AVG AntiVirus

Manual del usuario

Revisión del documento AVG.05 (15/06/2016)

Contenido

1. Introducción **3**

2. Requisitos de instalación de AVG **4**

2.1 Sistemas operativos compatibles 4

2.2 Requisitos mínimos y recomendados de hardware 4

3. Proceso de instalación de AVG **5**

3.1 ¡Bienvenido! 5

3.2 Ingrese su número de licencia 6

3.3 Personalice su instalación 8

3.4 Instalación de AVG 9

3.5 Instalación finalizada 10

4. Después de la instalación **11**

4.1 Actualización de la base de datos de virus 11

4.2 Registro del producto 11

4.3 Acceso a la interfaz de usuario 11

4.4 Análisis de todo el equipo 11

4.5 Prueba Eicar 11

4.6 Configuración predeterminada de AVG 12

5. Interfaz de usuario de AVG **13**

5.1 Navegación superior 14

5.2 Información del estado de seguridad 17

5.3 Descripción general de los componentes 18

5.4 Mis aplicaciones 19

5.5 Vínculos rápidos de análisis/actualización 19

5.6 Icono en la bandeja del sistema 20

5.7 AVG Advisor 21

5.8 AVG Accelerator 22

6. Componentes de AVG **23**

6.1 Protección del equipo 23

6.2 Protección de navegación web 27

6.3 Identity Protection 28

6.4 Protección del correo electrónico 30

6.5 PC Analyzer 32

7. Configuración avanzada de AVG **34**

7.1 Apariencia 34

7.2 Sonidos 36

7.3 Desactivar temporalmente la protección de AVG 37

7.4 Protección del equipo 38

7.5 Analizador de correo electrónico 43

7.6 Protección de navegación web 54
7.7 Identity Protection 57
7.8 Análisis 58
7.9 Programaciones 64
7.10 Actualizar 71
7.11 Excepciones 75
7.12 Bóveda de virus 77
7.13 Autoprotección AVG 78
7.14 Preferencias de privacidad 78
7.15 Ignorar estado de error 80
7.16 Advisor: Redes conocidas 81

8. Análisis de AVG 82
8.1 Análisis predefinidos 84
8.2 Análisis en el Explorador de Windows 93
8.3 Análisis desde línea de comandos 93
8.4 Programación de análisis 97
8.5 Resultados del análisis 105
8.6 Detalles de los resultados del análisis 106

9. AVG File Shredder 107

10. Bóveda de virus 108

11. Historial 109
11.1 Resultados del análisis 109
11.2 Resultados de la Protección Residente 110
11.3 Resultados de Identity Protection 113
11.4 Resultados de Protección del correo electrónico 114
11.5 Configuración de Online Shield 115
11.6 Historial de eventos 117

12. Actualizaciones de AVG 118

13. Preguntas frecuentes y asistencia técnica 119

1. Introducción

Este manual de usuario proporciona documentación completa para el usuario relacionada con **AVG AntiVirus**.

AVG AntiVirus ofrece protección en tiempo real contra las amenazas más sofisticadas. Puede conversar, realizar descargas e intercambiar archivos con confianza; jugar a juegos y mirar videos sin preocupaciones o interrupciones; realizar descargas, compartir archivos y enviar mensajes de forma segura; disfrutar su vida en redes sociales, o navegar y buscar con la confianza de una protección en tiempo real.

También puede optar por utilizar otras fuentes de información:

- ***Archivo de ayuda***: Está disponible una sección de *Solución de problemas* incluida directamente en el archivo de ayuda con **AVG AntiVirus** *(para abrir el archivo de ayuda, presione la tecla F1 en cualquier cuadro de diálogo de la aplicación)*. Esta sección proporciona una lista de las situaciones que se producen con más frecuencia cuando un usuario desea obtener ayuda profesional sobre una cuestión técnica. Seleccione la situación que mejor describa el problema y haga clic en ella para abrir instrucciones detalladas que le permitan solucionarlo.

- ***Centro de soporte del sitio web de AVG***: Como alternativa, puede buscar la solución al problema en el sitio web de AVG (http://www.avg.com/). En la sección ***Soporte*** puede encontrar una descripción general de los grupos temáticos vinculados con cuestiones técnicas y de ventas, una sección estructurada de preguntas frecuentes y todos los contactos disponibles.

- ***AVG ThreatLabs***: Un sitio web específico relacionado con AVG (http://www.avg.com/about-viruses) está dirigido a cuestiones de virus y brinda una descripción general estructurada de la información relacionada con las amenazas en línea. También encontrará instrucciones sobre cómo eliminar virus y spyware y cómo mantenerse protegido.

- ***Foro de discusión***: También puede utilizar el foro de discusión de usuarios de AVG en http://community.avg.com/.

2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG AntiVirus tiene como propósito proteger las estaciones de trabajo con los siguientes sistemas operativos:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (todas las ediciones)
- Windows 7 (todas las ediciones)
- Windows 8 (todas las ediciones)
- Windows 10 (todas las ediciones)

(y posiblemente Service Packs superiores para determinados sistemas operativos)

2.2. Requisitos mínimos y recomendados de hardware

Requisitos mínimos de hardware para **AVG AntiVirus**:

- CPU Intel Pentium a 1,5 GHz o superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memoria RAM
- 1,3 GB de espacio libre en el disco duro *(para la instalación)*

Requisitos de hardware recomendados para **AVG AntiVirus**:

- CPU Intel Pentium a 1,8 GHz o superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memoria RAM
- 1,6 GB de espacio libre en el disco duro *(para la instalación)*

3. Proceso de instalación de AVG

Para instalar **AVG AntiVirus** en su equipo debe obtener el archivo de instalación más reciente. Para asegurarse de instalar la versión actualizada de **AVG AntiVirus**, se recomienda que descargue el archivo de instalación del sitio web de AVG (http://www.avg.com/). La sección ***Soporte*** proporciona una descripción general estructurada de los archivos de instalación para cada edición de AVG. Una vez que ha descargado y guardado el archivo de instalación en el disco duro, puede iniciar el proceso de instalación. La instalación es una secuencia de cuadros de diálogo sencillos y fáciles de entender. Cada cuadro de diálogo describe brevemente qué se debe hacer en cada paso del proceso de instalación. Ofrecemos una explicación detallada de cada ventana de diálogo a continuación:

3.1. ¡Bienvenido!

El proceso de instalación se inicia con el cuadro de diálogo ***Bienvenido a AVG Internet Security***:

Selección de idioma

En este cuadro de diálogo puede seleccionar el idioma que se utilizará para el proceso de instalación. Haga clic en el cuadro combinado al lado de la opción ***Idioma*** para desplegar el menú de idiomas. Seleccione el idioma que desee y el proceso de instalación seguirá en el idioma elegido. Además, la aplicación se comunicará en el idioma seleccionado, con la opción de cambiar a inglés, que siempre se instala de forma predeterminada.

Contrato de licencia de usuario final y política de privacidad

Antes de que continúe con el proceso de instalación, le recomendamos que se familiarice con los documentos ***Contrato de licencia de usuario final*** y ***Política de privacidad***. Los documentos están disponibles a través de los vínculos activos en la parte inferior del diálogo. Haga clic en cualquiera de

los hipervínculos para abrir un nuevo diálogo o una nueva ventana del navegador, que muestra íntegramente el instrumento respectivo. Lea cuidadosamente estos documentos legalmente vinculantes. Haga clic en el botón ***Continuar*** para confirmar que está de acuerdo con estos documentos.

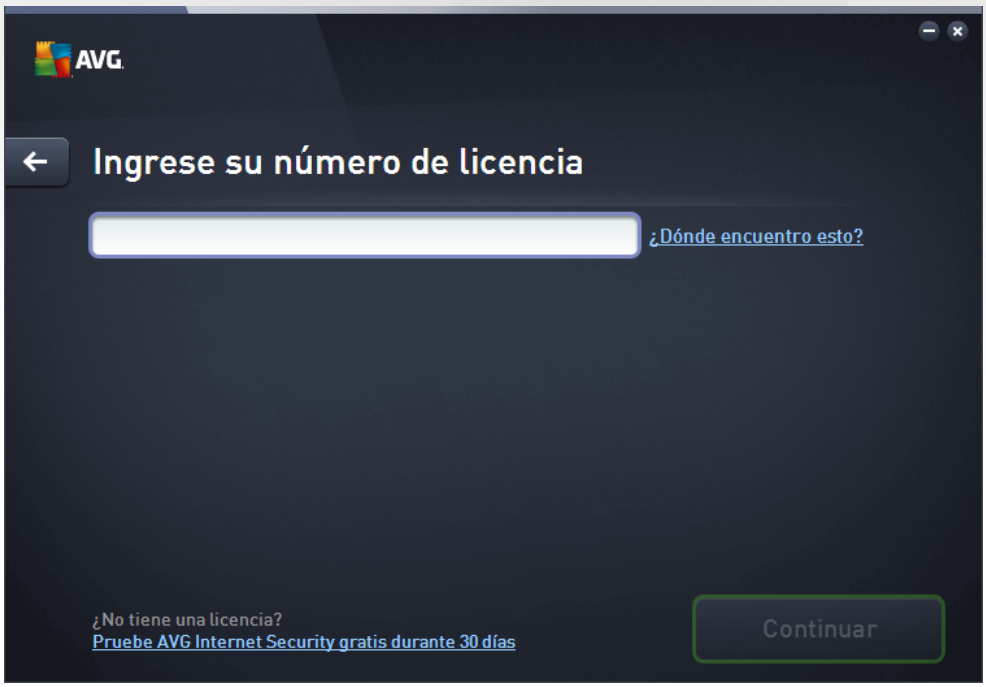
Continúe con la instalación

Para continuar con la instalación, simplemente haga clic en el botón ***Continuar***. Se le solicitará su número de licencia y, a continuación, el proceso de instalación se ejecutará en modo totalmente automático. Para la mayoría de los usuarios, se recomienda usar esta opción estándar para instalar **AVG AntiVirus** con todas las configuraciones predefinidas por el proveedor del programa. Esta configuración proporciona la máxima seguridad combinada con el uso óptimo de los recursos. En el futuro, si es necesario cambiar la configuración, siempre se puede hacer directamente en la aplicación.

De forma alternativa, existe la opción de ***Instalación personalizada***, disponible en forma de hipervínculo debajo del botón ***Continuar***. La instalación personalizada sólo la deben utilizar usuarios con experiencia que tengan un motivo importante para instalar la aplicación con una configuración distinta de la estándar (por ejemplo, para ajustarse a necesidades específicas del sistema). Si elige esta alternativa, después de ingresar su número de licencia, se lo redirigirá al cuadro de diálogo ***Personalice su instalación***, donde puede especificar su configuración.

3.2. Ingrese su número de licencia

En el diálogo ***Ingrese su número de licencia*** se lo invita a activar su licencia al escribirla *(o utilizar el método de copiar y pegar)* en el campo de texto proporcionado:



¿Dónde encuentro mi número de licencia?

El número de venta se puede encontrar en el empaquetado del CD en la caja de **AVG AntiVirus**. El número de

licencia se encuentra en el correo electrónico de confirmación que recibió después de la compra en línea de **AVG AntiVirus**. Debe escribir el número exactamente como se muestra. Si está disponible el formulario digital del número de licencia (*en el correo electrónico*), se recomienda utilizar el método de copiar y pegar para insertarlo.

Cómo utilizar el método de copiar y pegar

Si utiliza el método de ***copiar y pegar*** para especificar su número de licencia de **AVG AntiVirus** en el programa, se asegurará de que el número se introduce correctamente. Siga estos pasos:

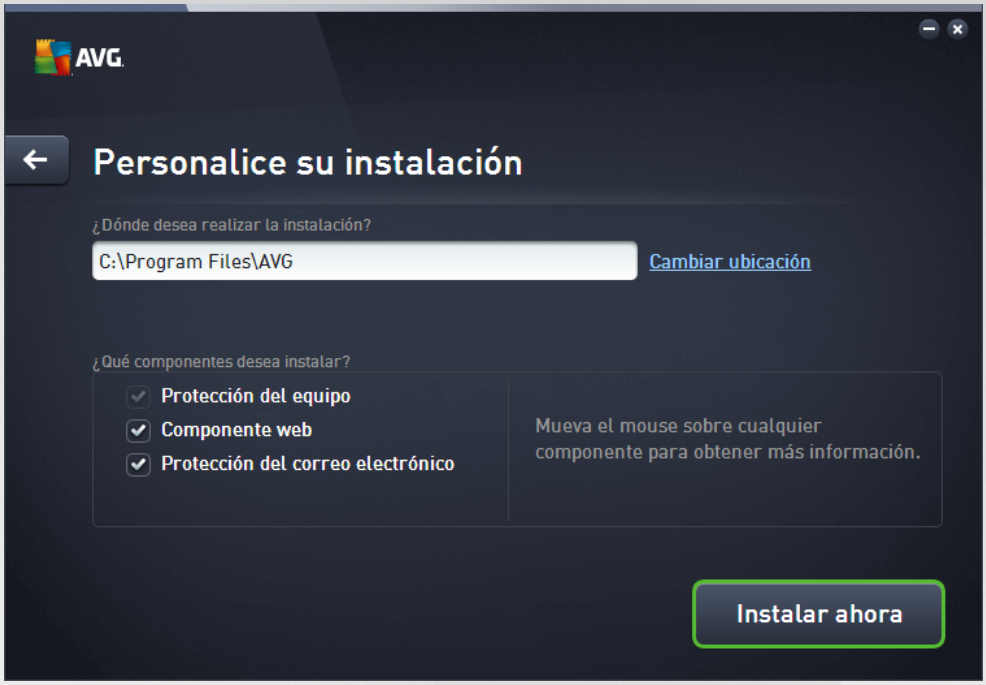
- Abra el correo electrónico que contiene su número de licencia.
- Haga clic con el botón primario del mouse al principio del número de licencia, manténgalo presionado, arrastre el mouse hasta el final del número y, entonces, suelte el botón. El número deberá quedar resaltado.
- Presione la tecla ***Ctrl***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

Continúe con la instalación

En la sección inferior del cuadro de diálogo puede encontrar el botón ***Instalar ahora***. El botón se activa al ingresar el número de licencia. Una vez activado, simplemente haga clic en el botón para iniciar el proceso de instalación. En caso de no tener un número de licencia válida disponible, puede elegir instalar la versión***AVG AntiVirus Free Edition*** de la aplicación. Lamentablemente, las ediciones gratuitas no tienen soporte para todas las funcionalidades disponibles en la versión profesional completa. Por lo tanto, puede visitar el sitio web de AVG (http://www.avg.com/) para obtener información detallada de las compras y las actualizaciones de AVG.

