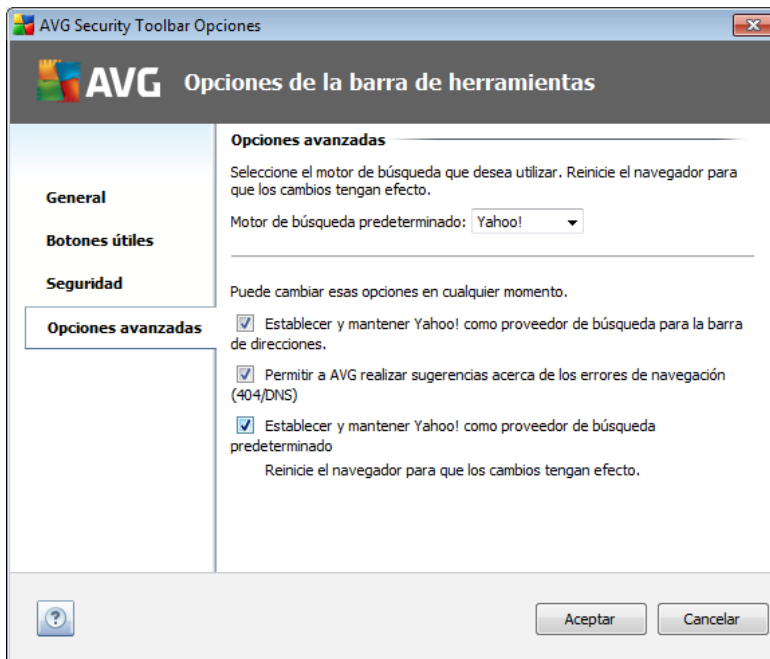
- **Seguridad del navegador de AVG:** seleccione este elemento para activar o desactivar el servicio [Search-Shield](#) o el servicio [Surf-Shield](#)
- **Clasificaciones:** seleccione los símbolos gráficos utilizados para las clasificaciones de los resultados de búsqueda por el componente [Search-Shield](#) que desee utilizar:
  -  la página es segura
  -  la página es algo sospechosa
  -  la página contiene vínculos a páginas definitivamente peligrosas
  -  la página contiene amenazas activas
  -  la página no es accesible, por lo tanto, no puede analizarse

Seleccione la opción correspondiente para confirmar que desea recibir información acerca de este nivel de amenaza específico. Sin embargo, la marca roja asignada a las páginas que contienen amenazas activas y peligrosas no se puede desactivar. **Nuevamente, se recomienda conservar la configuración**



**predeterminada que estableció el proveedor del programa a menos que cuente con una razón real para cambiarla.**

#### 8.2.4. Pestaña Opciones avanzadas



En la pestaña **Opciones avanzadas** seleccione primero qué motor de búsqueda desea utilizar de forma predeterminada. Puede elegir entre *Yahoo!*, *Baidu*, *WebHledani* y *Yandex*. Si ha cambiado el motor de búsqueda predeterminado, reinicie su navegador de Internet para que el cambio surta efecto.

Además, puede activar o desactivar más configuraciones específicas de la **Barra de herramientas AVG Security** (la lista incluida se refiere a la configuración predeterminada de Yahoo!):

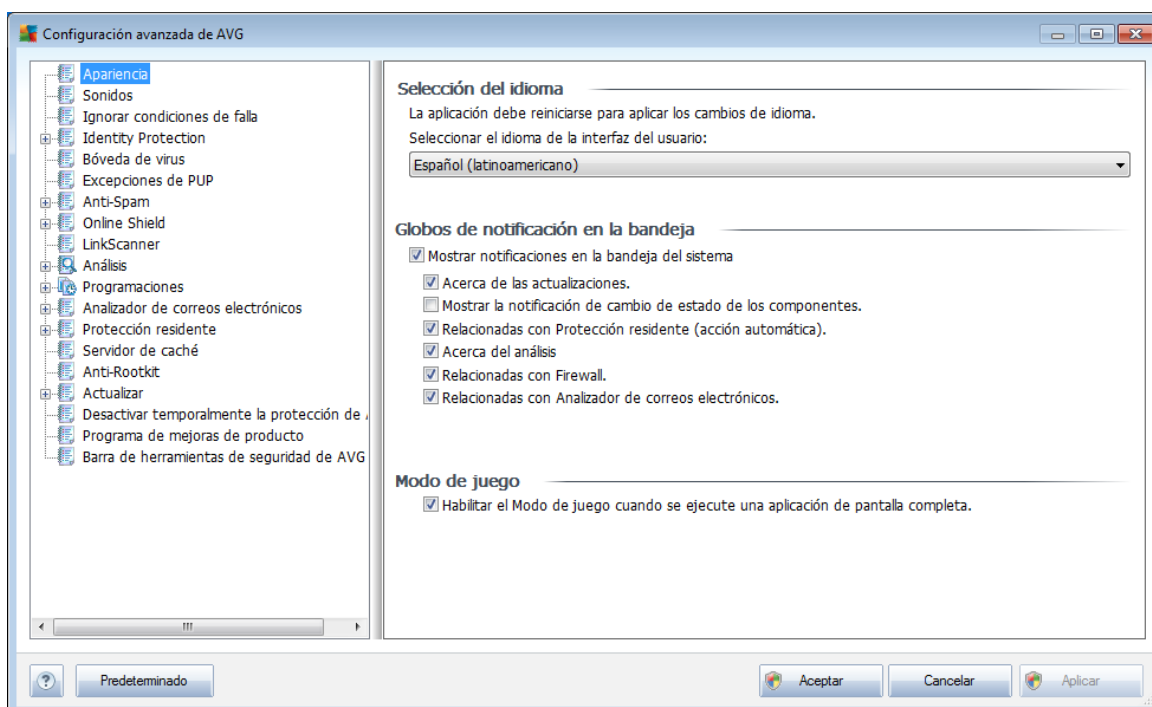
- **Establecer y mantener Yahoo! como el proveedor de búsqueda de la barra de direcciones:** si esta opción está seleccionada, puede escribir un término de búsqueda directamente en la barra de direcciones del navegador de Internet, y el servicio de Yahoo! se utilizará automáticamente para buscar los sitios web de interés.
- **Permitir a AVG realizar sugerencias acerca de los errores de navegación del navegador (404/DNS):** si durante la búsqueda en Internet se encuentra con una página que no existe o que no se puede visualizar (error 404), se le mostrará automáticamente una página web que permite seleccionar entre algunas páginas alternativas relacionadas con el tema.
- **Establecer y mantener Yahoo! como proveedor de búsqueda :** Yahoo! es el motor de búsqueda predeterminado para la búsqueda en Internet dentro de la **barra de herramientas AVG Security**, y al activar esta opción se puede convertir también en el motor de búsqueda predeterminado del navegador web.

## 9. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG Internet Security 2011** se abre en una ventana nueva denominada **Configuración avanzada de AVG**. La ventana está dividida en dos secciones: la parte izquierda ofrece una navegación organizada en forma de árbol hacia las opciones de configuración del programa. Seleccione el componente del que desea cambiar la configuración (*o su parte específica*) para abrir el diálogo de edición en la sección del lado derecho de la ventana.

### 9.1. Apariencia

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



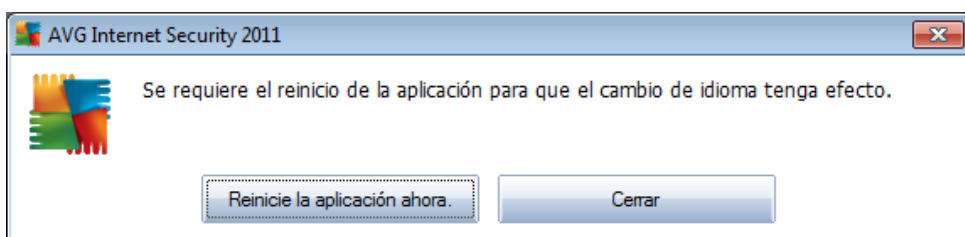
#### Selección de idioma

En la sección **Selección de idioma**, puede elegir el idioma deseado en el menú desplegable; este idioma será el que se utilice en toda la [Interfaz del usuario de AVG](#). El menú desplegable sólo ofrece los idiomas que seleccionó previamente para que se instalaran durante el [proceso de instalación](#) (*consulte el capítulo [Opciones personalizadas](#)*) además del inglés (*que se instala de forma predeterminada*). Sin embargo, para finalizar el cambio de la aplicación a otro idioma se debe reiniciar la interfaz del usuario; siguiendo estos pasos:

- Seleccione el idioma deseado de la aplicación y confirme su selección

presionando el botón **Aplicar** (esquina inferior derecha)

- Presione el botón **Aceptar** para confirmar
- El nuevo cuadro de diálogo emergente que le informa que el cambio de idioma de la interfaz del usuario de AVG requiere reiniciar la aplicación:



## Notificaciones de globo en la bandeja

Dentro de esta sección se puede suprimir la visualización de las notificaciones de globo sobre el estado de la aplicación en la bandeja del sistema. De manera predeterminada, se permite la visualización de las notificaciones de globo, y se recomienda mantener esta configuración. Las notificaciones de globo normalmente informan acerca del cambio de estado de algún componente AVG, y se les debe prestar atención.

Sin embargo, si por alguna razón decide que no se visualicen estas notificaciones, o desea que sólo se muestren ciertas notificaciones (relacionadas con un componente de AVG específico), se pueden definir y especificar las preferencias seleccionando o quitando la marca de selección de las siguientes opciones:

- **Mostrar notificaciones en la bandeja de sistema:** de manera predeterminada, este elemento está seleccionado (*activado*) y las notificaciones se visualizan. Quite la marca de selección de este elemento para desactivar la visualización de todas las notificaciones de globo. Cuando se encuentra activado, puede también seleccionar qué notificaciones en concreto deben visualizarse:
  - **Acerca de las actualizaciones:** decida si debe visualizarse información sobre la ejecución, el progreso y la finalización del proceso de actualización de AVG;
  - **Mostrar notificaciones de cambio de estado de los componentes:** decida si debe visualizarse información relativa a la actividad o inactividad de los componentes o los posibles problemas. A la hora de notificar un estado de error de un componente, esta opción equivale a la función informativa del [icono de la bandeja del sistema](#) (que cambia de color) que notifica un problema en cualquier componente AVG;
  - **Relacionadas con la Protección residente (acción automática):** decida si debe visualizarse o suprimirse la información relativa a los procesos de guardado, copia y apertura de archivos (*esta configuración sólo se muestra si la opción [Autoreparar](#) de la Protección residente está*



*activa*);

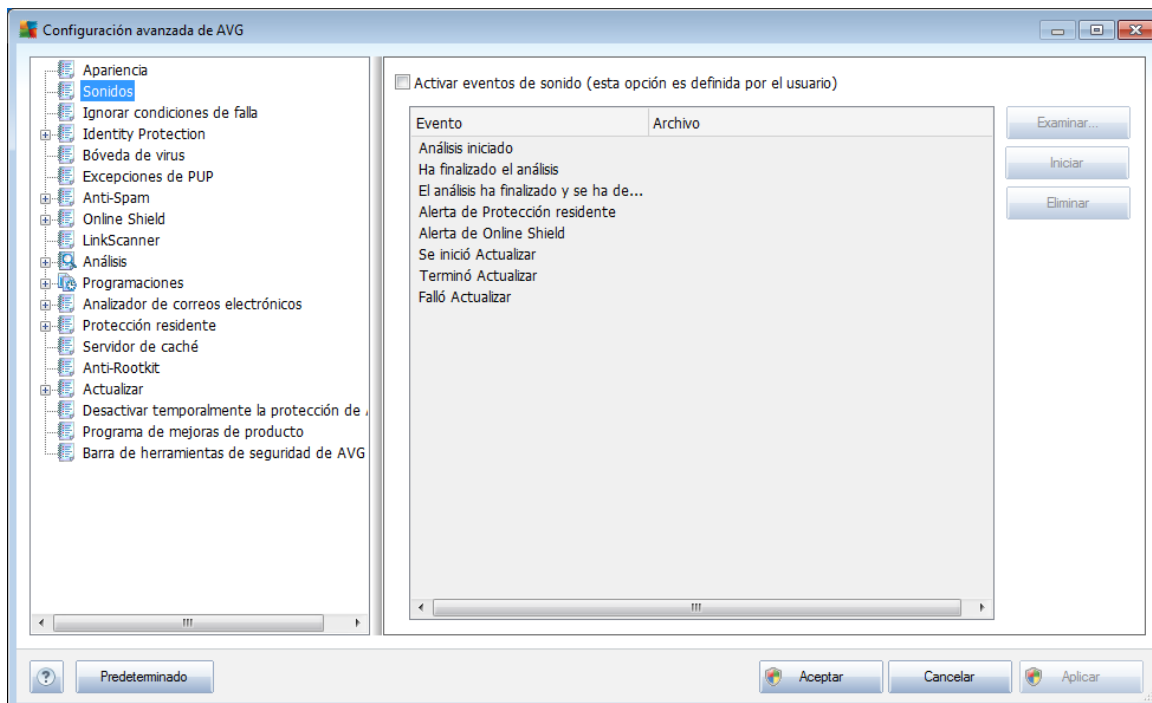
- **Acerca del análisis:** decida si debe visualizarse información sobre la ejecución automática del análisis programado, su progreso y resultados;
- **Relacionadas con el Firewall:** decida si debe visualizarse la información relativa al estado y los procesos relacionados con el Firewall, por ejemplo, las advertencias de activación/desactivación del componente, el posible bloqueo de tráfico, etc.
- **Relacionadas con Analizador de correos electrónicos:** decida si debe visualizarse información sobre el análisis de todos los mensajes de correo electrónico entrantes y salientes.

### **Modo de juego**

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

### **9.2. Sonidos**

En el cuadro de diálogo **Sonidos**, puede especificar si desea que se le informe acerca de acciones específicas de AVG mediante una notificación sonora. Si es así, seleccione la opción **Activar eventos de sonido** (*desactivada de forma predeterminada*) para activar la lista de acciones de AVG:



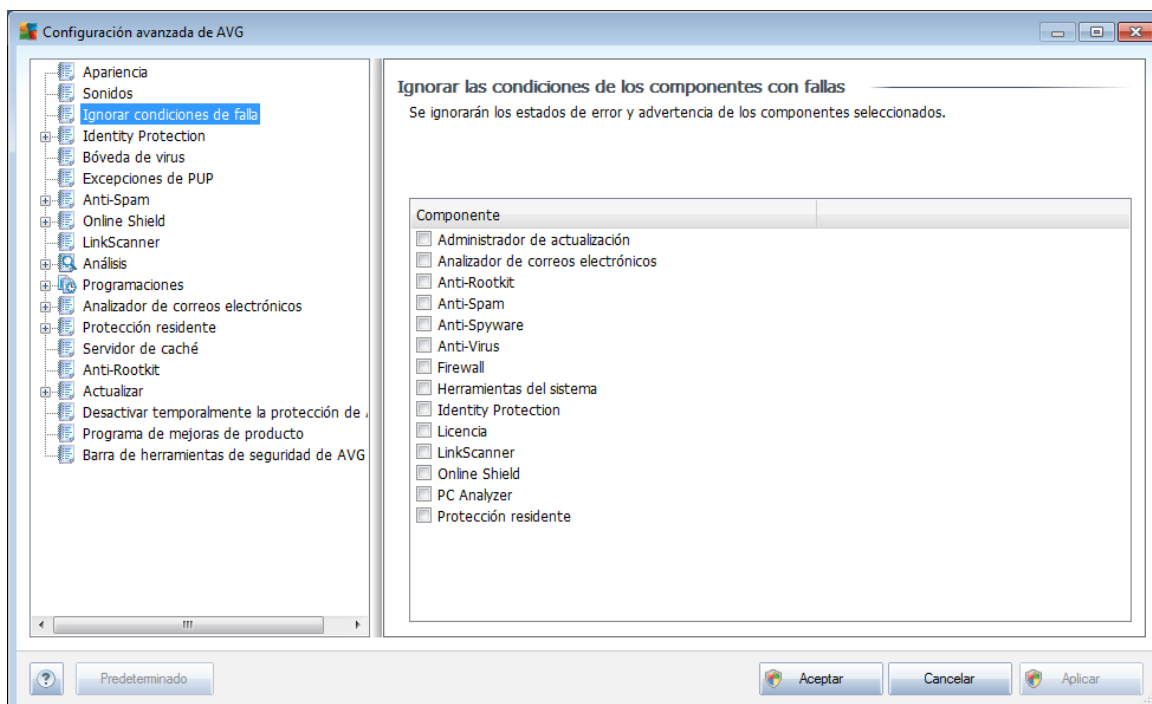
A continuación, seleccione el evento correspondiente de la lista y busque (**Examinar**) en el disco el sonido adecuado que desea asignar a este evento. Para escuchar el sonido seleccionado, resalte el evento en la lista y presione el botón **Reproducir**. Utilice el botón **Eliminar** para eliminar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

**Nota:** solamente los sonidos \*.wav son compatibles.



### 9.3. Ignorar condiciones de falla

En el cuadro de diálogo ***Ignorar condiciones de componentes con falla*** puede marcar aquellos componentes de los que no desea estar informado:



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

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

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

Para esta situación, dentro del cuadro de diálogo anterior puede seleccionar los componentes que pueden estar en un estado de error (*o desactivados*) y de los cuales

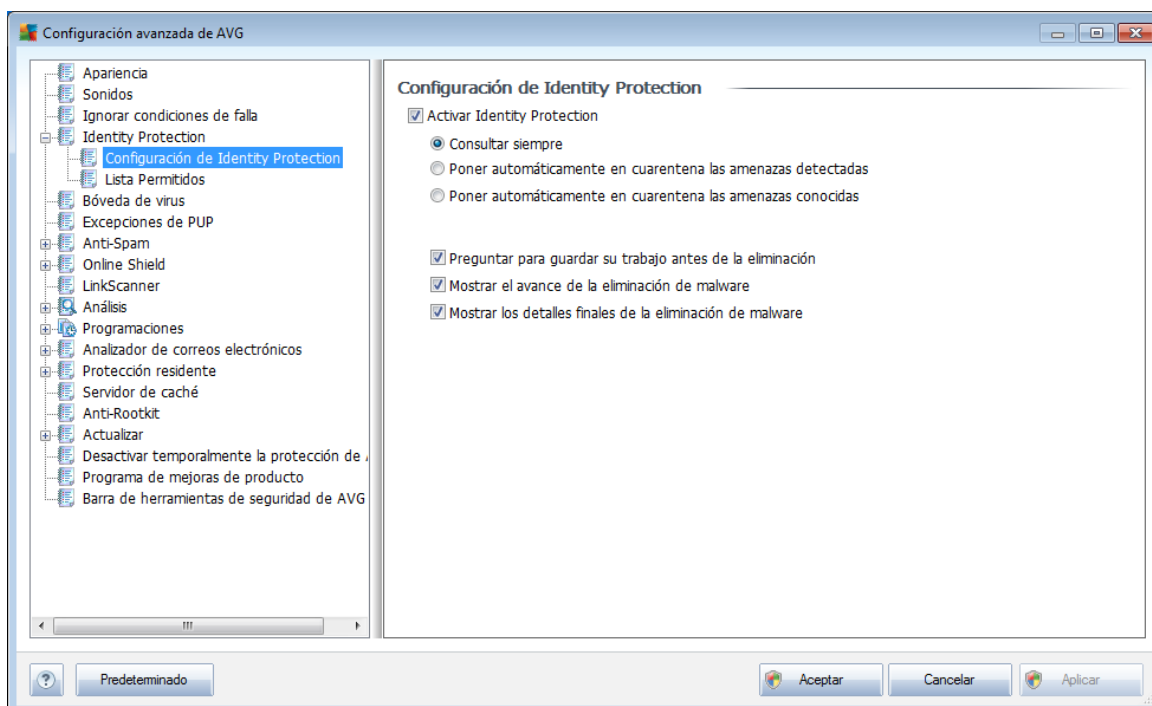


no desea estar informado. La misma opción de **Ignorar el estado del componente** también está disponible para componentes específicos directamente desde la [descripción general de los componentes en la ventana principal de AVG](#).

## 9.4. Identity Protection

### 9.4.1. Configuración de Identity Protection

El cuadro de diálogo [Configuración de Identity Protection](#) le permite activar y desactivar las funciones básicas del componente [Identity Protection](#):



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

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

Cuando [Identity Protection](#) está activa, se puede especificar qué hacer cuando se detecta una amenaza:

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



**Bóveda de virus AVG.** Si se mantiene la configuración predeterminada, cuando se detecte una amenaza se le preguntará si desea ponerla en cuarentena para tener la seguridad de que no se elimine ninguna de las aplicaciones que desee ejecutar.

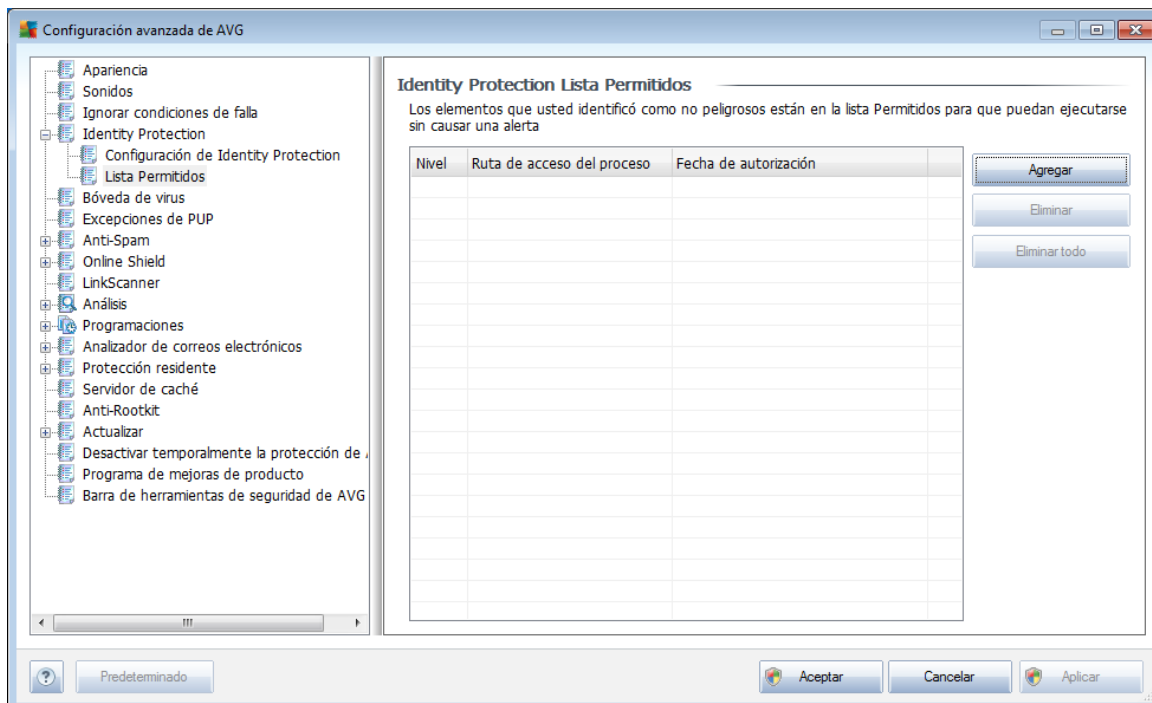
- ***Poner automáticamente en cuarentena las amenazas conocidas:*** mantenga este elemento marcado si desea que todas las aplicaciones detectadas como posible malware se muevan inmediatamente y de forma automática a la **Bóveda de virus AVG.**

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

- ***Solicitar guardar el trabajo antes de la eliminación (activada de forma predeterminada):*** mantenga este elemento seleccionado si desea que se le avise antes de que la aplicación detectada como posible malware se ponga en cuarentena. En caso de que precisamente sea la aplicación con la que trabaja será necesario guardar el proyecto, ya que podría perderlo. Este elemento está activo de forma predeterminada, y se recomienda encarecidamente conservarlo así.
- ***Mostrar el avance de la eliminación de malware (activada de forma predeterminada):*** con este elemento activado, cuando se detecta posible malware, se abre un nuevo cuadro de diálogo donde se muestra el progreso del malware que se está poniendo en cuarentena.
- ***Mostrar los detalles finales de la eliminación de malware (activada de forma predeterminada):*** con este elemento activado, ***Identity Protection*** muestra información detallada acerca de cada objeto puesto en cuarentena ( *nivel de severidad, ubicación, etc.*).

#### **9.4.2. Lista Permitidos**

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



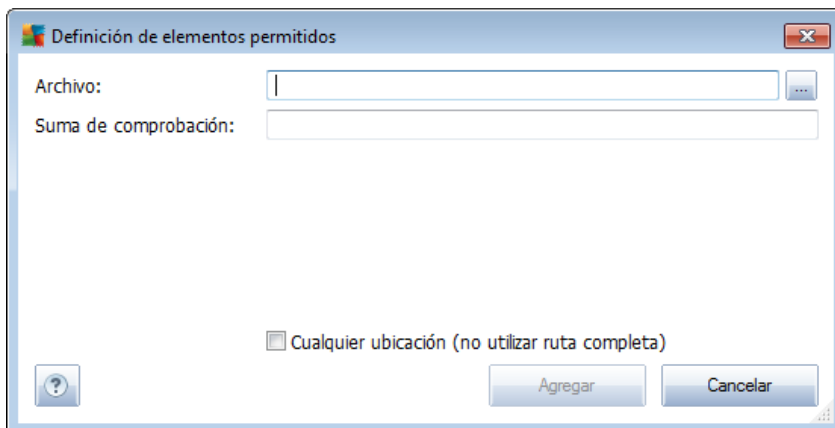
La **Lista Permitidos de Identity Protection** proporciona la información siguiente sobre cada aplicación:

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

### Botones de control

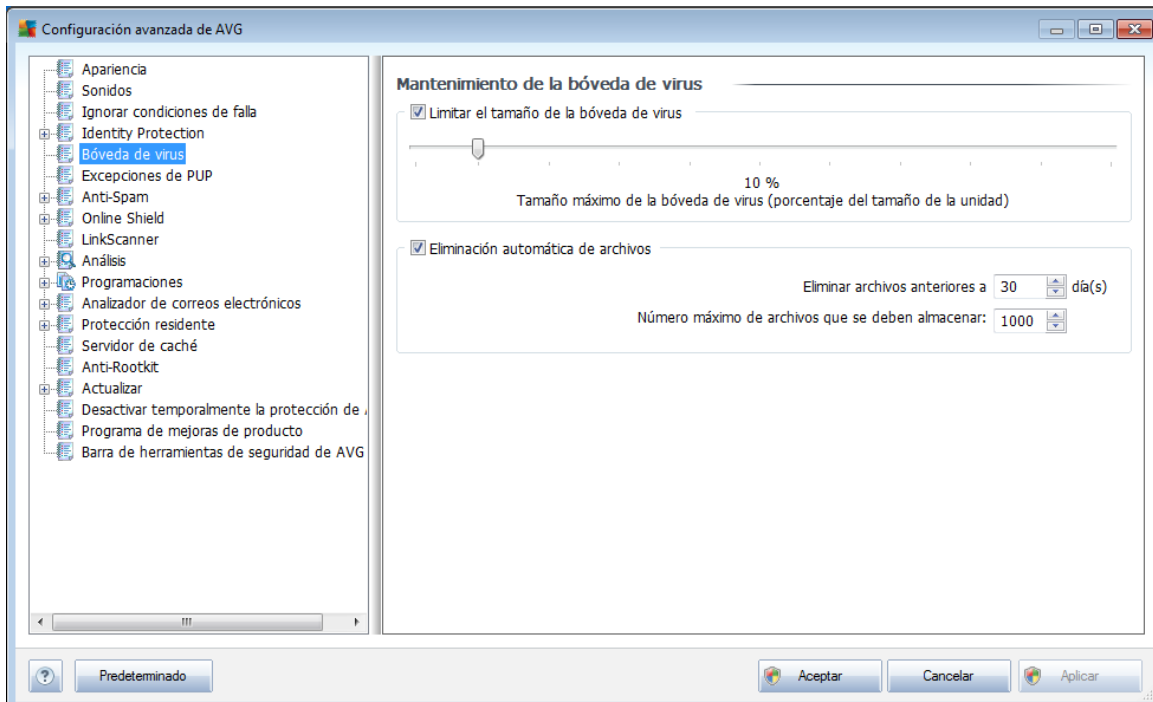
Los botones de control disponibles en el cuadro de diálogo **Lista Permitidos** son:

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



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

## 9.5. Bóveda de Virus

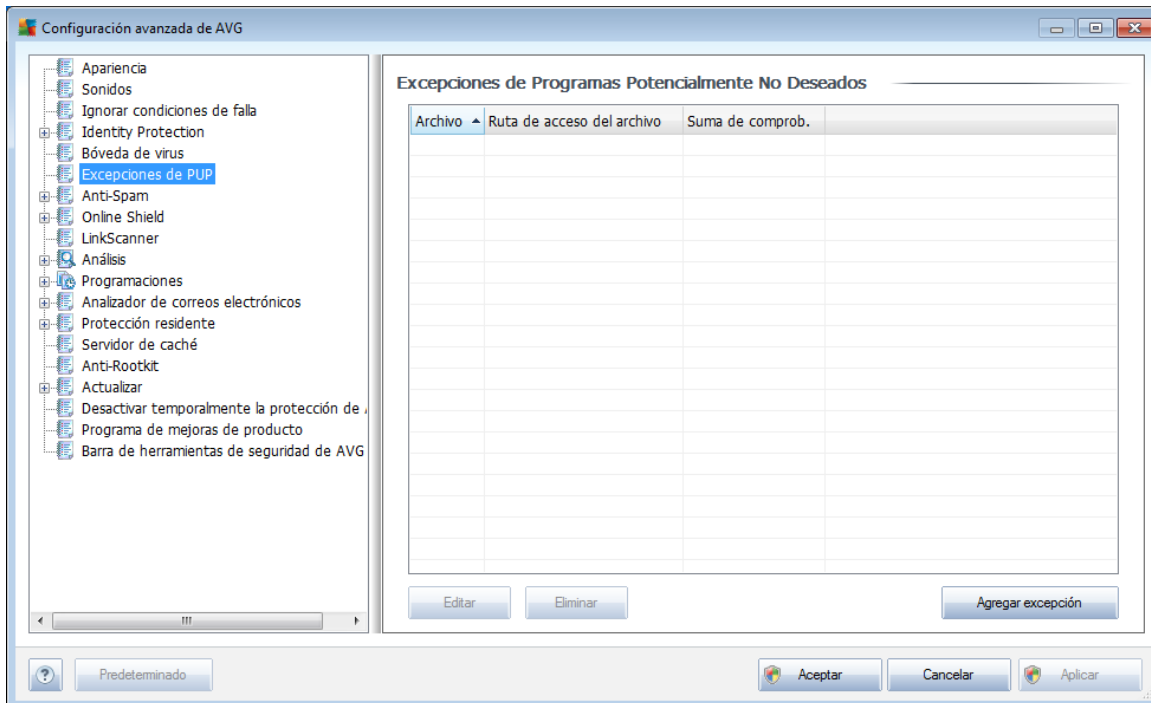


El cuadro de diálogo **Mantenimiento de la Bóveda de virus** permite definir varios parámetros relacionados con la administración de objetos almacenados en la **Bóveda de virus**:

- **Limitar el tamaño de la Bóveda de virus:** utilice el control deslizante para configurar el tamaño máximo de la **Bóveda de virus**. El tamaño se especifica proporcionalmente en comparación con el tamaño del disco local.
- **Eliminación automática de archivos:** en esta sección, defina la longitud máxima de tiempo que se almacenarán los objetos en la **Bóveda de Virus** (**Eliminar archivos anteriores a... días**) y el número máximo de archivos que se almacenarán en la **Bóveda de Virus** (**Número máximo de archivos que se deben almacenar**).

## 9.6. Excepciones de 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, el usuario puede querer mantener ciertos programas no deseados en el equipo (*programas que fueron instalados intencionalmente*). Algunos programas, en especial los gratuitos, incluyen adware. Dicho adware puede ser detectado y presentado por AVG como **un Programa potencialmente no deseado**. Si desea mantener este programa en su equipo, lo puede definir como una excepción de programas potencialmente no deseados:

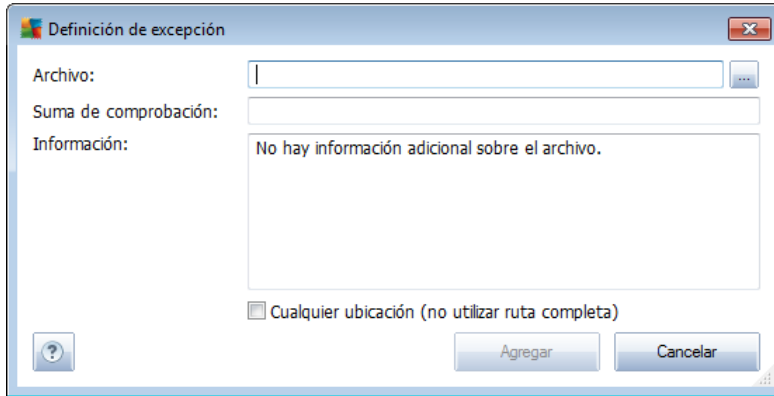


El cuadro de diálogo **Excepciones de Programas potencialmente no deseados** muestra una lista de excepciones definidas y válidas de programas potencialmente no deseados. Puede editar la lista, eliminar elementos existentes o agregar nuevas excepciones. En la lista, puede encontrar la siguiente información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

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

### Botones de control

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

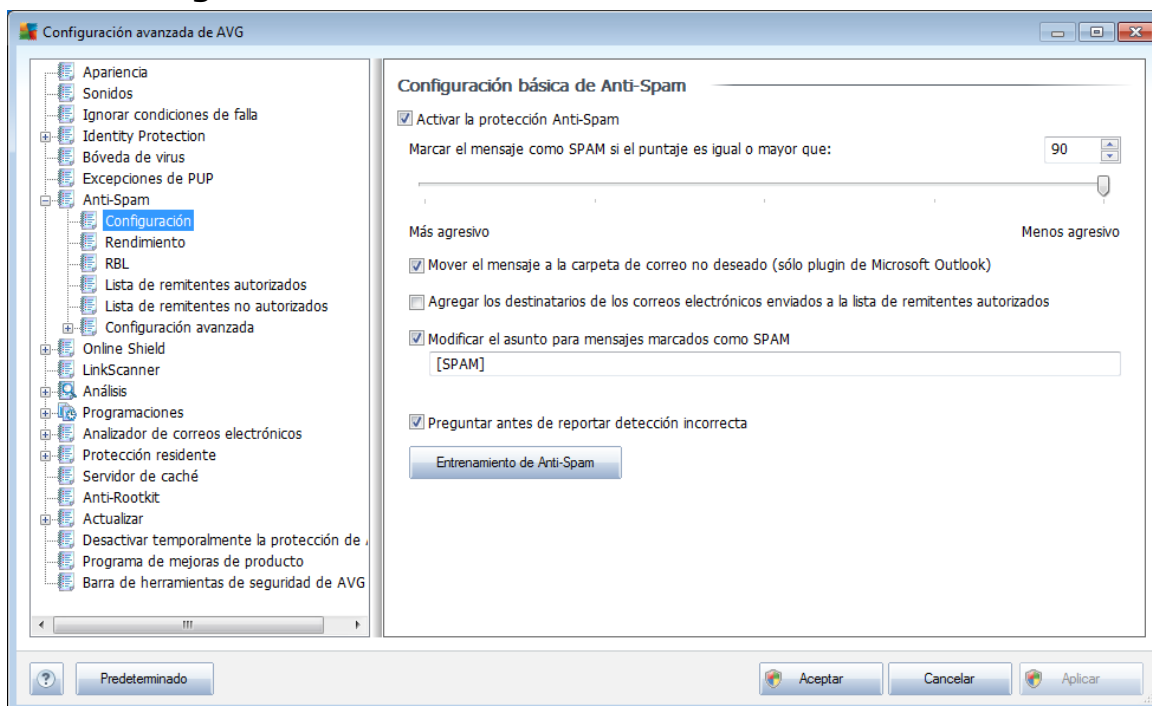


- **Archivo:** introduzca la ruta completa del archivo que desea marcar como una excepción
- **Suma de comprobación:** muestra la "firma" única del archivo elegido. Esta suma de comprobación es una cadena de caracteres generados automáticamente que permite a AVG distinguir de manera inequívoca los archivos elegidos de otros archivos. La suma de comprobación se genera y se muestra después de haber agregado el archivo correctamente.
- **Información del archivo:** muestra cualquier información disponible acerca del archivo (*información de licencia, versión, etc.*)
- **Cualquier ubicación (no utilizar ruta completa):** si desea definir este archivo como una excepción sólo para la ubicación específica, deje esta casilla sin marcar. Si la casilla de verificación está marcada, el archivo especificado se define como una excepción independientemente de donde se encuentre (*sin embargo, tendrá que introducir la ruta completa al archivo específico de todas formas; entonces el archivo se usará como único ejemplo para la posibilidad de que dos archivos del mismo nombre aparezcan en el sistema*).

## 9.7. Anti-Spam



### 9.7.1. Configuración



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

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

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

- **Valores 80-90:** se filtrarán los mensajes de correo electrónico que probablemente sean [spam](#). También se filtrarán, por equivocación, mensajes que no son spam.
- **Valores 60-79:** se considera una configuración bastante agresiva. Se filtrarán los mensajes de correo electrónico que probablemente son [spam](#). Es probable que también se incluyan mensajes que no lo son.
- **Valores 50-59:** configuración muy agresiva. Los mensajes de correo electrónico que no son spam probablemente se consideren mensajes de [spam](#).



Este rango de umbral no se recomienda para uso normal.

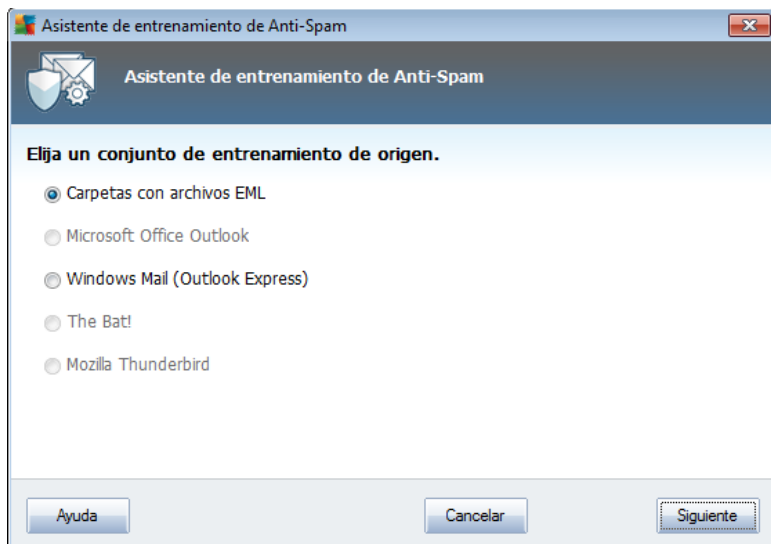
En el cuadro de diálogo **Configuración básica Anti-Spam**, puede definir de modo adicional cómo deben tratarse los mensajes de correo electrónico de [spam](#) detectados :

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

## Botones de control

El botón de **Entrenamiento Anti-Spam** abre el [Asistente de entrenamiento de Anti-Spam](#) que se describe a detalle en el [siguiente capítulo](#).