3.3. Personalice su instalación

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



¿Dónde desea realizar la instalación?

Aquí puede especificar dónde desea instalar la aplicación. La dirección del campo de texto lee la ubicación sugerida en la carpeta Archivos de programas. Si decide elegir otra ubicación, haga clic en el vínculo ***Cambiar ubicación*** para abrir una ventana nueva con la estructura de árbol del disco. Luego, navegue hasta la ubicación deseada y confirme.

¿Qué componentes desea instalar?

Esta sección proporciona una descripción general de todos los componentes que se pueden instalar. Si la configuración predeterminada no se adecua a sus necesidades, puede quitar componentes específicos. Sin embargo, sólo puede seleccionar entre los componentes incluidos en AVG AntiVirus. La única excepción es el componente ***Protección de la PC***, que no se puede excluir de la instalación. Cuando resalta cualquier elemento en esta sección, se mostrará una breve descripción del respectivo componente, del lado derecho. Para obtener información detallada sobre las funciones de cada componente, consulte el capítulo Descripción general de los componentes de esta documentación.

Continúe con la instalación

Para continuar con la instalación, simplemente haga clic en el botón ***Instalar ahora***. De otra manera, en caso de necesitar cambiar o verificar la configuración del idioma, puede volver un paso al cuadro de diálogo anterior con el botón de la flecha ← en la parte superior de este cuadro de diálogo.

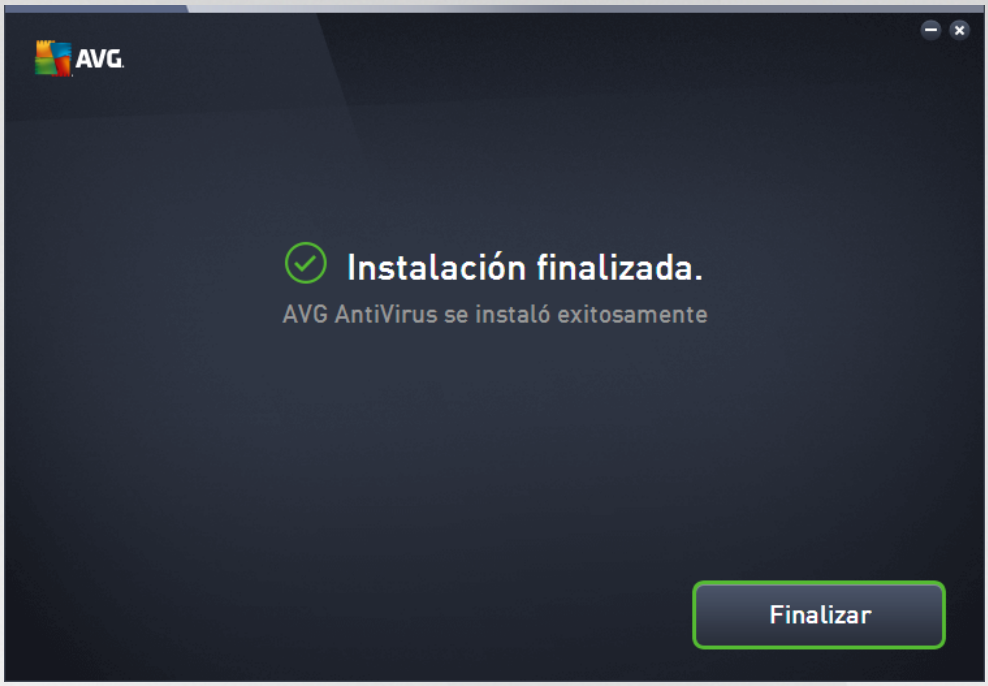
3.4. Instalación de AVG

Al confirmar el inicio de la instalación en el cuadro de diálogo anterior, el proceso de instalación se ejecuta de modo completamente automático y no requiere ninguna intervención:

una vez finalizado el proceso de instalación, se lo dirigirá al siguiente cuadro de diálogo.

3.5. Instalación finalizada

El cuadro de diálogo ***Instalación completa*** confirma que su AVG AntiVirus se instaló y configuró por completo:



haga clic en el botón ***Finalizar*** para finalizar el proceso de instalación.

4. Después de la instalación

4.1. Actualización de la base de datos de virus

Tenga en cuenta que en la instalación *(luego del reinicio del equipo, si corresponde)*, **AVG AntiVirus** actualiza su base de datos de virus automáticamente y todos los componentes y los pone en funcionamiento, lo cual puede llevarle un par de minutos. Mientras el proceso de actualización se está ejecutando, se lo notificará sobre el hecho por medio de la información que se muestra en el cuadro de diálogo principal. Espere mientras se ejecuta el proceso de actualización y tenga su **AVG AntiVirus** completamente listo para protegerlo

4.2. Registro del producto

Una vez finalizada la instalación de **AVG AntiVirus**, registre su producto en línea en el sitio web de AVG (http://www.avg.com/). Tras el registro, dispondrá de pleno acceso a la cuenta de usuario AVG, el boletín de actualizaciones de AVG y otros servicios que se ofrecen exclusivamente para los usuarios registrados. La forma más fácil de registrarse es directamente desde la interfaz del usuario de **AVG AntiVirus**. Seleccione el elemento Opciones / Inscribirse ahora en la navegación superior. Se lo dirigirá a la página ***Registro*** en el sitio web de AVG (http://www.avg.com/). Siga las instrucciones proporcionadas en la página.

4.3. Acceso a la interfaz de usuario

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

- haga doble clic en el icono del AVG AntiVirus sistema
- haga doble clic en el icono AVG Protection del escritorio
- desde el menú *Inicio / Todos los programas / AVG / AVG Protection*

4.4. 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 AntiVirus**. Por esta razón debe ejecutar un Análisis de todo el equipo para estar seguro de que no hay infecciones en su equipo. El primer análisis puede tardar un tiempo *(alrededor de una hora)* pero es recomendable ejecutarlo para asegurar de que su equipo no se alteró por una amenaza. Para obtener instrucciones sobre la ejecución de un Análisis de todo el equipo consulte el capítulo Análisis de AVG.

4.5. Prueba Eicar

Para confirmar que **AVG AntiVirus** se instaló correctamente, puede realizar la prueba EICAR.

El análisis EICAR es un método estándar y absolutamente seguro que se utiliza para comprobar el funcionamiento de un sistema antivirus. 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"). Puede descargar el virus EICAR del sitio web www.eicar.com. Allí también encontrará toda la información necesaria relacionada con el análisis EICAR.

Intente descargar el archivo eicar.com y guárdelo en el disco local. Inmediatamente después de confirmar la descarga del archivo de prueba, **AVG AntiVirus** reaccionará a él mediante una advertencia.

Esta notificación demuestra que AVG se ha instalado correctamente en su equipo.

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

4.6. Configuración predeterminada de AVG

La configuración predeterminada (*por ejemplo, la configuración de la aplicación inmediatamente después de la instalación*) de **AVG AntiVirus** 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.*** Si desea cambiar la configuración de AVG para que se adapte mejor a sus necesidades, vaya a Configuración avanzada de AVG: seleccione el elemento del menú principal del sistema *Opciones/ Configuración avanzada* y modifique la configuración de AVG en el cuadro de diálogo Configuración avanzada de AVG que aparece.

5. Interfaz de usuario de AVG

AVG AntiVirus abre con la ventana principal:

La ventana principal se divide en varias secciones:

- ***La navegación de la línea superior*** comprende cuatro vínculos activos alineados en la sección superior de la ventana principal *(Más de AVG, Informes, Soporte, Opciones).* Detalles >>
- ***Información del estado de seguridad*** proporciona información básica sobre el estado actual de su **AVG AntiVirus**. Detalles >>
- ***La descripción general de los componentes instalados*** puede encontrarse en una cinta horizontal de bloques en la sección central de la ventana principal. Los componentes se muestran como bloques verde claro etiquetados mediante el icono del componente respectivo, y proporcionan información sobre su estado. Detalles >>
- ***Mis aplicaciones*** se describen gráficamente en la cinta central inferior de la ventana principal y le ofrecen una descripción general de las aplicaciones complementarias a **AVG AntiVirus** que ya están instaladas en la PC o que se recomienda instalar. Detalles >>
- ***Los vínculos rápidos Analizar / Reparar / Actualizar*** están situados en la línea inferior de bloques de la ventana principal. Estos botones permiten un acceso inmediato a las funciones más importantes y de uso más frecuente de AVG. Detalles >>

Fuera de la ventana principal de **AVG AntiVirus**, hay un elemento más de control que puede usar para acceder a la aplicación:

- ***El Icono de la bandeja del sistema*** se ubica en la esquina derecha inferior del monitor *(en la bandeja del sistema)* e indica el estado actual de **AVG AntiVirus**. Detalles >>

5.1. Navegación superior

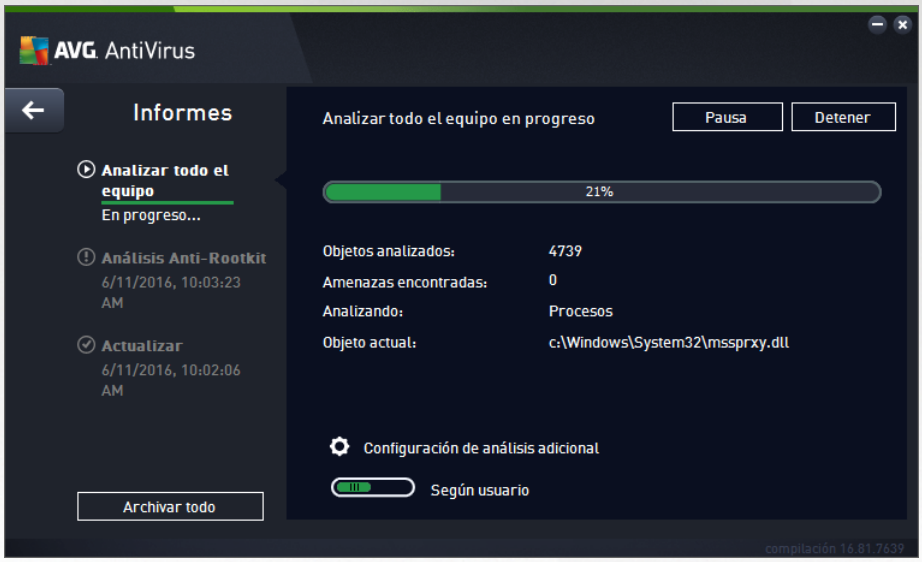
La ***navegación superior*** comprende varios vínculos activos alineados en la sección superior de la ventana principal. La navegación incluye los siguientes botones:

5.1.1. Más de AVG

Haga un solo clic en el vínculo para conectarse al sitio web de AVG y obtener toda la información sobre la protección de AVG para su máxima seguridad en internet.

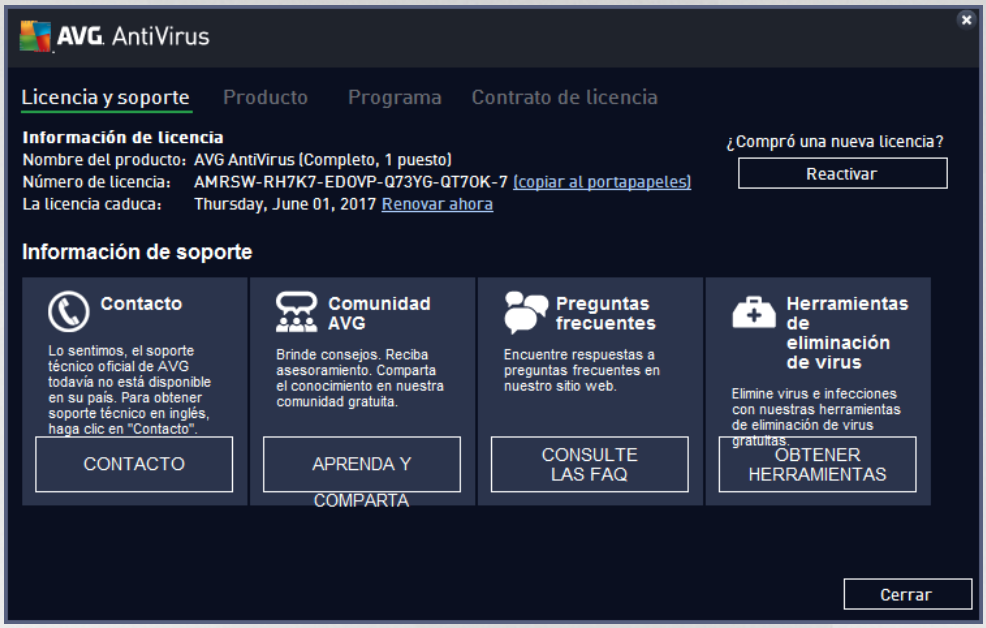
5.1.2. Informes

Abre un nuevo cuadro de diálogo ***Informes*** con una descripción general de todos los informes relevantes sobre análisis y procesos de actualización iniciados previamente. Si el análisis o la actualización se están ejecutando, se mostrará un círculo giratorio junto al texto ***Informes*** en la navegación superior de la interfaz de usuario principal. Haga clic en este círculo para ir al cuadro de diálogo que describe el progreso del proceso en ejecución:



5.1.3. Soporte

Abre un nuevo cuadro de diálogo estructurado en cuatro pestañas donde podrá encontrar información relevante sobre **AVG AntiVirus**:



- ***Licencia y soporte***: la pestaña proporciona información sobre el nombre del producto, el número de licencia y la fecha de vencimiento. En la sección inferior del cuadro de diálogo también encontrará una descripción general organizada claramente de todos los contactos disponibles para soporte al cliente. Los siguientes vínculos y botones activos están disponibles en la pestaña:

  - *(Re)Activar*: haga clic para abrir el nuevo cuadro de diálogo del ***software de activación de AVG***. Escriba su número de licencia en el campo correspondiente para reemplazar el número de venta *(que utiliza durante la instalación de AVG AntiVirus)*, o bien para cambiar el número de licencia actual por otro *(por ej., al actualizar a un producto de AVG superior)*.

  - *Copiar al portapapeles*: utilice este vínculo para copiar el número de licencia y pegarlo donde sea necesario. De esta forma puede tener la seguridad de que el número de licencia se ingrese correctamente.

  - *Renovar ahora*: le recomendamos que compre su renovación de licencia de **AVG AntiVirus** algún tiempo antes de que expire la licencia actual, al menos un mes antes. Se le notificará tiempo antes de que llegue la fecha de vencimiento. Haga clic en este vínculo para dirigirse al sitio web de AVG *(http://www.avg.com/)*, donde encontrará información detallada sobre el estado de su licencia, la fecha de vencimiento y la oferta de renovación/actualización.

- ***Producto***: la pestaña proporciona una descripción general de los datos técnicos más importantes de **AVG AntiVirus** en referencia a la información del producto de AV, los componentes instalados y la protección de correo electrónico instalada.

- ***Programa***: en esta pestaña, puede encontrar información técnica detallada acerca de la instalación de **AVG AntiVirus**, como el número de versión del producto principal y la lista de los números de versión de todos los productos correspondientes *(por ejemplo, Zen, PC TuneUp, etc.)*.
  A continuación, esta pestaña proporciona una descripción general de

todos los componentes instalados e información de seguridad específica *(números de versión de la base de datos de virus y LinkScanner)*.

- ***Contrato de licencia***: la pestaña ofrece el texto completo del contrato de licencia entre usted y AVG Technologies.

5.1.4. Opciones

Se puede acceder al mantenimiento de **AVG AntiVirus** a través del elemento ***Opciones***. Haga clic en la flecha para abrir el menú desplegable:

- ***Analizar la PC***: realiza un análisis de la PC completa.
- ***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 la PC.
- ***Analizar archivo...***: le permite ejecutar una evaluación a pedido sobre un único archivo específico. Haga clic en esta opción para abrir una nueva ventana con la estructura de árbol de su disco. Seleccione el archivo deseado y confirme la ejecución del análisis.
- ***Actualizar***: ejecuta automáticamente el proceso de actualización de **AVG AntiVirus**.
- ***Actualizar desde directorio...***: ejecuta el proceso de actualización desde los archivos de actualización ubicados en una carpeta específica en el disco local. Sin embargo, esta opción sólo se recomienda en casos de emergencia, como en situaciones en que no existe una conexión a internet disponible (por ejemplo, la PC se encuentra infectada y está desconectada de internet, la PC está conectada 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.
- ***Bóveda de virus***: abre la interfaz para el espacio de cuarentena, la Bóveda de virus, hacia donde AVG deriva todas las infecciones detectadas. Los archivos infectados se aíslan dentro de esta cuarentena, garantizando la seguridad de la PC, y al mismo tiempo se guardan los archivos infectados para repararlos en el futuro si existe la posibilidad.
- ***Historial***: ofrece otras opciones de submenú específicas:
  - *Resultados del análisis*: abre un cuadro de diálogo que proporciona una descripción general de los resultados del análisis.
  - *Resultados de la Protección Residente*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por la Protección Residente.
  - *Resultados de Identity Protection*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por el componente Identidad.
  - *Resultados de la Protección del correo electrónico*: abre un cuadro de diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente Protección del correo electrónico.
  - *Resultados de Online Shield*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por Online Shield.

- o *Registro de historial de eventos*: abre la interfaz del registro del historial de todas las acciones de **AVG AntiVirus** registradas.

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

- ***Contenidos de ayuda***: abre los archivos de ayuda de AVG.

- ***Obtener soporte***: abre el cuadro de diálogo de soporte que proporciona toda la información accesible de soporte y los contactos.

- ***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 del sitio web de AVG (http://www.avg.com/), donde puede buscar información detallada acerca del virus identificado.

- ***(Re)activar***: abre el cuadro de diálogo de activación y muestra el número de licencia que proporcionó durante el proceso de instalación. Dentro de este cuadro de diálogo puede editar el número de licencia para reemplazar el número de venta (*el cual instaló con AVG*) o para reemplazar el número de licencia antiguo (*p. ej., cuando se actualiza a un nuevo producto AVG*).
  Si utiliza la versión de prueba de **AVG AntiVirus**, los dos últimos elementos aparecen como ***Comprar ahora*** y ***Activar***, con lo que puede comprar la versión completa del programa inmediatamente. Para **AVG AntiVirus** instalado con un número de venta, los elementos aparecen como ***Registrar*** y ***Activar***:

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

- ***Acerca de AVG***: abre un nuevo cuadro de diálogo con cuatro pestañas que proporcionan datos sobre la licencia adquirida y el soporte accesible, información del producto y del programa y el texto completo del contrato de licencia. *(El mismo cuadro de diálogo puede abrirse mediante el enlace de Soporte de la navegación principal).*

5.2. Información del estado de seguridad

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

: El icono verde indica que su ***AVG AntiVirus está completamente operativo***. Su equipo está totalmente protegido, actualizado y todos los componentes instalados funcionan correctamente.

: El icono amarillo indica que ***uno o más componentes están configurados de manera incorrecta*** y debería prestar atención a su configuración o a sus propiedades. No hay problemas críticos en **AVG AntiVirus** y probablemente ha optado por desactivar un componente por alguna razón. Aún está protegido. Sin embargo, preste atención a la configuración de los componentes con problemas. El componente configurado incorrectamente se mostrará con

una cinta naranja de advertencia en la interfaz de usuario principal.

El icono amarillo aparece también si, por algún motivo, ha decidido ignorar el estado de error del componente. La opción ***Ignorar estado de error*** está disponible en la sección Configuración avanzada / Ignorar estado de error. Allí tendrá la opción de expresar que es consciente del estado de error del componente pero que, por alguna razón, desea conservar su **AVG AntiVirus** de esta manera y no desea que se le advierta al respecto. Puede ser necesario utilizar esta opción en una situación específica, pero es muy recomendable desactivar la opción ***Ignorar el estado de error*** a la mayor brevedad posible.

De forma alternativa, el icono amarillo también se mostrará si su **AVG AntiVirus** requiere reiniciar el equipo (***es necesario reiniciar***). Preste atención a esta advertencia y reinicie su equipo.

 : El icono naranja indica que ***AVG AntiVirus se encuentra en estado crítico***.
Uno o más componentes no funcionan correctamente y **AVG AntiVirus** no pueden 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 AntiVirus no esté configurado para un rendimiento óptimo, aparece un nuevo botón llamado Haga clic para reparar (de forma alternativa, Haga clic para 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 AntiVirus para un rendimiento óptimo y alcanzar el máximo nivel de seguridad.

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

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

5.3. Descripción general de los componentes

La ***descripción general de los componentes instalados*** puede encontrarse en una cinta horizontal de bloques en la sección central de la ventana principal. Los componentes se muestran como bloques verde claro etiquetados con el icono del componente respectivo. Cada bloque proporciona información sobre el estado actual de la protección. Si el componente está configurado correctamente y funciona en su totalidad, la información se indica en letras verdes. Si el componente se detiene, su funcionalidad es limitada o el componente está en estado de error, se le notificará mediante un texto de advertencia que se muestra en un campo de texto naranja. ***Se recomienda estrictamente que preste atención a la configuración del componente respectivo.***

Mueva el mouse sobre el componente para que aparezca un texto breve en la parte inferior de la ventana principal. El texto proporciona una introducción elemental a la funcionalidad del componente. Además, informa sobre su estado actual y especifica los servicios del componente que no están configurados correctamente.

Lista de componentes instalados

En **AVG AntiVirus,** la sección ***Descripción general de los componentes*** cuenta con información acerca de

los siguientes componentes:

- ***Equipo***: Este componente cubre dos servicios: ***AntiVirus Shield*** detecta virus, spyware, gusanos, troyanos, archivos ejecutables no deseados o bibliotecas dentro de su sistema y le brinda protección contra adware malicioso. ***Anti-Rootkit*** analiza rootkits peligrosos ocultos dentro de aplicaciones, controladores o bibliotecas. Detalles >>
- ***Navegación Web***: le brinda protección contra ataques basados en la Web mientras busca y navega por Internet. Detalles >>
- ***Identidad***: el componente ejecuta el servicio ***Identity Shield***, que brinda protección constante a los activos digitales contra amenazas nuevas y desconocidas en internet. Detalles >>
- ***Correos electrónicos***: comprueba sus mensajes de correo electrónico entrantes para detectar SPAM y bloquea virus, ataques de phishing u otras amenazas. Detalles >>

Acciones accesibles

- ***Mueva el mouse sobre el icono de cualquier componente*** para resaltarlo en la vista general de componentes. Simultáneamente aparece una descripción de las funciones básicas del componente en la parte inferior de la interfaz de usuario.
- ***Haga un solo clic en el icono del componente*** para abrir la propia interfaz del componente con la información sobre su estado actual, además de acceder a su configuración y datos estadísticos.

5.4. Mis aplicaciones

En el área ***Mis aplicaciones*** *(la línea de bloques verdes debajo del conjunto de componentes)* podrá encontrar una descripción general de otras aplicaciones de AVG ya instaladas en su equipo o que se recomienda instalar. Los bloques se muestran condicionalmente, y pueden representar cualquiera de las siguientes aplicaciones:

- ***Protección para dispositivos móviles*** es una aplicación que protege su teléfono celular de virus y malware. También le ofrece la posibilidad de seguir su smartphone de forma remota si en algún momento se separa de él.
- ***La aplicación PC Tuneup*** es una herramienta avanzada para el análisis y la corrección detallados del sistema, respecto a cómo podría mejorarse la velocidad y el rendimiento general de la PC.

Para obtener información detallada sobre cualquiera de las aplicaciones de ***Mis aplicaciones***, haga clic en el bloque correspondiente. Se lo dirigirá a la página web de AVG dedicada, donde también puede descargar el componente de forma inmediata.

5.5. Vínculos rápidos de análisis/actualización

Los ***Vínculos rápidos*** están ubicados en la línea inferior de botones de la interfaz de usuario de **AVG AntiVirus**. Estos vínculos le permiten un acceso inmediato a las funciones más importantes y de uso más común de la aplicación, es decir, análisis y actualizaciones. Los vínculos rápidos están disponibles en todos los cuadros de diálogo de la interfaz del usuario:

- ***Analizar ahora***: El botón está gráficamente dividido en dos secciones. Siga el vínculo ***Analizar ahora*** para iniciar Analizar todo el equipo de inmediato, y supervise su progreso y resultados en la ventana Informes que se abre automáticamente. El botón ***Opciones*** abre el cuadro de diálogo ***Opciones de análisis*** donde puede administrar análisis programados y editar parámetros de Analizar todo el equipo / Analizar carpetas o archivos. *(Para obtener información detallada, consulte el capítulo Análisis de AVG)*

- ***Reparar rendimiento****:* El botón lo dirige al servicio ***PC Analyzer***, una herramienta avanzada para un análisis y una corrección detallados del sistema con el fin de mejorar la velocidad y el rendimiento general de su equipo.