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



Existen las siguientes opciones entre las cuales elegir:

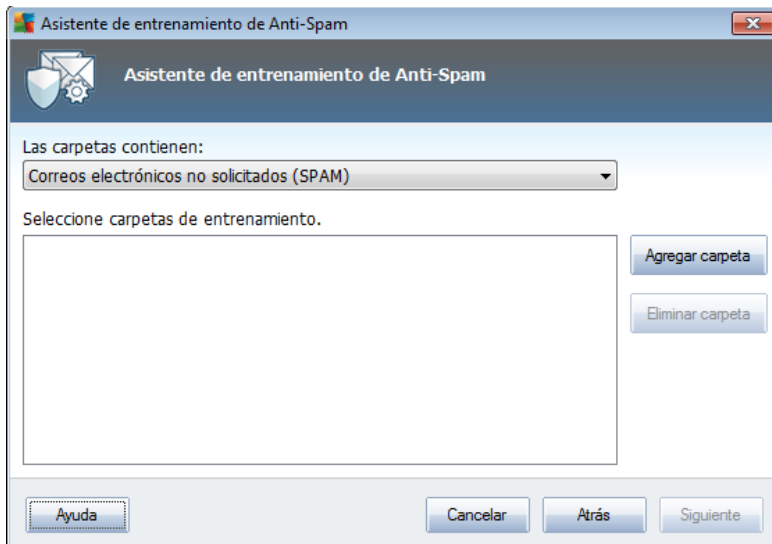
- **Un cliente de correo electrónico específico:** si utiliza uno de los clientes de correo electrónico listado (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), simplemente seleccione la opción respectiva
- **Carpeta con archivos EML:** si utiliza cualquier otro programa de correo electrónico, primero debe guardar los mensajes en una carpeta específica (*en formato .eml*) o estar seguro de que conoce la ubicación de las carpetas de mensajes del cliente de correo electrónico. A continuación seleccione **Carpeta con archivos EML**, lo cual le permitirá ubicar la carpeta deseada en el siguiente paso

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

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

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

### **Carpetas con archivos EML**



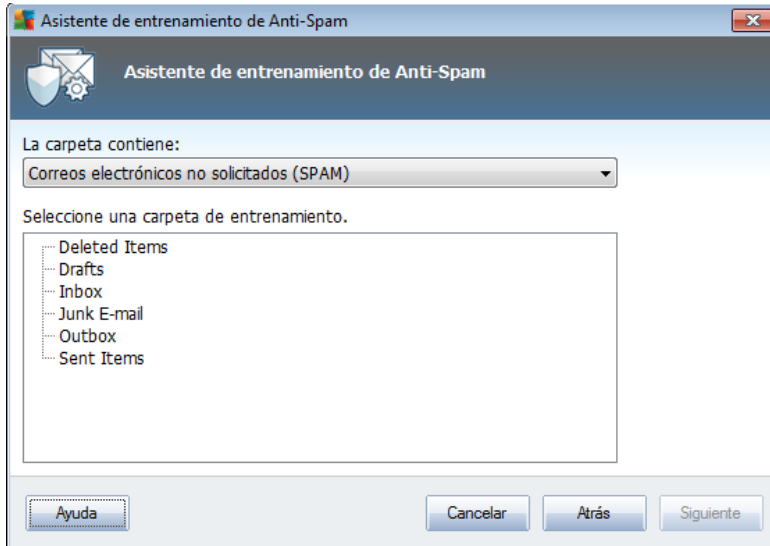
En este cuadro de diálogo, seleccione la carpeta con los mensajes que desea utilizar para entrenamiento. Presione el botón **Agregar carpeta** para ubicar la carpeta con los archivos .eml (*mensaje de correo electrónico guardados*). La carpeta seleccionada se mostrará a continuación en el cuadro de diálogo.

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

Cuando haya terminado, haga clic en **Siguiente** y continúe con las [Opciones de filtro de mensaje](#).

### **Especifique el cliente de correo electrónico**

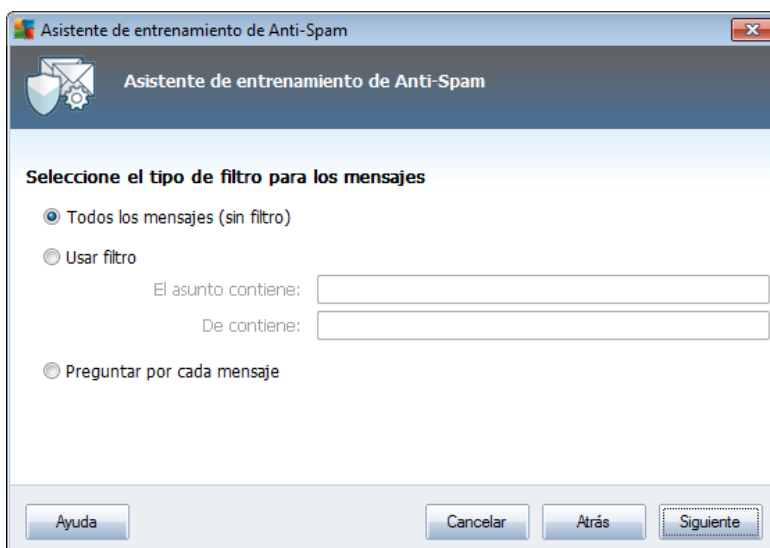
Una vez que haya confirmado una de las opciones, aparecerá el nuevo cuadro de diálogo.



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

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

Cuando haya terminado, haga clic en **Siguiente** para continuar con las [Opciones de filtro de mensaje](#).





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

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

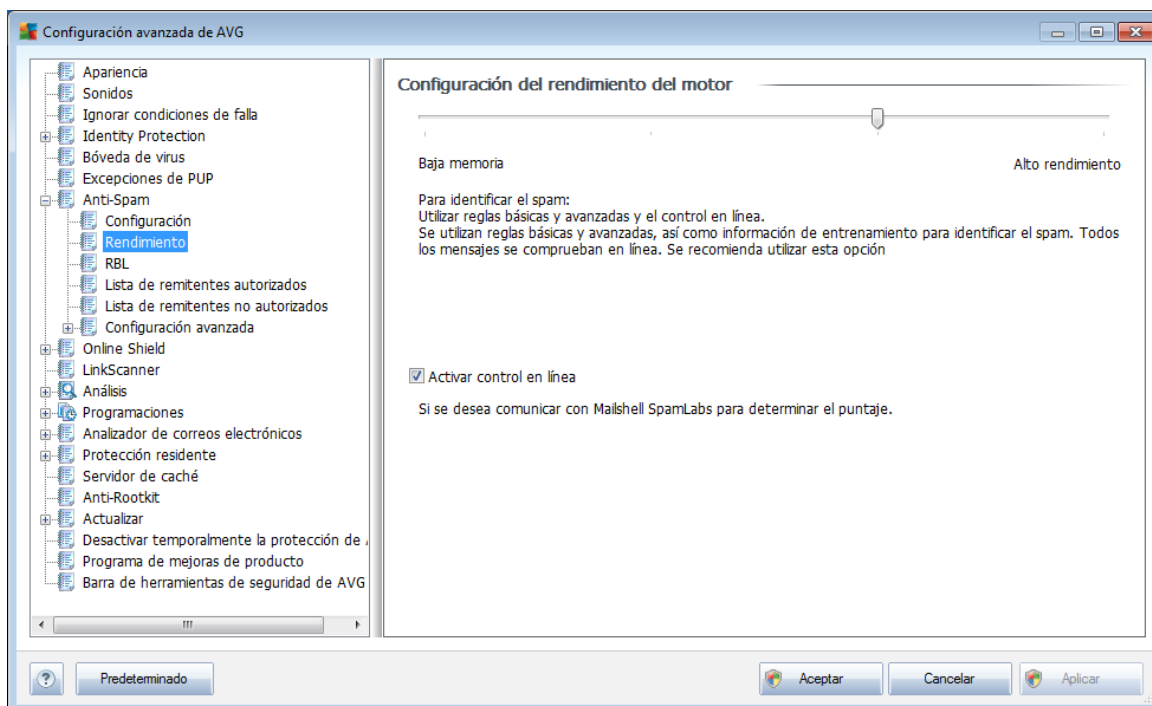
Si no está seguro de cuáles son los mensajes que se encuentran en la carpeta, y desea que el asistente le pregunte qué hacer con cada mensaje (para que pueda determinar si debe utilizarse para el entrenamiento o no), seleccione la opción **Preguntar por cada mensaje**.

Si desea un filtrado más avanzado, seleccione la opción **Usar filtro**. Puede escribir una palabra (*nombre*), parte de una palabra o frase que deba buscarse en los campos de asunto y remitente. Todos los mensajes que contengan exactamente los criterios se utilizarán para el entrenamiento, sin preguntar en cada uno.

**¡Atención!**: Al rellenar ambos campos de texto, las direcciones que cumplan con alguna de las dos condiciones también se utilizarán.

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

## 9.7.2. Rendimiento



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



de rendimiento del componente **Anti-Spam**. Mueva el control deslizante a la izquierda o la derecha para cambiar el nivel del rendimiento del análisis, que varía entre los modos **Poca memoria** y **Alto rendimiento**.

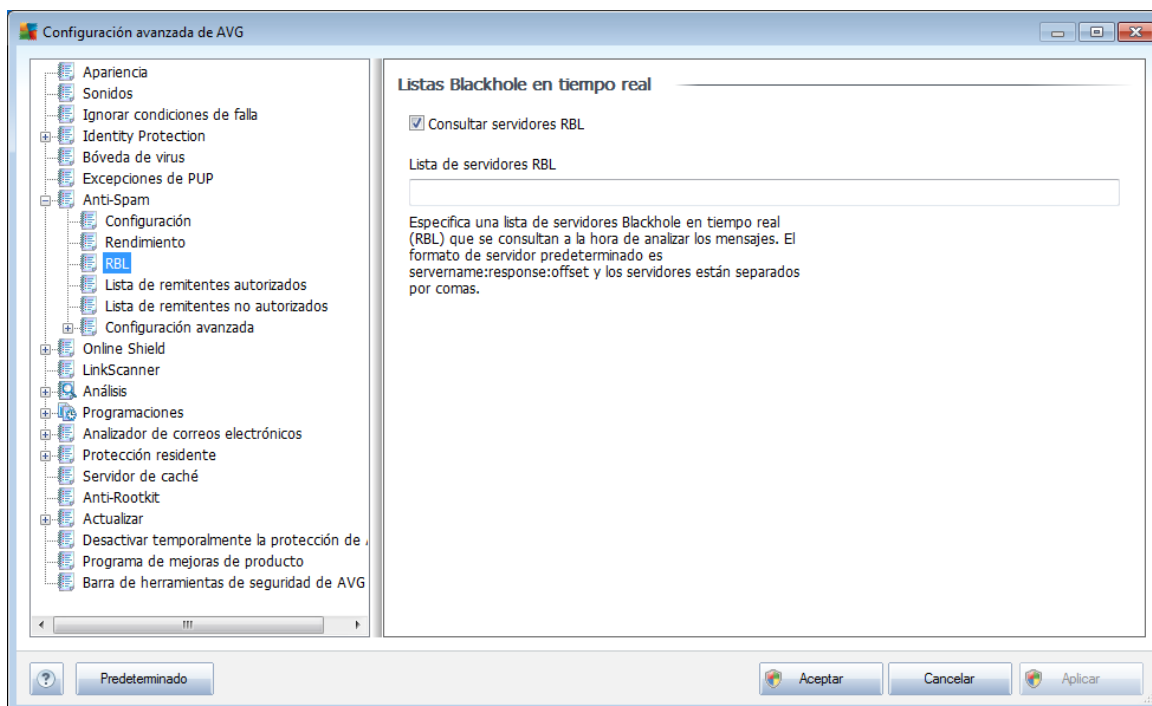
- **Poca memoria**: durante el proceso de análisis para identificar [spam](#), no se utilizará ninguna regla. Sólo se utilizarán los datos de aprendizaje para identificarlo. Este modo no se recomienda para los equipos de uso común, excepto si el hardware del equipo es muy pobre.
- **Alto rendimiento**: este modo utiliza una gran cantidad de memoria. Durante el proceso de análisis para identificar [spam](#), se utilizarán las funciones siguientes: reglas y caché de base de datos de [spam](#), reglas básicas y avanzadas, direcciones IP y bases de datos que suelen emitir spam.

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

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

### 9.7.3. RBL

El elemento **RBL** abre un diálogo de edición llamado **Listas Blackhole en tiempo real**:



En este diálogo puede activar o desactivar la función **Consultar servidores RBL**.



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

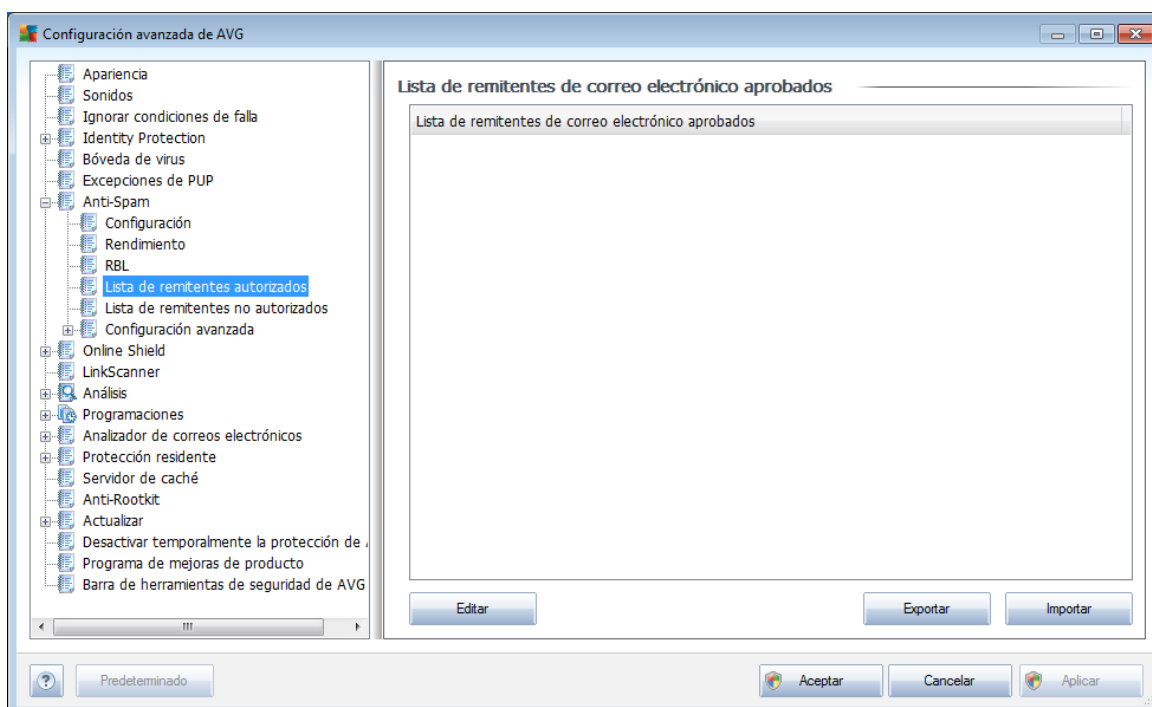
La **Lista de servidores RBL** le permite definir ubicaciones de servidores RBL específicos.

**Nota:** *activar esta función puede hacer más lento el proceso de recepción de correo electrónico en algunos sistemas y con algunas configuraciones, ya que todos y cada uno de los mensajes se comparan con la base de datos del servidor RBL.*

**No se envían datos personales al servidor.**

#### 9.7.4. Lista blanca

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



En la interfaz de edición, puede compilar una lista de remitentes de los cuales está seguro que nunca le enviarán mensajes no deseados (spam). También puede compilar una lista de nombres de dominio completos (*por ejemplo, avg.com*), que sabe que no





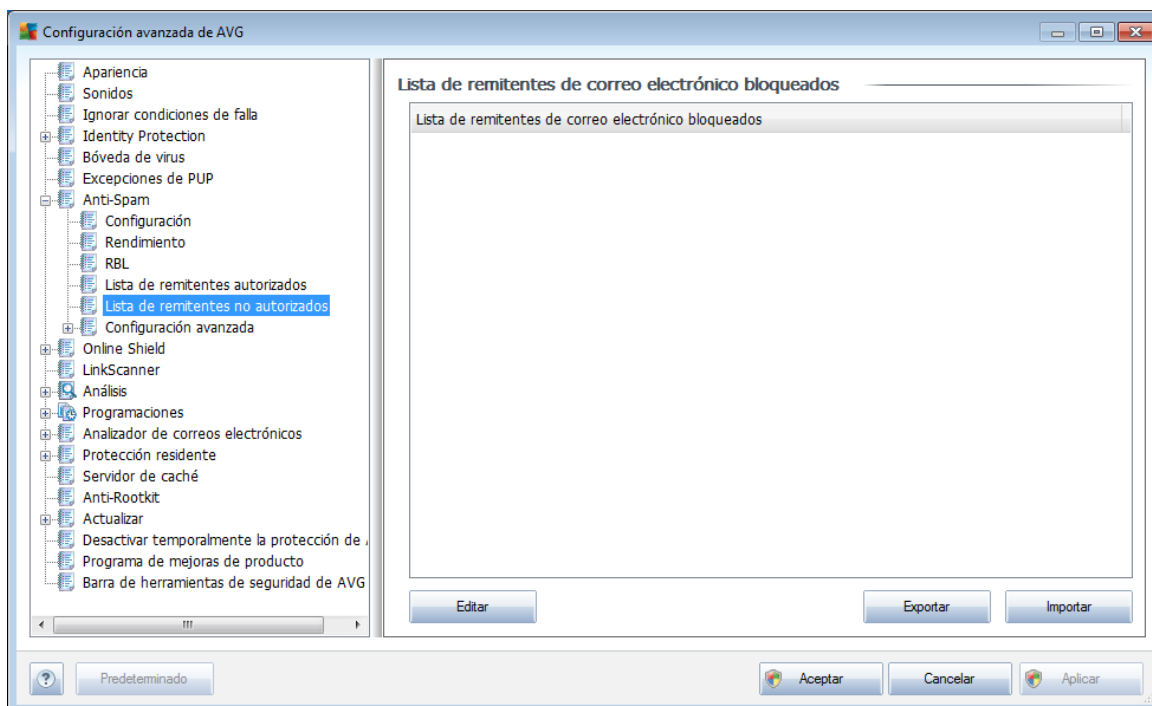
generan mensajes de spam.

Una vez que tenga preparada la lista con los nombres de los remitentes y/o dominios, puede introducirlos por cualquiera de los siguientes métodos: mediante entrada directa de cada dirección de correo electrónico o importando toda la lista de direcciones de una vez. Están disponibles los siguientes botones de control:

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

### 9.7.5. Lista negra

El elemento **Lista negra** abre un diálogo con una lista global de direcciones de correo electrónico de remitentes y nombres de dominios bloqueados cuyos mensajes siempre se marcarán como [spam](#).



En la interfaz de edición, puede indicar una lista de remitentes que estima que le enviarán mensajes no deseados ([spam](#)). También puede compilar una lista de nombres



de dominio completos (*como, por ejemplo, spammingcompany.com*) que estima que pueden enviarle mensajes de spam o que ya se los envían. Todos los mensajes de correo electrónico de las direcciones y los dominios de la lista se identificarán como spam.

Una vez que tenga preparada la lista con los nombres de los remitentes y/o dominios, puede introducirlos por cualquiera de los siguientes métodos: mediante entrada directa de cada dirección de correo electrónico o importando toda la lista de direcciones de una vez. Están disponibles los siguientes botones de control:

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

### 9.7.6. Configuración avanzada

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

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

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

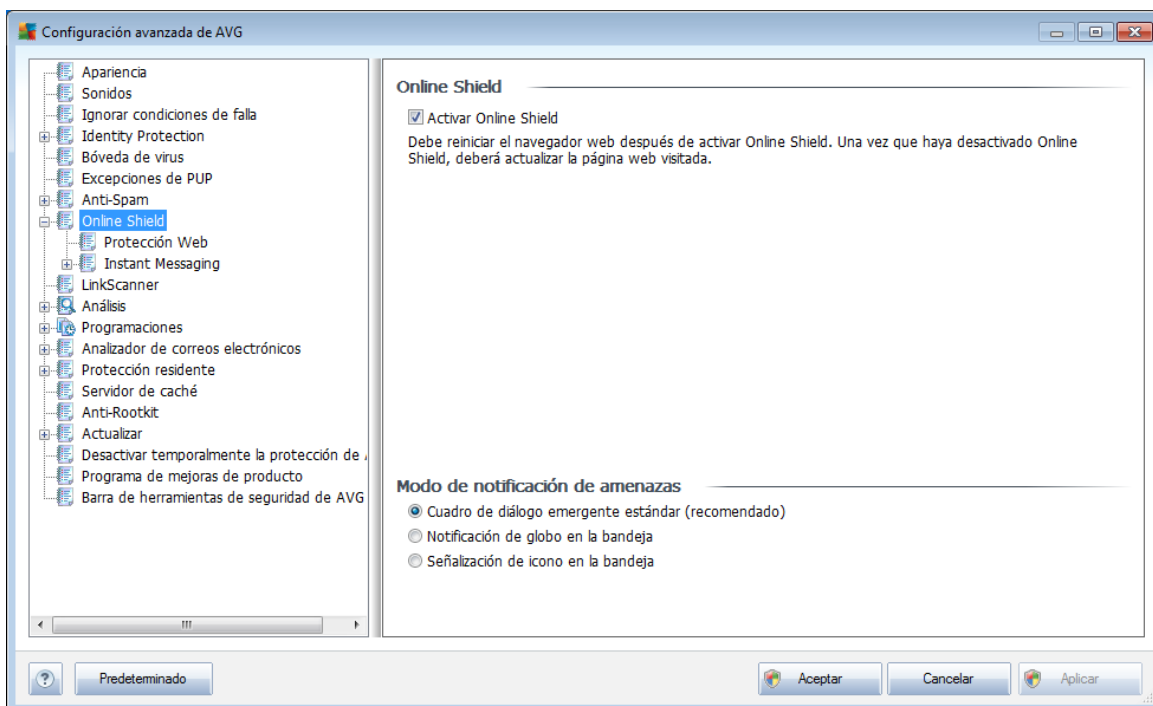
- **Caché :** huella digital, reputación del dominio, LegitRepute
- **Entrenamiento:** entradas máximas de palabras, umbral de auto-entrenamiento, peso
- **Filtro:** lista de idiomas, lista de países, IP aprobadas, IP bloqueadas, países



bloqueados, juegos de caracteres bloqueados, remitentes con identidad suplantada

- **RBL**: servidores RBL, aciertos múltiples, umbral, tiempo de espera, IP máximas
- **Conexión a Internet**: tiempo de espera, servidor proxy, autenticación de servidor proxy

## 9.8. Online Shield



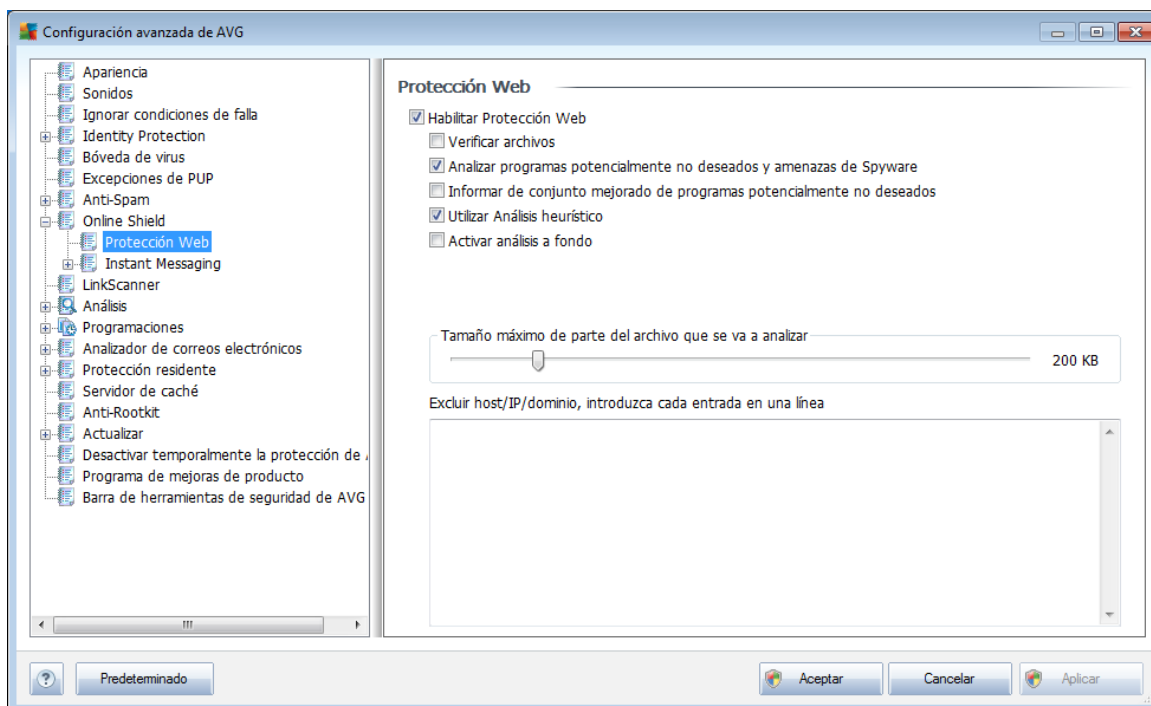
El cuadro de diálogo de **Online Shield** permite activar o desactivar todo el componente **Online Shield** mediante la opción **Activar Online Shield** (*activada de manera predeterminada*). Para ver más opciones de configuración avanzada de este componente, continúe con los cuadros de diálogo posteriores que se muestran en la navegación de árbol:

- [Protección Web](#)
- [Mensajería instantánea](#)

### Modo de notificación de amenazas

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

### 9.8.1. Protección web



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

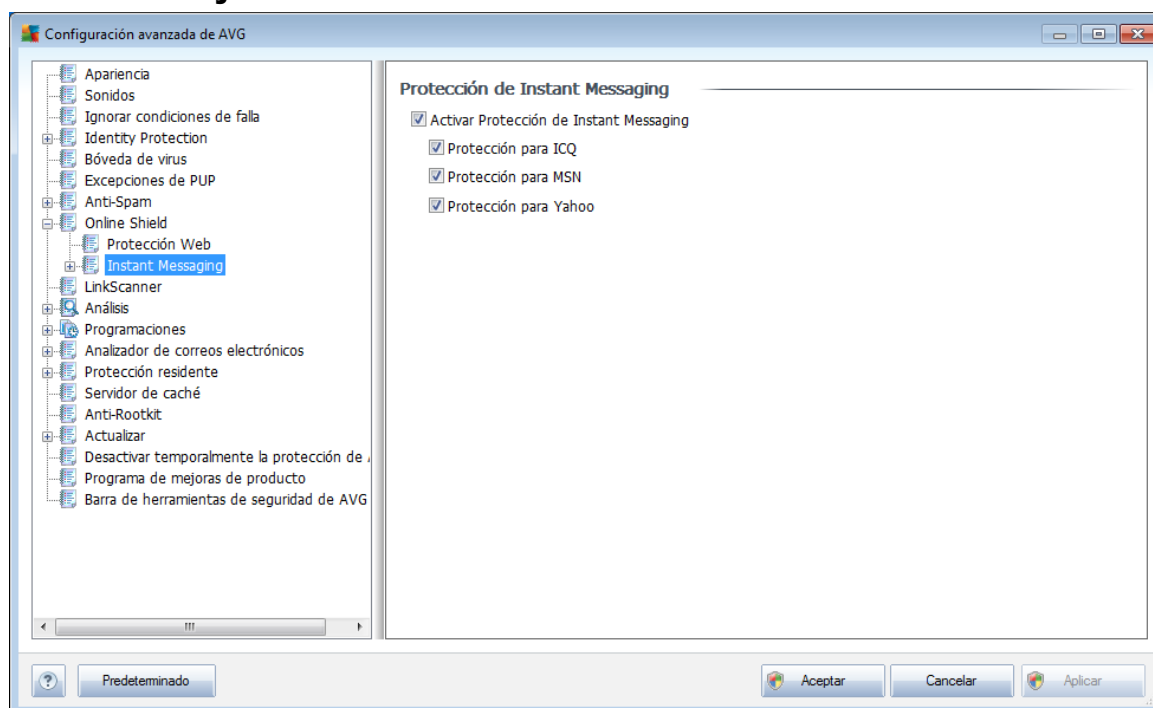
- **Habilitar Protección web:** esta opción confirma que **Online Shield** debe analizar el contenido de las páginas web. Mientras esta opción esté seleccionada (*valor predeterminado*), podrá activar o desactivar estos elementos:
  - **Analizar archivos:** (*desactivado de manera predeterminada*): analiza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



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

- **Utilizar método heurístico:** *(activado de manera predeterminada):* analiza el contenido de la página que se visualizará utilizando el método de [análisis heurístico](#) *(emulación dinámica de las instrucciones del objeto analizado en un entorno virtual).*
- **Activar análisis a fondo** *(desactivado de manera predeterminada):* en determinadas situaciones *(con sospechas de que el equipo está infectado)* puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Tamaño máximo de la parte del archivo que se va a analizar:** si los archivos incluidos están presentes en la página visualizada, también puede analizar su contenido incluso antes de que se descarguen en el equipo. Sin embargo, el análisis de archivos grandes toma bastante tiempo y es posible que la descarga de la página web se ralentice de modo notable. Puede emplear la barra deslizante para especificar el tamaño máximo de archivo que se analizará con [Online Shield](#). Aunque el tamaño del archivo descargado sea superior al valor especificado, y por consiguiente no se analice con Online Shield, seguirá estando protegido: si el archivo está infectado, la [Protección residente](#) lo detectará de inmediato.
- **Excluir host/IP/dominio:** en el campo de texto puede escribir el nombre exacto de un servidor *(host, dirección IP, dirección IP con máscara o URL)* o un dominio que [Online Shield](#) *no debe analizar*. Por lo tanto excluya sólo el host del que esté absolutamente seguro de que nunca le proveerá de contenido peligroso.

## 9.8.2. Mensajería instantánea

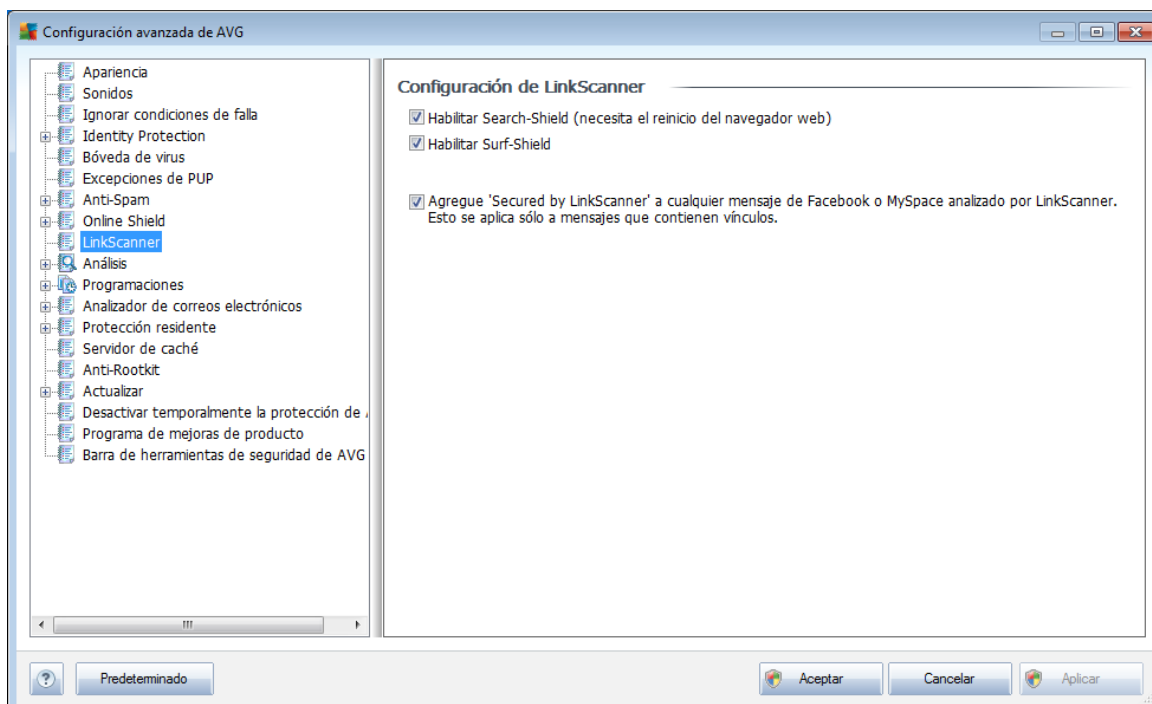


En el cuadro de diálogo **Protección de mensajería instantánea** puede editar la configuración del componente **Online Shield** relativa al análisis de la mensajería instantánea. Actualmente sólo se admiten tres programas de mensajería instantánea: **ICQ**, **MSN** y **Yahoo**: marque el elemento correspondiente a cada uno de ellos si desea que **Online Shield** compruebe que la comunicación en línea no contiene virus.

Para obtener una especificación más detallada de los usuarios permitidos y bloqueados, puede ver y editar el cuadro de diálogo correspondiente (**ICQ avanzado**, **MSN avanzado** o **Yahoo avanzado**) y especificar la **Lista de remitentes autorizados** (lista de usuarios a los que se permitirá la comunicación con su equipo) y la **Lista de remitentes no autorizados** (usuarios que se bloquearán).

## 9.9. Link Scanner

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



- **Habilitar Search-Shield** (activado de forma predeterminada): iconos asesores de notificación sobre las búsquedas realizadas con Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot que comprueban por adelantado el contenido de los sitios devueltos por el motor de búsqueda.
- **Habilitar Surf-Shield** (activado de forma predeterminada): protección activa (en tiempo real) contra sitios de explotación cuando se obtiene acceso a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario obtiene acceso a ellos a través de un navegador web (o cualquier otra aplicación que utilice HTTP).
- **Agregar "Asegurado con LinkScanner"...**: seleccione este elemento para confirmar que desea introducir el aviso de certificación sobre la comprobación de **LinkScanner** en todos los mensajes que contienen hipervínculos activos enviados desde las redes sociales Facebook y MySpace.

## 9.10. Análisis

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

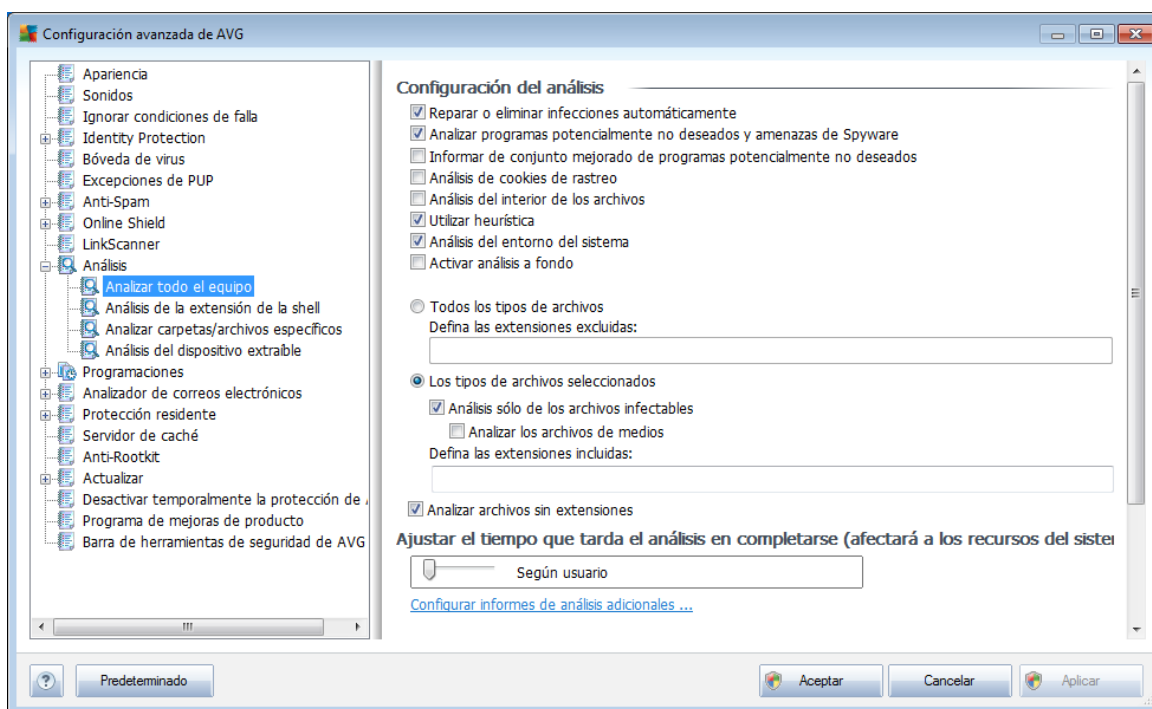
- **Análisis de todo el equipo** : análisis estándar predefinido de todo el equipo



- **Análisis de la extensión de la Shell** : análisis específico de un objeto seleccionado directamente del entorno del Explorador de Windows
- **Análisis de carpetas/archivos específicos** : análisis estándar predefinido de áreas seleccionadas del equipo
- **Análisis de dispositivos extraíbles**: análisis específico de dispositivos extraíbles conectados a su equipo

### 9.10.1. Análisis de todo el equipo

La opción **Analizar todo el equipo** permite editar los parámetros de uno de los análisis predefinidos por el proveedor de software, el **Análisis de todo el equipo**:



### Configuración del análisis

La sección **Configuración del análisis** ofrece una lista de parámetros de análisis que se pueden activar y desactivar:

- **Reparar o eliminar infecciones automáticamente** (activada de forma predeterminada): si se identifica un virus durante el análisis, se puede reparar automáticamente si existe una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la **Bóveda de virus**.
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (activada de forma predeterminada): seleccione esta opción para





activar el motor [Anti-Spyware](#) y analizar en busca de spyware así como de virus. [El spyware](#) representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- **Informar conjunto mejorado de programas potencialmente no deseados** (*desactivada de forma predeterminada*): seleccione esta opción para detectar un paquete extendido de [spyware](#), es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Analizar cookies de rastreo** (*desactivado de manera predeterminada*): este parámetro del componente [Anti-Spyware](#) define que las cookies deben detectarse ; (*las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de su carrito de compras electrónico*)
- **Analizar el interior de los archivos** (*activado de manera predeterminada*): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos (por ejemplo, ZIP, RAR...)
- **Utilizar heurística** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.
- **Analizar el entorno del sistema** (*activado de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- **Activar análisis a fondo** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.