- ***Actualizar ahora***: Presione el botón para iniciar la actualización inmediata del producto. Se le informará de los resultados de la actualización en el cuadro de diálogo deslizante situado sobre el icono del sistema AVG. *(Para obtener información detallada, consulte el capítulo Actualizaciones de AVG)*

5.6. Icono en la bandeja del sistema

El icono del sistema de AVG (en la barra de tareas de Windows, esquina inferior derecha del monitor) indica el estado actual de su **AVG AntiVirus**. Está visible en todo momento en el sistema, tanto si la interfaz de usuario de su **AVG AntiVirus**

Visualización del icono de la bandeja del sistema de AVG

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

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

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

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

Información del icono de la bandeja del sistema de AVG

El icono del sistema de AVG también lo informa acerca de las actividades actuales dentro de su **AVG**

AntiVirus y los posibles cambios de estado en el programa (p. ej., inicio automático de un análisis o una actualización programados, cambio de estado de un componente, ocurrencia de estado de error, etc.) a través de una ventana emergente que se abre desde el icono del sistema.

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

El icono del sistema de AVG se puede utilizar también como vínculo de acceso rápido a la interfaz de usuario de **AVG AntiVirus**; simplemente haga doble clic en el icono. Al hacer clic con el botón secundario en el icono se abre un pequeño menú contextual con las opciones siguientes:

- Abrir AVG: haga clic aquí para abrir la interfaz del usuario de **AVG AntiVirus**.
- Desactivar temporalmente la protección de AVG: la opción le permite desactivar la protección completa que usted realizó **AVG AntiVirus** anteriormente. Recuerde que no debe usar esta opción si no es absolutamente necesario. En la mayoría de los casos, no es necesario desactivar antes **AVG AntiVirus** de instalar nuevo software o controladores, ni siquiera si el instalador o el asistente de software le sugiere que cierre los programas y aplicaciones que se estén ejecutando para asegurarse de que no se producen interrupciones no deseadas durante el proceso de instalación. Si tiene que desactivar temporalmente **AVG AntiVirus**, debe volver a activarlo en cuanto termine. Si está conectado a Internet o a una red durante el tiempo que el software antivirus está desactivado, su equipo será vulnerable ante los ataques.
- Análisis: haga clic aquí para abrir el menú contextual de análisis predefinidos (Análisis de todo el equipo y Análisis de archivos/carpetas) y seleccione el análisis que corresponda; se iniciará inmediatamente.
- Análisis en ejecución... este elemento se muestra solo 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. Están disponibles también las siguientes acciones: Establecer prioridad para todos los análisis, Pausar todos los análisis o Detener todos los análisis.
- Reparar rendimiento: haga clic para ejecutar el componente PC Analyzer.
- Iniciar sesión en AVG MyAccount: Abre la página principal de MyAccount, donde puede administrar sus productos de suscripción, comprar protección adicional, descargar archivos de instalación, comprobar pedidos y facturas anteriores, y administrar su información personal.
- Actualizar ahora: Inicia inmediatamente una actualización.
- Ayuda: Abre el archivo de ayuda de la página de inicio.

5.7. AVG Advisor

AVG Advisor ha sido diseñado para detectar problemas que podrían poner su PC en riesgo y para recomendar una acción que solucione la situación. ***AVG Advisor*** es visible en forma de un cuadro de diálogo emergente que se desliza sobre la bandeja del sistema. El servicio detecta una posible ***red desconocida con un nombre familiar***. Esto por lo general solo se aplica a los usuarios que se conectan a varias redes, comúnmente con equipos portátiles: Si una red nueva y desconocida tiene el mismo nombre que una red conocida utilizada con frecuencia *(por ejemplo, Casa o MiWifi)*, se puede crear confusión y puede conectarse sin intención a una red completamente desconocida y potencialmente insegura. ***AVG Advisor*** puede evitar esto advirtiéndole que el nombre conocido se refiere en realidad a una red nueva. Por supuesto,

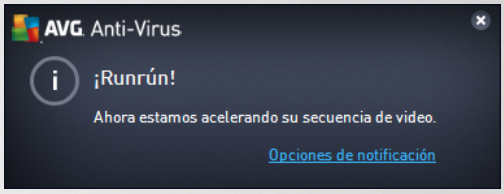
si decide que la red desconocida es segura, puede guardarla en la una lista de ***AVG Advisor*** de redes conocidas de modo que no se informe nuevamente.

Exploradores web compatibles

La característica funciona con los siguientes exploradores web: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

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



6. Componentes de AVG

6.1. Protección del equipo

El componente Equipo cubre dos servicios de seguridad principales: AntiVirus y Caja fuerte de datos:

- AntiVirus comprende un motor de análisis que protege todos los archivos, las áreas del sistema de la PC y los medios removibles (disco flash, etc.) y realiza análisis en busca de virus conocidos. Los virus detectados se bloquearán para que no puedan realizar ninguna acción y después se limpiarán o pondrán en la Bóveda de virus. Ni siquiera advertirá el proceso, dado que esta protección residente se ejecuta "en segundo plano". AntiVirus también usa el análisis heurístico, donde los archivos se analizan en busca de características comunes de virus. Esto significa que AntiVirus puede detectar un virus nuevo y desconocido si éste contiene algunas características típicas de los virus ya existentes. **AVG AntiVirus** también puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas dentro del sistema (distintas clases de spyware, adware, etc.). Además, AntiVirus analiza el registro de su sistema para comprobar si posee entradas sospechosas y archivos temporales de Internet, y le permite tratar todos esos elementos potencialmente no deseados de la misma manera en la que trata cualquier otra infección.

- La Caja Fuerte de Datos le permite crear bóvedas virtuales seguras para almacenar datos de valor o confidenciales. Los contenidos de la Caja Fuerte de Datos están encriptados y protegidos con una contraseña de su elección para que nadie pueda acceder a ellos sin autorización.

Controles del cuadro de diálogo

Para alternar entre ambas secciones del cuadro de diálogo, basta con que haga clic en cualquier lugar del panel de servicios respectivo. El panel luego se resalta en una sombra más clara de azul. En ambas secciones del cuadro de diálogo puede encontrar los siguientes controles. Su funcionalidad es la misma, ya sea que pertenezcan a un servicio de seguridad o a otro (AntiVirus o Caja Fuerte de Datos):

 Habilitado / Deshabilitado: el botón puede recordarle a un semáforo, tanto en

su apariencia como en su funcionalidad. Haga un solo clic para alternar entre dos posiciones. El color verde significa Habilitado, que implica que el servicio de seguridad AntiVirus está activo y completamente funcional. El color rojo representa el estado Desactivado; es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, se recomienda estrictamente que conserve la configuración predeterminada para todos los ajustes de seguridad. La configuración predeterminada garantiza el óptimo rendimiento de la aplicación, y su máxima seguridad. Si, por algún motivo, desea desactivar el servicio, se le advertirá acerca del posible riesgo de manera inmediata mediante el signo rojo Advertencia y la información de que no posee protección completa en ese momento. Tenga en cuenta que debe activar el servicio otra vez tan pronto sea posible.

Configuración: haga clic en el botón para redireccionarse a la interfaz de configuración avanzada. De forma precisa, el cuadro de diálogo respectivo se abre y le permite configurar el servicio seleccionado, es decir, AntiVirus. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus**, pero solamente se recomienda que lo hagan usuarios experimentados.

Flecha: utilice la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal con la descripción general de los componentes.

Cómo crear su caja de seguridad de datos

En la sección Caja Fuerte de Datos del cuadro de diálogo Protección de Equipos puede encontrar el botón Crear Caja Fuerte. Haga clic en el botón para abrir un nuevo cuadro de diálogo del mismo nombre, donde pueda especificar los parámetros de su caja fuerte planificada. Complete toda la información necesaria y siga las instrucciones que figuran en la aplicación:

Primero, debe especificar el nombre de la caja fuerte y crear una contraseña segura:

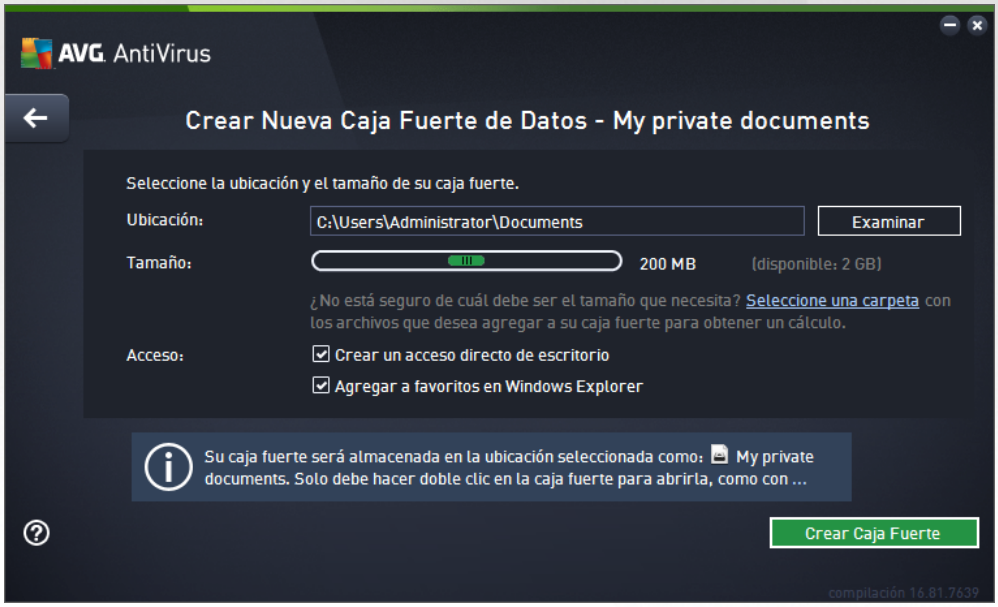
- Nombre de la caja fuerte: para crear una nueva caja fuerte de datos, primero debe elegir un nombre de caja fuerte adecuado, que pueda reconocer. Si comparte la PC con familiares, puede optar por incluir su nombre, así como también una indicación de los contenidos de seguridad, por ejemplo,

Correos electrónicos de papá.

- Crear contraseña / Volver a escribir la contraseña: cree una contraseña para su caja fuerte de datos y escríbala en los campos de texto respectivos. El indicador gráfico de la derecha le informará si su contraseña es débil (si es relativamente fácil de descifrar con herramientas especiales de software) o segura. Es recomendable elegir una contraseña con un nivel intermedio de seguridad. Puede hacer que su contraseña sea más segura incluyendo letras mayúsculas, números y otros caracteres como puntos, guiones, etc. Si quiere asegurarse de que escribió la contraseña correspondiente, puede marcar la casilla Mostrar contraseña (por supuesto, nadie más debe estar mirando su pantalla).

- Pista contraseña: también le recomendamos que cree una pista útil para recordar la contraseña, que le recuerde cuál es su contraseña, en caso de que la olvide. Recuerde que una Caja Fuerte de Datos está diseñada para mantener sus archivos asegurados, ya que permite el acceso únicamente mediante la contraseña; no hay alternativas para esto, por eso, si olvida la contraseña, no podrá acceder a su caja fuerte de datos.

Una vez que haya especificado todos los datos requeridos en los campos de texto, haga clic en el botón Siguiente para ir al siguiente paso:



Este cuadro de diálogo incluye las siguientes opciones de configuración:

- Ubicación indica dónde se guardará físicamente la caja fuerte de datos. Busque un lugar adecuado en su disco, o bien, puede mantener la ubicación predefinida, que es la carpeta Documentos. Recuerde que, una vez que ha creado una caja fuerte de datos, ya no puede cambiar su ubicación.

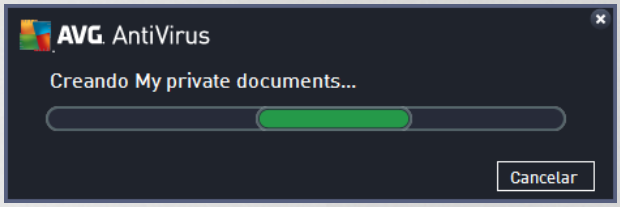
- Tamaño: puede predefinir el tamaño de su caja fuerte de datos, que asignará el espacio necesario en el disco. El valor con el cual se configurará no debe ser ni demasiado pequeño (no será suficiente para sus necesidades) ni demasiado grande (ocupará demasiado espacio en el disco sin necesidad). Si ya sabe qué desea colocar en la caja fuerte de datos, puede ubicar todos los archivos en una carpeta y luego utilizar el vínculo Seleccionar una carpeta para calcular automáticamente el tamaño total. Sin embargo, más adelante podrá cambiar el tamaño, según sus necesidades.

- Acceso: las casillas de verificación de esta sección le permiten crear

accesos directos convenientes a su caja fuerte de datos.

Cómo utilizar su caja fuerte de datos

Cuando esté satisfecho con la configuración, haga clic en el botón Crear Caja Fuerte. Aparece un nuevo cuadro de diálogo Su Caja Fuerte de Datos ahora está lista que anuncia que la caja fuerte está disponible para que almacene sus archivos. En este momento la caja fuerte está abierta y usted puede acceder a ella de inmediato. En cada intento siguiente de acceder a la caja fuerte, se le invitará a desbloquear la caja fuerte con la contraseña que haya definido:



Para utilizar su nueva caja fuerte de datos, primero debe abrirla: haga clic en el botón Abrir Ahora. Después de hacerlo, la caja fuerte de datos aparece en su equipo como un nuevo disco virtual. Asígnele una letra de su elección del menú desplegable (sólo se le permitirá seleccionar de discos actualmente libres). Normalmente, no podrá elegir las letras C (usualmente asignada a su disco duro), A (unidad de disco flexible) o D (unidad de DVD). Recuerde que cada vez que desbloquee una caja fuerte de datos, podrá elegir una letra diferente para la unidad.

Cómo desbloquear su caja fuerte de datos

En su siguiente intento de acceder a la caja fuerte de datos, se le invitará a desbloquear la caja fuerte con la contraseña que haya definido:

En el campo de texto, escriba la contraseña para darse permiso y haga clic en el botón Desbloquear. Si necesita ayuda para recordar la contraseña, haga clic en Consejo para mostrar la pista para la contraseña que definió cuando creó la caja fuerte de datos. La nueva caja fuerte de datos aparecerá en la descripción general de sus cajas fuertes de datos como DESBLOQUEADA, y podrá agregar o eliminar los archivos que contiene, según lo necesite.

6.2. Protección de navegación web

La Protección de navegación web comprende dos servicios: LinkScanner Surf-Shield y Online Shield:

- LinkScanner Surf-Shield 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 lo protege analizando las páginas web que se esconden en los vínculos de cualquier página web que esté viendo y se asegura de que sean seguras en el único momento en que verdaderamente importa: cuando está por hacer clic sobre ellas. LinkScanner Surf-Shield no se diseñó para proteger plataformas de servidor.

- 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 la PC. 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. Esta poderosa protección bloqueará el contenido malicioso de cualquier página que intente abrir y evitará que se descargue en la PC. Con esta característica activada, al hacer clic en un vínculo o escribir la URL de un sitio peligroso, se evitará que se abra la página web, protegiéndolo de infecciones inadvertidas. Es importante recordar que las páginas web vulnerables pueden infectar su equipo simplemente mediante una visita al sitio afectado. Online Shield no se diseñó para proteger plataformas de servidor.

Controles del cuadro de diálogo

Para alternar entre ambas secciones del cuadro de diálogo, basta con que haga clic en cualquier lugar del panel de servicios respectivo. El panel luego se resalta en una sombra más clara de azul. En ambas secciones del cuadro de diálogo puede encontrar los siguientes controles. Su funcionalidad es similar ya sea que pertenezcan a un servicio de seguridad o a otro (LinkScanner Surf-Shield u Online Shield):

 Habilitado / Deshabilitado: el botón puede recordarle a un semáforo, tanto en su apariencia como en su funcionalidad. Haga un solo clic para alternar entre dos posiciones. El color verde significa Activado, que implica que el servicio de seguridad LinkScanner Surf-Shield / Online Shield está activo y completamente funcional. El color rojo representa el estado Desactivado; es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, se recomienda estrictamente que conserve la configuración predeterminada para todos los ajustes de seguridad. La configuración predeterminada garantiza el óptimo rendimiento de la aplicación, y su máxima seguridad. Si, por algún motivo, desea desactivar el servicio, se le advertirá acerca del posible riesgo de manera inmediata mediante el signo rojo Advertencia y la información de que no posee protección completa en ese momento. Tenga en cuenta que debe activar el servicio otra vez tan pronto sea posible.

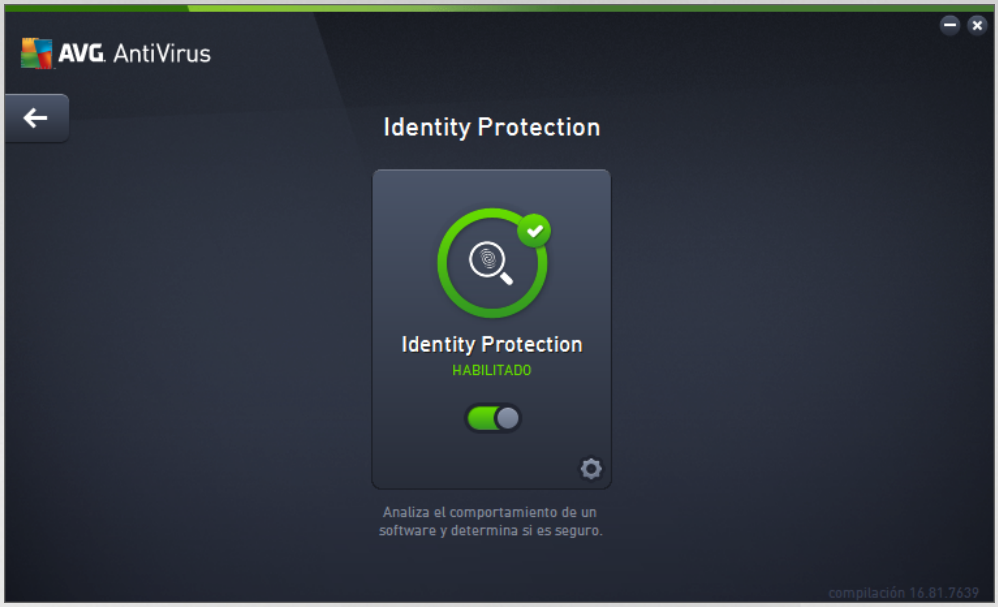
 Configuración: haga clic en el botón para redireccionarse a la interfaz de configuración avanzada. De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado; es decir, LinkScanner Surf-Shield u Online Shield. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus**, pero solamente se recomienda que lo hagan usuarios experimentados.

 Flecha: utilice la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal con la descripción general de los componentes.

6.3. Identity Protection

El componente Identity Protection ejecuta el servicio Identity Shield, que brinda protección constante a sus activos digitales contra amenazas nuevas y desconocidas en Internet:

- Identity Protection es un servicio anti-malware que ofrece protección contra todo tipo de malware (spyware, bots, robo de identidad, etc.) mediante tecnologías conductuales que proporcionan protección desde el día cero frente a nuevos virus. Identity Protection va dirigido a prevenir posibles robos de contraseñas, detalles de cuentas bancarias, números de tarjeta de crédito y otros datos digitales personales de valor ocasionados por toda clase de software malicioso (malware) en su equipo. Asegura que todos los programas que se ejecuten en su equipo o en su red compartida funcionen correctamente. Identity Protection detecta y bloquea comportamientos sospechosos de forma continua, y protege su equipo de cualquier malware nuevo. Identity Protection da a su equipo protección en tiempo real contra amenazas nuevas e incluso desconocidas. Supervisa todos los procesos (incluso los ocultos) y más de 285 comportamientos diferentes, y puede determinar si está ocurriendo algo malicioso dentro de su sistema. Por este motivo, hasta puede mostrar amenazas que aún no están descritas en la base de datos de virus. Cuando una parte de código desconocida llega a su equipo, inmediatamente se comprueba si tiene un comportamiento malicioso y se realiza un seguimiento. Si se considera que el archivo es malicioso, Identity Protection eliminará el código, lo trasladará a la Bóveda de virus y deshará los cambios que hayan podido realizarse en el sistema (inyecciones de código, cambios del registro, apertura de puertos, etc.). No es necesario iniciar un análisis para estar protegido. Esta tecnología es muy proactiva, raras veces necesita actualización y siempre está de guardia.



Controles del cuadro de diálogo

En el cuadro de diálogo, puede encontrar los siguientes controles:

Habilitado / Deshabilitado: el botón puede recordarle a un semáforo, tanto en su apariencia como en su funcionalidad. Haga un solo clic para alternar entre dos posiciones. El color verde significa Activado, que implica que el servicio de seguridad Identity Protection está activo y completamente funcional. El color rojo representa el estado Desactivado; es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, se recomienda estrictamente que conserve la configuración predeterminada para todos los ajustes de seguridad. La configuración predeterminada garantiza el óptimo rendimiento de la aplicación, y su máxima seguridad. Si, por algún motivo, desea desactivar el servicio, se le advertirá acerca del posible riesgo de manera inmediata mediante el signo rojo Advertencia y la información de que no posee protección completa en ese momento. Tenga en cuenta que debe activar el servicio otra vez tan pronto sea posible.

Configuración: haga clic en el botón para redireccionarse a la interfaz de configuración avanzada. De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, Identity Protection. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus**, pero solamente se recomienda que lo hagan usuarios experimentados.

Flecha: utilice la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal con la descripción general de los componentes.

Lamentablemente, en **AVG AntiVirus**, el servicio Identity Alert no está incluido. Si desea usar este tipo de protección, siga el botón Actualizar para Activar para dirigirse a la página web dedicada donde puede comprar la licencia de Identity Alert.

Tenga en cuenta que incluso con las ediciones de AVG Premium Security, el servicio Identity *Alert está disponible actualmente en determinadas regiones solamente: Estados Unidos, Reino Unido, Canadá e Irlanda.*

6.4. Protección del correo electrónico

El componente ***Protección del correo electrónico*** cubre los siguientes dos servicios de seguridad: ***Analizador de correo electrónico*** y ***Anti-Spam*** *(solo se puede acceder al servicio Anti-Spam en las ediciones Internet / Premium Security)*.

- ***Analizador de correo electrónico***: Una de las fuentes más comunes de virus y troyanos es a través de correo electrónico. El phishing (suplantación de identidad) y el spam hacen del correo electrónico una fuente aún mayor de riesgos. Las cuentas de correo electrónico gratuitas aumentan la probabilidad de recibir esos correos maliciosos *(ya que es muy raro que empleen tecnología anti-spam)*, y los usuarios domésticos confían demasiado en tales correos. Asimismo, al navegar por sitios desconocidos y rellenar formularios en línea con datos personales *(como la dirección de correo electrónico)*, los usuarios domésticos están más expuestos a ataques a través del correo electrónico. Las compañías normalmente utilizan cuentas de correo electrónico corporativas y emplean filtros anti-spam, etc, para reducir el riesgo. El componente Protección del correo electrónico es responsable de analizar cada mensaje de correo electrónico enviado o recibido; cuando se detecta un virus en un correo electrónico, se coloca en la Bóveda de virus de manera inmediata. El componente también puede filtrar determinados tipos de archivos adjuntos de correo electrónico, así como agregar un texto de certificación a los mensajes no infectados. ***El Analizador de correos electrónicos no está diseñado para plataformas de servidor.***

- ***Anti-Spam*** comprueba todos los mensajes de correo electrónico entrantes y marca correos electrónicos no deseados como spam *(spam hace referencia a correo electrónico no solicitado, mayormente publicidades de un producto o un servicio que se envían de forma masiva a una gran cantidad de direcciones de correo electrónico al mismo tiempo, lo que llena los buzones de correo de los destinatarios. Los correos de spam no son correos comerciales legítimos para los que los consumidores dan su consentimiento).* Anti-Spam puede modificar el asunto del correo electrónico *(identificado como spam)* agregando una cadena de texto especial. Luego puede filtrar fácilmente sus mensajes en el cliente de correo electrónico. El componente Anti-Spam usa varios métodos de análisis para procesar cada mensaje y ofrece la mayor protección posible contra mensajes de correo electrónico no deseados. Anti-Spam utiliza una base de datos que se actualiza regularmente para la detección del spam. También es posible usar servidores RBL *(bases de datos públicas con direcciones de correo electrónico de "spammers conocidos")*, así como agregar manualmente direcciones de correo electrónico a la Lista de usuarios autorizados *(nunca marcar como spam)* y a la Lista negra *(marcar siempre como spam)*.

Controles del cuadro de diálogo

Para alternar entre ambas secciones del cuadro de diálogo, basta con que haga clic en cualquier lugar del panel de servicios respectivo. El panel luego se resalta en una sombra más clara de azul. En ambas secciones del cuadro de diálogo puede encontrar los siguientes controles. Su funcionalidad es similar ya sea que pertenezcan a un servicio de seguridad o a otro *(Analizador del correo electrónico o Anti-Spam)*:

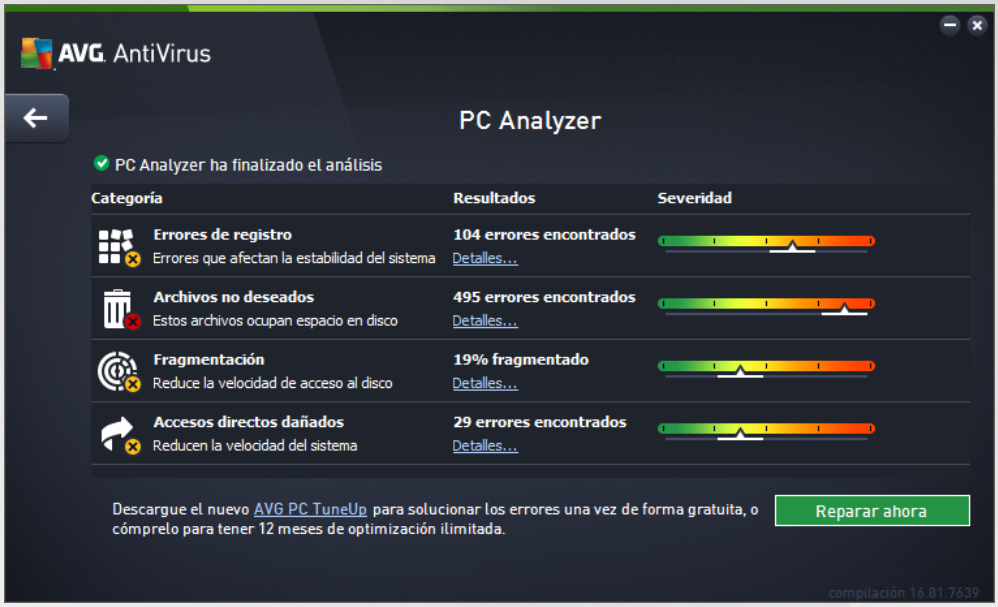
Habilitado / Deshabilitado: el botón puede recordarle a un semáforo, tanto en su apariencia como en su funcionalidad. Haga un solo clic para alternar entre dos posiciones. El color verde significa ***Activado***, que implica que el servicio de seguridad está activo y completamente funcional. El color rojo representa el estado ***Desactivado***; es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, se recomienda estrictamente que conserve la configuración predeterminada para todos los ajustes de seguridad. La configuración predeterminada garantiza el óptimo rendimiento de la aplicación, y su máxima seguridad. Si, por algún motivo, desea desactivar el servicio, se le advertirá acerca del posible riesgo de manera inmediata mediante el signo rojo ***Advertencia*** y la información de que no posee protección completa en ese momento. ***Tenga en cuenta que debe activar el servicio otra vez tan pronto sea posible.***

Configuración: haga clic en el botón para redireccionarse a la interfaz de configuración avanzada. De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado; es decir, Analizador de correos electrónicos o Anti-Spam. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus** , pero solamente se recomienda que lo hagan usuarios experimentados.