Después sería conveniente decidir si desea analizar

- **Todos los tipos de archivos** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas (*una vez guardado, la coma pasa a ser punto y coma*);
- **Tipos de archivos seleccionados**: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin*

*formato u otros archivos no ejecutables*), incluyendo los archivos multimedia ( *archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

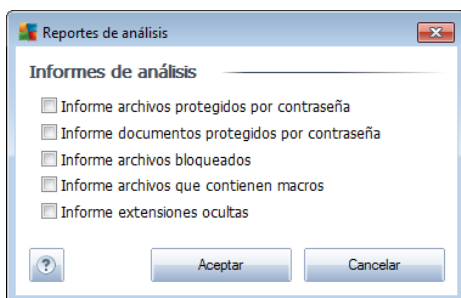
- De manera opcional, puede decidir si desea **Analizar archivos sin extensiones**: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

### Ajustar el tiempo que tarda el análisis en completarse

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

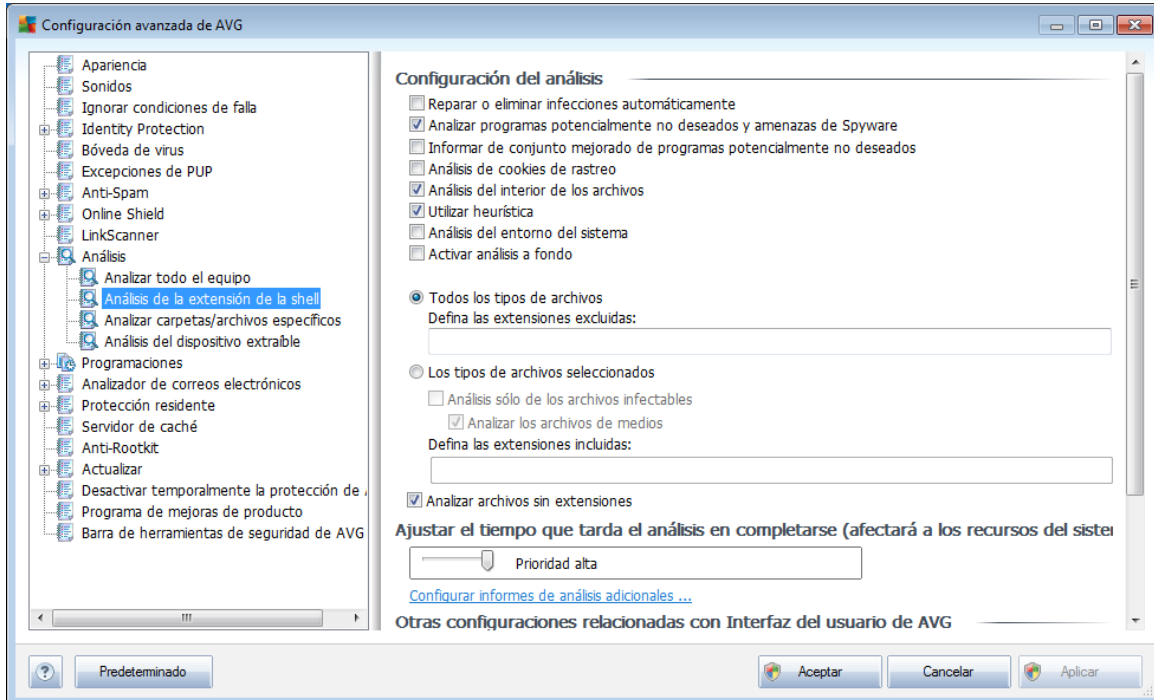
### Configurar informes de análisis adicionales ...

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



#### 9.10.2. Análisis de la extensión de la shell

De modo parecido al anterior elemento [Análisis de todo el equipo](#), este elemento denominado **Análisis de la extensión de la shell** también ofrece varias opciones para editar el análisis predefinido por el proveedor de software. En esta ocasión, la configuración está relacionada con el [análisis de objetos específicos ejecutados directamente desde el entorno del Explorador de Windows](#) (*extensión de la shell*); consulte el capítulo [Análisis en el Explorador de Windows](#):



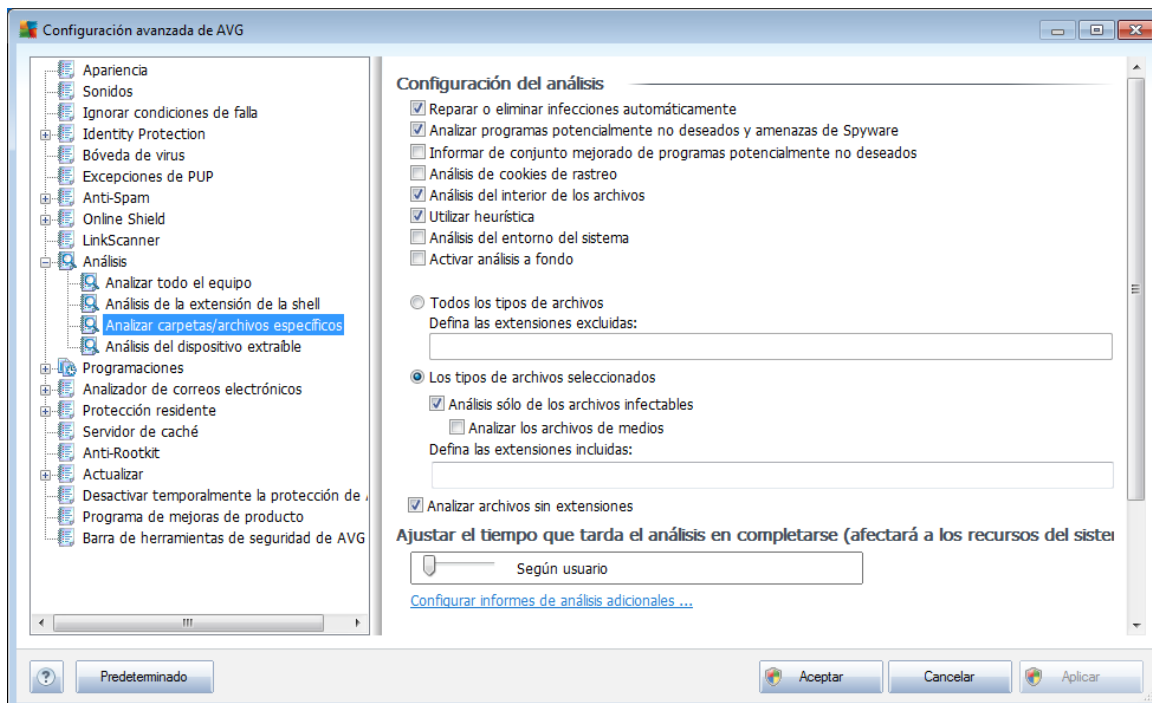
La lista de parámetros muestra parámetros idénticos a los que están disponibles en el [Análisis de todo el equipo](#). Sin embargo, la configuración predeterminada es diferente (por ejemplo, el [Análisis de todo el equipo](#) no comprueba de manera predeterminada los archivos, pero sí analiza el entorno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

**Nota:** Para obtener una descripción de los parámetros específicos, consulte el capítulo [Configuración avanzada de AVG/Análisis/Análisis de todo el equipo](#).

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

### 9.10.3. Análisis de carpetas o archivos específicos

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

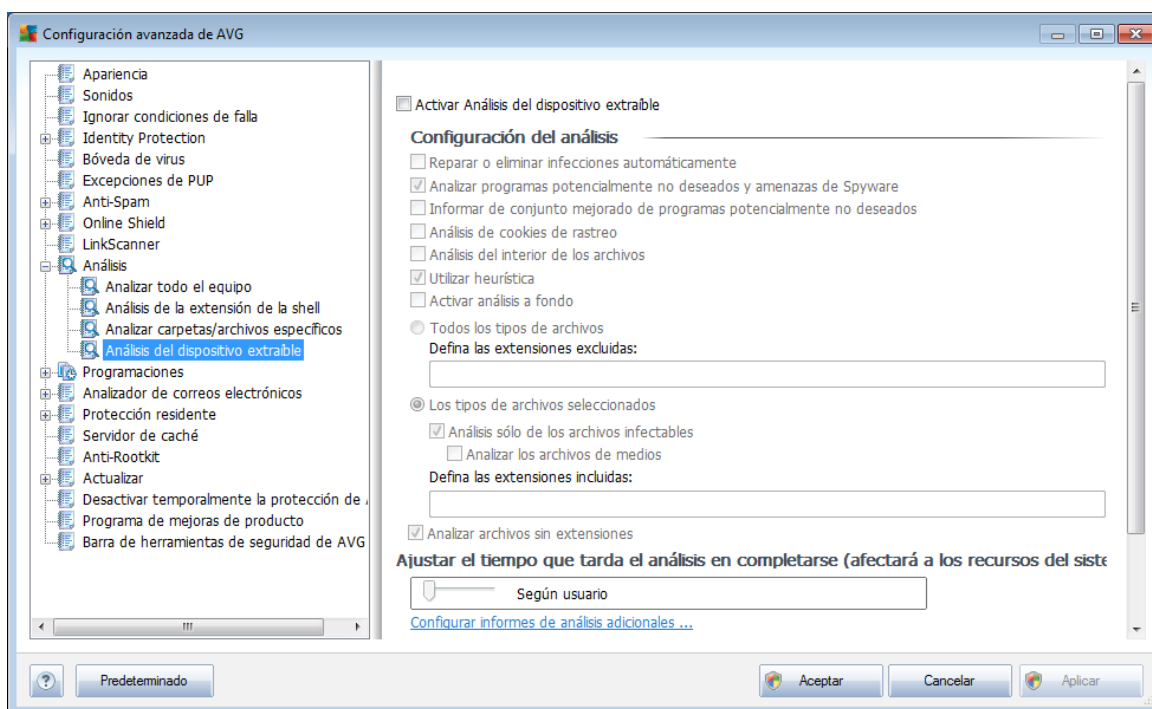


Todos los parámetros definidos en este cuadro de diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con **[Análisis de archivos o carpetas específicos](#)**.

**Nota:** Para obtener una descripción de los parámetros específicos, consulte el capítulo **[Configuración avanzada de AVG / Análisis / Análisis de todo el equipo](#)**.

#### 9.10.4. Análisis de dispositivos extraíbles

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



El **Análisis del dispositivo extraíble** se inicia automáticamente cada vez que conecta algún dispositivo extraíble a su equipo. De forma predeterminada, este análisis está desactivado. Sin embargo, es crucial analizar los dispositivos extraíbles en busca de amenazas potenciales, ya que éstos son una fuente importante de infección. Para tener este análisis listo y activarlo de forma automática cuando sea necesario, marque la opción **Activar análisis del dispositivo extraíble**.

**Nota:** Para obtener una descripción de los parámetros específicos, consulte el capítulo [Configuración avanzada de AVG / Análisis / Análisis de todo el equipo](#).

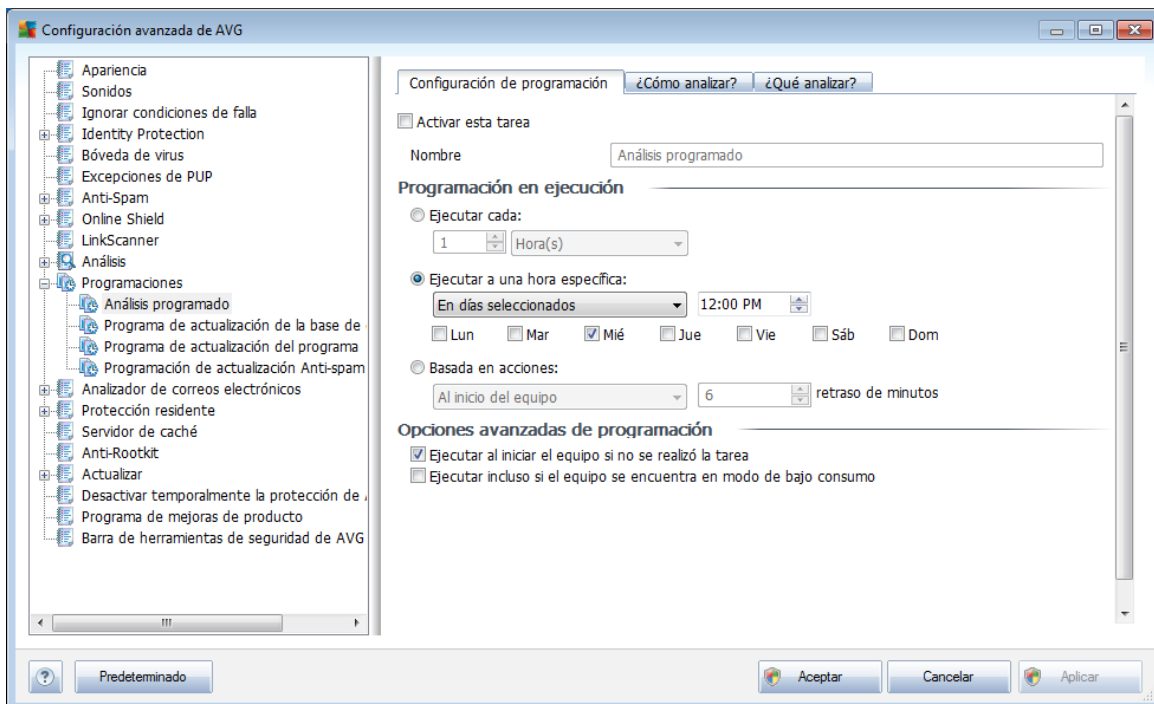
#### 9.11. Programaciones

En la sección **Programas** 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

Los parámetros del análisis programado se pueden editar (o se puede configurar una nueva programación) en tres pestañas:



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

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

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

En este cuadro de diálogo puede definir con más detalle los siguientes parámetros del



análisis:

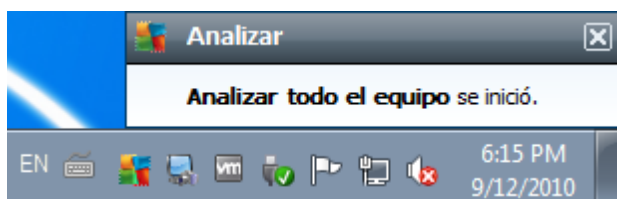
### Programación en ejecución

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

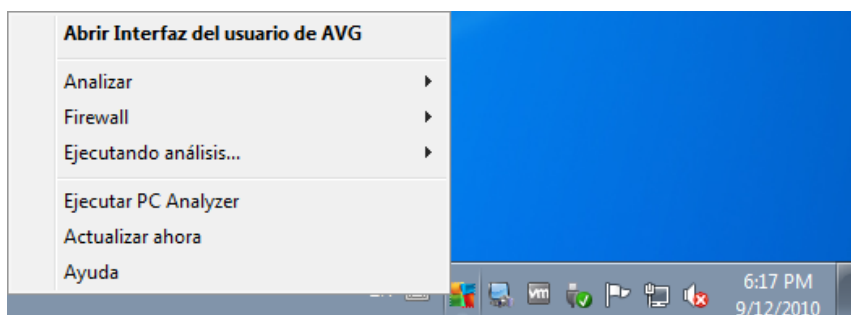
### Opciones avanzadas de programación

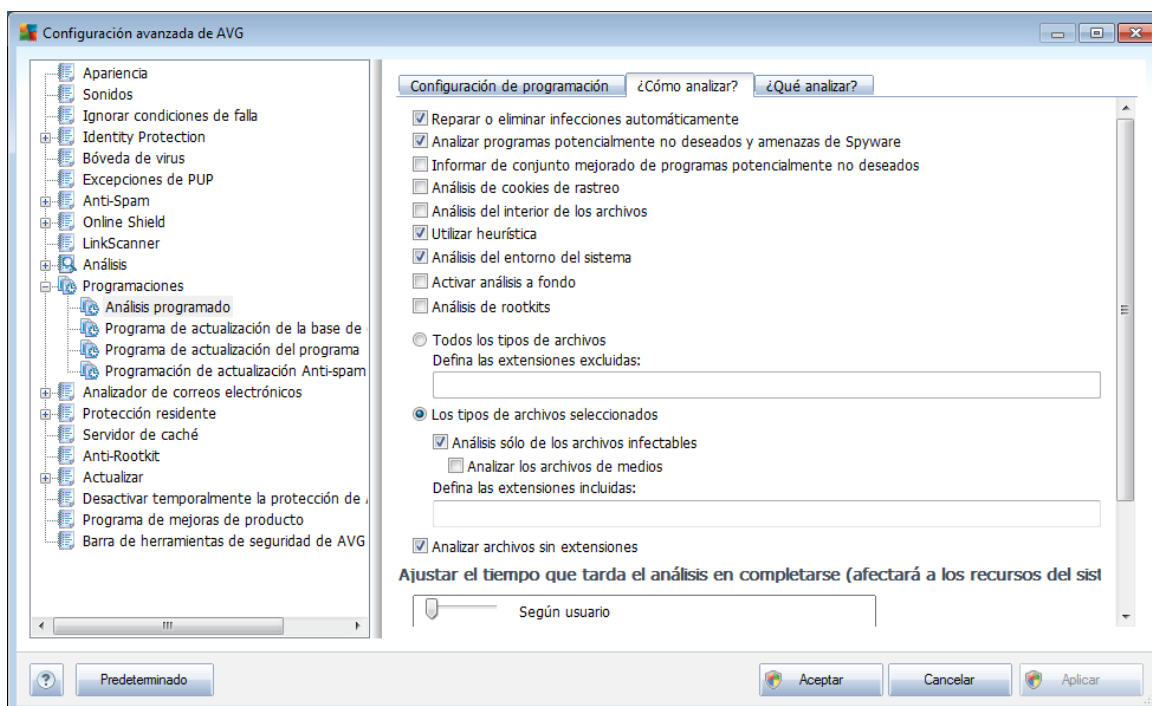
Esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

Una vez que se inicia el análisis programado en la hora que se especificó, se le informará de este hecho mediante una ventana emergente que se abre sobre el [icono en la bandeja de sistema AVG](#):



A continuación aparece un nuevo [icono de la bandeja del sistema AVG](#) (a todo color y brillante) informando de que se está ejecutando un análisis programado. Haga clic con el botón secundario en el icono de ejecución del análisis AVG para abrir un menú contextual donde puede decidir pausar o detener la ejecución del análisis, y también para cambiar la prioridad del análisis que se está ejecutando en ese momento:





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

- **Reparar o eliminar infecciones automáticamente** (activado de manera predeterminada): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si hay una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (seleccionada de modo predeterminado): seleccione la opción para activar el motor [Anti-Spyware](#) y analizar en busca de spyware así como de virus. [El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito.](#) Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar conjunto mejorado de programas potencialmente no deseados** (desactivada de forma predeterminada): seleccione esta opción para detectar un paquete extendido de [spyware](#), es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada





está desactivada.

- **Analizar cookies de rastreo** (*desactivado de forma predeterminada*): este parámetro del componente **Anti-Spyware** define que deben detectarse las cookies durante el análisis; (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica acerca de los usuarios, como los sitios que prefieren o los contenidos de sus carritos de compra electrónicos*)
- **Analizar el interior de los archivos** (*desactivado de manera predeterminada*): este parámetro define que el análisis debe comprobar todos los archivos, aún aquellos que se encuentran comprimidos dentro de algún tipo de archivo, por ejemplo ZIP, RAR, etc.
- **Utilizar heurística** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.
- **Analizar el entorno del sistema** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo;
- **Activar análisis a fondo** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Análisis de rootkits** (*desactivado de forma predeterminada*): seleccione este elemento si desea incluir la detección de rootkits en el análisis de todo el equipo. La detección de rootkits también está disponible de forma independiente en el componente **Anti-Rootkit**;

Después sería conveniente decidir si desea analizar

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



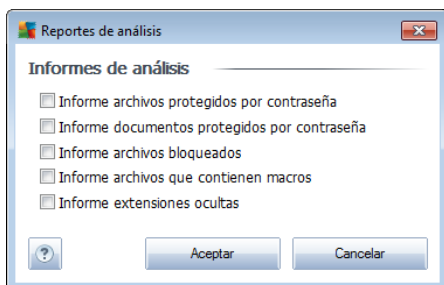
se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

### Ajustar el tiempo que tarda el análisis en completarse

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

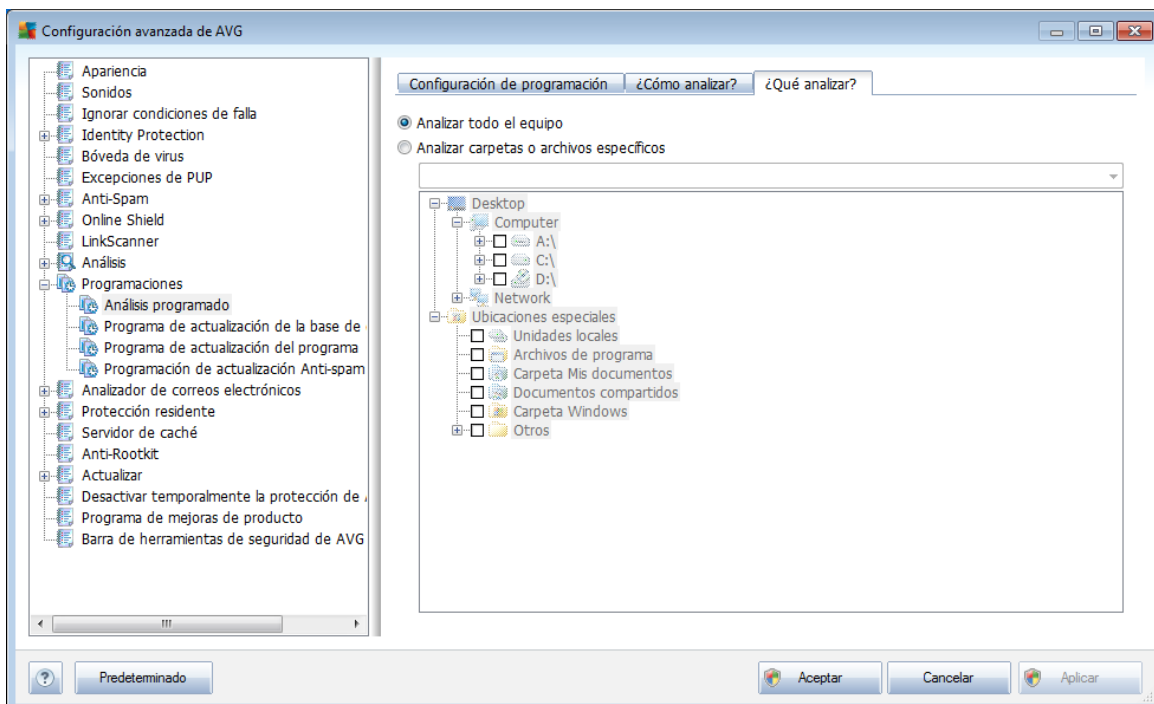
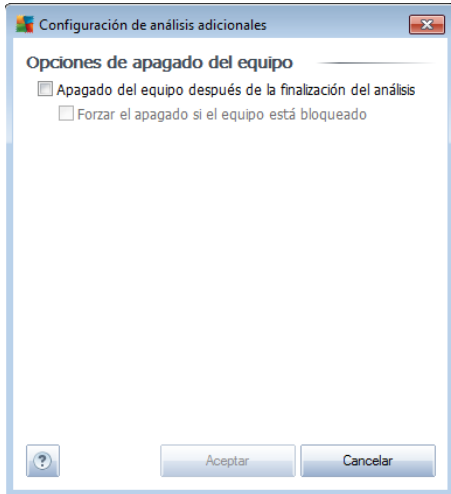
### Configurar informes de análisis adicionales

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



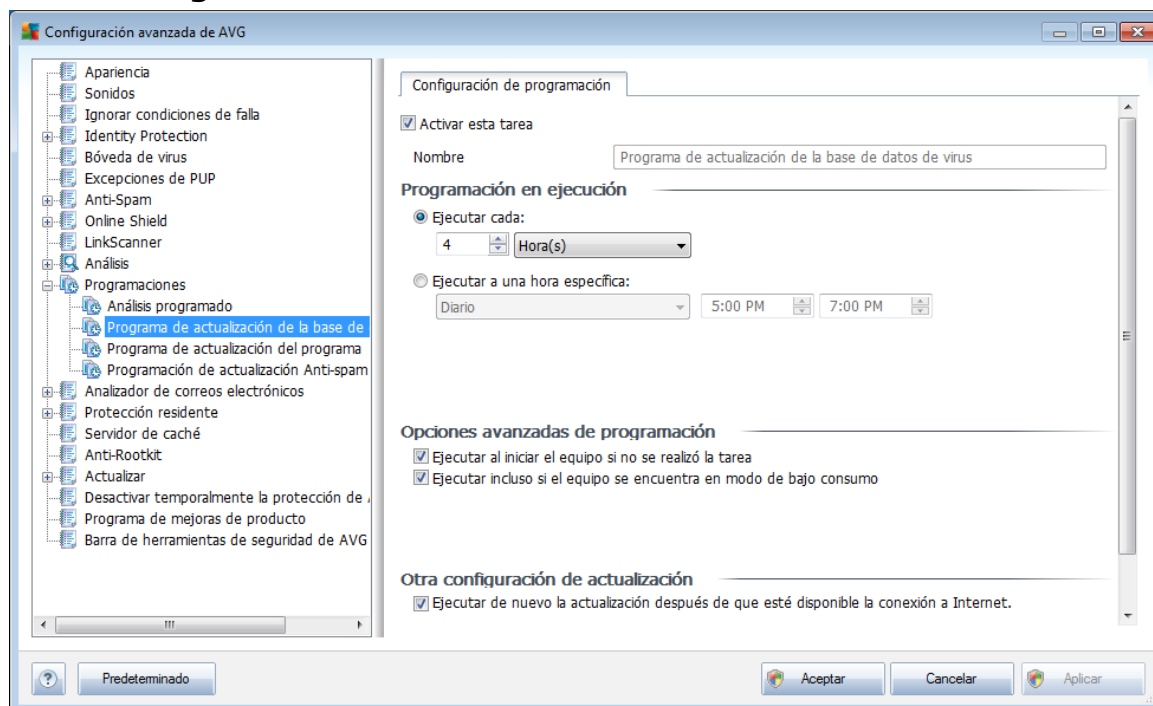
### Configuración de análisis adicionales

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



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

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



En la pestaña **Configuración de programación** puede seleccionar o cancelar la selección del elemento **Activar esta tarea** para desactivar la actualización de la base de datos de virus programada de forma temporal, y volverla a activar cuando sea necesario. La programación de actualización básica de la base de datos de virus se trata en el componente [Administrador de actualizaciones](#). En este diálogo puede configurar algunos parámetros detallados de la programación de actualización de la base de datos de virus. En el campo de texto denominado **Nombre** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

#### Programación en ejecución

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

#### Opciones avanzadas de programación

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

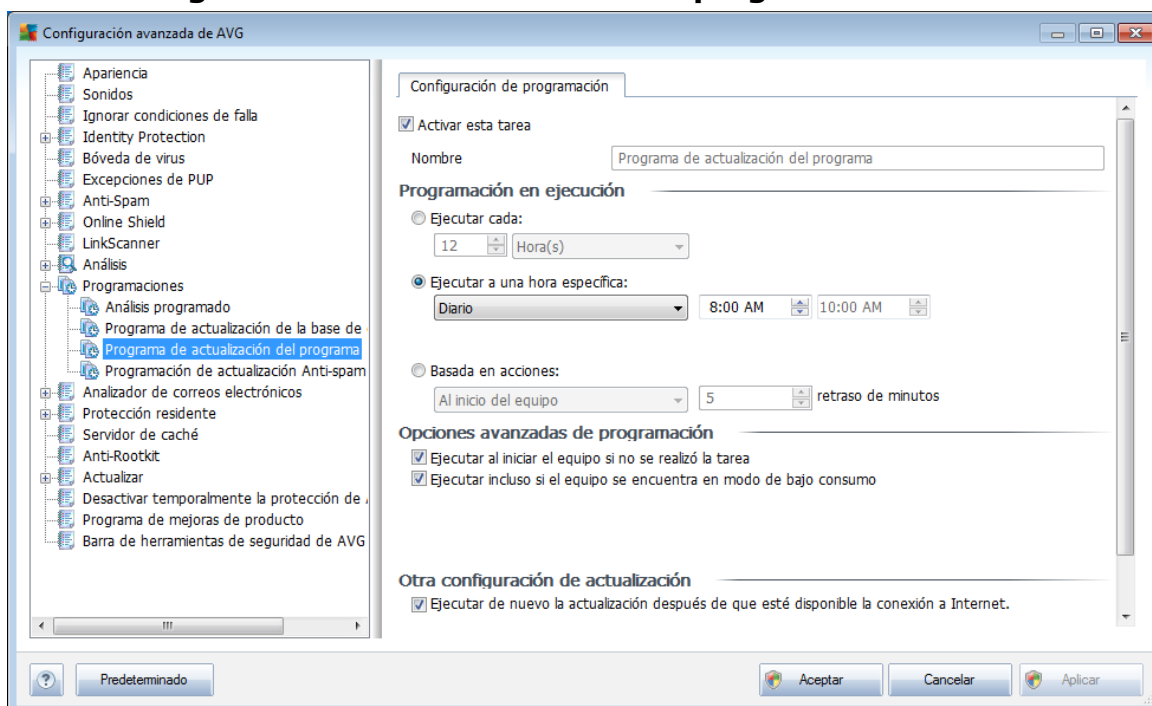


## Otra configuración de actualización

Finalmente, seleccione la opción **Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet** para asegurarse de que, en caso de que se interrumpa la conexión a Internet y se detenga el proceso de actualización, éste se vuelva a iniciar tan pronto se restablezca.

Una vez que se ejecuta la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el [icono de la bandeja del sistema AVG](#) (siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo [Configuración avanzada/Apariencia](#)).

### 9.11.3. Programación de actualización del programa



En la pestaña **Configuración de programación** puede seleccionar o cancelar la selección del elemento **Activar esta tarea** para desactivar la actualización programada de forma temporal, y volverla a activar cuando sea necesario. En el campo de texto denominado **Nombre** (desactivado para todas las programaciones predeterminadas) existe un nombre asignado a esta programación por el proveedor del programa.

## Programación en ejecución

Aquí, especifique los intervalos de tiempo para la ejecución de la actualización del programa recién programada. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto periodo de tiempo (**Ejecutar cada ...**), definiendo



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

### **Opciones avanzadas de programación**

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

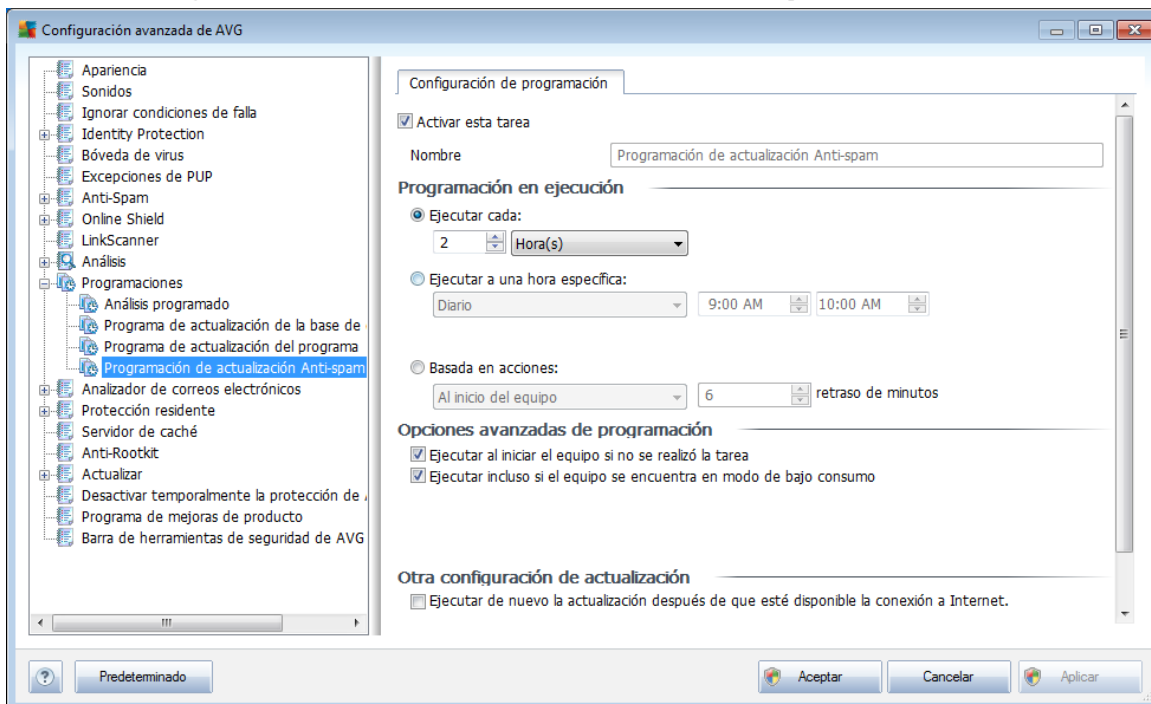
### **Otra configuración de actualización**

Seleccione la opción ***Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet*** para asegurarse de que en caso de interrupción del proceso de actualización debido a una falla en la conexión a Internet, el proceso se reinicie inmediatamente después de recuperarla.

Una vez que se ejecuta la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el [icono de la bandeja del sistema AVG](#) (siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo [Configuración avanzada/Apariencia](#)).

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

#### 9.11.4. Programación de actualización de Anti-Spam



En la pestaña **Configuración de programación** puede seleccionar o cancelar la selección del elemento **Activar esta tarea** simplemente para desactivar temporalmente la actualización programada del **Anti-Spam** y volver a activarla cuando sea necesario. La programación de actualización básica del **Anti-Spam** está formado por el componente **Administrador de actualizaciones**. En este diálogo puede configurar algunos parámetros detallados de la programación de actualización. En el campo de texto denominado **Nombre** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

#### Programación en ejecución

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

#### Opciones avanzadas de programación

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



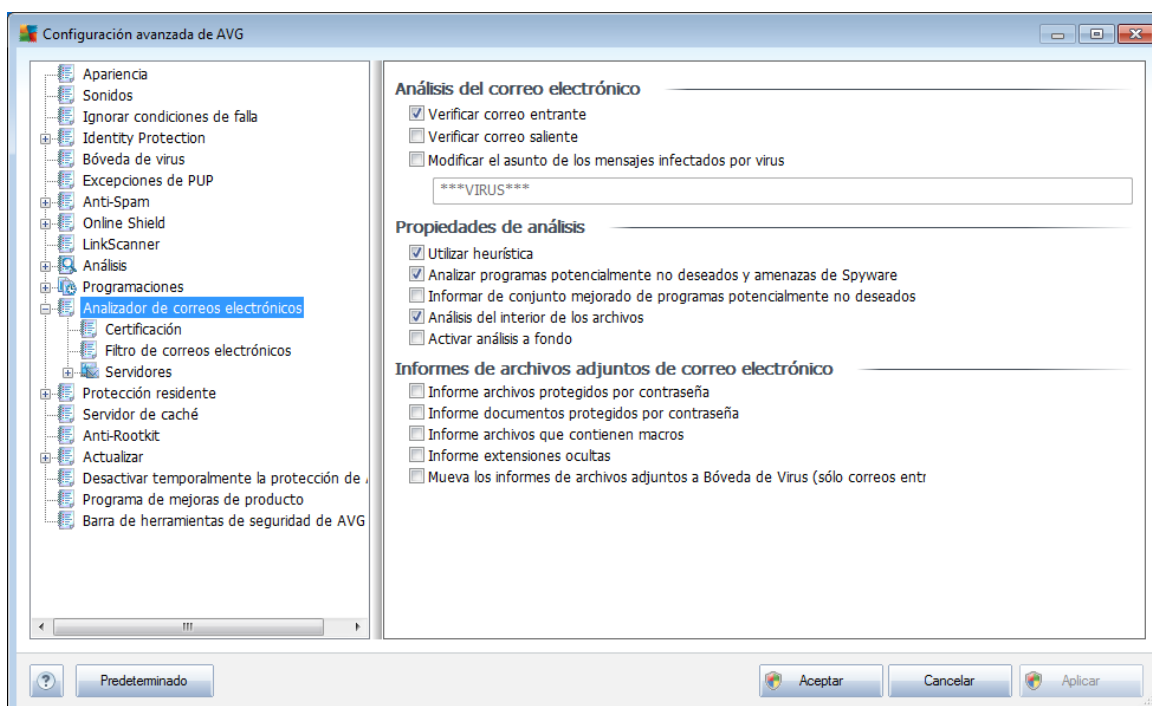
## Otra configuración de actualización

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

Una vez que se inicia el análisis programado en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el [icono de la bandeja del sistema AVG](#) (siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo [Configuración avanzada/Apariencia](#)).

## 9.12. Analizador de correos electrónicos

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



### Análisis del correo electrónico

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

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





esta opción para activar o desactivar la opción de analizar todos los correos electrónicos enviados desde su cuenta

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

### Propiedades de análisis

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

- **Utilizar heurística** (*activada de forma predeterminada*): seleccione esta opción para utilizar el [método de detección heurístico](#) al analizar mensajes de correo electrónico. Cuando esta opción está activada, no sólo se pueden filtrar los archivos adjuntos de correo electrónico por extensión sino que también se considerará el contenido real del archivo adjunto. El filtro se puede establecer en el cuadro de diálogo [Filtros de correos electrónicos](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (*activada de forma predeterminada*): seleccione esta opción para activar el motor [Anti-Spyware](#) y analizar en busca de spyware así como de virus. [El spyware](#) representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar conjunto mejorado de programas potencialmente no deseados** (*desactivada de forma predeterminada*): seleccione esta opción para detectar un paquete extendido de [spyware](#), es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Analizar el interior de los archivos** (*activada de forma predeterminada*): seleccione esta opción para analizar el contenido de los archivos adjuntos a los mensajes de correo electrónico.
- **Activar análisis a fondo** (*desactivada de forma predeterminada*): en determinadas situaciones (*por ejemplo, sospechas de que el equipo está infectado por un virus o una vulnerabilidad*), puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.



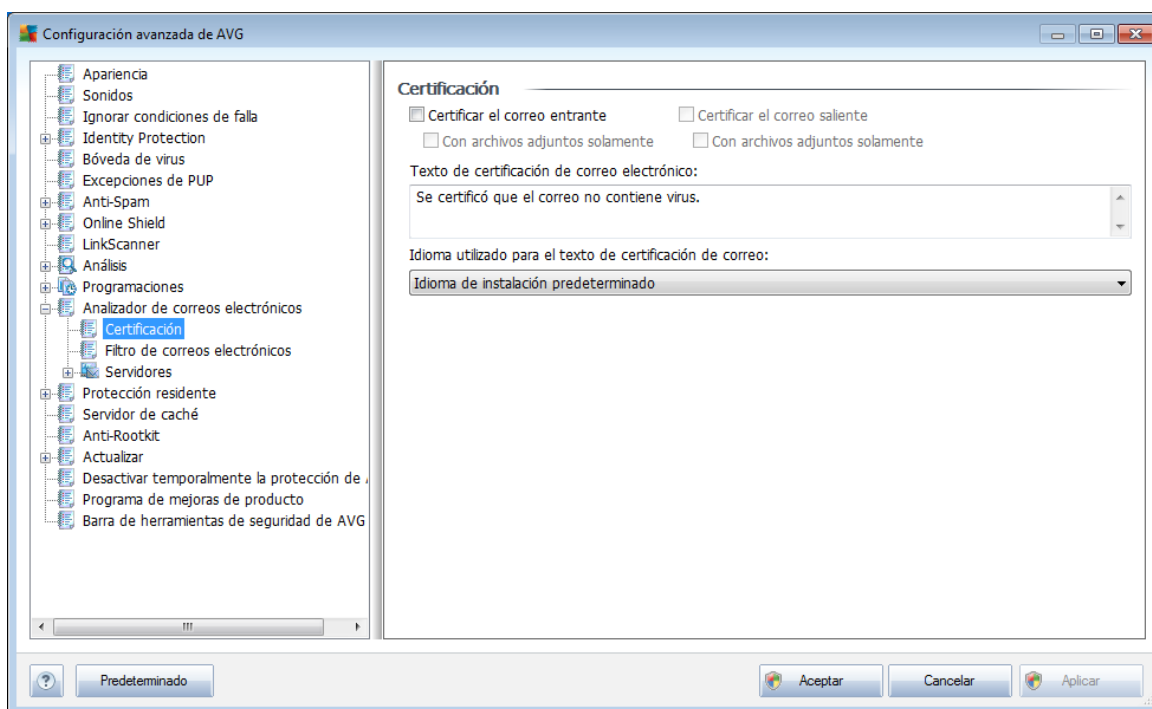
## Informes de archivos adjuntos de correo electrónico

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

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

### 9.12.1. Certificación

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



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

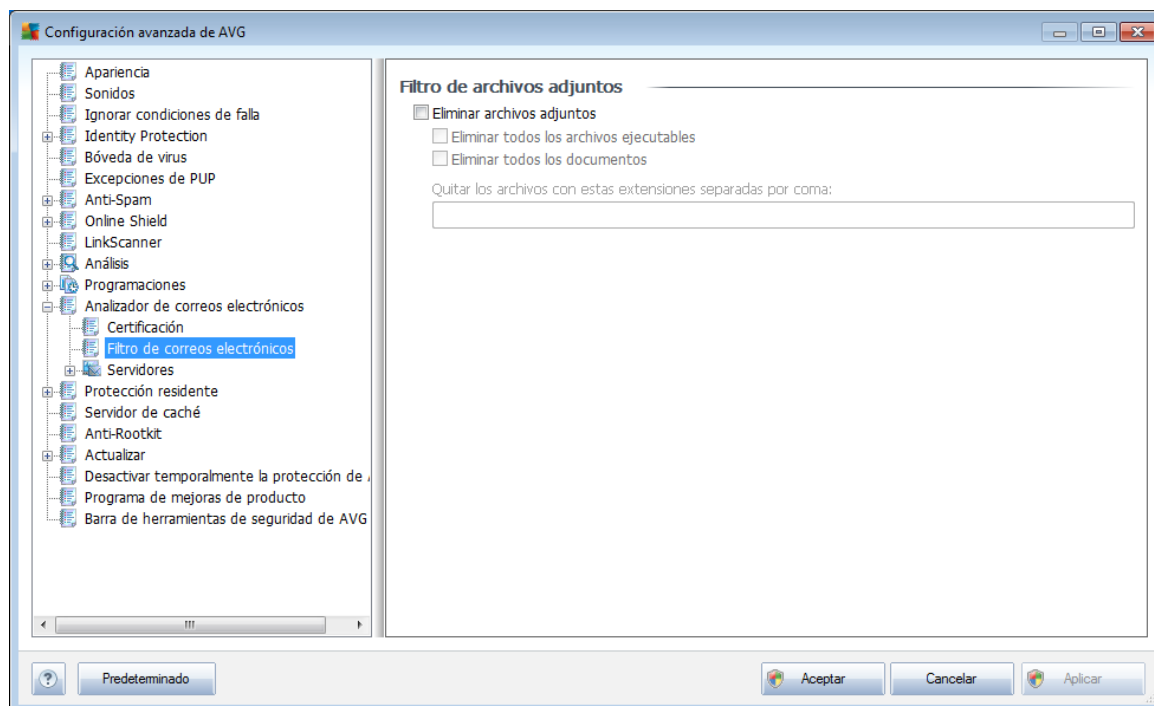
*Se certificó que el correo no contiene virus.*

*Analizado por AVG.*

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

Si decide utilizar la certificación de los mensajes de correo electrónico entrantes o salientes, en este cuadro de diálogo también puede especificar el texto exacto de la parte del usuario del texto de la certificación (**Texto de certificación de correo electrónico**) y elegir qué idioma debe utilizarse para la parte del sistema generada automáticamente (**Idioma utilizado para el texto de certificación de correo**).

### 9.12.2. Filtros de correos electrónicos

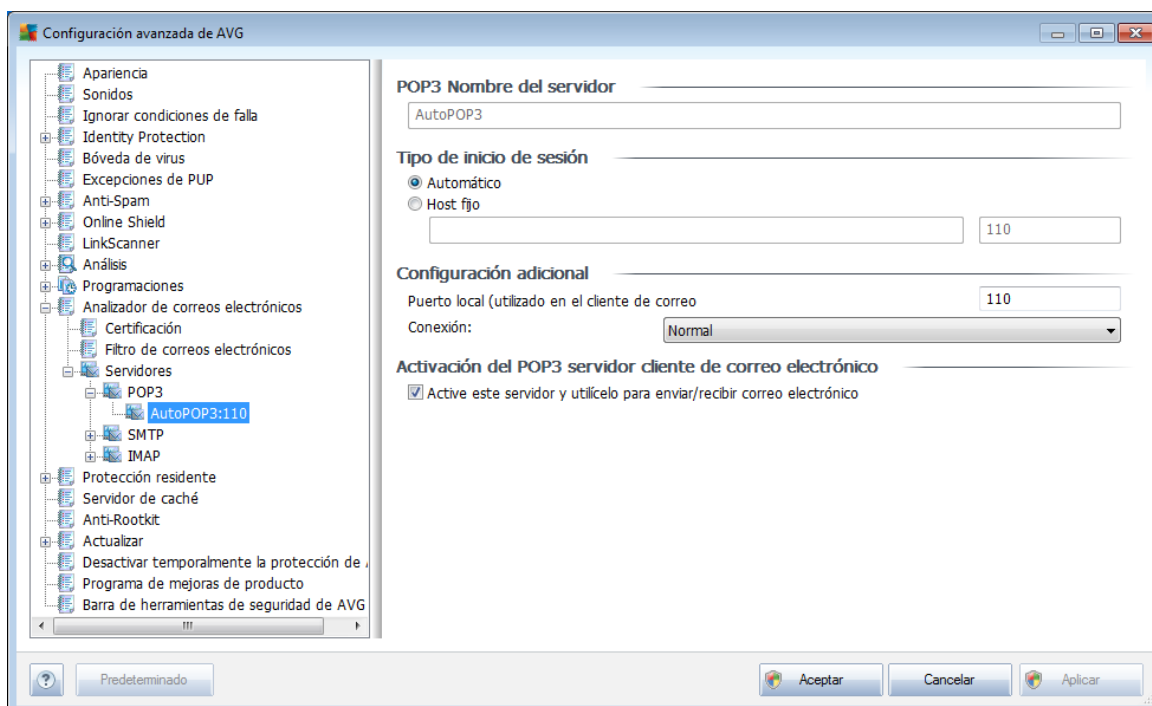


El cuadro de diálogo **Filtro de archivos adjuntos** le permite establecer los parámetros para el análisis de los archivos adjuntos de los mensajes de correo electrónico. De manera predeterminada, la opción **Quitar archivos adjuntos** está desactivada. Si decide activarla, todos los archivos adjuntos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

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

### 9.12.3. Servidores

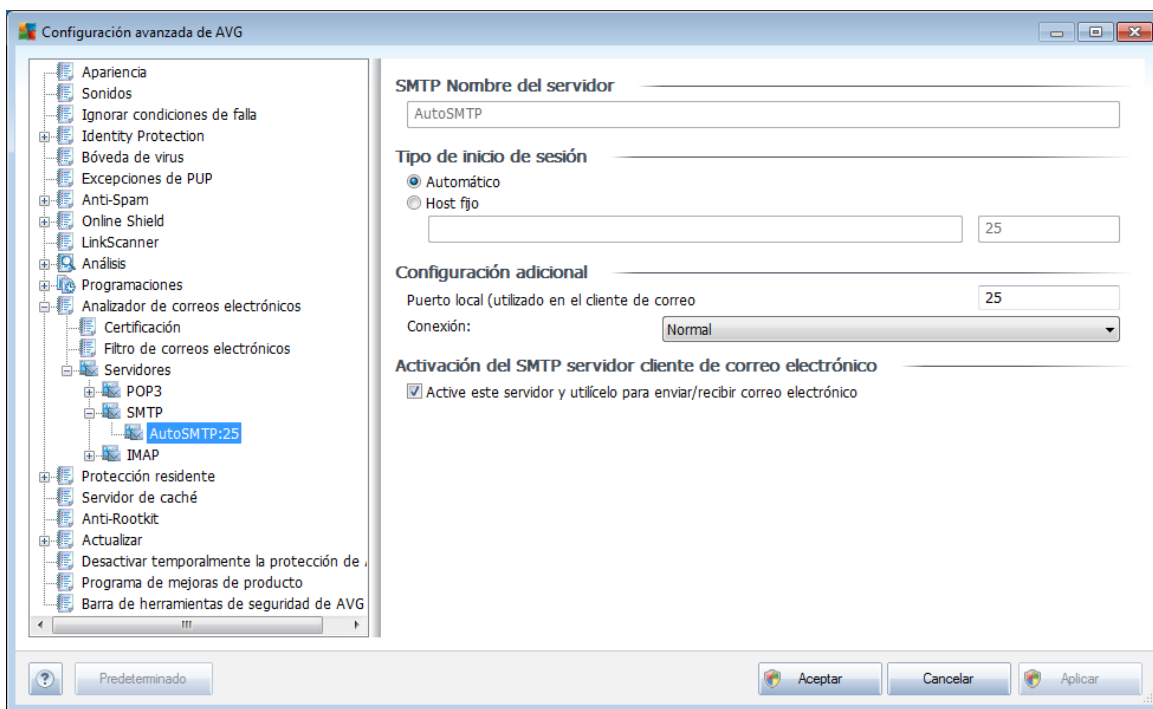
En la sección **Servidores** puede editar los parámetros de los servidores del componente **Analizador de correos electrónicos**, o establecer algún servidor nuevo utilizando el botón **Agregar nuevo servidor**.



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

- **Nombre del servidor POP3:** en este campo podrá especificar el nombre de los servidores nuevos (*para agregar un servidor POP3, haga clic con el botón secundario del mouse en el elemento POP3 del menú de navegación de la izquierda*). Para el servidor "AutoPOP3" creado automáticamente, este campo está desactivado.
- **Tipo de inicio de sesión:** define el método para determinar el servidor de correo empleado para el correo entrante:
  - **Automático:** el inicio de sesión se realizará de manera automática, de acuerdo con la configuración del cliente de correo electrónico.
  - **Host fijo:** en este caso, el programa siempre utilizará el servidor especificado aquí. Especifique la dirección o el nombre de su servidor de correo. El nombre de inicio de sesión permanece sin cambiar. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, pop.acme.com*), así como una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (*por ejemplo, pop.acme.com:8200*). El puerto estándar para comunicaciones POP3 es 143.
- **Configuración adicional:** especifica los parámetros con más detalle:

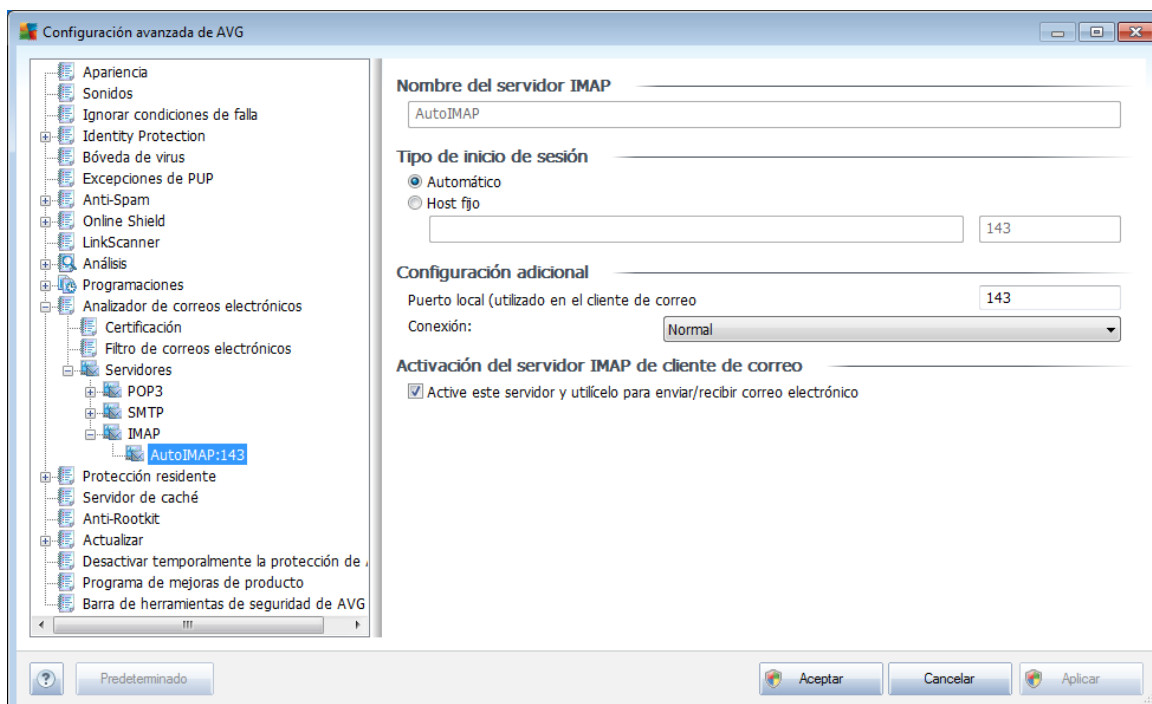
- **Puerto local:** especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Luego debe especificar en su aplicación de correo este puerto como el puerto para comunicaciones POP3.
- **Conexión:** en el menú desplegable, puede especificar la clase de conexión que desea utilizar (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.
- **Activación del servidor de cliente POP3 de correo electrónico:** seleccione o quite la marca de selección de este elemento para activar o desactivar el servidor POP3 especificado



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

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

- **Automático:** el inicio de sesión se efectuará automáticamente, según la configuración del cliente de correo electrónico.
- **Host fijo:** en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (por ejemplo, *smtp.acme.com*), así como una dirección IP (por ejemplo, *123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (por ejemplo, *smtp.acme.com:8200*). El puerto estándar para comunicaciones SMTP es el 25.
- **Configuración adicional:** especifica los parámetros con mayor detalle:
  - **Puerto local:** especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Posteriormente deberá especificar en su aplicación de correo este puerto como puerto para la comunicación SMTP.
  - **Conexión:** en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.
- **Activación del servidor SMTP en el cliente de correo electrónico:** seleccione o quite la marca de selección de este elemento para activar o desactivar el servidor SMTP especificado anteriormente





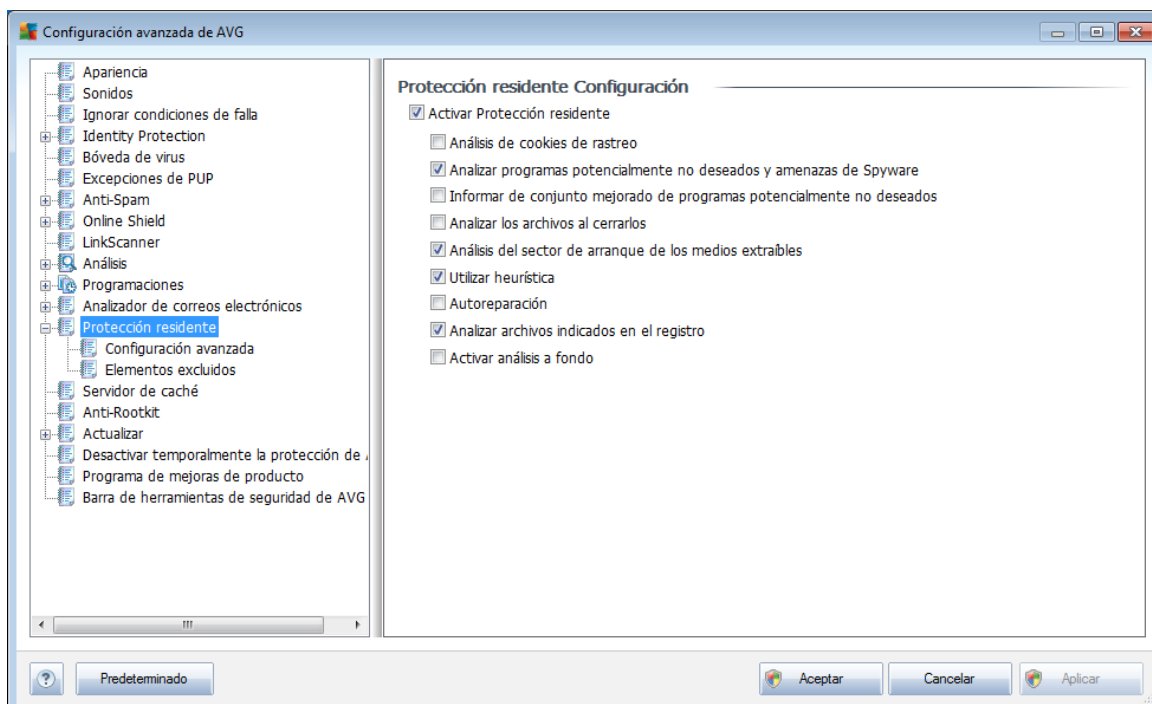
En este cuadro de diálogo (al que se obtiene acceso mediante **Servidores/IMAP**) puede configurar un nuevo servidor para el **Analizador de correos electrónicos** utilizando el protocolo IMAP para el correo saliente:

- **Nombre del servidor IMAP:** en este campo podrá especificar el nombre de los servidores recién agregados (*para agregar un servidor IMAP, haga clic con el botón secundario del mouse en el elemento IMAP del menú de navegación de la izquierda*). Para el servidor "AutoIMAP" creado automáticamente, este campo está desactivado.
- **Tipo de inicio de sesión:** define el método para determinar el servidor de correo empleado para el correo saliente:
  - **Automático:** el inicio de sesión se efectuará automáticamente, según la configuración del cliente de correo electrónico.
  - **Host fijo:** en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, smtp.acme.com*), así como una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (*por ejemplo, imap.acme.com:8200*). El puerto estándar para comunicaciones SMTP es el 25.
- **Configuración adicional:** especifica los parámetros con más detalle:
  - **Puerto local:** especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Posteriormente deberá especificar en su aplicación de correo este puerto como puerto para la comunicación IMAP.
  - **Conexión:** en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.
- **Activación del servidor IMAP en el cliente de correo electrónico:** seleccione o quite la marca de esta casilla para activar o desactivar el servidor SMTP especificado anteriormente



### 9.13. Protección residente

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



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

- **Analizar cookies de rastreo** (desactivado de manera predeterminada): este parámetro define que se deben detectar las cookies durante el análisis. (las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico.)
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (seleccionada de modo predeterminado): seleccione la opción para activar el motor **Anti-Spyware** y analizar en busca de spyware así como de virus. El **spyware** representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar conjunto mejorado de programas potencialmente no deseados** (desactivado de manera predeterminada): seleccione esta opción para

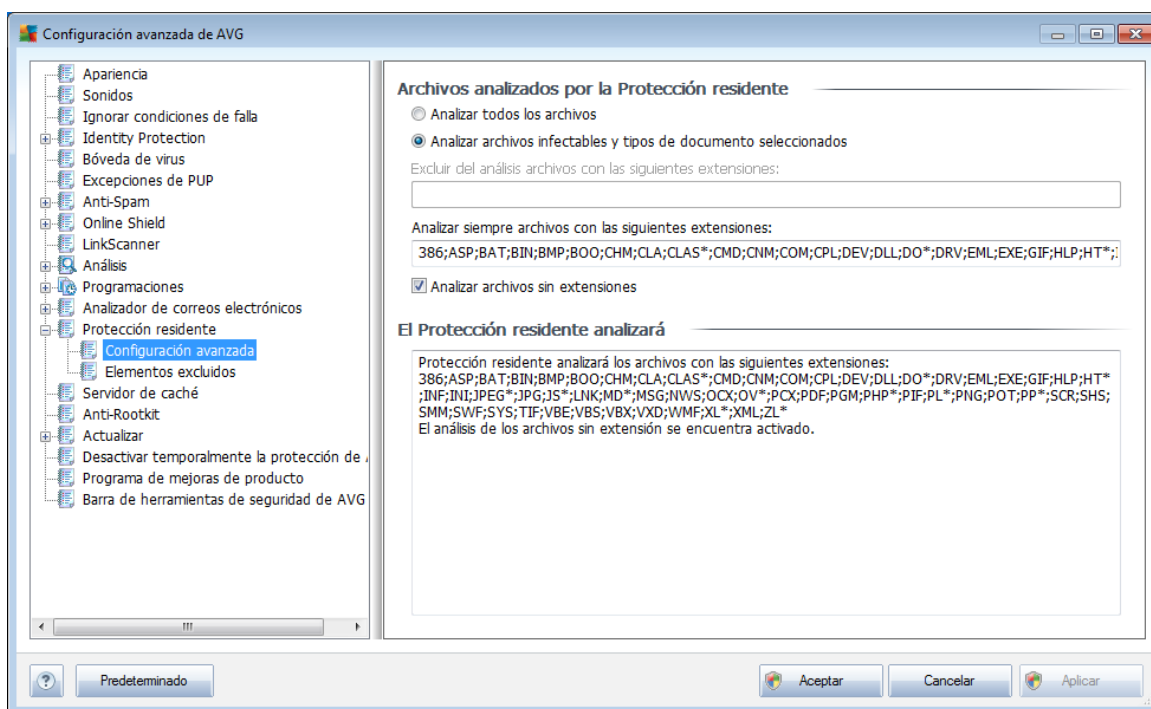


detectar un paquete extendido de [spyware](#), es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo,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

- **Analizar los archivos al cerrarlos** (*desactivado de manera predeterminada*): el análisis al cerrar garantiza que el programa AVG analiza los objetos activos (aplicaciones, documentos, etc.) cuando se abren y también cuando se cierran; esta función contribuye a proteger el equipo frente a algunos tipos de virus sofisticados.
- **Analizar sectores de arranque de los medios extraíbles** (*activado de manera predeterminada*)
- **Utilizar heurística:** (*activado de manera predeterminada*) se utilizará el [análisis heurístico](#) para la detección (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).
- **Autoreparar** (*desactivado de manera predeterminada*): todas las infecciones que se detecten se repararán automáticamente si es posible, y todas las infecciones que no se puedan reparar se eliminarán.
- **Analizar archivos indicados en el registro** (*activado de manera predeterminada*): este parámetro define que AVG analizará todos los archivos ejecutables añadidos al registro de inicio para evitar que una infección conocida se ejecute durante el siguiente inicio del equipo.
- **Activar análisis a fondo** (*desactivado de manera predeterminada*) : en determinadas situaciones (*en un estado de extrema emergencia*) puede marcar esta opción para activar los algoritmos más minuciosos, que comprobarán a fondo todos los objetos remotamente amenazantes. Pero recuerde que este método consume mucho tiempo.

### 9.13.1. Configuración avanzada

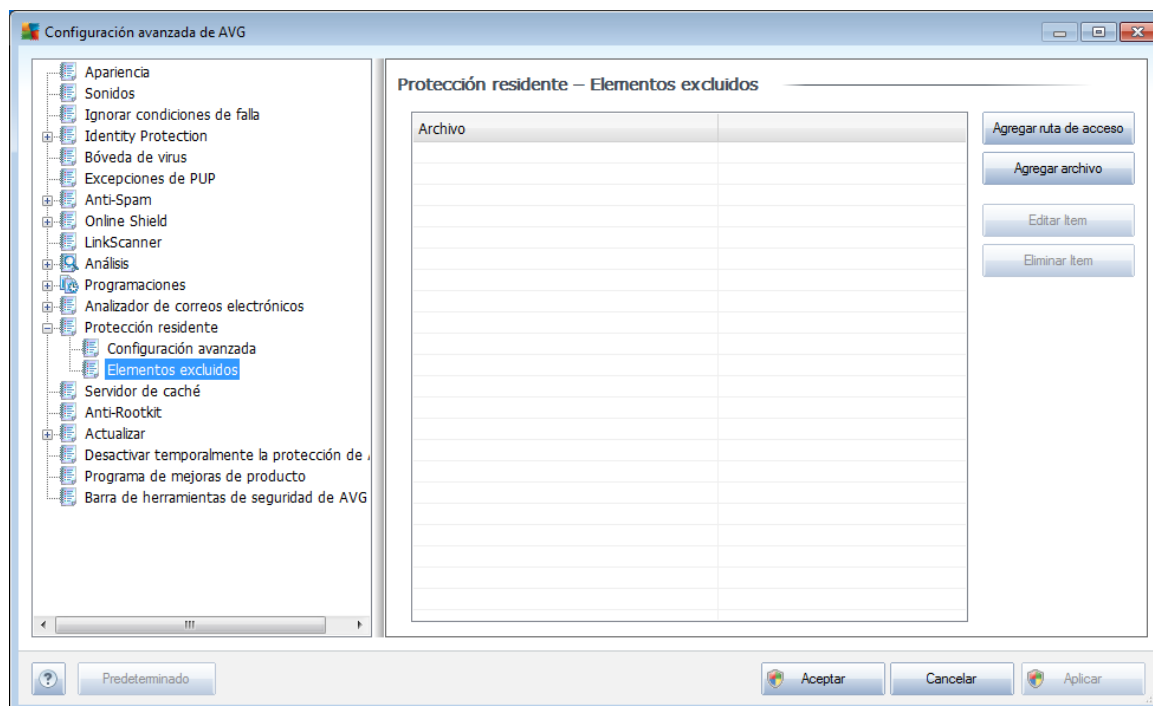
En el cuadro de diálogo **Archivos analizados por la Protección residente** es posible configurar qué archivos se van a analizar (*por medio de las extensiones específicas*):



Decida si desea que se analicen todos los archivos o sólo los archivos infectables; si escoge esta última opción, puede especificar una lista con las extensiones que definan los archivos que se deben excluir del análisis, así como una lista de las extensiones de los archivos que se deben analizar siempre.

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

### 9.13.2. Elementos excluidos



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

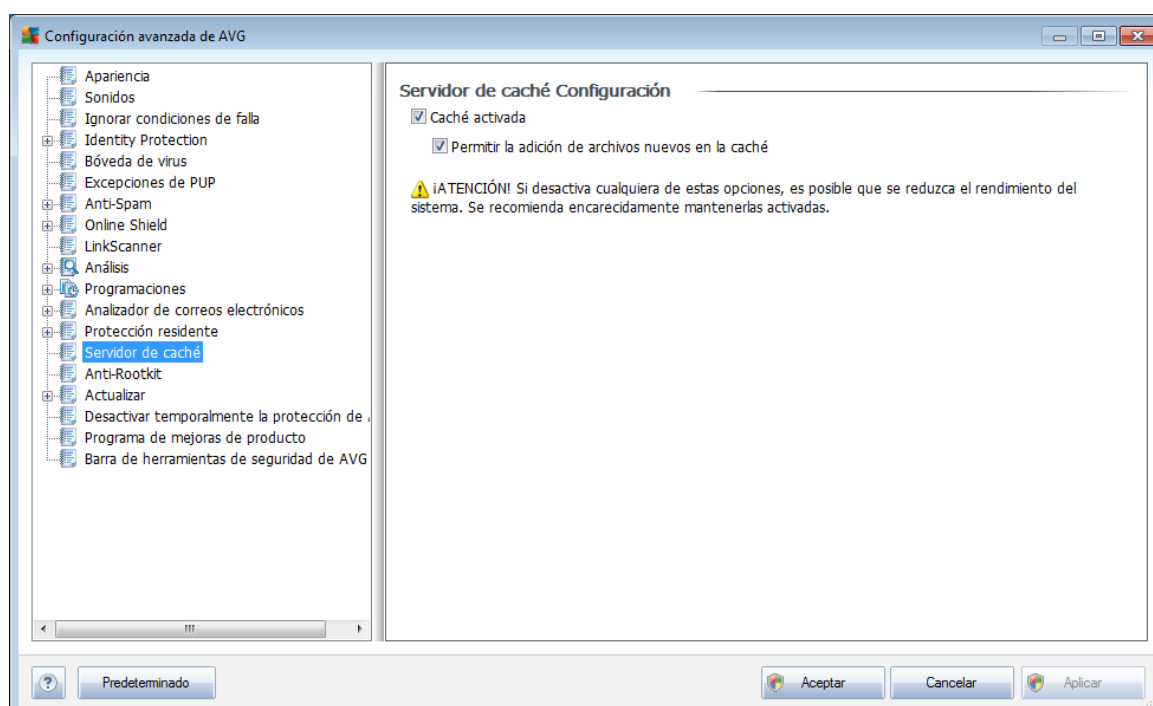
**Si no es absolutamente necesario, le recomendamos no excluir ningún elemento.**

El cuadro de diálogo proporciona los siguientes botones de control:

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

## 9.14. Servidor de caché

El **Servidor de caché** es un proceso diseñado para acelerar cualquier análisis (*análisis a pedido, análisis programado de todo el equipo, análisis de [Protección residente](#)*). Reúne y mantiene información de los archivos confiables (*archivos de sistema con firma digital, etc.*): estos archivos se consideran seguros y se omiten durante el análisis.

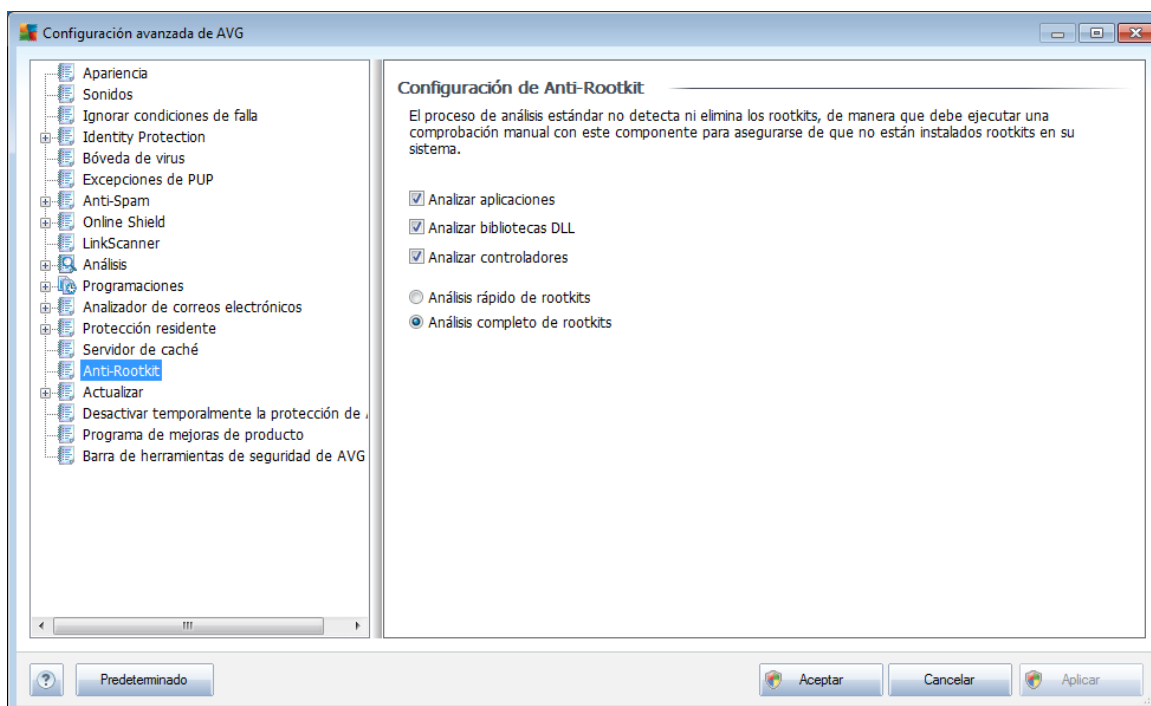


El cuadro de diálogo de configuración presenta dos opciones:

- **Caché activada** (*activada de forma predeterminada*): quite la marca de la casilla para desactivar el **Servidor de caché** y vacíe la memoria caché. Tenga en cuenta que el análisis puede ralentizar y reducir el rendimiento general de su equipo, porque primero se analizarán todos y cada uno de los archivos en uso en busca de virus y spyware.
- **Permitir la adición de archivos nuevos en la caché** (*activada de forma predeterminada*): quite la marca de la casilla para dejar de agregar archivos en la memoria caché. Se guardarán y usarán todos los archivos ya almacenados en caché hasta que el almacenamiento en caché se desactive completamente o hasta la siguiente actualización de la base de datos de virus.

## 9.15. Anti-Rootkit

En este diálogo puede editar la configuración del componente [Anti-Rootkit](#):



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

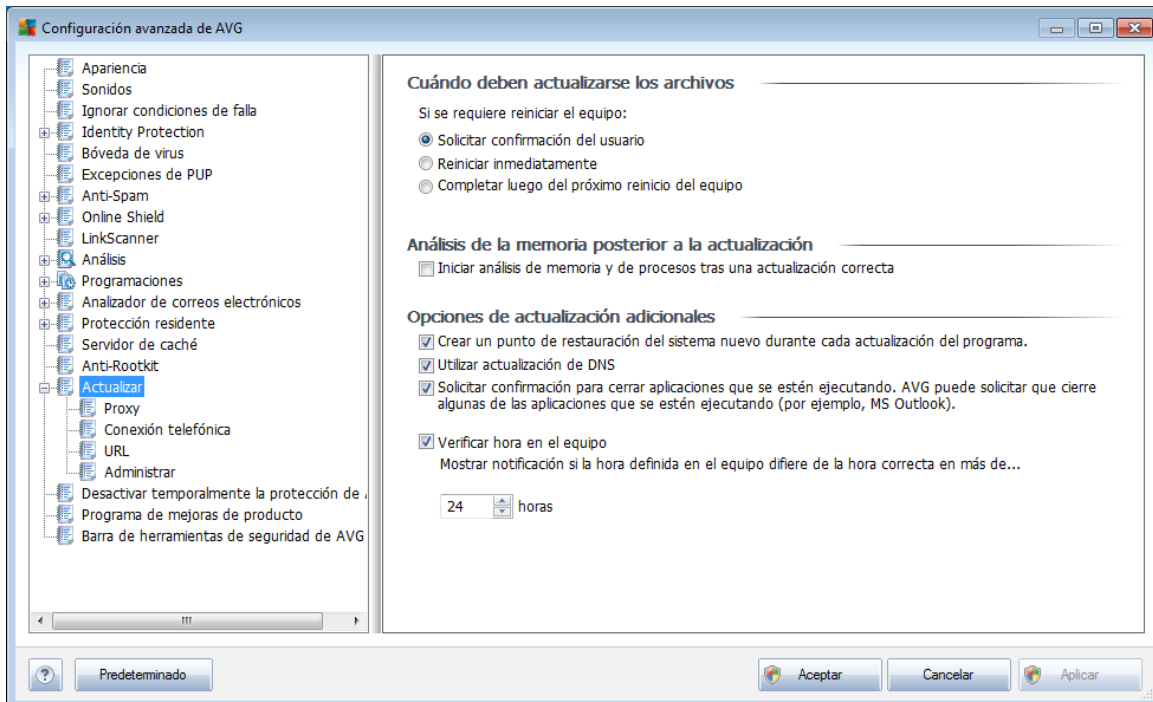
Marque las casillas de verificación respectivas para especificar los objetos que deben analizarse:

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

También puede seleccionar el modo de análisis de rootkits:

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

## 9.16. Actualización



El elemento de navegación **Actualizar** abre un nuevo cuadro de diálogo en el que puede especificar los parámetros generales relacionados con la [actualización de AVG](#):

### Cuándo deben actualizarse los archivos

En esta sección, puede seleccionar entre dos opciones alternativas: [actualización](#), que se puede programar para el siguiente reinicio del equipo o puede ejecutar la [actualización](#) inmediatamente. De manera predeterminada, está seleccionada la opción de actualización inmediata, dado que de esta forma AVG puede garantizar el máximo nivel de seguridad. La programación de una actualización para el siguiente reinicio del equipo sólo se puede recomendar si está seguro de que el equipo se reiniciará regularmente (al menos diariamente).

Si decide mantener la configuración predeterminada y ejecuta el proceso de actualización inmediatamente, puede especificar las circunstancias bajo las cuales se debe llevar a cabo un posible reinicio requerido:

- **Solicitar confirmación del usuario:** se le pedirá que apruebe un reinicio del equipo, necesario para finalizar el [proceso de actualización](#)
- **Reiniciar inmediatamente:** el equipo se reiniciará inmediatamente de forma automática después de que el [proceso de actualización](#) haya finalizado, no será necesaria la aprobación del usuario.
- **Completar luego del próximo reinicio del equipo :** la finalización del [proceso](#)



[de actualización](#) se pospondrá hasta el siguiente reinicio del equipo. Nuevamente, tenga en cuenta que esta opción sólo se recomienda si puede estar seguro de que el equipo se reinicia regularmente (al menos diariamente).