Flecha: utilice la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal con la descripción general de los componentes.

6.5. PC Analyzer

El componente ***PC Analyzer*** es una herramienta avanzada para un análisis y una corrección detallados del sistema con el fin de mejorar la velocidad y el rendimiento general de su equipo. Se abre desde el botón ***Reparar rendimiento*** ubicado en la interfaz de diálogo del usuario principal o desde la misma opción que aparece en el menú contextual del icono de AVG de la bandeja del sistema. Posteriormente podrá ver el progreso del análisis y los resultados directamente en el gráfico:



Se pueden analizar las siguientes categorías: errores de registro, archivos no deseados, fragmentación y accesos directos dañados:

- ***Errores en el registro*** mostrará el número de errores en el Registro de Windows que podrían estar reduciendo la velocidad de su equipo o haciendo que aparezcan mensajes de error.
- ***Archivos no deseados*** proporciona el número de archivos que consumen espacio en el disco duro y que probablemente se eliminen. 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.
- ***Accesos directos dañados*** encontrará los accesos directos que ya no funcionan, que conducen a ubicaciones inexistentes, etc.

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

Botones de control

- ***Detener análisis*** (*se muestra mientras se ejecuta el análisis*): presione este botón para interrumpir el

análisis del equipo inmediatamente.

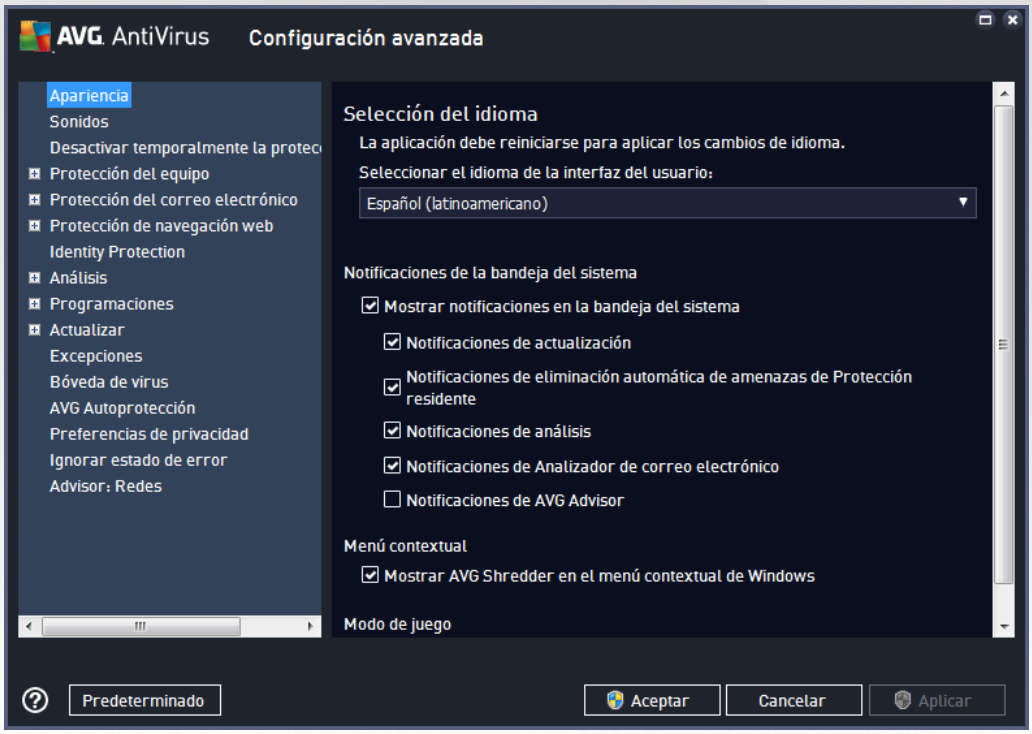
- ***Reparar ahora*** (*se muestra cuando el análisis ha terminado*: lamentablemente, la funcionalidad de PC Analyzer dentro de **AVG AntiVirus** está limitada al análisis de estado actual de su PC. Sin embargo, AVG brinda una herramienta avanzada para un análisis y una corrección detallados del sistema con el fin de mejorar la velocidad y el rendimiento general de su equipo. Haga clic en el botón para redireccionarse al sitio web correspondiente para obtener más información .

7. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG AntiVirus** 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.

7.1. Apariencia

El primer elemento del árbol de navegación, ***Apariencia***, se refiere a la configuración general de la interfaz de usuario de **AVG AntiVirus** y proporciona algunas opciones básicas del comportamiento de la aplicación:



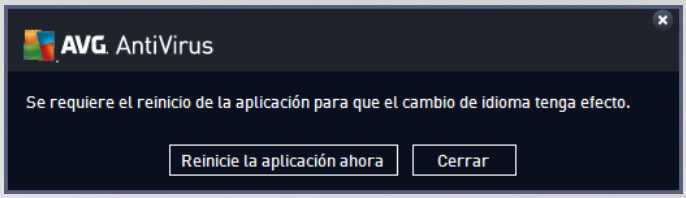
Selección de idioma

En la sección ***Selección de idioma***, puede seleccionar el idioma deseado en el menú desplegable. El idioma seleccionado se usará para la interfaz de usuario completa de **AVG AntiVirus**. El menú desplegable sólo ofrece los idiomas que haya seleccionado con anterioridad para instalarse durante el proceso de instalación además del inglés (*que se instala automáticamente, de forma predeterminada*). Para terminar de cambiar el idioma de su **AVG AntiVirus** debe reiniciar la aplicación. Siga estos pasos:

- En el menú desplegable, seleccione el idioma deseado de la aplicación.
- Para confirmar la selección, presione el botón ***Aplicar*** *(esquina inferior derecha del cuadro de diálogo).*
- Presione el botón ***Aceptar*** para confirmar.

- Se abre un nuevo cuadro de diálogo que le informa de que para cambiar el idioma de la aplicación debe reiniciar su **AVG AntiVirus.**

- Presione el botón ***Reiniciar AVG ahora*** para aceptar el reinicio del programa y espere un momento a que el cambio de idioma surta efecto:



Notificaciones de la bandeja del sistema

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

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

- ***Mostrar notificaciones en la bandeja del sistema*** *(activada de forma predeterminada)*: De forma predeterminada se muestran todas las notificaciones. Quite la marca de selección de este elemento para desactivar completamente la visualización de todas las notificaciones del sistema. Cuando se encuentra activada, también puede seleccionar qué notificaciones en concreto deben visualizarse:

  - ***Notificaciones de actualización*** *(activada de forma predeterminada)*: Decida si debe visualizarse información sobre la ejecución, el progreso y la finalización del proceso de actualización de **AVG AntiVirus**.

  - ***Notificaciones de eliminación automática de amenazas de Protección Residente*** *(activada de forma predeterminada)*: Decida si debe visualizarse o suprimirse la información relativa a los procesos de guardado, copia y apertura de archivos (*esta configuración sólo se muestra si la opción Autorreparar de Protección Residente está activada*).

  - ***Notificaciones de análisis*** *(activada de forma predeterminada)*: Decida si debe visualizarse información sobre la ejecución automática del análisis programado, el progreso y los resultados.

  - ***Las notificaciones de Analizador de correo electrónico*** *(activada de forma predeterminada)*: Decida si debe visualizarse información sobre el análisis de todos los mensajes de correo electrónico entrantes y salientes.

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

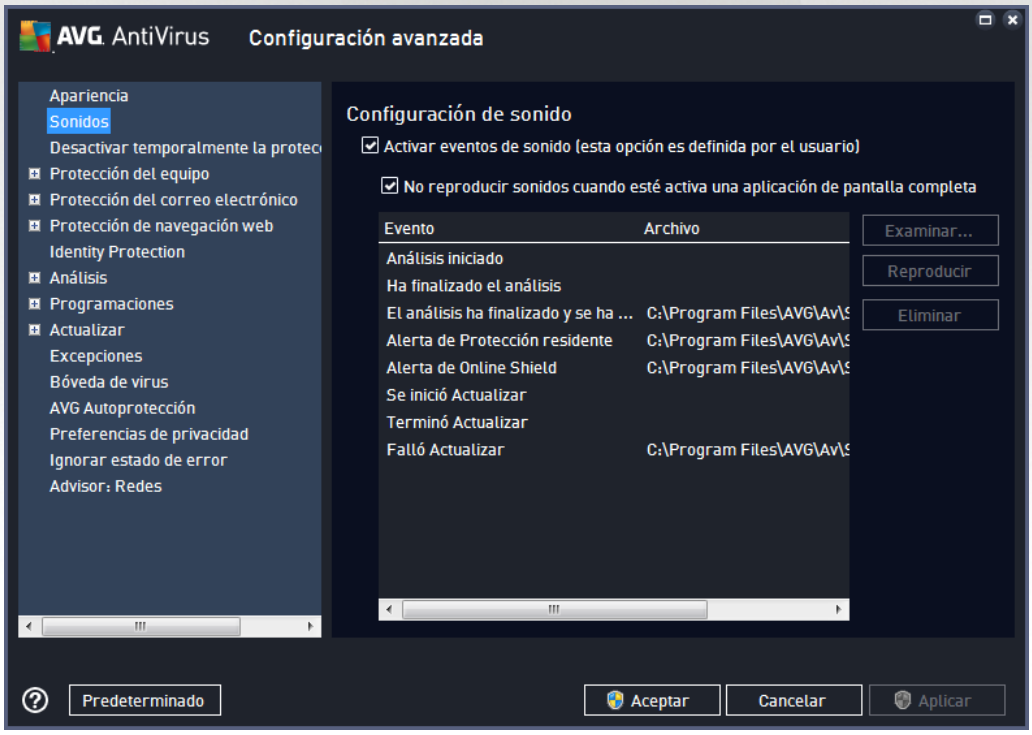
- **Notificaciones de AVG Advisor** *(activada de forma predeterminada):* decida si se debe mostrar la información de las actividades de AVG Advisor en el panel deslizante de la bandeja del sistema.

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*).

7.2. Sonidos

En el cuadro de diálogo ***Configuración de sonido***, puede especificar si desea que se le informe acerca de acciones específicas de **AVG AntiVirus** mediante una notificación sonora:



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

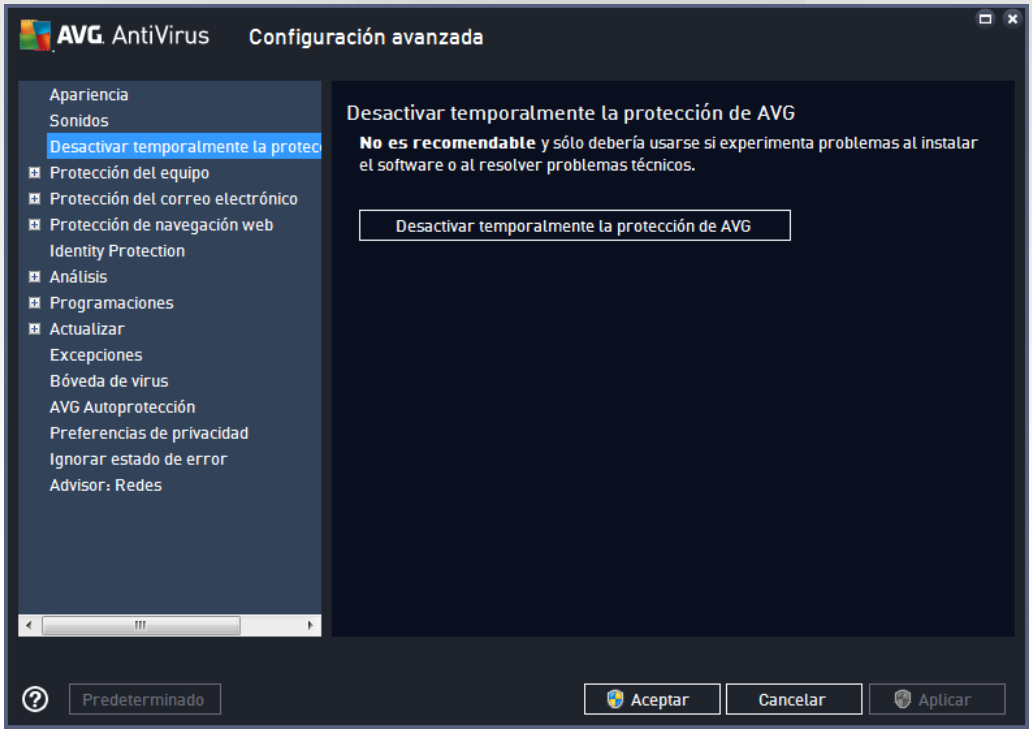
Botones de control

- ***Examinar***: una vez seleccionado el evento correspondiente en la lista, utilice el botón ***Examinar*** para buscar en su disco el archivo de sonido que desee asignar a él. *(Tenga en cuenta que por el momento sólo se admiten archivos de sonido *.wav).*
- ***Reproducir***: para escuchar el sonido seleccionado, resalte el evento en la lista y presione el botón ***Reproducir***.
- ***Eliminar***: utilice el botón ***Eliminar*** para quitar el sonido asignado a un evento específico.