### **Análisis de la memoria posterior a la actualización**

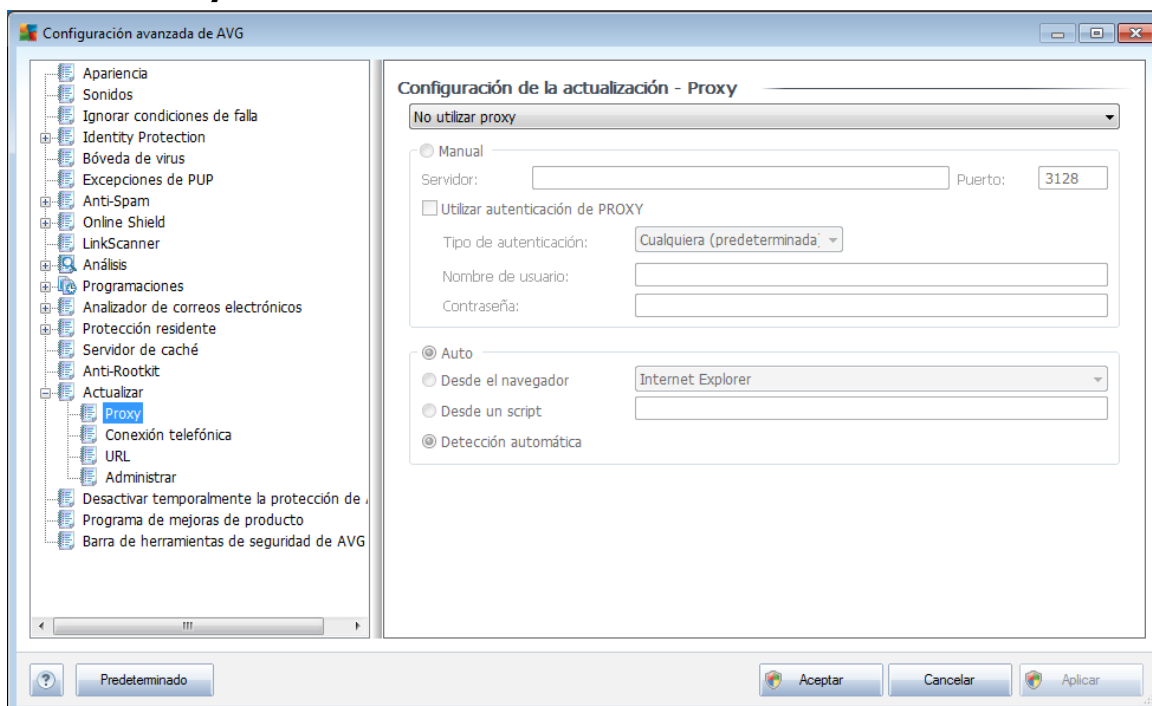
Seleccione esta casilla de verificación para especificar que desea ejecutar un nuevo análisis de la memoria después de cada actualización completada correctamente. La última actualización descargada podría contener definiciones de virus nuevas, y éstas podrían aplicarse en el análisis de forma inmediata.

### **Opciones de actualización adicionales**

- **Crear un nuevo punto de restauración del equipo durante cada actualización del programa:** antes de iniciar cada actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Se puede obtener acceso a esta opción mediante Inicio/Todos los programas/Accesorios/Herramientas del sistema/Restaurar sistema, pero se recomienda que sólo los usuarios experimentados realicen cambios. Mantenga esta casilla seleccionada si desea hacer uso de esta funcionalidad.
- **Utilizar actualización de DNS:** marque esta casilla para confirmar que desea utilizar el método de detección de los archivos de actualización que elimina la cantidad de datos transferidos entre el servidor de actualización y el cliente AVG;
- **Solicitar confirmación para cerrar aplicaciones que se estén ejecutando (activado de forma predeterminada):** con este elemento tendrá la seguridad de que ninguna aplicación actualmente en ejecución se cerrará sin su permiso, si esto se requiere para que el proceso de actualización finalice;
- **Verificar hora del equipo:** marque esta opción para declarar que desea recibir una notificación en caso de que la hora del equipo difiera por más horas de las especificadas de la hora correcta.



### 9.16.1. Proxy



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

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

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

#### Configuración manual

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

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



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

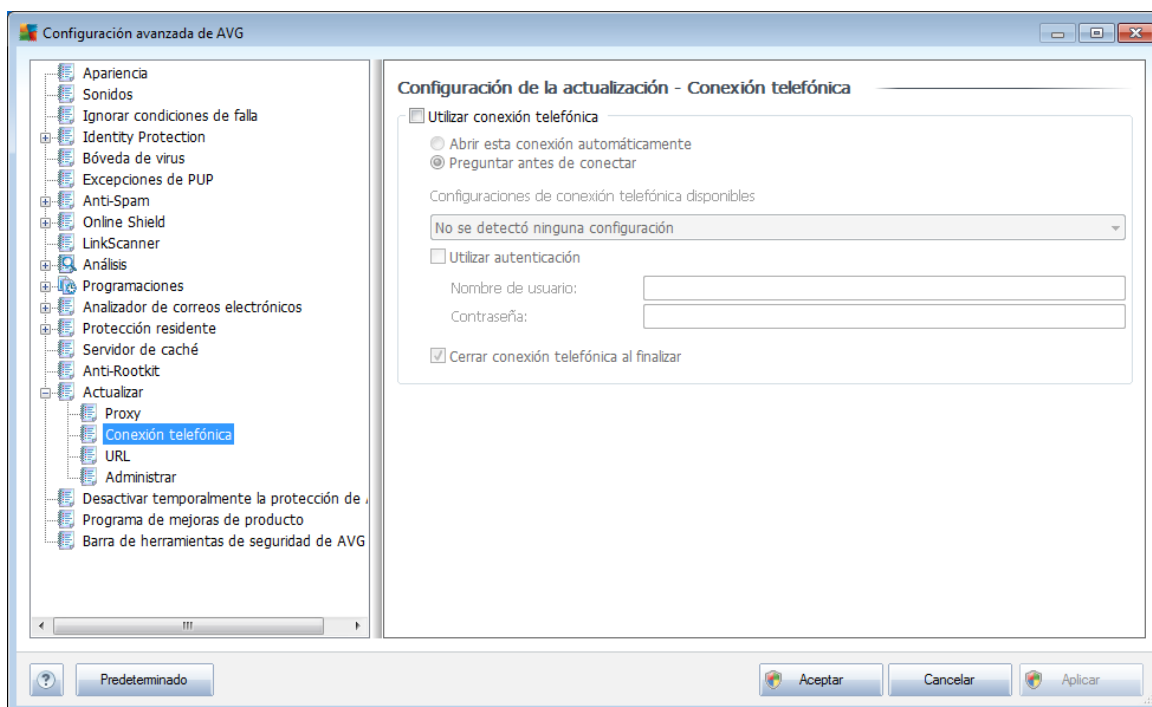
El servidor proxy también puede tener reglas específicas configuradas para cada usuario. Si el servidor proxy está configurado de este modo, seleccione la opción **Utilizar autenticación de PROXY** para verificar que el nombre de usuario y la contraseña sean válidos para la conexión a Internet mediante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

### Configuración automática

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

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

### 9.16.2. Conexión telefónica

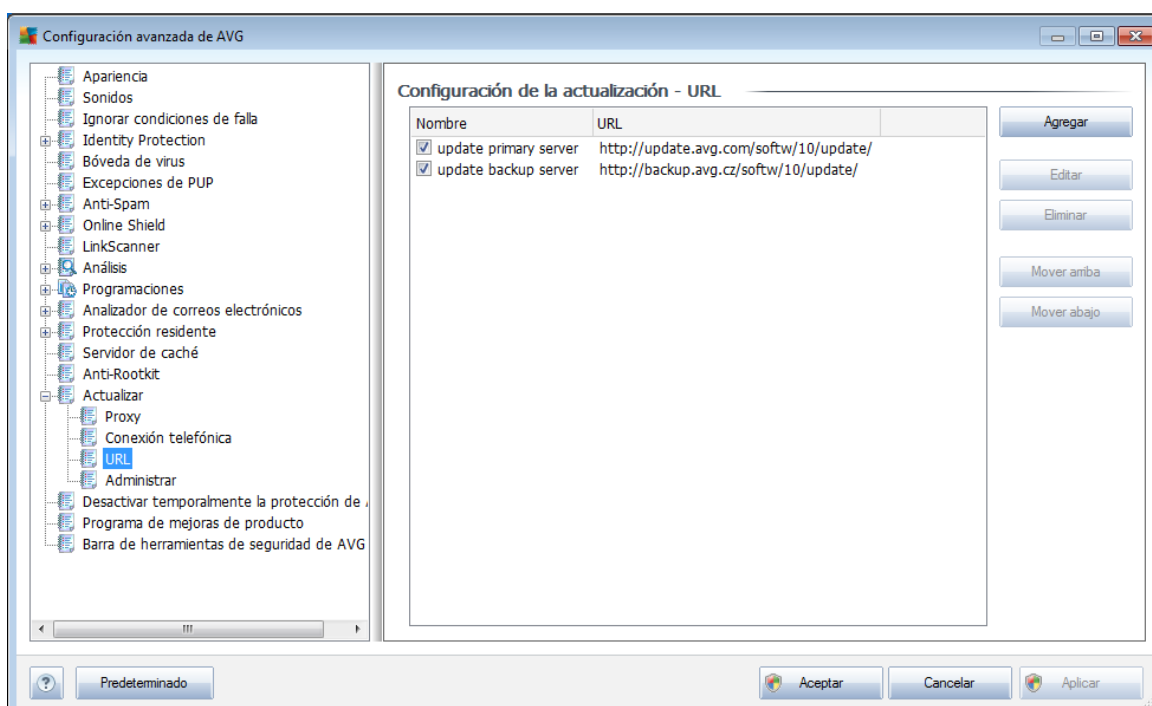


Todos los parámetros definidos de modo opcional en el diálogo **Actualizar**

**configuración - Conexión telefónica** hacen referencia a la conexión telefónica a Internet. Los campos del diálogo están inactivos hasta que se selecciona la opción **Utilizar conexión telefónica**, que los activa.

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

### 9.16.3. URL

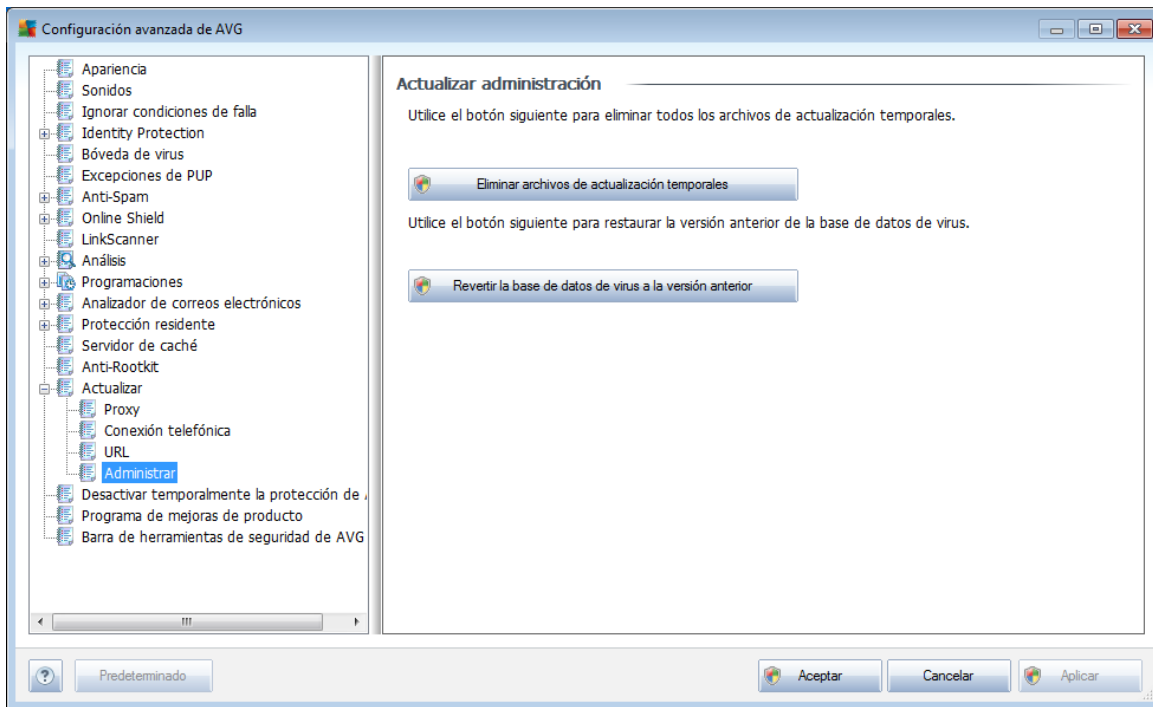


El diálogo **URL** ofrece una lista de direcciones de Internet desde las que se pueden descargar los archivos de actualización. La lista y los elementos se pueden modificar por medio de los siguientes botones de control:

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

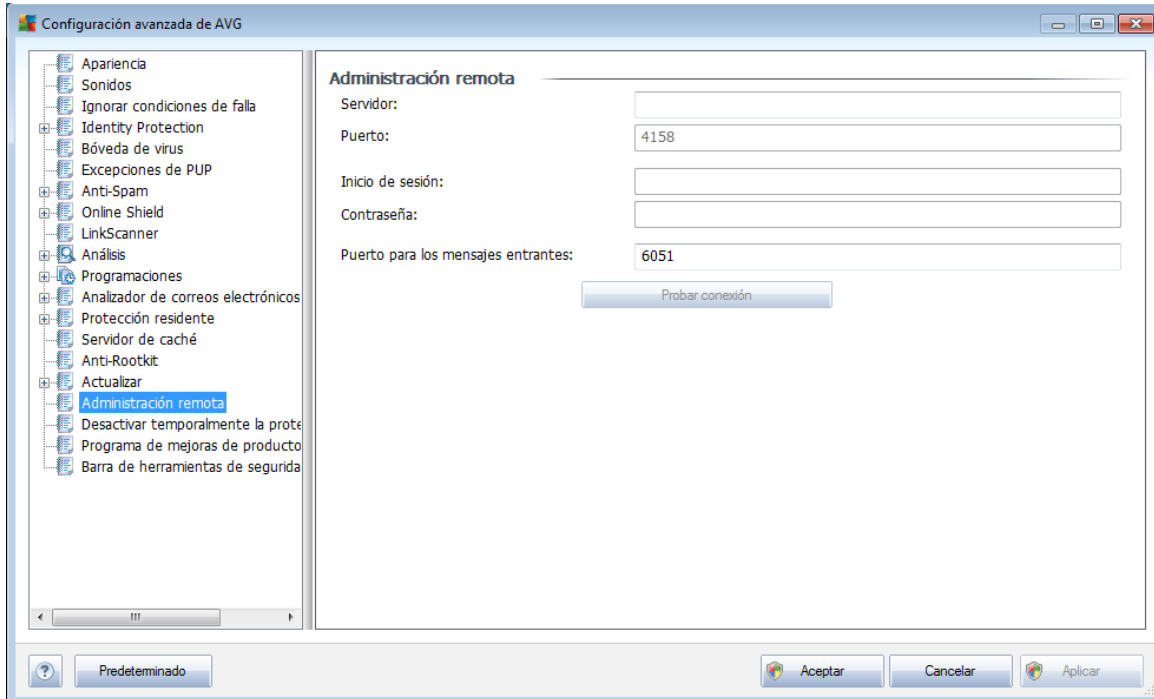
#### 9.16.4. Administrar

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



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

## 9.17. Remote administration



La configuración de **Remote Administration** hace referencia a la conexión de la estación cliente AVG con el sistema de administración remota. Si tiene previsto conectar la estación correspondiente con el sistema de administración remota, especifique los parámetros siguientes:

- **Servidor:** nombre del servidor (o dirección IP del servidor) donde está instalado el Servidor de AVG Admin.
- **Puerto:** indique el número del puerto en que el cliente AVG se comunica con el Servidor de AVG Admin (*el número de puerto 4158 se considera predeterminado; si utiliza este número de puerto, no es necesario que lo especifique explícitamente*).
- **Inicio de sesión:** si la comunicación entre el cliente AVG y el Servidor de AVG Admin está definida como segura, indique el nombre de usuario...
- **Contraseña:** especifique la contraseña.
- **Puerto de mensajes entrantes:** número del puerto en que el cliente AVG acepta los mensajes entrantes del Servidor de AVG Admin.

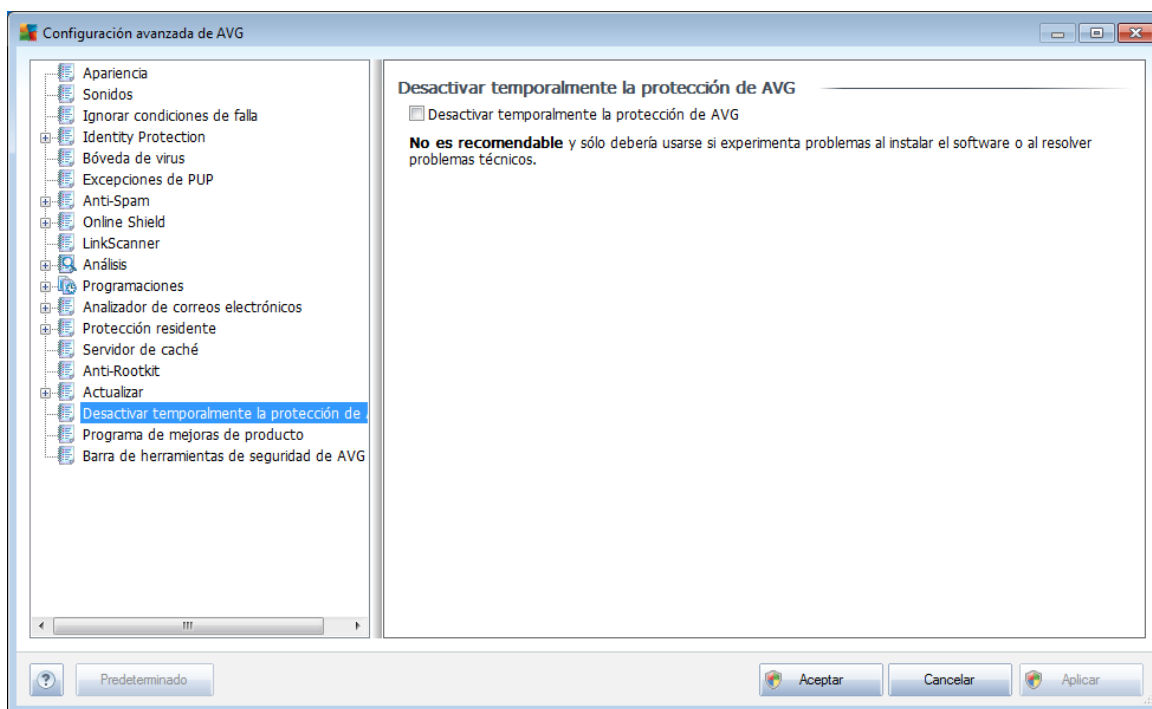
El botón **Probar conexión** le ayuda a comprobar que todos los datos establecidos anteriormente están disponibles y se pueden utilizar para conectarse de manera exitosa al DataCenter.

**Nota:** Para ver una descripción detallada de la administración remota, consulte la



documentación de AVG edición para pymes.

## 9.18. Desactivar temporalmente la protección de AVG



En el cuadro de diálogo **Desactivar temporalmente la protección de AVG** tiene la opción de desactivar toda la protección que proporciona **AVG Internet Security 2011** a la vez.

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

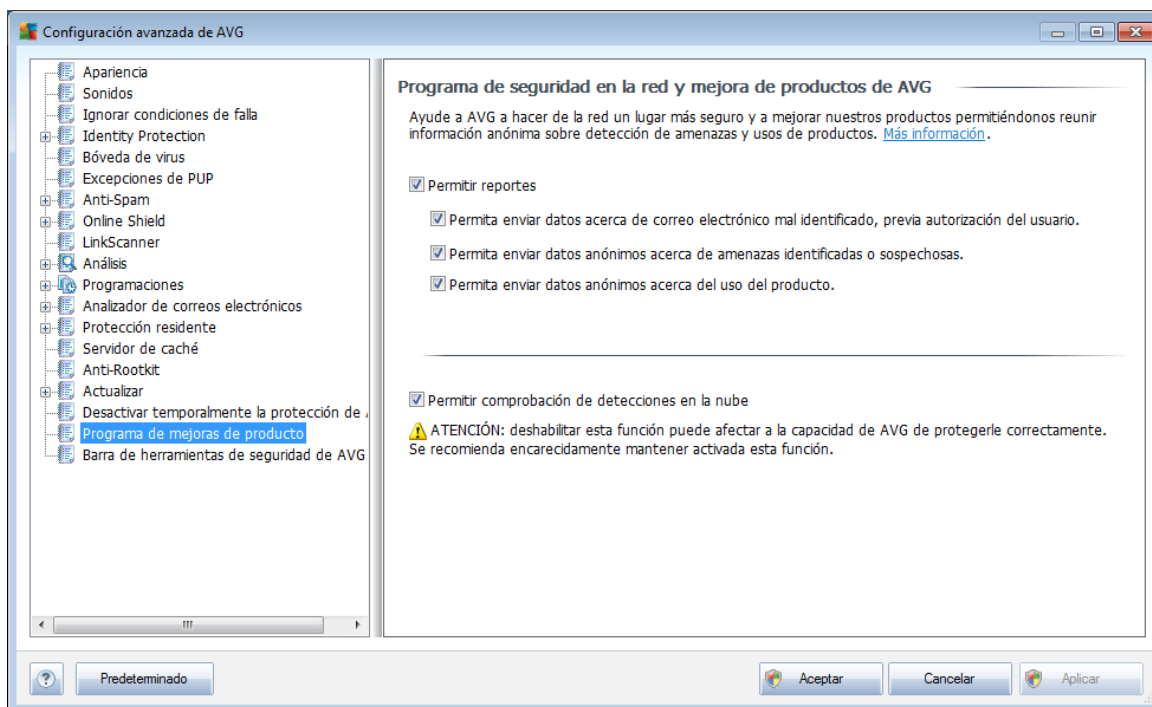
En la mayoría de los casos, no **es necesario** desactivar AVG antes de instalar nuevo software o controladores, ni siquiera si el instalador o el asistente de software le sugiere que cierre los programas y aplicaciones que se estén ejecutando para asegurarse de que no se producen interrupciones no deseadas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

## 9.19. Programa de mejora de productos

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



**Los reportes se realizan automáticamente, por lo tanto no le causan ninguna molestia, y no se incluye en ellos ningún dato de identificación personal.** La función de envío de reportes de amenazas detectadas es opcional; sin embargo, le agradeceremos que active esta función, ya que esto nos ayuda a mejorar la protección para usted y para los demás usuarios de AVG.



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

- **Un virus** es un código malicioso que se copia y propaga por sí solo, frecuentemente sin ser notado hasta que el daño está hecho. Algunos virus son una amenaza seria, que eliminan o cambian deliberadamente la forma de los archivos, mientras que otros virus pueden hacer algo aparentemente inofensivo, como tocar una pieza de música. Sin embargo, todos los virus son peligrosos debido a su capacidad básica para multiplicarse: aún un virus simple puede apoderarse de toda la memoria del equipo en un instante, y causar una falla.
- **Un gusano** es una subcategoría de virus que, a diferencia de un virus normal, no necesita un objeto "portador" al que adjuntarse, sino que se envía a sí mismo a otros equipos de manera independiente, normalmente a través del correo electrónico y, como resultado, con frecuencia sobrecarga los servidores de correo electrónico y los sistemas de red.
- El **Spyware** se define normalmente como una categoría de malware (*malware* = cualquier software malicioso, incluyendo programas que contienen virus),



normalmente caballos de Troya, encaminados a robar información personal, contraseñas, números de tarjeta de crédito, o a infiltrarse en un equipo y permitir al atacante controlarlo de manera remota; todo, por supuesto, sin el conocimiento o el consentimiento del propietario del equipo.

- Los **programas potencialmente no deseados** son un tipo de spyware que puede ser peligroso para su equipo, pero no tiene por qué serlo necesariamente. Un ejemplo específico de un PUP es el adware, un software diseñado para distribuir publicidad, normalmente mostrando ventanas emergentes con anuncios publicitarios; resulta molesto, pero no es realmente nocivo.
- Ταμβίβ λασ **cookies de rastreo** se pueden considerar una clase de spyware, ya que estos pequeños archivos, almacenados en el navegador web y enviados automáticamente al sitio web "primario" cuando lo visita nuevamente, pueden contener datos como su historial de navegación y otra información similar.
- **Vulnerabilidad** es un código malicioso que se aprovecha de una falla o vulnerabilidad en un sistema operativo, navegador de Internet u otro programa esencial.
- Ελ **phishing** es un intento por conseguir datos personales confidenciales fingiendo ser una organización confiable y bien conocida. Normalmente, se ponen en contacto con las víctimas potenciales mediante un correo electrónico masivo pidiéndoles, por ejemplo, que actualicen los detalles de su cuenta bancaria. Para hacerlo, se les invita a que sigan el vínculo que se les proporciona, el cual los lleva al sitio web del banco falso.
- **Hoax (engaño)** es un correo electrónico masivo que contiene información peligrosa, alarmante o sólo molesta e inútil. Muchas de las amenazas anteriores utilizan mensajes de correo electrónico masivo para propagarse.
- Los **sitios web maliciosos** son aquellos que deliberadamente instalan el software malicioso en su equipo, y los sitios objeto de piratería que hacen lo mismo, sólo que estos son sitios web legítimos que han sido alterados para infectar a los visitantes.

**Para protegerlo de todos estos diferentes tipos de amenazas, AVG incluye estos componentes especializados:**

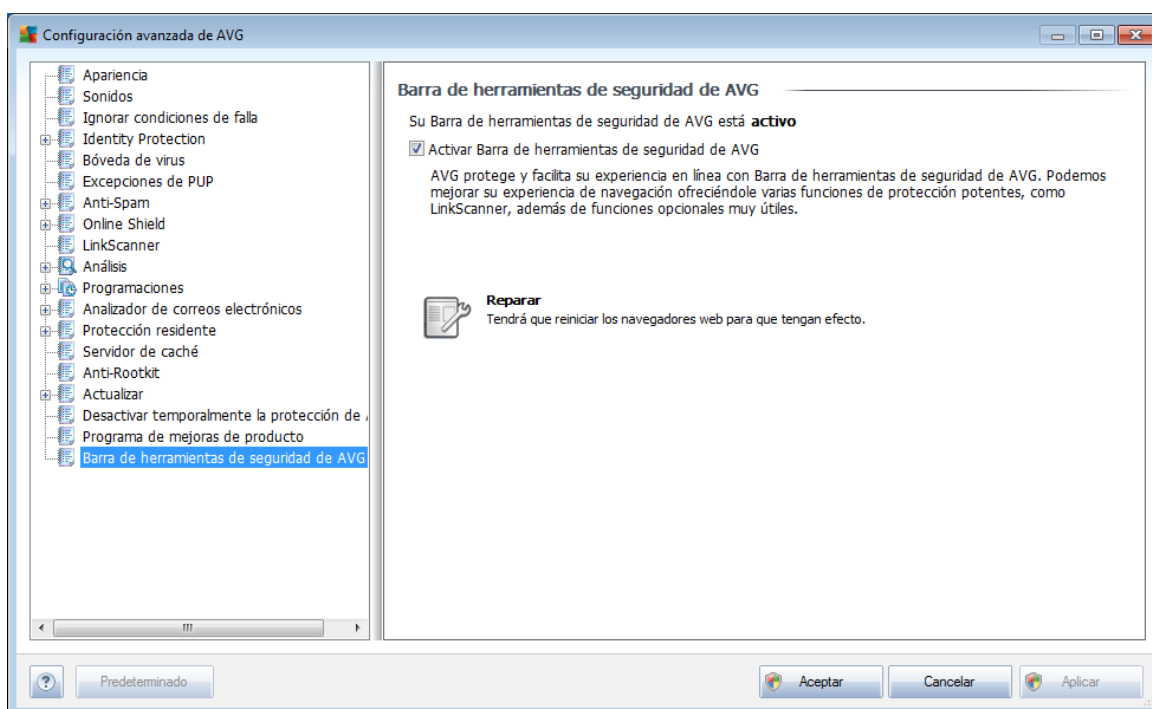
- **Anti-Virus** para proteger su equipo de los virus,
- **Anti-Spyware** para proteger su equipo del spyware,
- **Online Shield** para protegerlo de los virus y spyware cuando navega en Internet,
- **LinkScanner** para protegerlo de otras amenazas en línea mencionadas en este capítulo.





## 9.20. Barra de herramientas AVG Security

La **barra de herramientas AVG Security** es una nueva herramienta que funciona con el componente **LinkScanner**. La **Barra de herramientas AVG Security** se puede utilizar para controlar las funciones de **LinkScanner** y para ajustar su comportamiento. Si elige instalar la barra de herramientas durante la instalación de **AVG Internet Security 2011**, ésta se agregará automáticamente a su navegador web (*Internet Explorer 6.0 o superior y Mozilla Firefox 3.0 o superior*). De momento no es compatible con ningún otro navegador de Internet.



En este cuadro de diálogo de la **Barra de herramientas AVG Security** puede activar o desactivar todo el componente **Barra de herramientas AVG Security** desde la interfaz de configuración avanzada de la aplicación AVG, mediante la opción **Activar barra de herramientas AVG Security**.

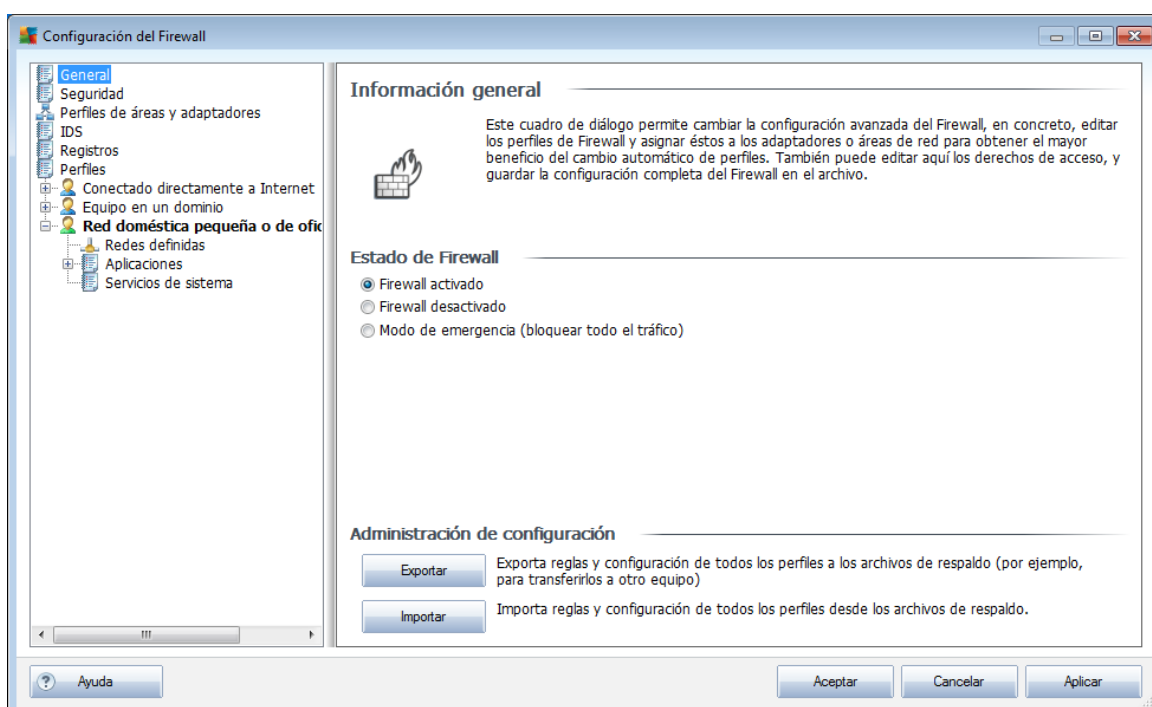
El botón **Reparar** devolverá todas las partes de la **Barra de herramientas AVG Security** a un estado totalmente funcional (*volver a la configuración predeterminada*) y asegurará que la **Barra de herramientas AVG Security** funcione sin errores en todos los navegadores de Internet compatibles. Si ha desactivado la **Barra de herramientas AVG Security** anteriormente, ya sea a través de este cuadro de diálogo o directamente en el navegador de Internet, presione el botón **Reparar** para activar el componente.

## 10. Configuración del Firewall

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

### 10.1. General

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



### Estado del Firewall

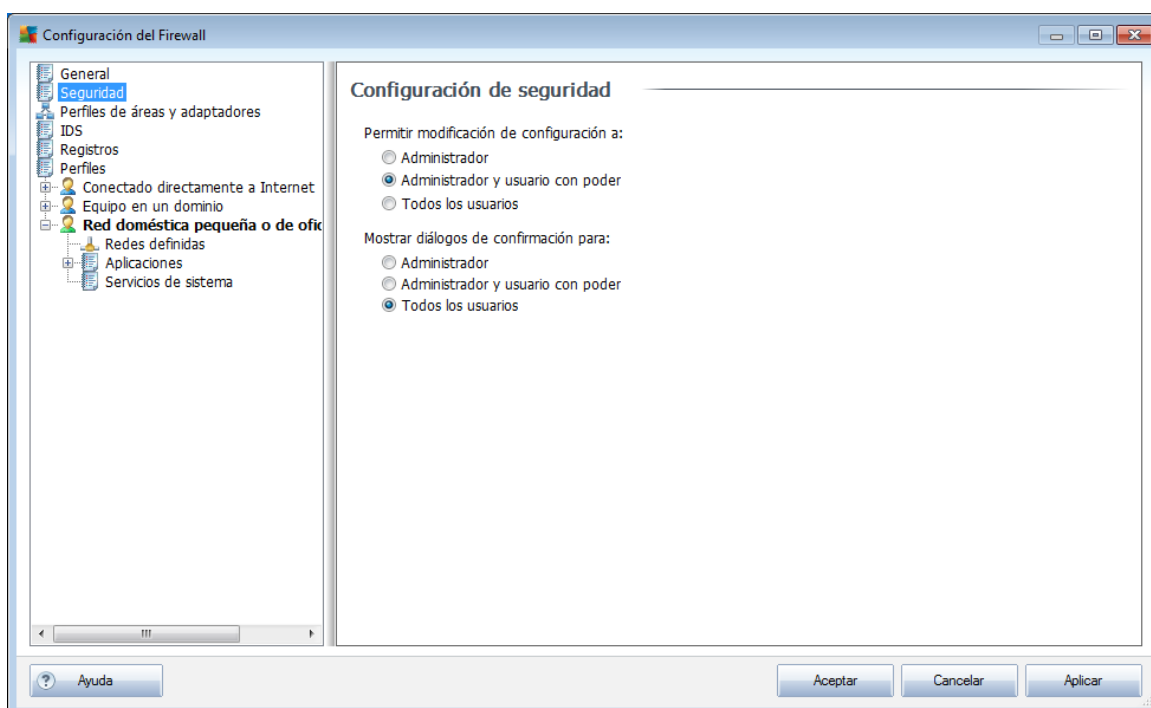
En la sección **Estado del Firewall** puede cambiar el estado del **Firewall** cuando sea necesario:

- **Firewall activado:** seleccione esta opción para permitir la comunicación con aquellas aplicaciones que tienen la asignación de 'permitido' en el conjunto de reglas definido dentro del **Perfil de Firewall**
- **Firewall desactivado:** esta opción desactiva el **Firewall** por completo, se permite todo el tráfico pero no se analiza
- **Modo de emergencia (bloquear todo el tráfico de Internet):** seleccione esta opción para bloquear todo el tráfico en todos los puertos de red; el **Firewall** aún está en ejecución pero se detiene todo el tráfico de red

## Administración de configuración

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

## 10.2. Seguridad



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

- **Permitir la modificación de la configuración a** - especifique a quién le está permitido cambiar la configuración del **Firewall**
- **Mostrar el diálogo de confirmación para:** especifique a quién se deben mostrar los diálogos de confirmación (*diálogos solicitando una decisión en una situación no cubierta por una regla definida del **Firewall***)

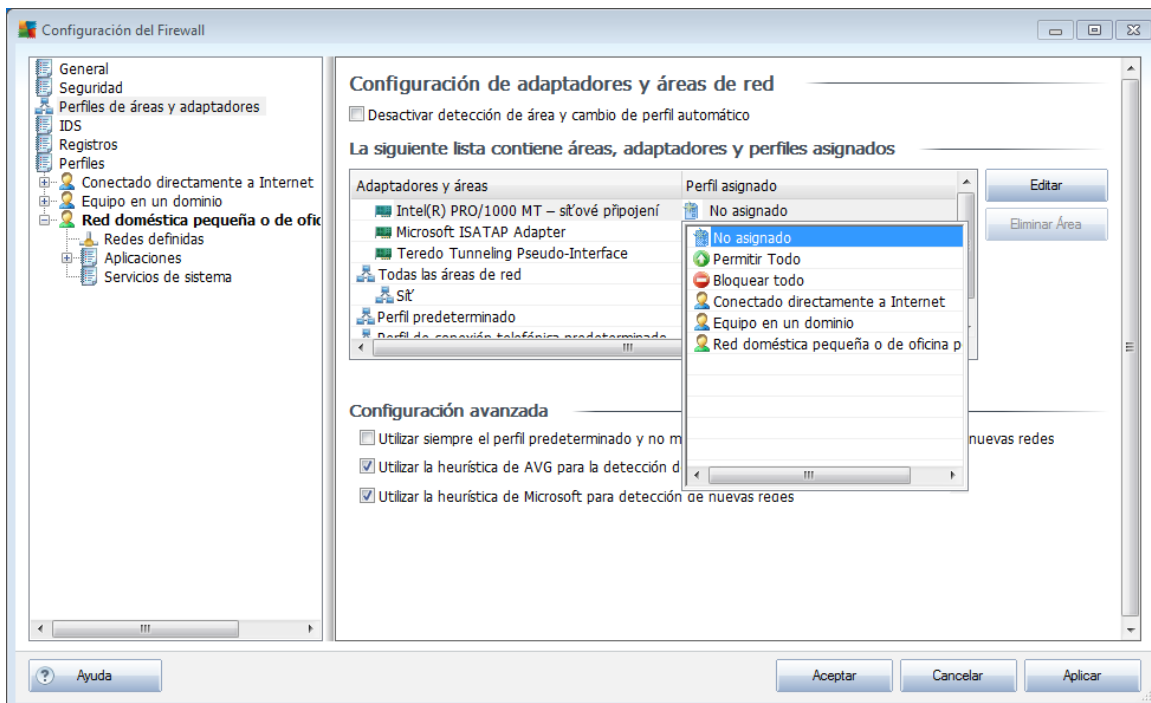
En ambos casos puede asignar el derecho específico a uno de los siguientes grupos de usuarios:

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

- **Administrador y usuario con poder** el administrador puede asignar a cualquier usuario a un grupo especificado (*Usuario con poder*) y definir las autoridades de los integrantes del grupo
- **Todos los usuarios:** otros usuarios no asignados a ningún grupo específico

### 10.3. Perfiles de áreas y adaptadores

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



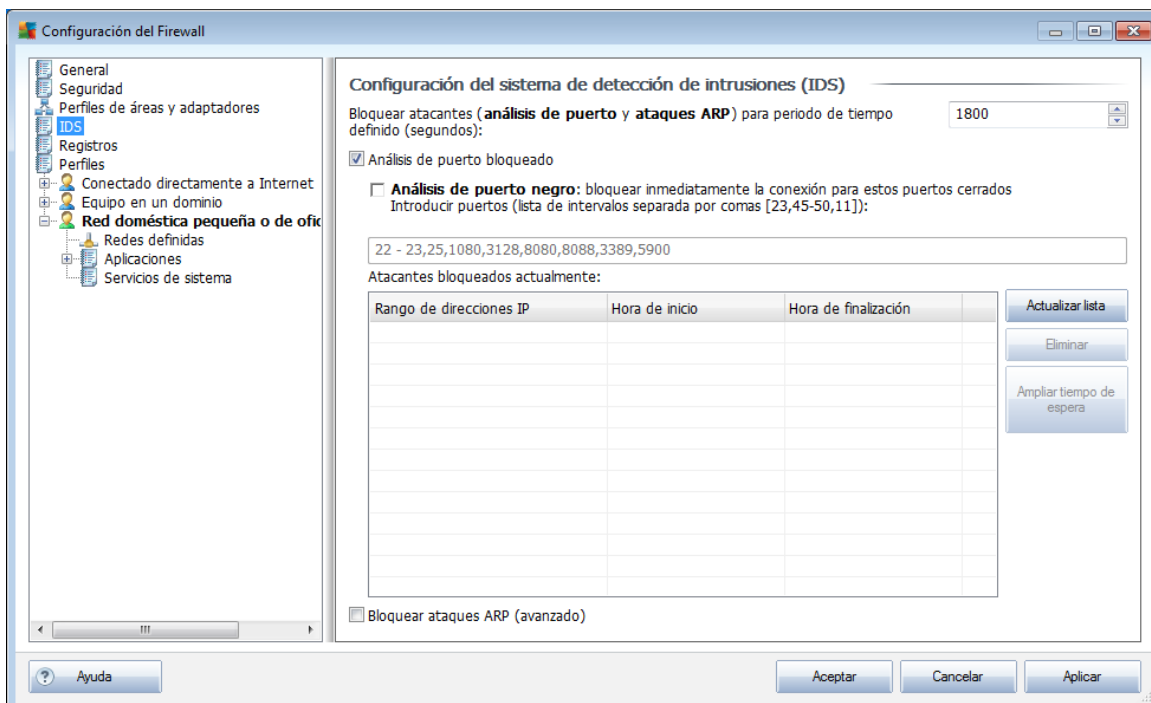
- **Desactivar detección de área y cambio de perfil automático:** uno de los perfiles definidos puede asignarse a cada tipo de interfaz de red, de forma respectiva a cada área. Si no desea definir perfiles específicos, se utilizará un perfil común. Sin embargo, si decide diferenciar los perfiles y asignarlos a áreas y adaptadores específicos, y después, por alguna razón, desea cambiar esta configuración de forma temporal, haga clic en la opción **Desactivar detección de área y cambio de perfil automático**.
- **Lista de adaptadores, áreas y perfiles asignados:** en esta lista puede encontrar una descripción general de los adaptadores y áreas detectados. Para cada uno de ellos, puede asignar un perfil específico en el menú de perfiles definidos. Para abrir este menú, haga clic en el elemento respectivo en la lista de adaptadores, y seleccione el perfil.

### Configuración avanzada

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

## 10.4. IDS

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



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

- **Bloquear atacantes para periodo de tiempo definido:** aquí puede especificar cuántos segundos debe estar bloqueado un puerto, siempre que se



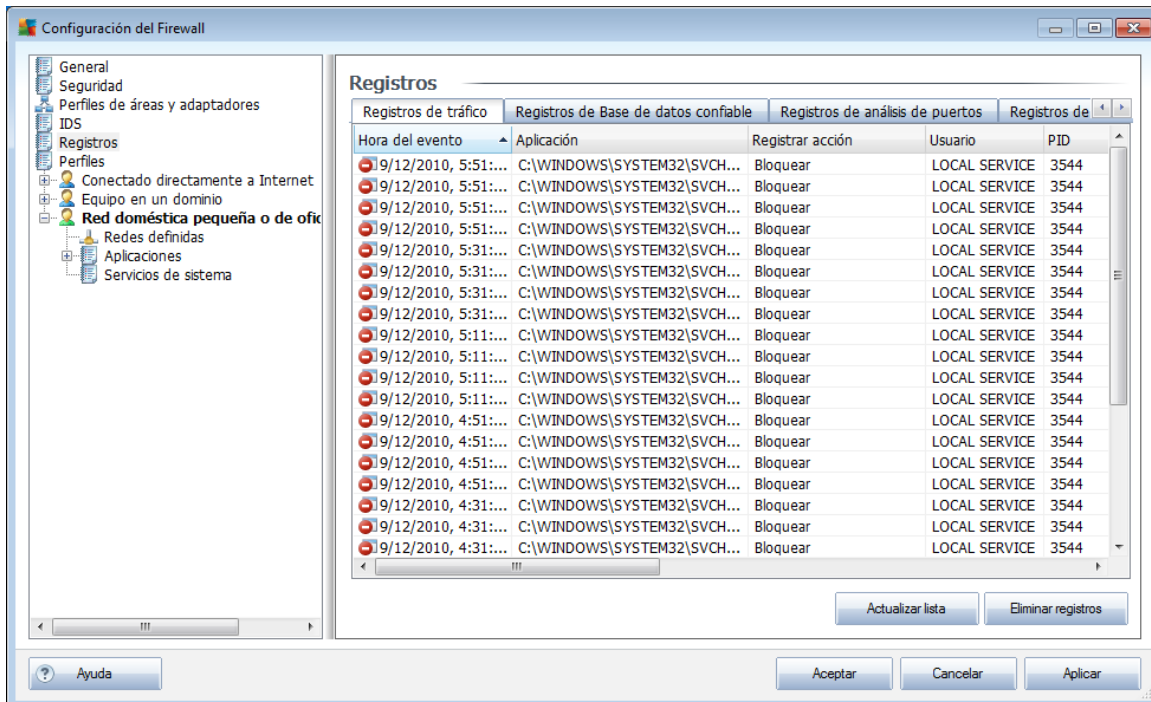
detecte un intento de comunicación sospechoso en él. De forma predeterminada, el rango de tiempo está establecido en 1800 segundos (30 minutos).

- **Análisis de puerto bloqueado:** seleccione la casilla para bloquear los intentos de comunicación en todos los puertos TCP y UDP del equipo procedentes del exterior. Para estos tipos de conexión, se permiten cinco intentos y el sexto se bloquea.
  - **Análisis de puerto negro:** seleccione la casilla para bloquear inmediatamente cualquier intento de comunicación en los puertos especificados en el campo de texto de abajo. Los distintos puertos o rangos de puertos se deben separar mediante comas. Hay una lista predefinida de puertos recomendados por si desea utilizar esta función.
  - **Atacantes bloqueados actualmente:** en esta sección se enumeran los intentos de comunicación que el **Firewall** tiene bloqueados actualmente. El historial completo de los intentos bloqueados se puede visualizar en el cuadro de diálogo **Registros** (pestaña *Registros de análisis de puertos*).
- **Bloquear ataques ARP** activa el bloqueo de clases especiales de intentos de comunicación dentro de una red local detectada por **IDS** como potencialmente peligrosos. Se aplica el tiempo establecido en **Bloquear atacantes para periodo de tiempo definido**. Recomendamos que sólo los usuarios avanzados, familiares con el tipo y el nivel de riesgo de su red, utilicen esta función.

### Botones de control

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

## 10.5. Registros



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

- **Registros de tráfico:** ofrece información acerca de la actividad de todas las aplicaciones que han intentado conectarse a la red.
- **Registros de Base de datos confiable:** la *Base de datos confiable* es la base de datos interna de AVG que recopila información acerca de aplicaciones certificadas y confiables a las que siempre se les puede permitir comunicarse en línea. La primera vez que una nueva aplicación intenta conectarse a la red (*es decir, aún no existen reglas del firewall especificadas para esta aplicación*), es necesario determinar si se le debe permitir la comunicación con la red. Primero, AVG busca en la *Base de datos confiable* y, si la aplicación se encuentra en la lista, se le concederá automáticamente acceso a la red. Sólo después de que se comprueba que no existe información disponible acerca de la aplicación en la base de datos, se le preguntará en un cuadro de diálogo independiente si desea permitir que la aplicación obtenga acceso a la red.
- **Registros de análisis de puertos:** proporciona el registro de todas las actividades del **sistema de detección de intrusiones**.
- **Registros de ARP:** información de registro sobre el bloqueo de clases especiales de intentos de comunicación dentro de una red local (opción



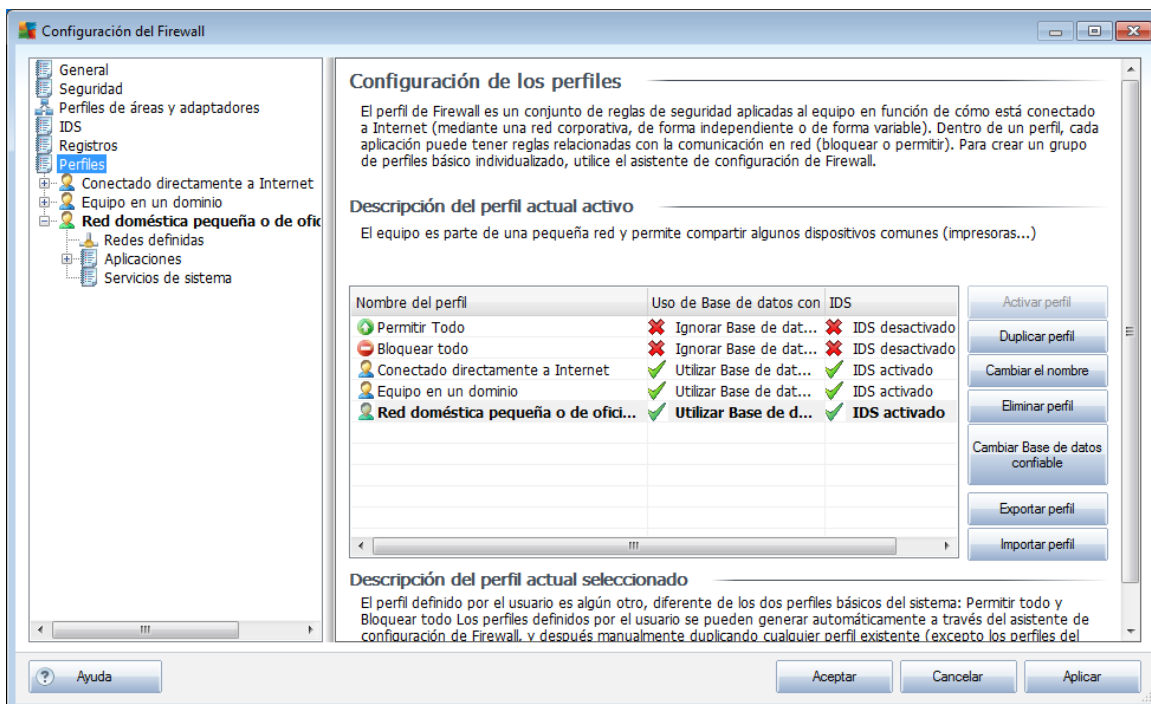
[Bloquear ataques ARP](#)) detectados por el [sistema de detección de intrusiones](#) como potencialmente peligrosos.

## Botones de control

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

## 10.6. Perfiles

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



Todos los demás [perfiles](#) del sistema pueden editarse en este mismo cuadro de diálogo utilizando los siguientes botones de control:

- **Activar perfil:** este botón establece el perfil seleccionado como activo, lo cual significa que el **Firewall** utilizará el perfil seleccionado para controlar el tráfico de la red.
- **Duplicar perfil:** crea una copia idéntica del perfil seleccionado; posteriormente es posible editar y cambiar el nombre de la copia para crear un perfil nuevo





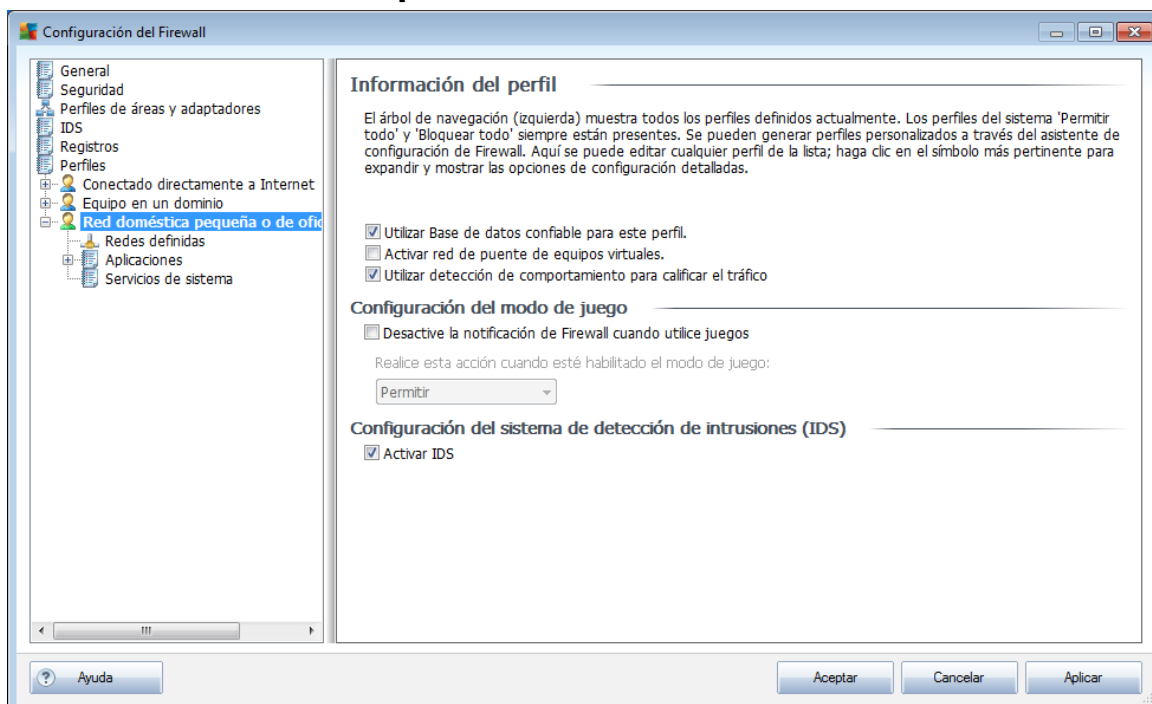
basado en el original duplicado

- **Cambiar el nombre:** permite definir un nombre nuevo para un perfil seleccionado
- **Eliminar perfil:** elimina el perfil seleccionado de la lista
- **Cambiar la Base de datos confiable:** para el perfil seleccionado puede elegir utilizar la información de la *Base de datos confiable* (la Base de datos confiable es una base de datos interna de AVG que recopila información acerca de las aplicaciones confiables y certificadas a las cuales siempre se puede permitir la comunicación en línea.)
- **Exportar perfil:** registra la configuración del perfil seleccionado en un archivo que se guardará para utilizarse en el futuro
- **Importar perfil:** configura el perfil seleccionado basándose en la información exportada en un archivo de copia de resguardo de la configuración

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

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

### 10.6.1. Información del perfil





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

- **Utilizar base de datos confiable para este perfil** (seleccionada de modo predeterminado): seleccione la opción para activar la *base de datos confiable* (es decir, la base de datos interna de AVG que recopila información acerca de comunicaciones en línea confiables y certificadas. Si aún no existe una regla especificada para la aplicación, es necesario averiguar si se puede otorgar a la aplicación acceso a Internet. AVG busca primero en la Base de datos confiable y, si la aplicación se encuentra en la lista, se considerará segura y se le permitirá la comunicación a través de la red. En caso contrario, se le solicitará que decida si se debe permitir a la aplicación comunicarse a través de la red ) con el perfil correspondiente.
- **Activar red de puente de equipos virtuales** (desactivado de manera predeterminada): seleccione este elemento para permitir que las máquinas virtuales de VMware se conecten directamente a la red.
- **Utilizar detección de comportamiento para calificar el tráfico** (seleccionada de modo predeterminado): seleccione esta opción para permitir que el **Firewall** utilice las funciones de **Identity Protection** al evaluar una aplicación. **Identity Protection** puede determinar si la aplicación muestra algún comportamiento sospechoso, o si se puede confiar en ella y se le debe permitir la comunicación en línea.

### Configuración del modo de juego

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

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

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

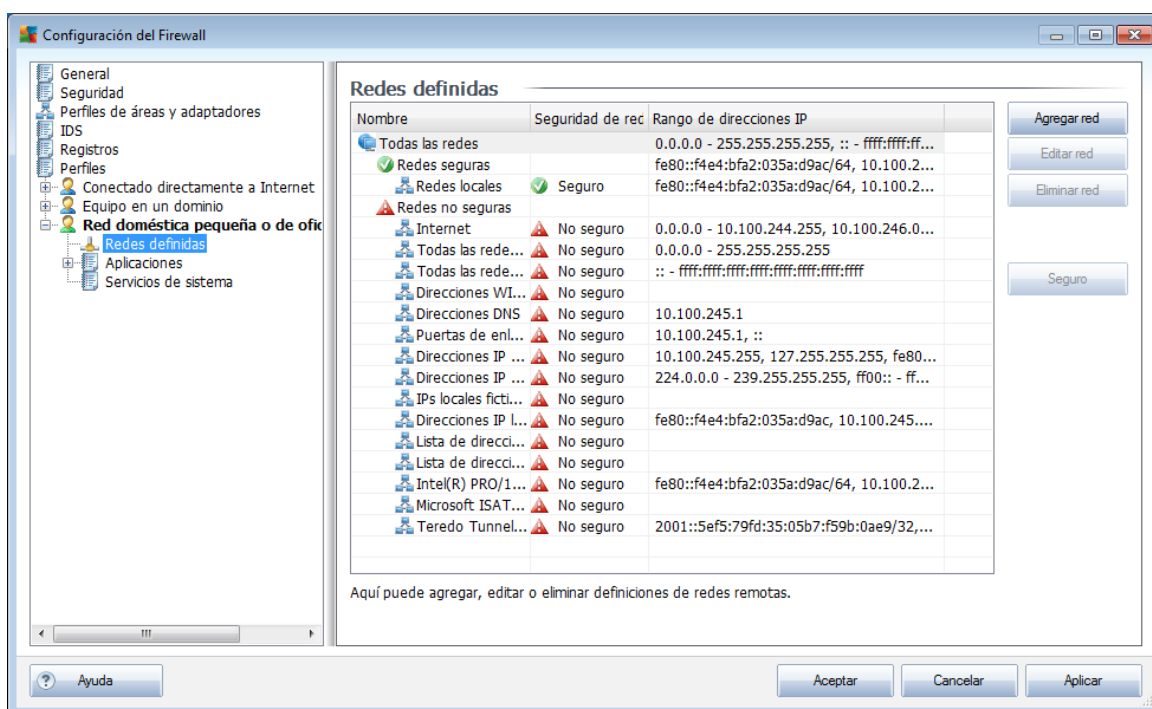
### Configuración del sistema de detección de intrusiones (IDS)

Marque la casilla de verificación **Activar IDS** para activar una función especial de análisis diseñada para identificar y bloquear intentos de comunicación sospechosos a través de determinados puertos de su equipo ([para obtener más detalles sobre la](#)

[configuración de esta función, consulte el capítulo sobre IDS de esta documentación\).](#)

### 10.6.2. Redes definidas

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

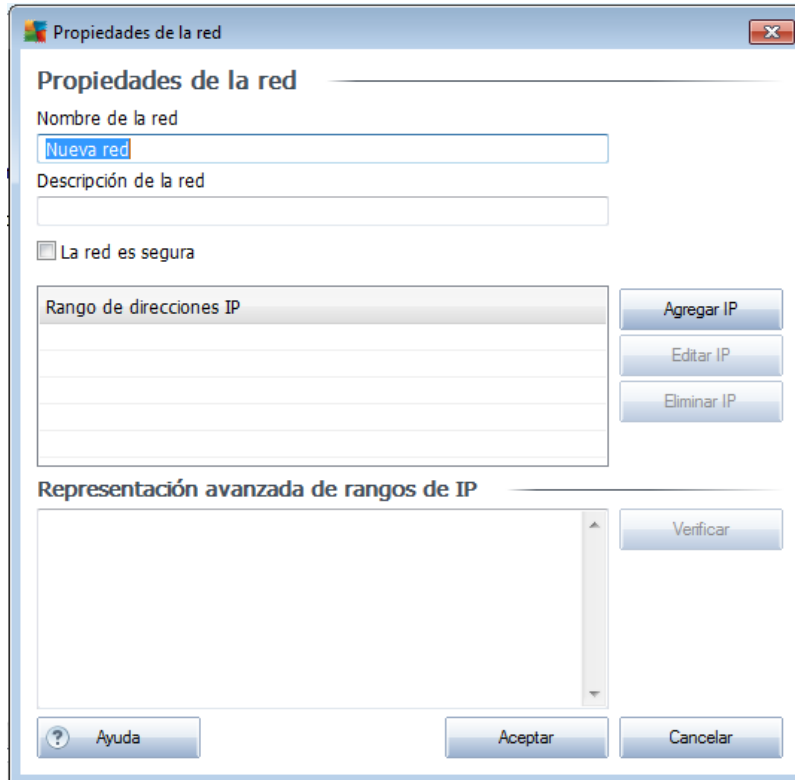


De cada red detectada se proporciona la siguiente información:

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

#### Botones de control

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



Dentro de este cuadro de diálogo, puede especificar el **Nombre de la red**, dar la **Descripción de red** y posiblemente asignar la red como segura. La nueva red puede definirse de forma manual en un cuadro de diálogo independiente que se abre mediante el botón **Agregar IP** (de forma alternativa, **Editar IP/Eliminar IP**); dentro de este cuadro de diálogo puede especificar la red utilizando su rango o máscara IP.

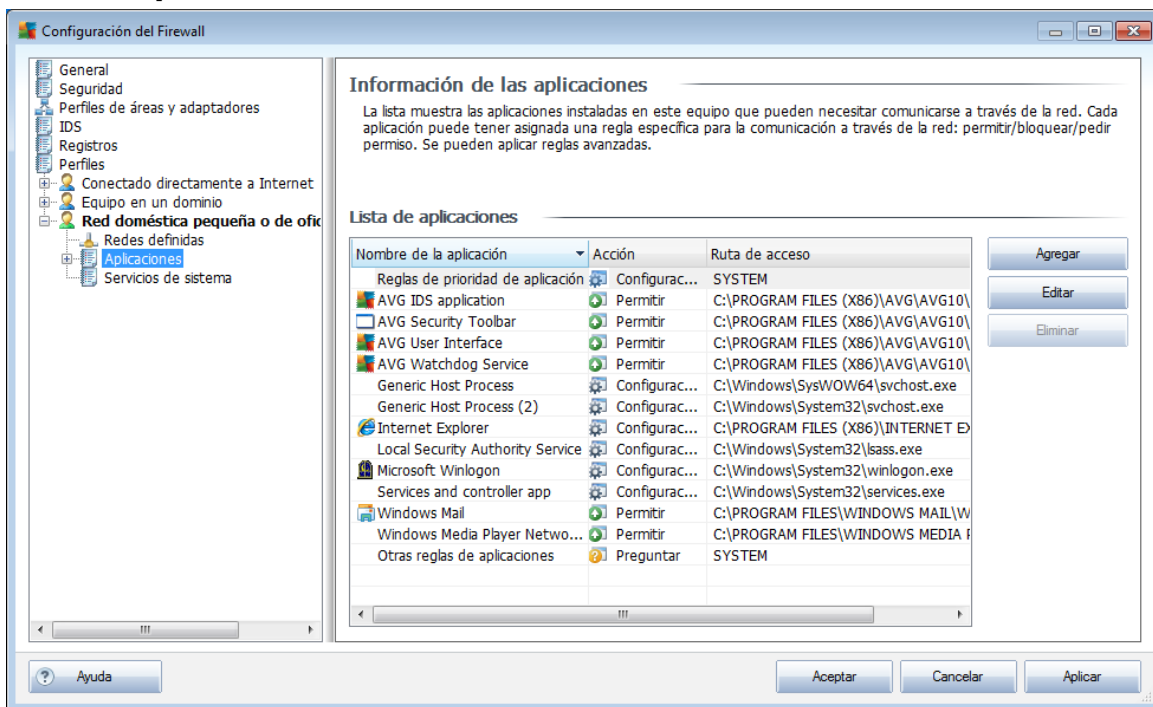
Para establecer varias redes que deben definirse como parte de una red creada recientemente, puede utilizar la opción de **Representación avanzada de rango IP**: introduzca la lista de todas las redes en el campo de texto respectivo (*es compatible con cualquier formato estándar*) y presione el botón **Verificar** para asegurarse de que se pueda reconocer el formato. A continuación, presione **Aceptar** para confirmar y guardar la información.

- **Editar red**: abre la ventana del cuadro de diálogo **Propiedades de red** (ver arriba), donde puede editar los parámetros de una red ya definida (*el cuadro de diálogo es idéntico al diálogo para agregar una red nueva, consulte la descripción en el párrafo anterior*)
- **Eliminar red**: elimina la nota de una red seleccionada de una lista de redes
- **Marcar como segura**: de forma predeterminada, todas las redes se consideran no seguras, y sólo debe utilizar este botón para asignar el estado de segura a una red si está seguro de que la red lo es (*y viceversa, una vez que la red tiene asignado el estado de segura, el texto del botón cambia a "Marcar como*



no segura").

### 10.6.3. Aplicaciones



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

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

Las aplicaciones de la lista son las que se detectaron en el equipo (y se les asignaron acciones respectivas).

**Nota:** sólo se pueden detectar las aplicaciones ya instaladas, por lo que, si instala una aplicación nueva en el futuro, deberá definir las reglas de Firewall para ésta. De manera predeterminada, cuando la aplicación nueva intenta conectarse a través de la red por primera vez, el Firewall crea una regla automáticamente de acuerdo con la Base de datos confiable o le solicita que



**confirme si desea permitir o bloquear la comunicación. En el segundo caso, podrá guardar la respuesta como regla permanente (que se mostrará entonces en este cuadro de diálogo).**

Por supuesto, también puede definir reglas para la nueva aplicación de forma inmediata: en este cuadro de diálogo, presione **Agregar** e introduzca los detalles de la aplicación.

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

- **Las reglas prioritarias de aplicaciones** (en la parte superior de la lista) son preferenciales y siempre se aplican antes que las reglas específicas de las aplicaciones.
- **Otras reglas de aplicaciones** (en la parte inferior de la lista) se utilizan como "último recurso" cuando no se aplican reglas específicas para la aplicación, por ejemplo, para una aplicación desconocida e indefinida.

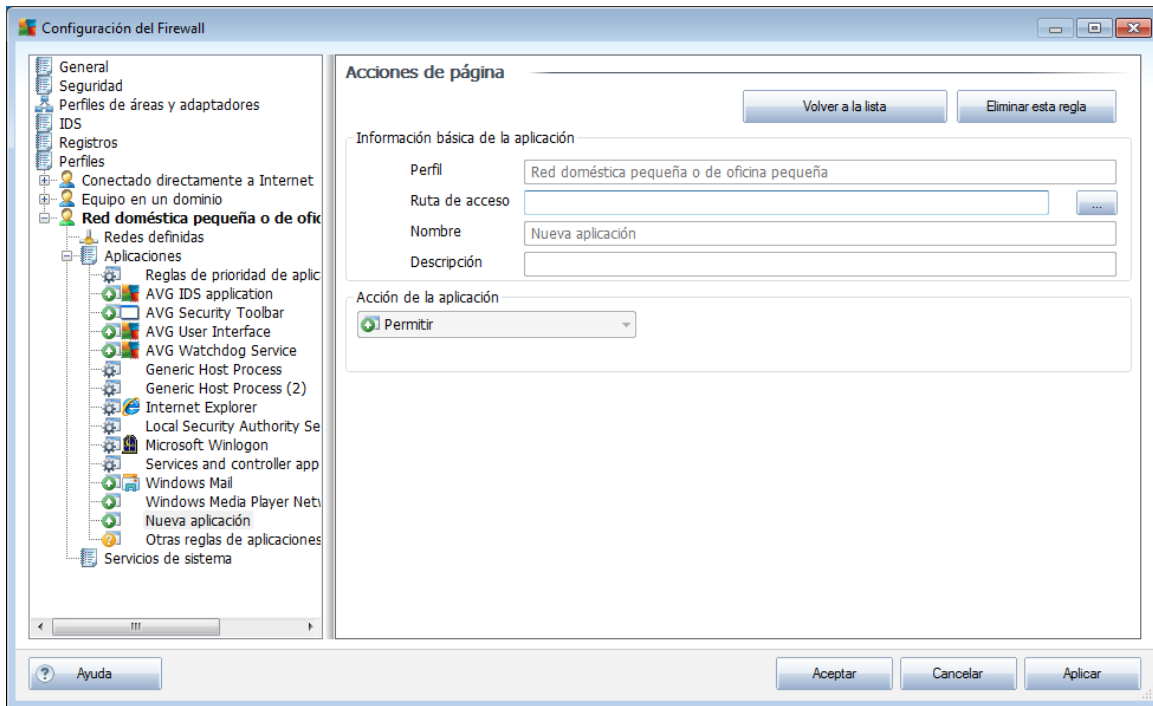
**Estos elementos tienen diferentes opciones de configuración para aplicaciones comunes y sólo deben utilizarlos los usuarios experimentados. Se recomienda encarecidamente no modificar la configuración**

### **Botones de control**

La lista puede editarse utilizando los siguientes botones de control:

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

En este cuadro de diálogo, puede definir la configuración detallada para la aplicación respectiva:



### Acciones de página

- **El botón Volver a la lista** mostrará la descripción general de todas las reglas de aplicaciones definidas.
- **El botón Eliminar esta regla** borrará la regla de aplicación mostrada. Tenga en cuenta que esta acción no puede revertirse.

### Información básica de la aplicación






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

### Acción de la aplicación

**\*\*\***En el menú desplegable, puede seleccionar la regla de Firewall para la aplicación, por ejemplo, lo que el Firewall debe hacer cuando la aplicación intenta comunicarse



mediante la red: **\*\*\***

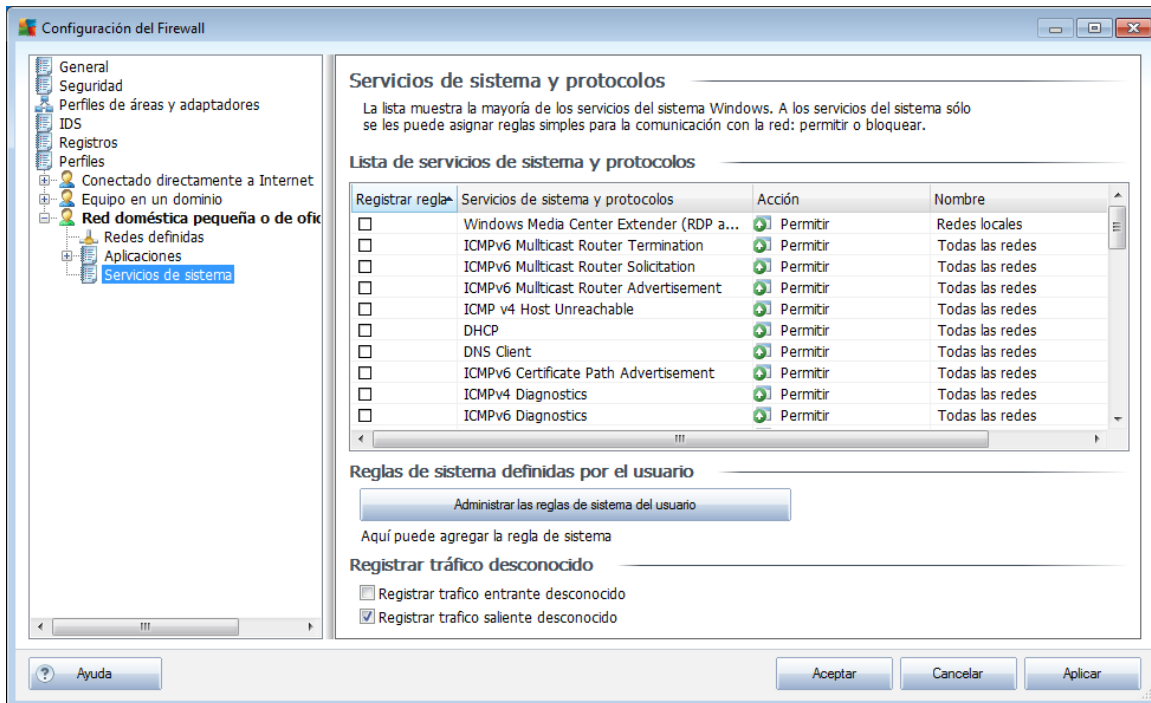
-  - **Permitir** permitirá que la aplicación que se comunique utilizando todas las redes y adaptadores definidos sin limitaciones.
-  - **Permitir seguras** sólo permitirá que la aplicación se comunique utilizando redes definidas como Seguras (confiables).
-  - **Bloquear** prohibirá la comunicación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

#### 10.6.4. Servicios del sistema

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




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





## Lista de servicios de sistema y protocolos

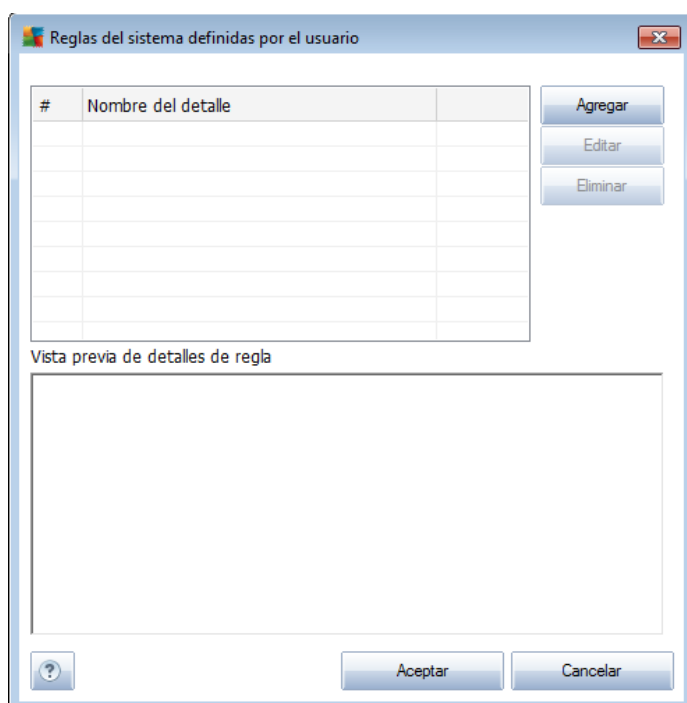
La tabla tiene las siguientes columnas:

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

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

## Reglas de sistema definidas por el usuario

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



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

## Registrar tráfico desconocido

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

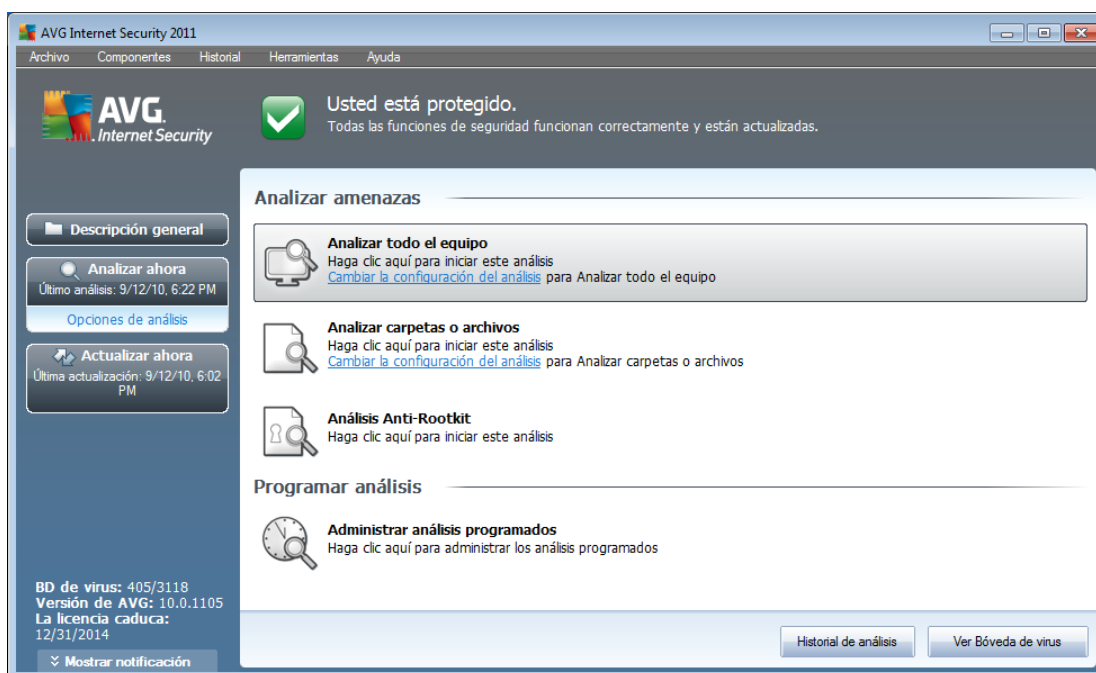


*predeterminada*) : marque la casilla para guardar en los Registros todos los intentos desconocidos que realice su equipo para conectarse a una ubicación externa.

## 11. Análisis de AVG

El análisis es una parte crucial de la funcionalidad de **AVG Internet Security 2011**. Puede realizar análisis a petición o [programarlos para que se ejecuten periódicamente](#) en los momentos apropiados.