7.3. Desactivar temporalmente la protección de AVG

En el cuadro de diálogo Desactivar temporalmente la protección de AVG tiene la opción de desactivar toda la protección que proporciona **AVG AntiVirus** 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 AntiVirus** antes de instalar nuevo software o controladores, ni siquiera si el asistente del software o instalador le sugiere que cierre los programas y las aplicaciones que se están ejecutando para asegurarse de que no se produzcan interrupciones no deseadas durante el proceso de instalación. Si realmente experimenta problemas durante la instalación, intente desactivar la protección residente (en el diálogo vinculado, desmarque primero el elemento Activar la Protección Residente). Si tiene que desactivar temporalmente **AVG AntiVirus**, debe volver a activarlo en cuanto termine. Si está conectado a Internet o a una red durante el tiempo que el software antivirus está desactivado, su equipo será vulnerable ante los ataques.

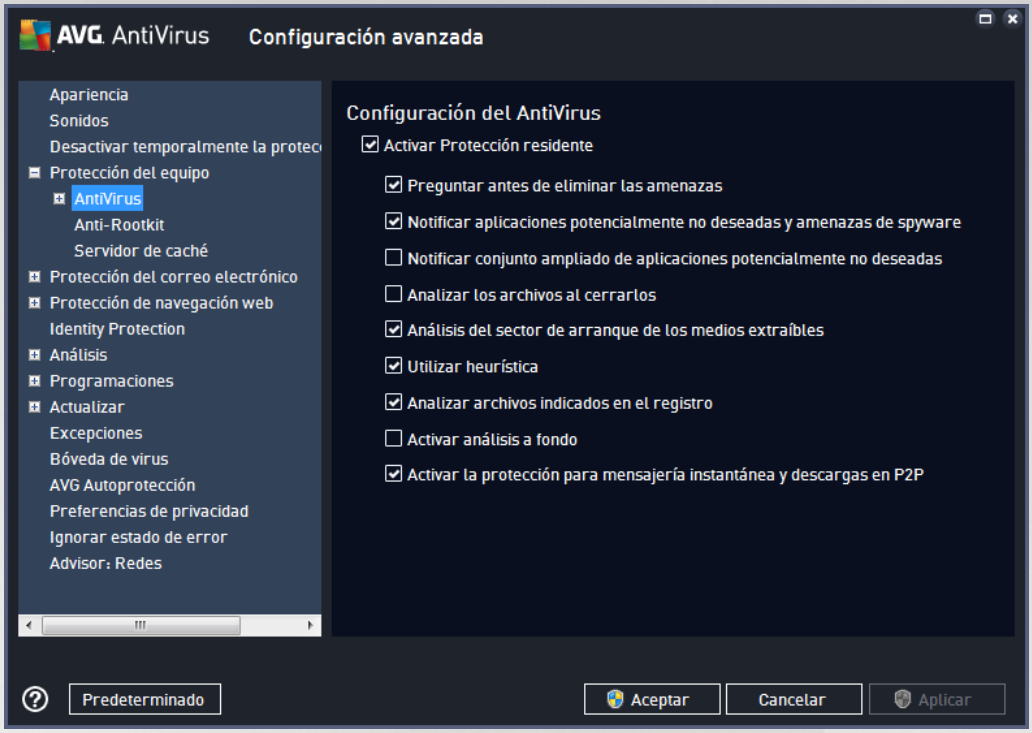
Cómo desactivar la protección de AVG

Marque la casilla de verificación Desactivar temporalmente la protección de AVG y presione el botón Aplicar para confirmar su elección. En el cuadro de diálogo Desactivar temporalmente la protección de AVG recién abierto, especifique por cuánto tiempo desea desactivar su **AVG AntiVirus**. La protección se desactivará durante 10 minutos de forma predeterminada, lo que debería ser suficiente para cualquier tarea común, como la instalación de nuevo software, etc. Puede optar por un período de tiempo más prolongado; sin embargo, esta medida no se recomienda salvo que sea absolutamente necesaria. Posteriormente, todos los componentes desactivados se activarán automáticamente otra vez. Como máximo, puede desactivar la protección de AVG hasta reiniciar nuevamente el equipo.

7.4. Protección del equipo

7.4.1. Antivirus

AntiVirus junto con ***Protección Residente*** protegen su equipo de manera continua de todos los tipos de virus, spyware y malware conocidos en general *(incluidos el denominado malware inactivo y no peligroso, es decir, malware que se ha descargado, pero que no se ha activado aún)*.



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

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

- ***Analizar aplicaciones potencialmente no deseadas y amenazas de spyware*** (*activada de forma predeterminada*): Seleccione esta opción para activar el análisis de spyware y virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad de la PC.

- ***Informar sobre conjunto mejorado de aplicaciones potencialmente no deseadas*** (*desactivada de forma predeterminada*): Seleccione esta opción para detectar paquetes extendidos de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente.
  Esta es una medida adicional que aumenta aún más la seguridad de la PC, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

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

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

Seleccione esta opción para analizar los sectores de arranque de los discos flash USB insertados, las unidades de disco externas y cualquier otro medio extraíble en busca de amenazas.

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

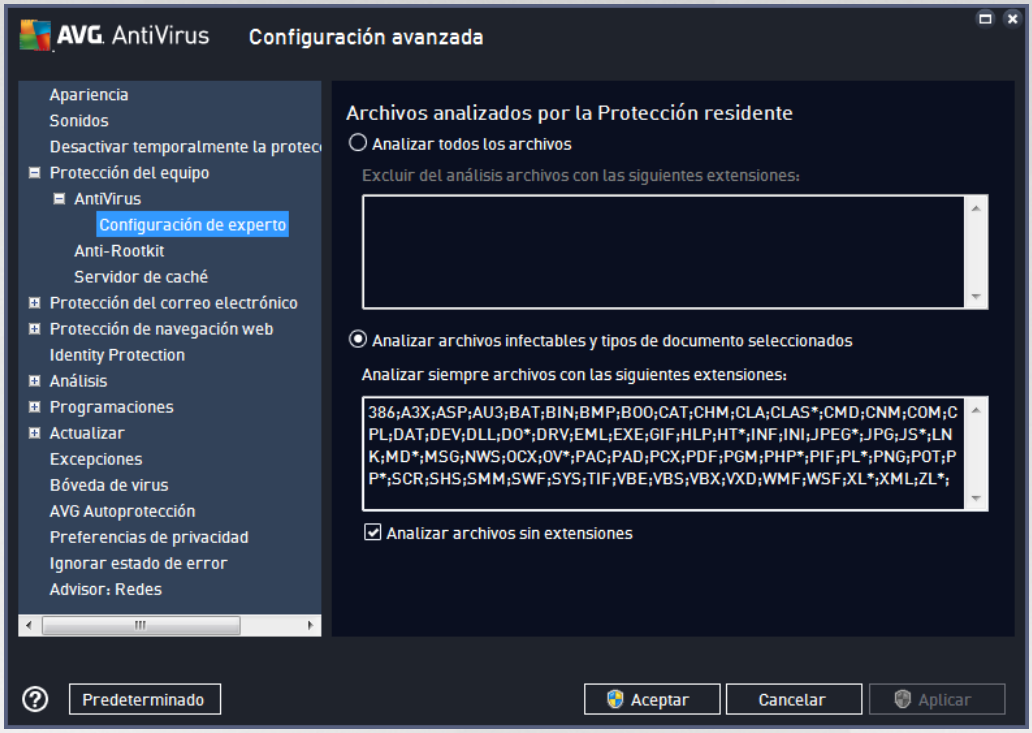
- ***Analizar archivos indicados en el registro*** (*activada de forma predeterminada*): Este parámetro define que AVG analizará todos los archivos ejecutables añadidos al registro de inicio para evitar que una infección conocida se ejecute durante el siguiente inicio del equipo.

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

- ***Activar la protección para mensajería instantánea y descargas en P2P*** (*activada de forma predeterminada*): Seleccione esta opción si desea verificar que la comunicación de mensajería instantánea (*por ejemplo, AIM, Yahoo!, ICQ, Skype, MSN Messenger, etc.*) y los datos descargados dentro de redes punto a punto *(redes que permiten la conexión directa entre clientes, sin un servidor, lo que resulta potencialmente peligroso; comúnmente utilizadas para compartir archivos de música)* no tengan virus.

Nota: *Si se instala AVG en Windows 10, un elemento más denominado* ***Habilite Antimalware Scan Interface (AMSI) de Windows para realizar análisis de software más profundos*** *se presenta en la lista. Esta función mejora la protección antivirus, ya que permite que Windows y AVG cooperen más de cerca al revelar códigos maliciosos, lo que hace que la protección sea más confiable y se reduzca la cantidad de falsos positivos.*

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

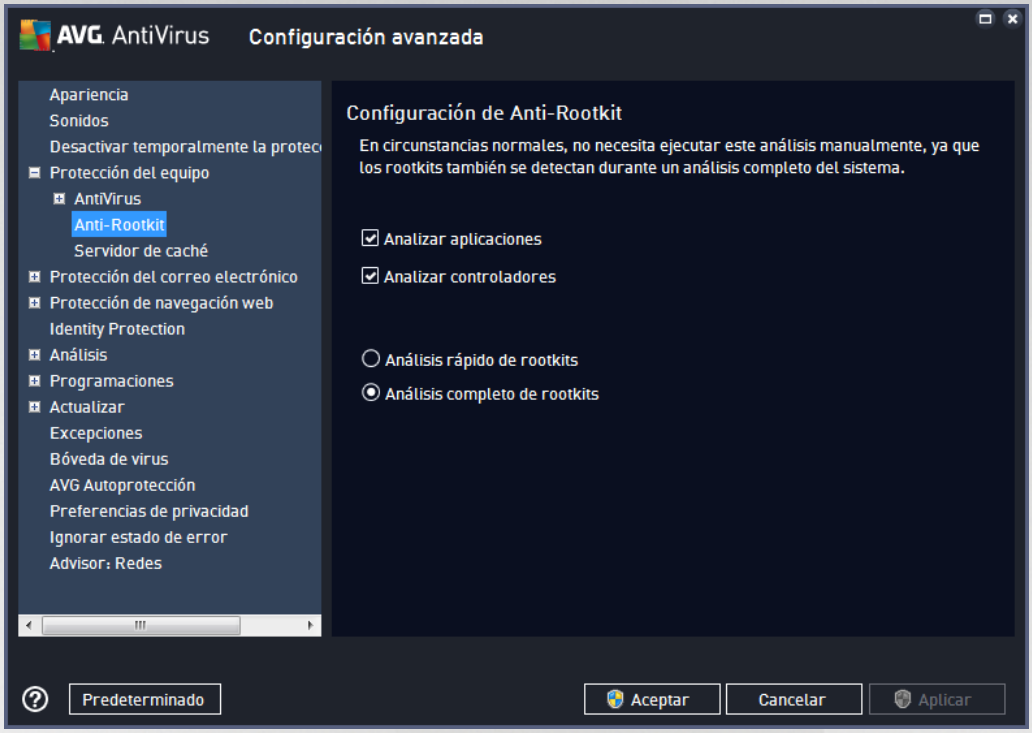


Marque la casilla de verificación respectiva para decidir si desea ***Analizar todos los archivos*** o solamente ***Analizar archivos infectables y tipos de documento seleccionados***. Para agilizar el análisis y proporcionar al mismo tiempo el nivel máximo de protección, recomendamos que conserve la configuración predeterminada. De esta forma sólo se analizarán los archivos infectables. En la sección respectiva del cuadro de diálogo, también puede buscar una lista editable de extensiones que definen los archivos que se incluyen en el análisis.