### 11.1. Interfaz de análisis



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

- Descripción general de los [análisis predefinidos](#): existen tres tipos de análisis definidos por el proveedor de software para su uso inmediato, ya sea a pedido o a los intervalos programados:
  - [Análisis de todo el equipo](#)
  - [Analizar carpetas o archivos específicos](#)
  - [Análisis Anti-Rootkit](#)
- [Sección de programación de análisis](#): en ella puede definir nuevos análisis y crear nuevas programaciones según convenga.

### Botones de control



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

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

## 11.2. Análisis predefinidos

Una de las funciones principales de **AVG Internet Security 2011** es el análisis a pedido. Los análisis a pedido están diseñados para analizar varias partes de su equipo cuando existen sospechas de una posible infección de virus. De todas formas, se recomienda llevar a cabo dichos análisis con regularidad aun si no cree que se vayan a detectar virus en su equipo.

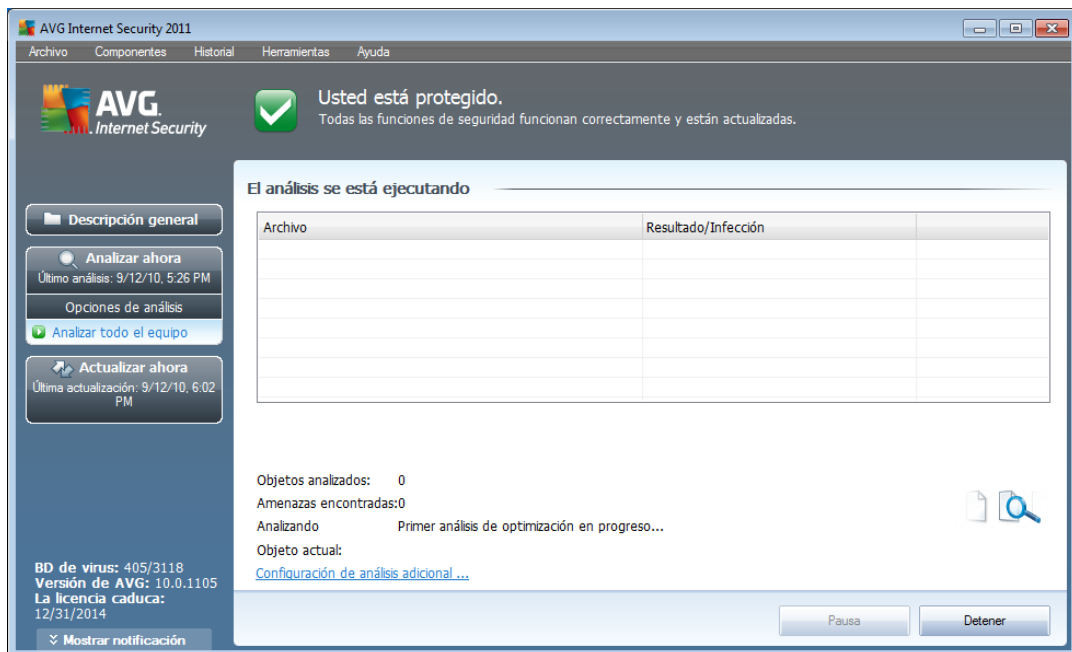
En **AVG Internet Security 2011** encontrará los siguientes tipos de análisis predefinidos por el proveedor del software:

### 11.2.1. Análisis de todo el equipo

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

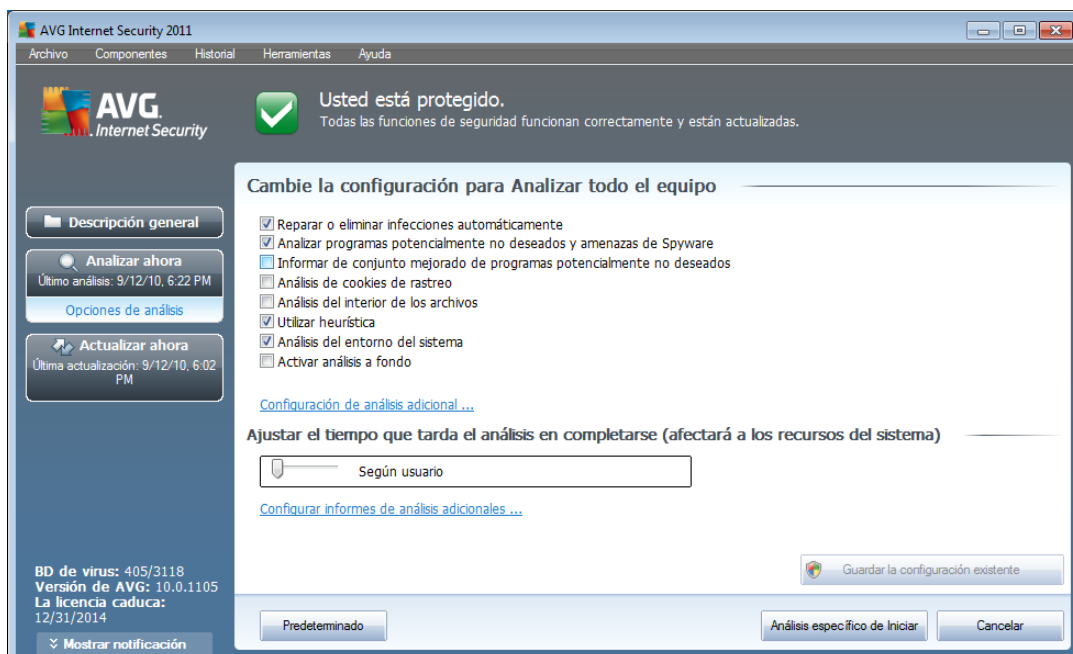
### Ejecución del análisis

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



### Edición de la configuración de análisis

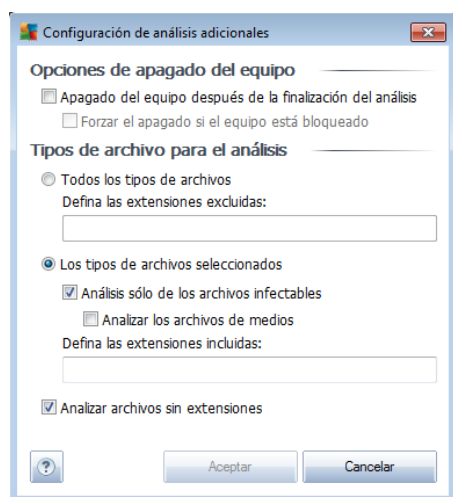
Tiene la opción de editar la configuración predeterminada predefinida del **Análisis de todo el equipo**. Presione el vínculo de **Cambiar la configuración de análisis** para ir al cuadro de diálogo **Cambiar configuración para Analizar todo el equipo** (al que se obtiene acceso desde la [interfaz de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



- **Parámetros de análisis:** en la lista de parámetros de análisis puede activar o desactivar parámetros según sea necesario:
  - **Reparar o eliminar infecciones automáticamente** (activado de manera predeterminada): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si hay una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la **Bóveda de virus**.
  - **Analizar programas potencialmente no deseados y amenazas de Spyware** (activada de forma predeterminada): seleccione esta opción para activar el motor **Anti-Spyware** y analizar en busca de spyware así como de virus. [El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito.](#) Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
  - **Informar conjunto mejorado de programas potencialmente no deseados** (desactivada de forma predeterminada): seleccione esta opción para detectar un paquete extendido de **spyware**, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
  - **Analizar cookies de rastreo** (desactivado de manera predeterminada): este parámetro del componente **Anti-Spyware** define que las cookies

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

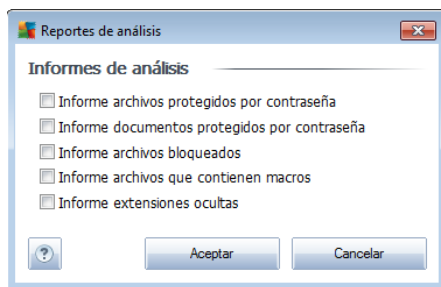
- **Analizar el interior de los archivos** (activado de manera predeterminada): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos (por ejemplo, ZIP, RAR...
  - **Utilizar heurística** (activado de manera predeterminada): el análisis heurístico (la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual) será uno de los métodos empleados para la detección de virus durante el análisis.
  - **Analizar el entorno del sistema** (activado de manera predeterminada): el análisis también comprobará las áreas del sistema del equipo.
  - **Activar análisis a fondo** (desactivado de manera predeterminada): en determinadas situaciones (con sospechas de que el equipo está infectado) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Configuración de análisis adicionales:** el vínculo abre un nuevo cuadro de diálogo **Configuración de análisis adicionales**, donde puede especificar los siguientes parámetros:



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



- **Defina los tipos de archivo para el análisis:** debe decidir si desea analizar:
  - **Todos los tipos de archivos** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;
  - **Tipos de archivos seleccionados:** puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.
  - De manera opcional, puede decidir si desea **Analizar archivos sin extensiones:** esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.
- **Ajustar el tiempo que tarda el análisis en completarse:** puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, la prioridad se establece al nivel medio, que optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).
- **Configurar informes de análisis adicionales:** el vínculo abre un nuevo cuadro de diálogo **Informes de análisis**, donde puede seleccionar qué tipos de posibles hallazgos se debería informar:



**Advertencia:** Estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo [Análisis de AVG/Programación de análisis/Cómo analizar](#). Si decide cambiar la configuración predeterminada para



**Analizar todo el equipo**, puede guardar la nueva configuración como la predeterminada que se usará para posteriores análisis del equipo completo.

### 11.2.2. Análisis de carpetas o archivos específicos

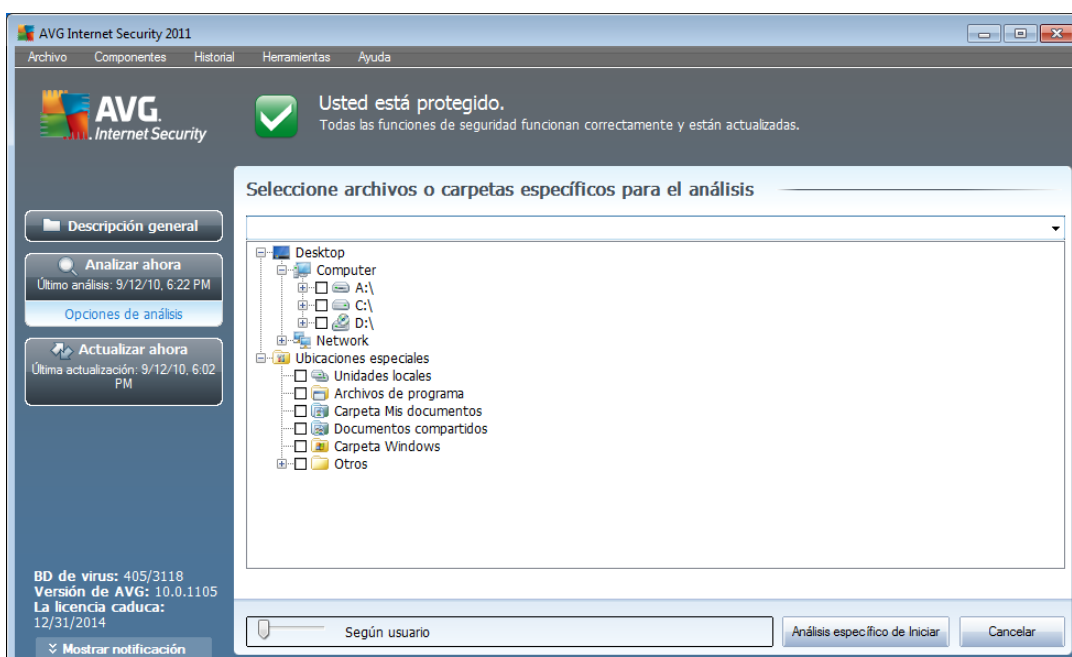
**Analizar carpetas o archivos específicos:** analiza únicamente las áreas del equipo seleccionadas (*carpetas, discos duros, discos flexibles, CD, etc.*). El procedimiento de análisis en caso de detección de virus y su tratamiento es el mismo que se realiza con el análisis de todo el equipo: los virus encontrados se reparan o eliminan a la [Bóveda de Virus](#). Puede emplear el análisis de archivos o carpetas específicos para configurar sus propios análisis y programas en función de sus necesidades.

#### Ejecución de análisis

El **análisis de archivos o carpetas específicos** se puede ejecutar directamente desde la [interfaz de análisis](#) haciendo clic en el icono del análisis. Se abre un nuevo cuadro de diálogo denominado **Selección de archivos o carpetas específicos para el análisis**. En la estructura de árbol del equipo, seleccione aquellas carpetas que desea analizar. La ruta a cada carpeta seleccionada se genera automáticamente y aparece en el cuadro de texto de la parte superior de este cuadro de diálogo.

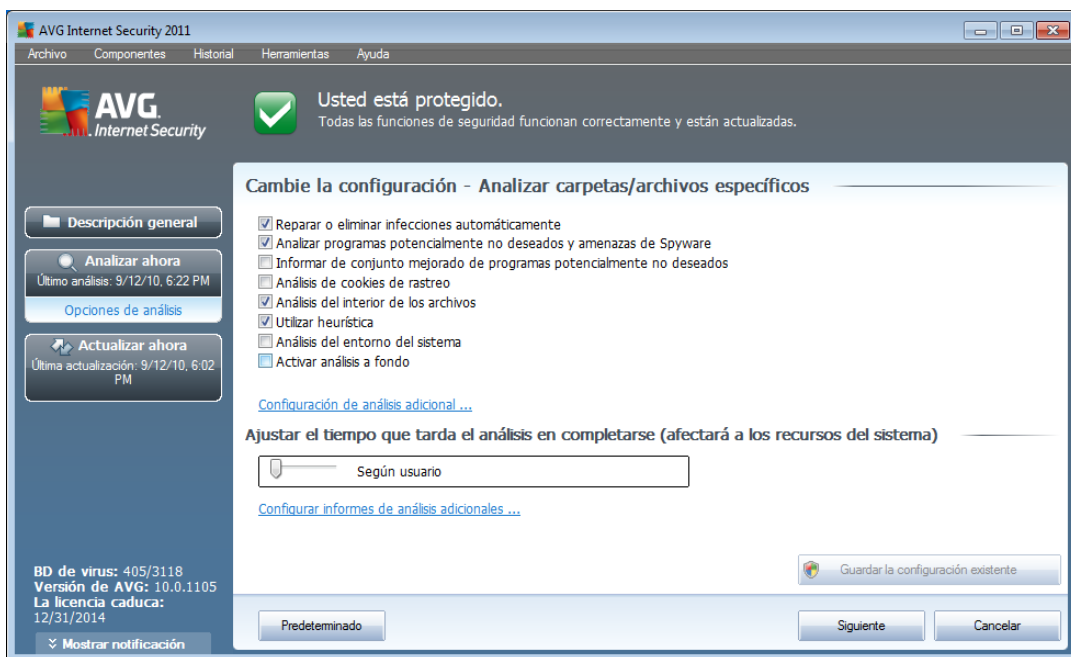
También existe la posibilidad de analizar una carpeta determinada y, a la vez, excluir de este análisis sus subcarpetas; para ello, escriba un signo menos "-" delante de la ruta generada automáticamente (*consulte la captura de pantalla*). Para excluir toda la carpeta del análisis utilice el parámetro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

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



## Edición de la configuración de análisis

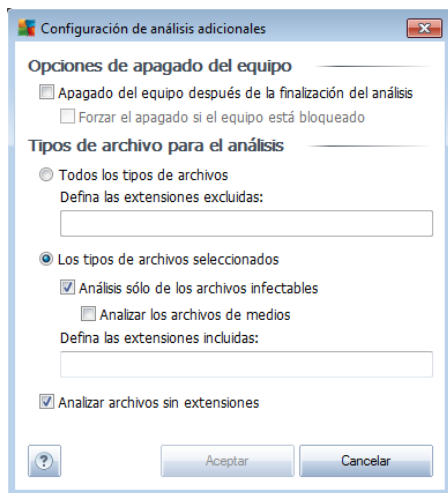
Tiene la opción de editar la configuración predeterminada predefinida del **Análisis de archivos o carpetas específicos**. Presione el vínculo **Cambiar la configuración de análisis** para ir al cuadro de diálogo **Cambiar configuración de análisis de archivos o carpetas específicos**. **Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.**



- **Parámetros de análisis:** en la lista de parámetros de análisis puede activar o desactivar parámetros según sea necesario:
  - **Reparar o eliminar infecciones automáticamente** (activado de manera predeterminada): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si hay una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la **Bóveda de virus**.
  - **Analizar programas potencialmente no deseados y amenazas de Spyware** (activada de forma predeterminada): seleccione esta opción para activar el motor **Anti-Spyware** y analizar en busca de spyware así como de virus. **El spyware** representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
  - **Informar conjunto mejorado de programas potencialmente no deseados** (desactivada de forma predeterminada): seleccione esta

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

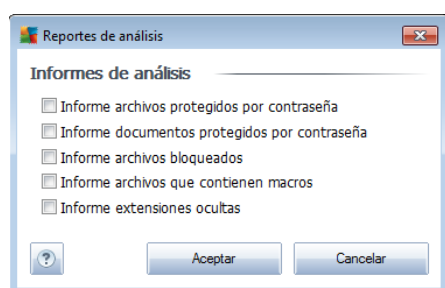
- **Analizar cookies de rastreo** (*desactivado de manera predeterminada*): este parámetro del componente [Anti-Spyware](#) define que las cookies deben detectarse; (*las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de su carrito de compras electrónico*).
- **Analizar el interior de los archivos** (*activado de manera predeterminada*): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos (por ejemplo, ZIP, RAR...).
- **Utilizar heurística** (*desactivado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.
- **Analizar el entorno del sistema** (*desactivado de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- **Activar análisis a fondo** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Configuración de análisis adicionales**: el vínculo abre un nuevo cuadro de diálogo **Configuración de análisis adicionales**, donde puede especificar los siguientes parámetros:



- **Opciones de apagado del equipo:** decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (**Apagado del equipo después de la finalización del análisis**), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (**Forzar el apagado si el equipo está bloqueado**).
- **Defina los tipos de archivo para el análisis:** será conveniente decidir si desea analizar:
  - **Todos los tipos de archivos** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;
  - **Tipos de archivos seleccionados:** puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.
  - De manera opcional, puede decidir si desea **Analizar archivos sin extensiones:** esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.
- **Prioridad del proceso de análisis:** puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De forma predeterminada, la prioridad se establece al nivel medio (*Análisis automático*), que optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma

alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

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



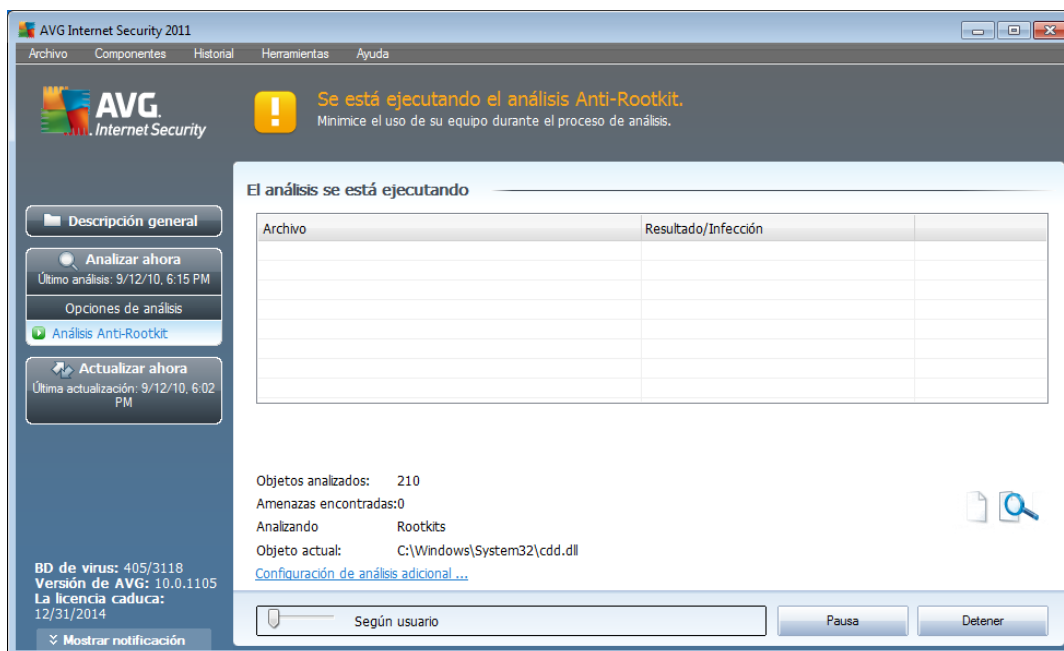
**Advertencia:** estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo [Análisis de AVG/Programación de análisis/Cómo analizar](#). Si decide cambiar la configuración predeterminada del **Análisis de archivos o carpetas específicos** puede guardar la nueva configuración como la predeterminada que se usará para todos los análisis de archivos o carpetas específicos posteriores. Asimismo, esta configuración se utilizará como plantilla para todos los nuevos análisis programados ([todos los análisis personalizados se basan en la configuración actual del análisis de archivos o carpetas específicos](#)).

### 11.2.3. Análisis Anti-Rootkit

El **Análisis Anti-Rootkit** busca en el equipo algún posible rootkit (*programas y tecnologías que puedan ocultar actividades de malware en su equipo*). Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

### Ejecución de análisis

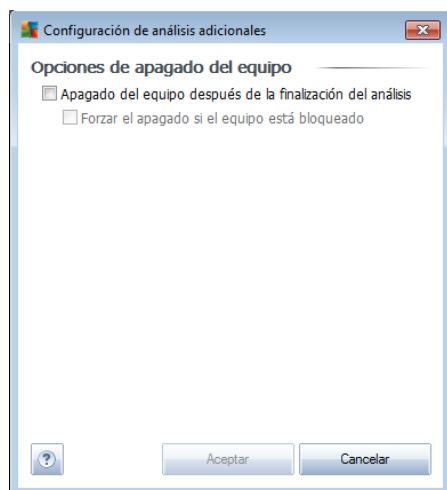
**El análisis Anti-Rootkit** se puede ejecutar directamente desde la [interfaz de análisis](#) haciendo clic en el icono del análisis. No se deben configurar más parámetros específicos para este tipo de análisis; el análisis empezará inmediatamente en el cuadro de diálogo **El análisis se está ejecutando** (*consulte la captura de pantalla*). El análisis puede interrumpirse temporalmente (**Pausar**) o se puede cancelar (**Detener**) si es necesario.



## Edición de la configuración de análisis

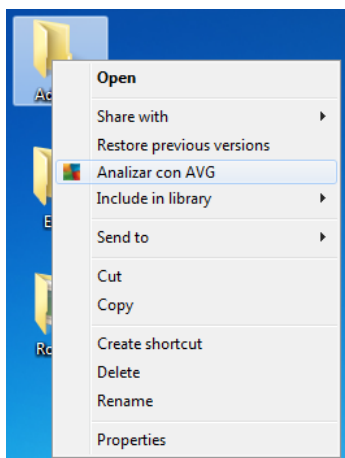
**El análisis Anti-Rootkit** siempre se ejecuta en la configuración predeterminada, y la edición de los parámetros de análisis sólo es accesible en el cuadro de diálogo [Configuración avanzada de AVG/Anti-Rootkit](#). En la interfaz de análisis, dispone de la configuración siguiente, pero sólo mientras se está ejecutando el análisis:

- **Análisis automático:** puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De forma predeterminada, la prioridad se establece al nivel medio (*Análisis automático*), que optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).
- **Configuración de análisis adicional:** este vínculo abre un nuevo cuadro de diálogo **Configuración de análisis adicional** en el cual se pueden definir condiciones posibles de apagado del equipo relacionadas con el **Análisis Anti-Rootkit** (**Apagado del equipo después de la finalización del análisis, posiblemente Forzar el apagado si el equipo está bloqueado**):



### 11.3. Análisis en el Explorador de Windows

Además de los análisis predefinidos ejecutados para todo el equipo o sus áreas seleccionadas, **AVG Internet Security 2011** también ofrece la opción de análisis rápido de un objeto específico directamente en el entorno del Explorador de Windows. Si desea abrir un archivo desconocido y no está seguro de su contenido, puede analizarlo a pedido. Siga estos pasos:



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





#### 11.4. Análisis desde línea de comandos

En **AVG Internet Security 2011** existe la opción de realizar el análisis desde la línea de comandos. Puede utilizar esta opción, por ejemplo, en servidores, o bien al crear un script por lotes que se ejecutará automáticamente una vez reiniciado el equipo. Desde la línea de comandos, puede ejecutar el análisis con la mayoría de los parámetros ofrecidos en la interfaz gráfica de usuario de AVG.

Para ejecutar el análisis de AVG desde la línea de comandos, ejecute el siguiente comando en la carpeta donde se encuentra instalado AVG:

- **avgscanx** para SO de 32 bits
- **avgscana** para SO de 64 bits

#### Sintaxis del comando

La sintaxis del comando es la siguiente:

- **avgscanx /parámetro** ... p. ej., **avgscanx /comp** para analizar todo el equipo
- **avgscanx /parámetro /parámetro** .. al utilizar varios parámetros, estos deben alinearse en una fila y separarse mediante un espacio y un signo de barra
- si un parámetro requiere que se proporcione un valor específico (p. ej., el parámetro **/scan** requiere información sobre qué áreas seleccionadas del equipo se deben analizar, por lo que debe proporcionar una ruta de acceso exacta hasta la sección seleccionada), los valores se separan mediante punto y coma, por ejemplo: **avgscanx /scan=C:\;D:\**

#### Parámetros del análisis

Para mostrar una descripción completa de los parámetros disponibles, escriba el comando respectivo junto con el parámetro **/?** o **/HELP** (por ejemplo, **avgscanx /?**). El único parámetro obligatorio es **/SCAN** para especificar cuáles áreas del equipo se deben analizar. Para obtener una explicación más detallada de las opciones, consulte la [descripción general de los parámetros de la línea de comandos](#).

Para ejecutar el análisis, presione **Intro**. Durante el análisis, puede detener el proceso mediante **Ctrl+C** o **Ctrl+Pausa**.

#### Análisis desde CMD iniciado desde la interfaz gráfica

Cuando ejecuta su equipo en el modo seguro de Windows, existe también la posibilidad de iniciar el análisis desde la línea de comandos desde la Interfaz gráfica de usuario. El



análisis en sí mismo se iniciará desde la línea de comandos, el diálogo **Compositor de línea de comandos** sólo le permite especificar la mayoría de los parámetros de análisis en la comodidad de la interfaz gráfica.

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

#### 11.4.1. Parámetros del análisis desde CMD

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

- **/SCAN** [Analizar carpetas o archivos específicos](#) /SCAN=ruta de acceso;ruta de acceso (por ejemplo /SCAN=C:\;D:\)
- **/COMP** [Análisis de todo el equipo](#)
- **/HEUR** Utilizar análisis heurístico\*\*\*
- **/EXCLUDE** Excluir ruta de acceso o archivos del análisis
- **/@** Archivo de comandos /nombre de archivo/
- **/EXT** Analizar estas extensiones /por ejemplo EXT=EXE,DLL/
- **/NOEXT** No analizar estas extensiones /por ejemplo NOEXT=JPG/
- **/ARC** Analizar archivos
- **/CLEAN** Borrar automáticamente
- **/TRASH** Mover los archivos infectados a la bóveda de virus\*\*\*
- **/QT** Análisis rápido
- **/MACROW** Notificar macros
- **/PWDW** Notificar archivos protegidos por contraseña
- **/IGNLOCKED** Omitir archivos bloqueados
- **/REPORT** Informar a archivo /nombre de archivo/
- **/REPAPPEND** Anexar al archivo de reporte
- **/REPOK** Notificar archivos no infectados como correctos
- **/NOBREAK** No permitir la anulación mediante CTRL+BREAK
- **/BOOT** Activar la comprobación de MBR/BOOT



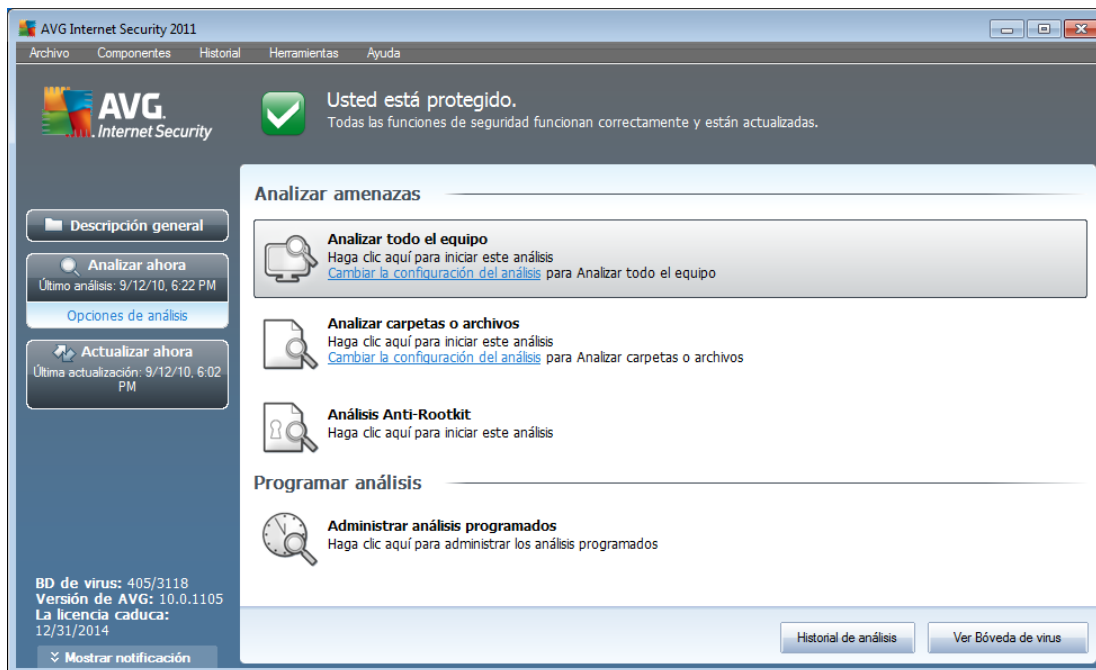
- **/PROC** Analizar los procesos activos
- **/PUP** Informar "[Programas potencialmente no deseados](#)"
- **/REG** Analizar el registro
- **/COO** Analizar cookies
- **/?** Mostrar ayuda sobre este tema
- **/HELP** Visualizar ayuda sobre este tema
- **/PRIORITY** Establecer prioridad de análisis /Baja, Automática, Alta/  
(consulte [Configuración avanzada/Análisis](#))
- **/SHUTDOWN** Apagar el equipo después de la finalización del análisis
- **/FORCESHUTDOWN** Forzar el apagado del equipo tras la finalización del análisis
- **/ADS** Analizar flujo de datos alternos (sólo NTFS)
- **/ARCBOMBSW** Informar archivos recomprimidos

### 11.5. Programación de análisis

Con **AVG Internet Security 2011** puede ejecutar el análisis a pedido (por ejemplo cuando sospecha que se ha arrastrado una infección a su equipo) o según un plan programado. Es muy recomendable ejecutar el análisis basado en una programación: de esta manera puede asegurarse de que su equipo está protegido contra cualquier posibilidad de infección, y no tendrá que preocuparse de si y cuándo ejecutar el análisis.

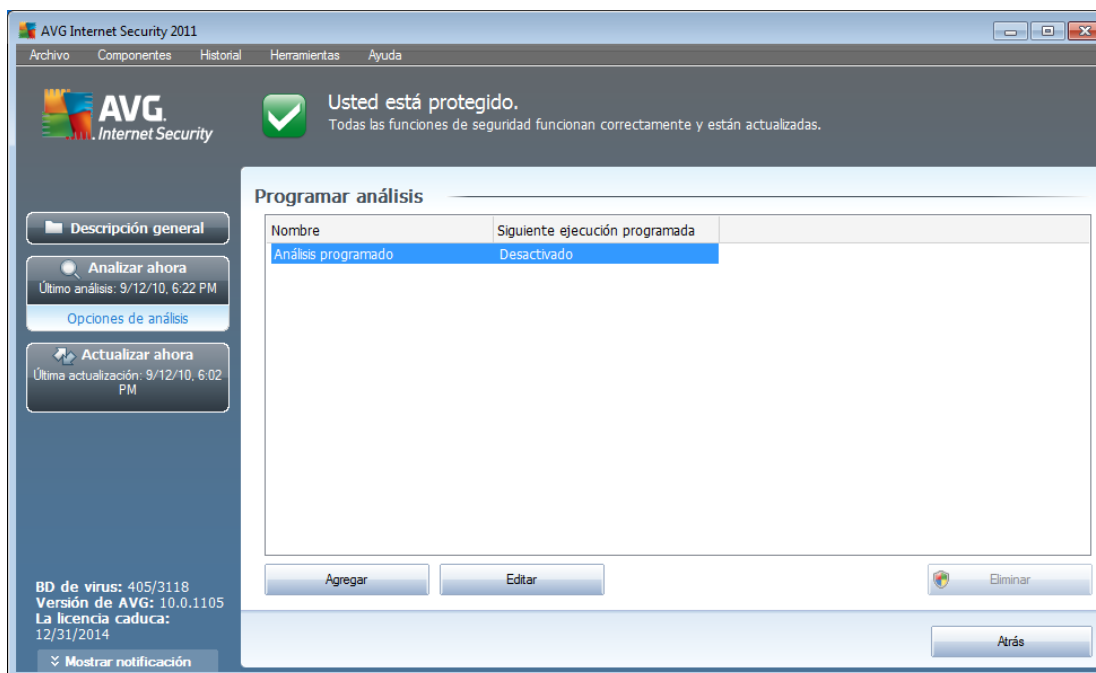
Se debe ejecutar el [Análisis de todo el equipo](#) periódicamente, al menos una vez a la semana. Sin embargo, si es posible, ejecute el análisis de todo su equipo diariamente, como está establecido en la configuración predeterminada de programación del análisis. Si el equipo siempre está encendido, se pueden programar los análisis fuera del horario de trabajo. Si el equipo algunas veces está apagado, se puede programar que los análisis ocurran [durante un arranque del equipo, cuando no se haya ejecutado la tarea](#).

Para crear nuevas programaciones de análisis, consulte la [interfaz de análisis de AVG](#) y encuentre la sección en la parte inferior llamada **Programación de análisis**:



## Programar análisis

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



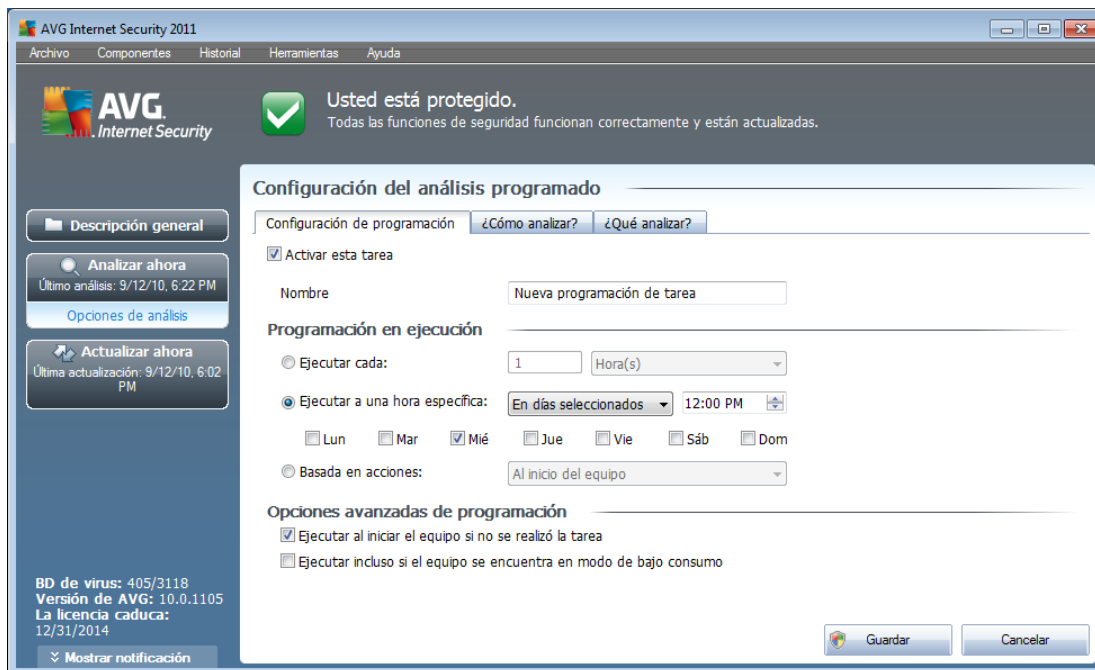


Puede editar o agregar análisis utilizando los siguientes botones de control:

- **Agregar programación de análisis:** el botón abre el cuadro de diálogo **Configuración del análisis programado** en la pestaña **Configuración de programación**. En este cuadro de diálogo puede especificar los parámetros del análisis recientemente definido.
- **Editar la programación de análisis:** este botón sólo se puede emplear si ha seleccionado previamente un análisis existente en la lista de análisis programados. En ese caso el botón aparece como activo y puede hacer clic en él para ir al cuadro de diálogo **Configuración del análisis programado**, pestaña **Configuración de programación**. Los parámetros del análisis seleccionado ya están especificados aquí y se pueden editar.
- **Eliminar la programación de análisis:** este botón también está activo si ha seleccionado previamente un análisis existente en la lista de análisis programados. Este análisis se puede eliminar de la lista presionando el botón de control. Sin embargo, sólo puede eliminar sus propios análisis; la **Programación de análisis de todo el equipo** predefinida dentro de la programación predeterminada nunca se puede eliminar.
- **Atrás:** permite volver a la [interfaz de análisis de AVG](#)

### 11.5.1. Configuración de programación

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



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

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

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

En este cuadro de diálogo puede definir con mayor detalle los siguientes parámetros del análisis:

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



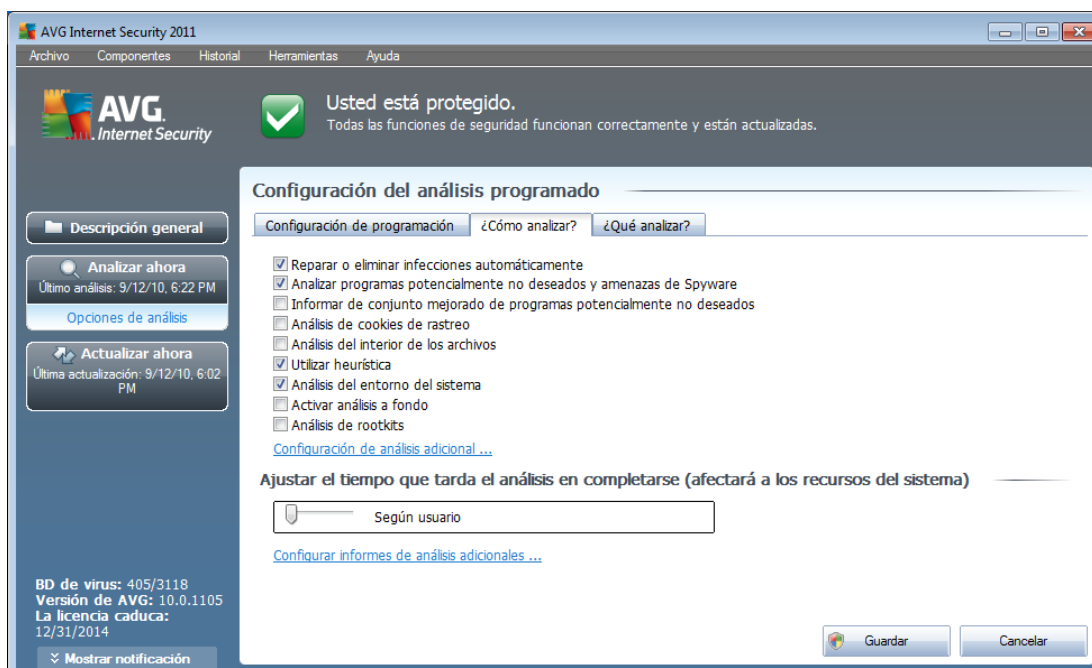
de alimentación baja o totalmente apagado.

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

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

- **Guardar:** guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al [cuadro de diálogo predeterminado de la interfaz de análisis de AVG](#). Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después que haya especificado todos los requisitos.
- **Cancelar:** cancela los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al [cuadro de diálogo predeterminado de la interfaz de análisis de AVG](#).

### 11.5.2. Cómo analizar



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



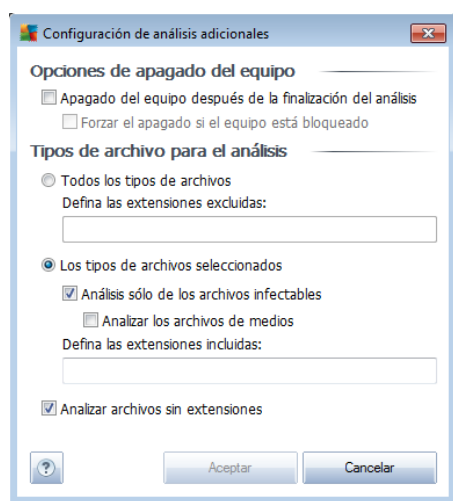
- **Reparar o eliminar infecciones automáticamente** (*activada de forma predeterminada*): si se identifica un virus durante el análisis, se puede reparar automáticamente si existe una cura disponible. Si no se puede reparar automáticamente el archivo infectado o decide desactivar esta opción, cada vez que se detecte un virus se le avisará y tendrá que decidir qué hacer con la infección detectada. El método recomendado consiste en eliminar el archivo infectado a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (*activada de forma predeterminada*): seleccione esta opción para activar el motor [Anti-Spyware](#) y analizar en busca de spyware así como de virus. [El spyware](#) representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar conjunto mejorado de programas potencialmente no deseados** (*desactivada de forma predeterminada*): seleccione esta opción para detectar un paquete extendido de [spyware](#), es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Analizar cookies de rastreo** (*desactivado de forma predeterminada*): este parámetro del componente [Anti-Spyware](#) define que las cookies deben detectarse durante el análisis (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica acerca de los usuarios, como los sitios que prefieren o el contenido de sus carritos de compra electrónicos*).
- **Analizar el interior de los archivos** (*desactivado de forma predeterminada*): este parámetro define que el análisis debe comprobar todos los archivos, incluso aquellos que se encuentran comprimidos dentro de algún tipo de archivo, por ejemplo, ZIP, RAR, ...
- **Utilizar heurística** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.
- **Analizar el entorno del sistema** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- **Activar análisis a fondo** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.



- **Análisis de rootkits** (*desactivado de forma predeterminada*): seleccione este elemento si desea incluir la detección de rootkits en el análisis de todo el equipo. La detección de rootkits también está disponible de forma independiente en el componente [Anti-Rootkit](#).

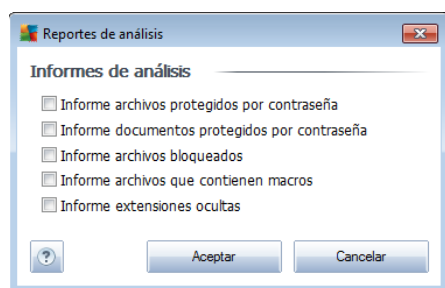
A continuación, puede cambiar la configuración de análisis de la siguiente manera:

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



- **Opciones de apagado del equipo**: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (**Apagado del equipo después de la finalización del análisis**), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (**Forzar el apagado si el equipo está bloqueado**).
- **Defina los tipos de archivo para el análisis**: debe decidir si desea analizar:
  - **Todos los tipos de archivos** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;
  - **Los tipos de archivos seleccionados**: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

- De manera opcional, puede decidir si desea **Analizar archivos sin extensiones**: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.
- **Ajustar el tiempo que tarda el análisis en completarse**: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. El nivel medio optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).
- **Configurar informes de análisis adicionales**: el vínculo abre un nuevo cuadro de diálogo **Informes de análisis**, donde puede seleccionar de qué tipos de posibles hallazgos se debería informar:



**Nota:** De manera predeterminada, la configuración del análisis está programada para un rendimiento óptimo. A menos que se tenga una razón válida para cambiar la configuración del análisis, se recomienda encarecidamente que se mantenga la configuración predefinida. Sólo los usuarios experimentados pueden llevar a cabo cambios en la configuración. Para las opciones adicionales de configuración del análisis, consulte el cuadro de diálogo [Configuración avanzada](#) disponible través del elemento del menú del sistema **Archivo/Configuración avanzada**.

## Botones de control

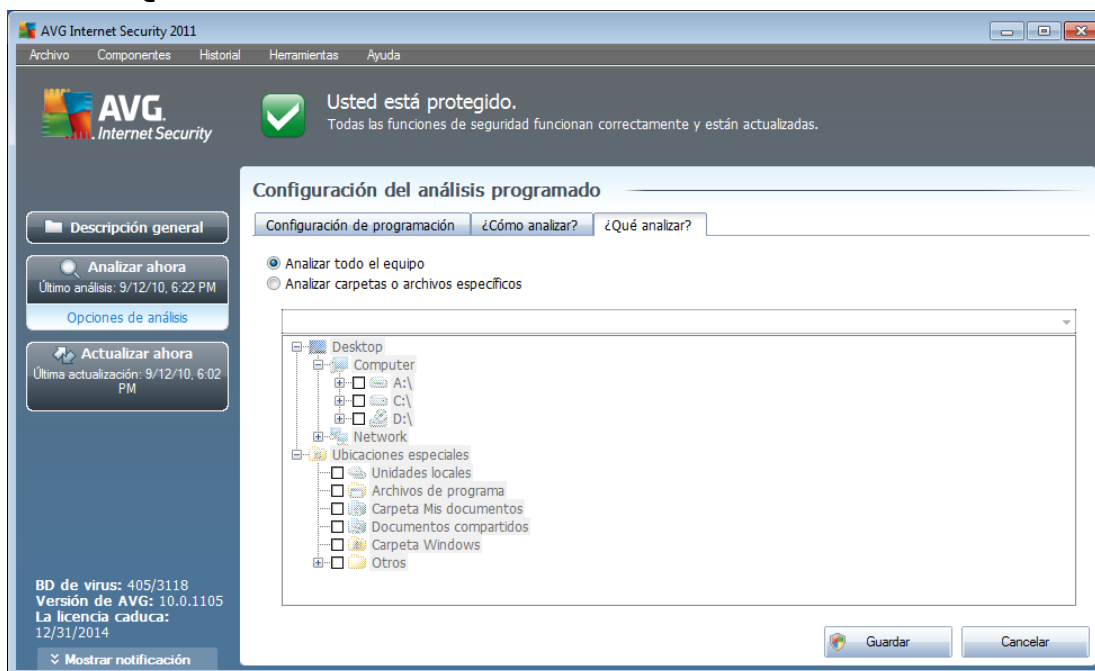
Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo **Configuración del análisis programado** ([Configuración de programación](#), [¿Cómo analizar?](#) y [¿Qué analizar?](#)) y tienen el mismo funcionamiento sin importar en cuál pestaña se encuentre:

- **Guardar**: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al [cuadro de diálogo predeterminado de la interfaz de análisis de AVG](#). Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después que haya especificado todos los requisitos.



- **Cancelar:** cancela los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al [cuadro de diálogo predeterminado de la interfaz de análisis de AVG](#).

### 11.5.3. Qué analizar



En la pestaña **Qué analizar** puede definir si desea programar el [análisis de todo el equipo](#) o el [análisis de archivos o carpetas específicos](#).

Si selecciona analizar archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activará la estructura de árbol visualizada y podrá especificar las carpetas que se analizarán (*expanda los elementos haciendo clic en el nodo "más" hasta que encuentre la carpeta que desea analizar*). Puede seleccionar varias carpetas, seleccionando las casillas respectivas. Las carpetas seleccionadas aparecerán en el campo de texto en la parte superior del cuadro de diálogo, y el menú desplegable mantendrá el historial de análisis seleccionados para uso posterior. De manera alternativa, puede introducir manualmente la ruta de acceso completa a la carpeta deseada (*si introduce varias rutas de acceso, es necesario separarlas con punto y coma, sin espacios*).

En la estructura de árbol también puede ver una rama denominada **Ubicaciones especiales**. A continuación encontrará una lista de ubicaciones que se analizarán si se marca la casilla de verificación correspondiente:

- **Unidades locales:** todas las unidades de disco duro de su equipo
- **Archivos de programa**
  - C:\Program Files\



- en la versión de 64 bits C:\Program Files (x86)

- **Carpeta Mis documentos**

- para Windows XP: C:\Documents and Settings\Default User\My Documents\  
Documents\
  - para Windows Vista/7: C:\Users\user\Documents\  
Documents\

- **Documentos compartidos**

- para Windows XP: C:\Documents and Settings\All Users\Documents\  
Documents\
  - para Windows Vista/7: C:\Users\Public\Documents\  
Documents\

- **Carpeta de Windows:** C:\Windows\  
Windows\

- **Otros**

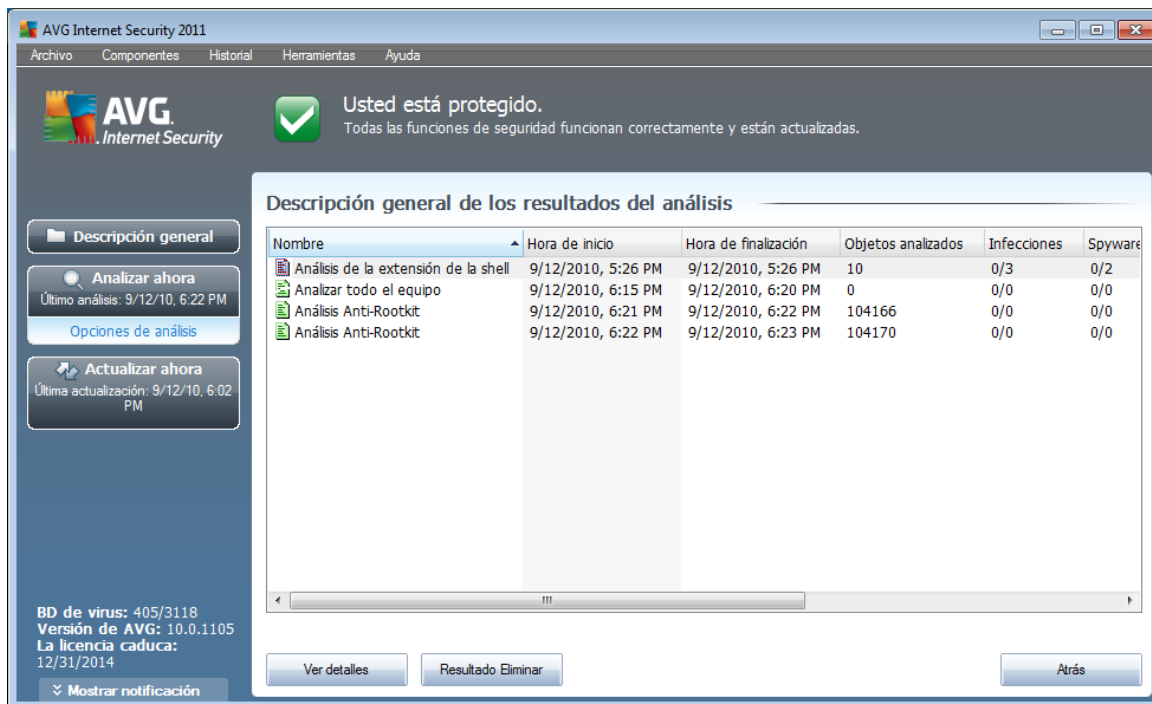
- *Unidad del sistema:* el disco duro en el cual está instalado el sistema operativo (normalmente C:)
- *Carpeta del sistema:* C:\Windows\System32\  
System32\
- *Carpeta de archivos temporales:* C:\Documents and Settings\User\Local\Temp\  
(Windows XP); o C:\Users\user\AppData\Local\Temp\  
(Windows Vista/7)
- *Archivos temporales de Internet:* C:\Documents and Settings\User\Local Settings\Temporary Internet Files\  
(Windows XP); o C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

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

Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo **Configuración del análisis programado** ([Configuración de programación](#), [¿Cómo analizar?](#) y [¿Qué analizar?](#), y tienen el mismo funcionamiento sin importar en qué pestaña se encuentre:


- **Guardar:** guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al [cuadro de diálogo predeterminado de la interfaz de análisis de AVG](#). Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después de haber especificado todos los requisitos.
- **Cancelar:** cancela los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al [cuadro de diálogo predeterminado de la interfaz de análisis de AVG](#).


## 11.6. Descripción general de los resultados del análisis




El diálogo **Descripción general de los resultados del análisis** está disponible desde la [interfaz de análisis de AVG](#) a través del botón **Historial de análisis**. El diálogo proporciona una lista de todos los análisis ejecutados anteriormente y la información de sus resultados:

- **Nombre:** designación del análisis; puede ser el nombre de uno de los [análisis predefinidos](#) o un nombre que le haya dado a [su propio análisis programado](#). Cada nombre incluye un icono que indica el resultado del análisis.

 - el icono verde indica que durante el análisis no se detectó ninguna infección

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

 - el icono rojo indica que durante el análisis se detectó una infección y que no se pudo eliminar

Cada icono puede ser sólido o cortado a la mitad: los iconos sólidos representan un análisis que se completó y finalizó adecuadamente; el icono cortado a la mitad significa que el análisis se canceló o se interrumpió.

**Nota:** para obtener información detallada sobre cada análisis, consulte el diálogo [Resultados del análisis](#) disponible a través del botón **Ver detalles** (en la parte inferior de este diálogo).



- **Hora de inicio:** fecha y hora en que se inició el análisis
- **Hora de finalización:** fecha y hora en que finalizó el análisis
- **Objetos analizados:** número de objetos que se verificaron durante el análisis
- **Infecciones:** número de [infecciones de virus](#) detectadas/eliminadas
- **Spyware :** número de [spyware](#) detectados/eliminados
- **Advertencias:** número de [objetos sospechosos detectados](#)
- **Rootkits:** número de [rootkits detectados](#)
- **Información de registros del análisis :** información relacionada con el curso y el resultado del análisis (normalmente sobre su finalización o interrupción)

### Botones de control

Los botones de control para el diálogo **Descripción general de los resultados del análisis** son:

- **Ver detalles:** presione este botón para pasar al cuadro de diálogo [Resultados del análisis](#) para ver la información detallada sobre el análisis seleccionado
- **Eliminar resultado:** presione este botón para eliminar el elemento seleccionado de la descripción general de resultados
- **Atrás:** regresa al diálogo predeterminado de la [interfaz de análisis de AVG](#)

### 11.7. Detalles de los resultados del análisis

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

El diálogo está dividido en varias pestañas:

- **Descripción general de los resultados:** esta pestaña se visualiza en todo momento y proporciona los datos estadísticos que describen el progreso del análisis.
- **Infecciones:** esta pestaña se visualiza sólo si durante el análisis se detectó una [infección de virus](#).
- **Spyware:** esta pestaña se visualiza sólo si durante el análisis se detectó un [spyware](#).
- **Advertencias:** esta pestaña se muestra si, por ejemplo, se detectaron cookies



durante el análisis

- **Rootkits**: esta pestaña se visualiza sólo si durante el análisis se detectaron [rootkits](#).
- **Información**: esta pestaña se visualiza sólo si se detectaron algunas amenazas potenciales pero no se pudieron clasificar en ninguna de las categorías anteriores; entonces la pestaña proporciona un mensaje de advertencia del hallazgo. También se mostrará información sobre objetos que no pudieron analizarse (por ejemplo, archivos protegidos por contraseña).

### 11.7.1. Pestaña Descripción general de los resultados

The screenshot shows the AVG Internet Security 2011 interface. At the top, it says "Usted está protegido." (You are protected). Below that, the "Resultados del análisis" (Analysis Results) section is active. It shows a summary table for "Infecciones" (Infections) and "Spyware".

|             | Encontrado | Eliminado y reparado | No eliminados o reparados |
|-------------|------------|----------------------|---------------------------|
| Infecciones | 3          | 0                    | 3                         |
| Spyware     | 2          | 0                    | 2                         |

Below the table, it lists the folders analyzed: "Carpetas seleccionadas para el análisis: C:\Users\User.PC10\Desktop\Adware; C:\Users\User.PC10\Desktop\Eicar; C:\Users\User.PC10\Desktop\...". It also shows the start and end times of the analysis, the total number of objects analyzed (10), and the user who initiated the scan (User).

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

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

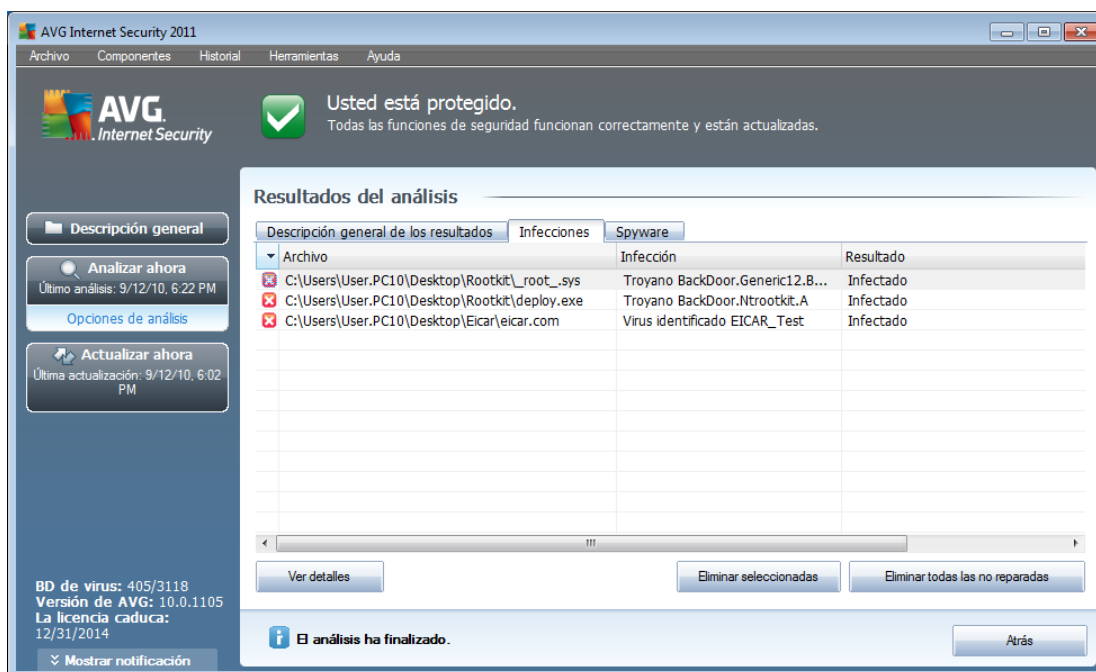
También encontrará información sobre la fecha y la hora exactas de la ejecución del análisis, el número total de objetos analizados, la duración del análisis y el número de errores que se han producido durante el análisis.

### Botones de control



En este diálogo, solo hay un botón de control disponible. El botón **Cerrar resultados** permite volver al diálogo [Descripción general de los resultados del análisis](#).

### 11.7.2. Pestaña Infecciones



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

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

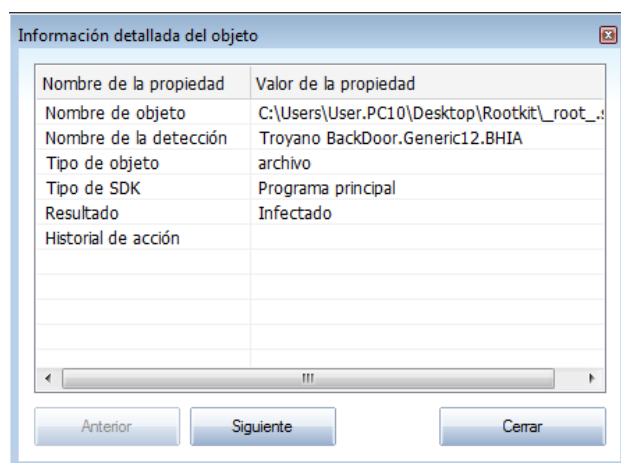


- **Agregado a excepciones de PUP:** el hallazgo se ha evaluado como una excepción y se ha agregado a la lista de excepciones de PUP (configurada en el cuadro de diálogo [Excepciones de PUP](#) en la configuración avanzada)
- **Archivo bloqueado, no analizado :** el objeto correspondiente está bloqueado,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

## Botones de control

Hay tres botones de control disponibles en este cuadro de diálogo:

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



En este cuadro de diálogo puede encontrar información detallada sobre el objeto infeccioso detectado (*por ejemplo, el nombre y la ubicación del objeto infectado, el tipo de objeto, el tipo de SDK, el resultado de la detección y el historial de acciones relativas al objeto detectado*). Mediante los botones **Anterior/Siguiente** puede ver información sobre hallazgos concretos. Utilice el botón **Cerrar** para cerrar este cuadro de diálogo.

- **Eliminar seleccionadas:** utilice este botón para mover el hallazgo seleccionado a la [Bóveda de Virus](#)



- **Eliminar todas las no reparadas:** este botón elimina todos los hallazgos que no se pueden reparar ni mover a la [Bóveda de Virus](#)
- **Cerrar resultados:** termina la descripción general de información detallada y permite volver al cuadro de diálogo [Descripción general de los resultados del análisis](#).

### 11.7.3. Pestaña Spyware

The screenshot shows the AVG Internet Security 2011 interface. At the top, it says "Usted está protegido." Below that, the "Resultados del análisis" dialog is open, with the "Spyware" tab selected. The dialog contains a table with the following data:

| Archivo  | Infección         | Resultado                    |
|--|-------------------|------------------------------|
| C:\Users\User.PC10\Desktop\Adware\01210828.ex1 | Adware.Generic.IZ | Objeto potencialmente dañino |
| C:\Users\User.PC10\Desktop\Adware\01210827.ex1 | Adware.Generic.IP | Objeto potencialmente dañino |

At the bottom of the dialog, there are buttons for "Ver detalles", "Eliminar seleccionadas", and "Eliminar todas las no reparadas". A status bar at the bottom indicates "El análisis ha finalizado."

La pestaña **Spyware** sólo se visualiza en el cuadro de diálogo **Resultados del análisis** si se ha detectado [spyware](#) durante el análisis. La pestaña se divide en tres secciones que facilitan la información siguiente:

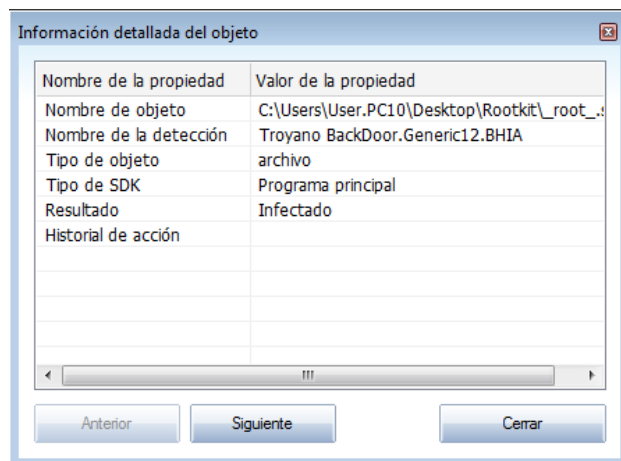
- **Archivo:** ruta completa de la ubicación original del objeto infectado.
- **Infecciones:** nombre del [spyware](#) detectado (*para obtener detalles sobre virus específicos, consulte la [Enciclopedia de Virus](#) en línea*)
- **Resultado:** define el estado actual del objeto detectado durante el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

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

## Botones de control

Hay tres botones de control disponibles en este cuadro de diálogo:

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



En este cuadro de diálogo puede encontrar información detallada sobre el objeto infeccioso detectado (*por ejemplo, el nombre y la ubicación del objeto infectado, el tipo de objeto, el tipo de SDK, el resultado de la detección y el historial de acciones relativas al objeto detectado*). Mediante los botones **Anterior/Siguiente** puede ver información sobre hallazgos concretos. Utilice el botón **Cerrar** para salir de este cuadro de diálogo.

- **Eliminar seleccionadas:** utilice este botón para mover el hallazgo



seleccionado a la [Bóveda de Virus](#)

- **Eliminar todas las no reparadas:** este botón elimina todos los hallazgos que no se pueden reparar ni mover a la [Bóveda de Virus](#)
- **Cerrar resultados:** termina la descripción general de información detallada y permite volver al cuadro de diálogo [Descripción general de los resultados del análisis](#).

#### 11.7.4. Pestaña Advertencias

La pestaña **Advertencias** muestra información sobre los objetos "sospechosos" (*normalmente archivos*) detectados durante el análisis. Una vez detectados por la [Protección residente](#), se bloquea el acceso a estos archivos. Son ejemplos típicos de este tipo de hallazgos los archivos ocultos, las cookies, las claves de registro sospechosas, los documentos o archivos protegidos mediante contraseñas, etc. Estos archivos no presentan ninguna amenaza directa a su equipo o a su seguridad. La información acerca de estos archivos es generalmente útil en caso de que se detecte un adware o un spyware en el equipo. Si sólo hay advertencias detectadas por un análisis de AVG, no es necesaria ninguna acción.

Esta es una breve descripción de los ejemplos más comunes de tales objetos:

- **Archivos ocultos:** de manera predeterminada, los archivos ocultos no son visibles en Windows, y algunos virus y otras amenazas pueden intentar evitar su detección almacenando sus archivos con este atributo. Si AVG informa acerca de un archivo oculto que sospecha que es malicioso, puede moverlo a la [Bóveda de virus AVG](#).
- **Cookies:** las cookies son archivos de texto sin formato que utilizan los sitios Web para almacenar información específica del usuario, que posteriormente se utiliza para cargar el diseño personalizado del sitio Web, rellenar previamente el nombre de usuario, etc.
- **Claves de registro sospechosas:** algunos malware almacenan su información en el registro de Windows, con el fin de asegurarse de que se cargan al iniciar el equipo o para prolongar su efecto en el sistema operativo.

#### 11.7.5. Pestaña Rootkits

La pestaña **Rootkits** muestra información sobre los rootkits detectados durante el análisis si ha iniciado el [Análisis Anti-Rootkit](#).

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



esconder archivos o datos del sistema al sistema operativo.

La estructura de esta pestaña es básicamente la misma que la de la [pestaña Infecciones](#) o la [pestaña Spyware](#).

### 11.7.6. Pestaña Información

La pestaña **Información** contiene datos sobre los "hallazgos" que no se pueden clasificar como infecciones, spyware, etc. No se pueden etiquetar positivamente como peligrosos pero, sin embargo, merecen su atención. El análisis de AVG puede detectar archivos que quizás no están infectados pero que son sospechosos. Estos archivos se notifican como [Advertencia](#) o como **Información**.

La **Información** de severidad se puede notificar por uno de los siguientes motivos:

- **Tiempo de ejecución comprimido:** el archivo fue comprimido con uno de los empaquetadores de tiempo de ejecución menos comunes, algo que puede indicar un intento de evitar el análisis de dicho archivo. No obstante, no todos los reportes de dicho archivo indican la existencia de un virus.
- **Tiempo de ejecución comprimido recursivo:** parecido al anterior, pero menos frecuente en software común. Estos archivos son sospechosos y se debería tener en cuenta la posibilidad de eliminarlos o someterlos a un análisis.
- **Archivo o documento protegido por contraseña:** AVG no puede analizar los archivos protegidos por contraseña (*ni cualquier otro programa anti-malware en general*).
- **Documento con macros:** el documento notificado contiene macros, que pueden ser maliciosos.
- **Extensión oculta:** los archivos con la extensión oculta pueden aparentar que son, por ejemplo, imágenes, pero en realidad son archivos ejecutables (*por ejemplo, imagen.jpg.exe*). La segunda extensión no es visible en Windows de forma predeterminada, y AVG reporta estos archivos para prevenir que se abran accidentalmente.
- **Ruta de acceso del archivo incorrecta:** si algún archivo importante del sistema se ejecuta desde otra ruta de acceso que no sea la predeterminada (*por ejemplo, si winlogon.exe se ejecuta desde otra carpeta que no sea Windows*), AVG notifica esta discrepancia. En algunos casos, los virus utilizan nombres de procesos estándar del sistema para hacer que su presencia sea menos aparente en el sistema.
- **Archivo bloqueado:** el archivo notificado está bloqueado, por lo que AVG no puede analizarlo. Esto suele significar que el sistema utiliza un archivo constantemente (*por ejemplo, un archivo swap*).



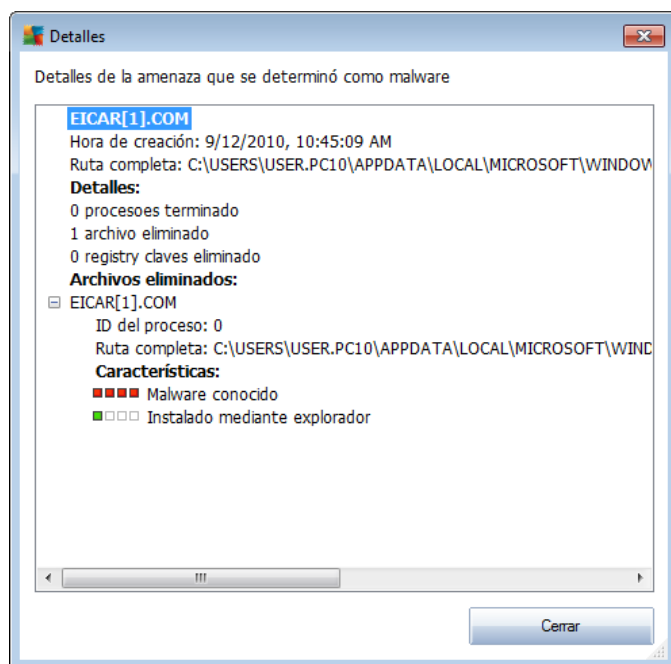


- **Nombre del objeto original:** todos los objetos detectados listados en la tabla se han etiquetado con el nombre estándar dado por AVG durante el proceso de análisis. Si el objeto tenía un nombre original específico que es conocido (*por ejemplo el nombre de un dato adjunto de correo electrónico que no responde al contenido real del dato adjunto*), se proporcionará en esta columna.
- **Fecha de almacenamiento:** fecha y hora en que se ha detectado el archivo sospechoso y se ha eliminado a la **Bóveda de Virus**.

### Botones de control

Se puede tener acceso a los botones de control siguientes desde la interfaz de la **Bóveda de Virus**:

- **Restaurar:** devuelve el archivo infectado a su ubicación original en el disco.
- **Restaurar como:** si decide mover el objeto infeccioso detectado de la **Bóveda de virus** hacia una carpeta seleccionada, utilice este botón. El objeto sospechoso y detectado se guardará con su nombre original. Si el nombre original no se conoce, se utilizará el nombre estándar.
- **Detalles:** este botón sólo se aplica a las amenazas detectadas por **Identity Protection**. Al hacer clic, aparece una descripción general de los detalles de la amenaza (*archivos o procesos que se han visto afectados, características del proceso, etc.*). Observe que para los elementos que no hayan sido detectados por IDP, este botón aparece en gris y está inactivo!



- **Eliminar:** elimina el archivo infectado de la **Bóveda de virus** de forma total e



irreversible.

- **Vaciar bóveda:** elimina todo el contenido de la **Bóveda de virus** permanentemente. Al eliminar los archivos de la **Bóveda de Virus**, estos archivos se borran del disco de forma irreversible (*no se transfieren a la Papelera de reciclaje*).





## 12. Actualizaciones de AVG

**Mantener AVG actualizado es crucial para asegurar que todos los virus recién descubiertos se detecten tan pronto sea posible.**

Debido a que las actualizaciones de AVG no se publican de acuerdo con una programación fija, sino como reacción a la cantidad y severidad de las nuevas amenazas, se recomienda buscar actualizaciones al menos una vez al día o incluso con más frecuencia. Sólo de este modo puede asegurarse de que **AVG Internet Security 2011** también está actualizado durante el día.

### 12.1. Niveles de actualización

AVG permite seleccionar dos niveles de actualización:

- **Actualización de definiciones** contiene los cambios necesarios para una protección anti-virus, anti-spam y anti-malware confiable. Por lo general, no incluye cambios del código y sólo actualiza la base de datos de definiciones. Esta actualización se debe aplicar tan pronto como esté disponible.
- **Actualización del programa** contiene diferentes modificaciones, arreglos y mejoras del programa.

Al [programar una actualización](#), es posible seleccionar qué nivel de prioridad se descargará y se aplicará.

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

### 12.2. Tipos de actualización

Puede distinguir entre dos tipos de actualización:

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

### 12.3. Proceso de actualización

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



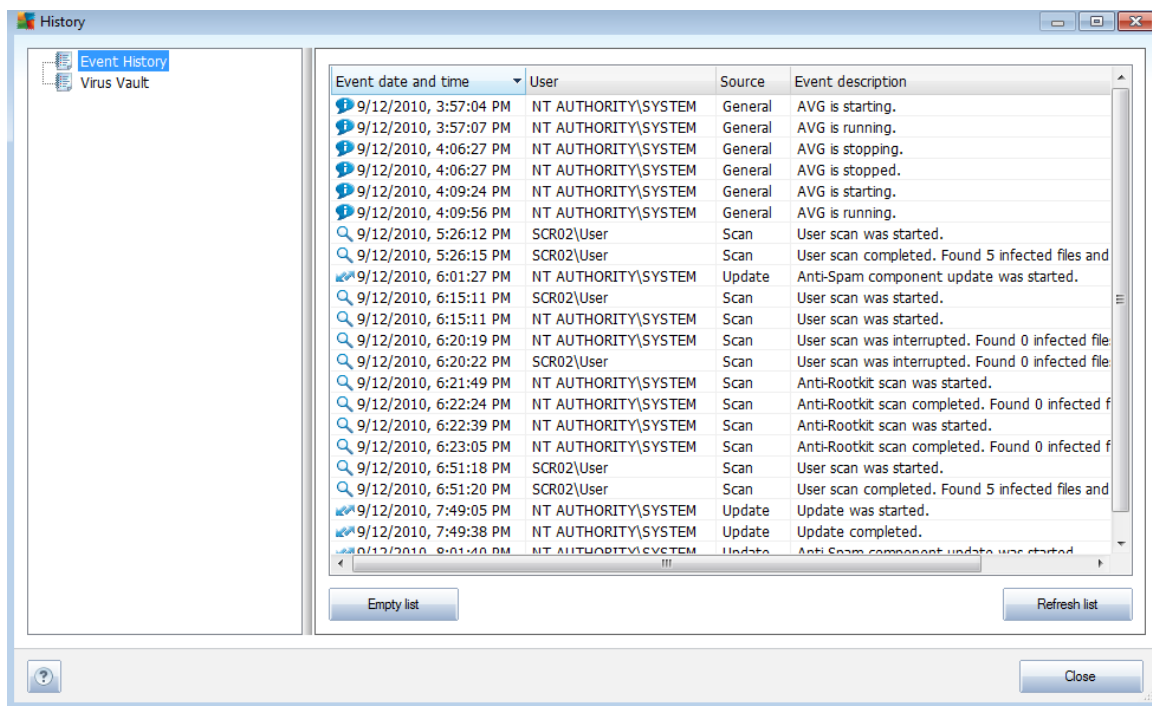
### [Administrador de actualizaciones](#) .

Una vez que se inicia la actualización, AVG verificará primero si hay nuevos archivos de actualización disponibles. De ser así, AVG empieza su descarga e inicia el proceso de actualización por sí mismo. Durante el proceso de actualización, se le enviará a la interfaz de **Actualización**, en donde puede ver una representación gráfica del progreso del proceso, así como una descripción general de los parámetros estadísticos relevantes (*tamaño del archivo actualizado, datos recibidos, velocidad de descarga, tiempo transcurrido, etc.*).

**Nota:** *antes del inicio de la actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Puede obtener acceso a esta opción mediante Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema. Recomendado sólo para usuarios avanzados.*



## 13. Historial de eventos



Se puede obtener acceso al cuadro de diálogo **Historial** desde el [menú del sistema](#), mediante el elemento **Historial/Registro de historial de eventos**. En este cuadro de diálogo puede encontrar un resumen de los eventos importantes que se han producido durante el funcionamiento de **AVG Internet Security 2011**. **Historial** registra los tipos de eventos siguientes:

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

Para cada evento, se muestra la información siguiente:

- **Fecha y hora del evento** da la fecha y hora exactas en que ocurrió el evento
- **Usuario** establece quién inició el evento
- **Origen** da el componente de origen o la otra parte del sistema AVG que desencadenó el evento



- **Descripción del evento** da un breve resumen del evento

#### **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 frecuentes y soporte técnico

Si se produce algún problema con AVG, ya sea comercial o técnico, consulte la sección ***Preguntas frecuentes*** del sitio Web de AVG (<http://www.avg.com/>).

Si no logra encontrar ayuda de esta manera, póngase en contacto con el servicio de soporte técnico a través del correo electrónico. Utilice el formulario de contacto, disponible en el menú del sistema a través de ***Ayuda/Obtener ayuda en línea***.