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

7.4.2. Anti-Rootkit

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

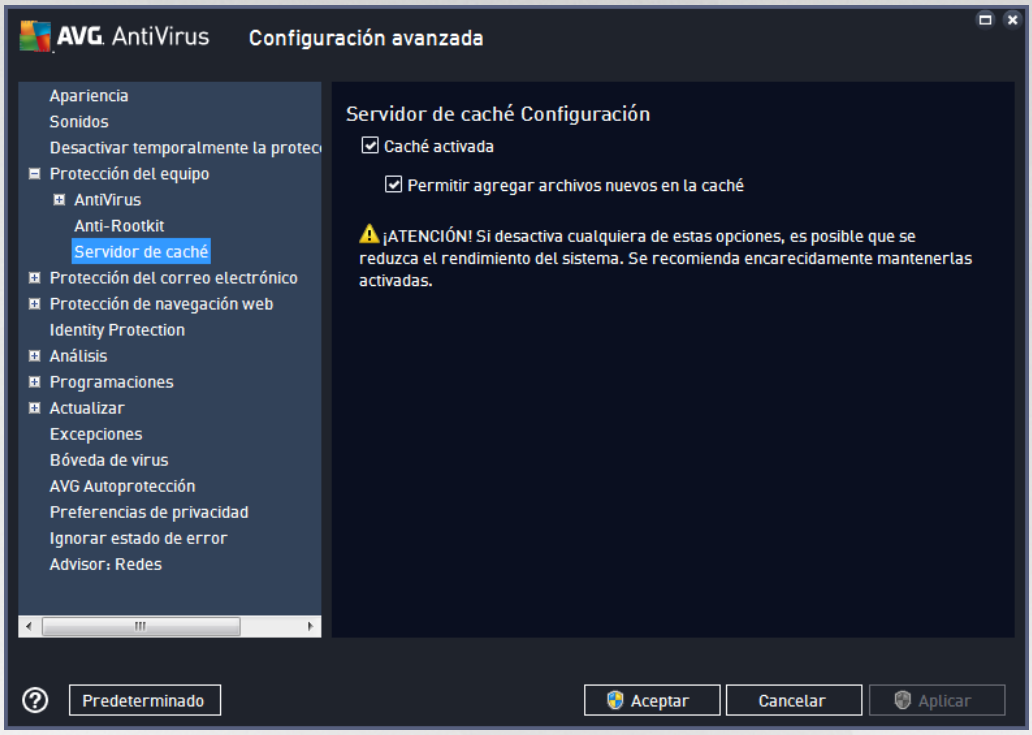


Analizar aplicaciones y ***Analizar controladores*** le permiten especificar en detalle qué debe incluirse en el análisis anti-rootkit. Esta configuración está diseñada para usuarios avanzados; le recomendamos mantener todas las opciones activadas. También puede seleccionar el modo de análisis de rootkits:

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

7.4.3. Servidor de caché

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



El servidor de caché recopila y conserve la información en archivos de confianza (*un archivo se considera de confianza si está firmado digitalmente en una fuente de confianza*). Estos archivos se consideran seguros de forma automática y no deben volver a analizarse; por lo tanto, estos archivos se omiten durante el análisis.

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

- ***Almacenamiento en caché activado*** (*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 bajar la velocidad y reducir el rendimiento general de la PC porque primero se analizarán todos y cada uno de los archivos en uso en busca de virus y spyware.

- ***Permitir agregar archivos nuevos en la caché*** (*activada de forma predeterminada*): quite la marca de la casilla para dejar de agregar archivos en la memoria caché. Se guardarán y usarán todos los archivos ya almacenados en caché hasta que el almacenamiento en caché se desactive completamente o hasta la siguiente actualización de la base de datos de virus.

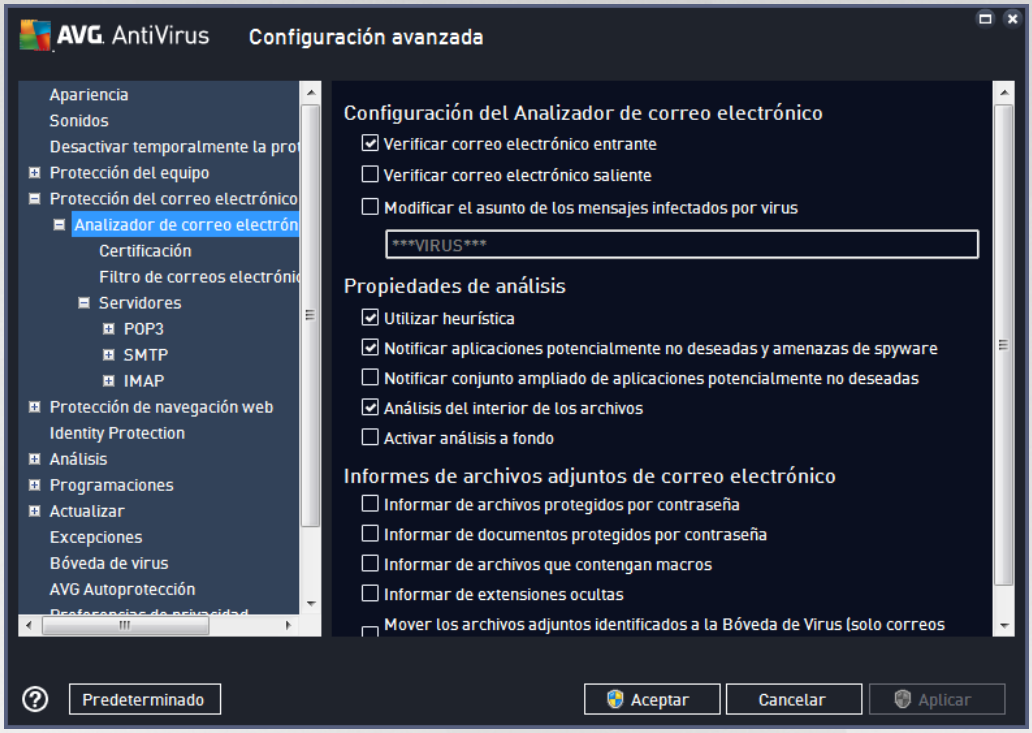
A menos que tenga un buen motivo para desactivar el servidor de caché, se recomienda especialmente que conserve la configuración predeterminada y deje las opciones activadas. De lo contrario, puede experimentar una disminución significativa en la velocidad y el rendimiento de su sistema.

7.5. Analizador de correo electrónico

En esta sección se puede editar la configuración detallada del Analizador de correos electrónicos y Anti-Spam:

7.5.1. Analizador de correo electrónico

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



Análisis de 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 infectado, 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 podrá filtrar los archivos adjuntos de correo electrónico por extensión, sino también por su contenido real. El filtro se puede establecer en el cuadro de diálogo Filtro de correos electrónicos.

- ***Analizar aplicaciones potencialmente no deseadas y amenazas de spyware*** (*activada de forma predeterminada*): Seleccione esta opción para activar el análisis de spyware y 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

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

- ***Análisis del 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 un ataque*), puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que no se infectan a menudo, 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 informes se enumerarán en el cuadro de diálogo Detección mediante la Protección del correo electrónico:

- ***Informar archivos protegidos por contraseña***: no es posible analizar archivos (*ZIP; RAR, etc.*) protegidos por contraseña en busca de virus; seleccione la casilla para informarlos como potencialmente peligrosos.

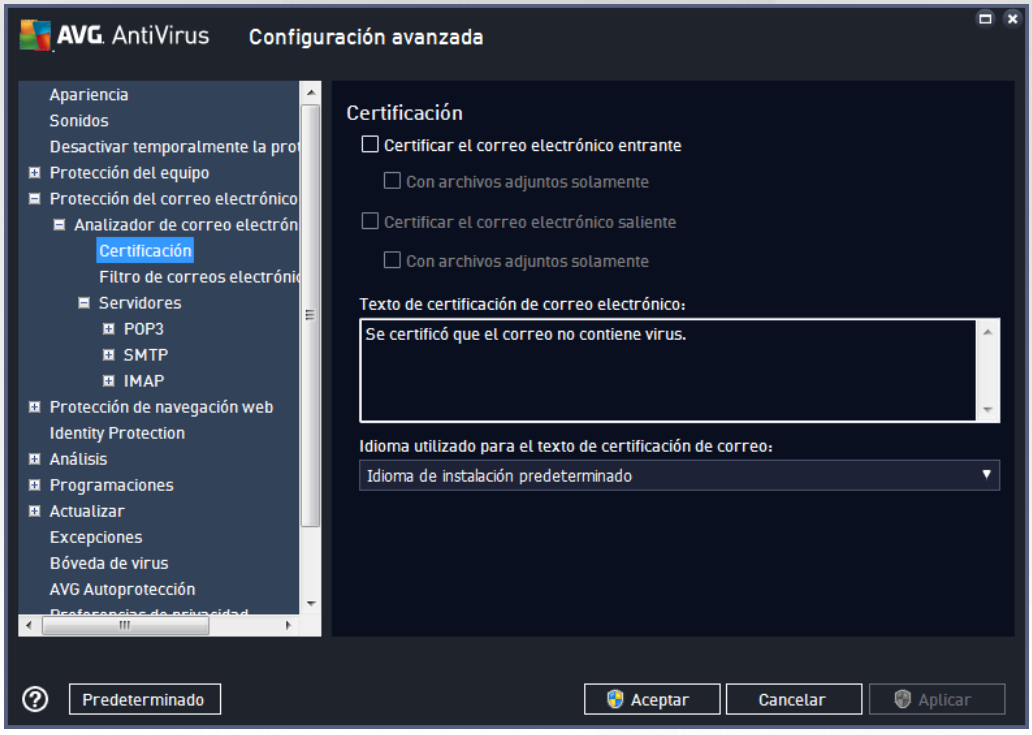
- ***Notificar documentos protegidos por contraseña***: No es posible analizar los documentos protegidos por contraseña en busca de virus; seleccione la casilla para notificarlos como potencialmente peligrosos.

- ***Notificar archivos que contienen macros***: Una macro es una secuencia predefinida de pasos encaminados a hacer que ciertas tareas sean más fáciles para el usuario(*las macros de MS Word son ampliamente conocidas*). Como tal, una macro puede contener instrucciones potencialmente peligrosas, y podría ser útil seleccionar la casilla para garantizar que los archivos con macros se informen como sospechosos.

- ***Notificar extensiones ocultas***: Las extensiones ocultas pueden hacer, por ejemplo, que un archivo ejecutable sospechoso "algo.txt.exe" parezca un archivo de texto simple e inofensivo "algo.txt"; seleccione la casilla para notificar estos archivos como potencialmente peligrosos.

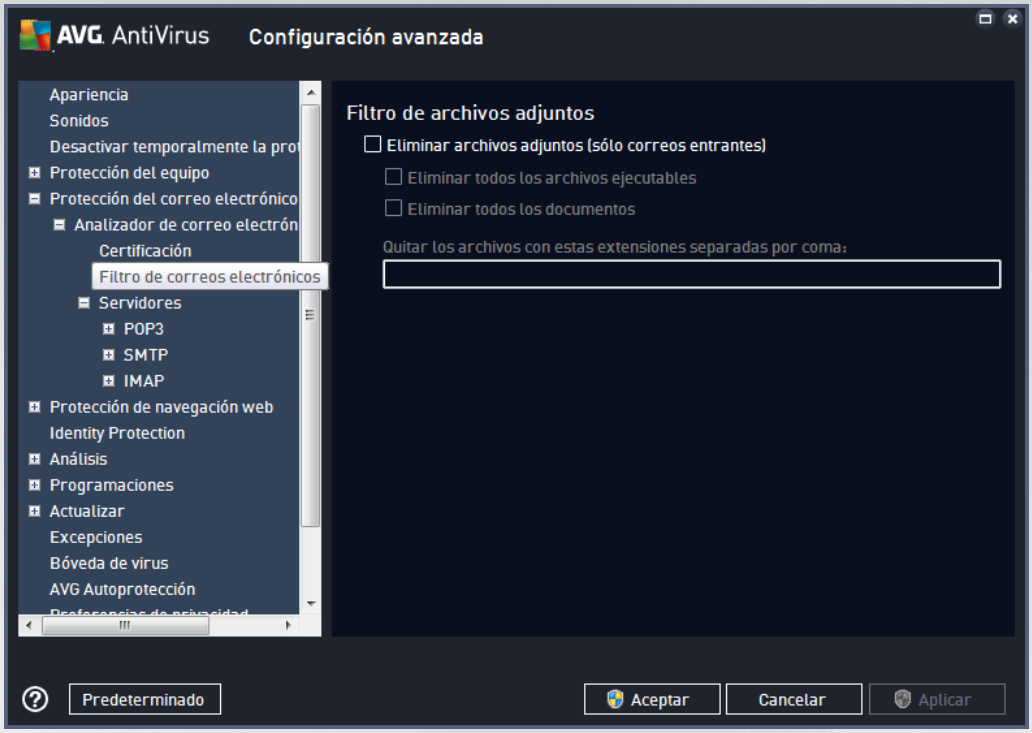
- ***Mover los informes de archivos adjuntos a la Bóveda de virus***: Especifique si desea que se le notifique mediante correo electrónico acerca de los archivos y documentos protegidos por contraseña, los archivos que contienen macros y los archivos con extensión oculta detectados como un dato adjunto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

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



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

Nota: *Tenga en cuenta que solamente se mostrará el texto predeterminado en el idioma solicitado; el texto personalizado no se traducirá automáticamente.*



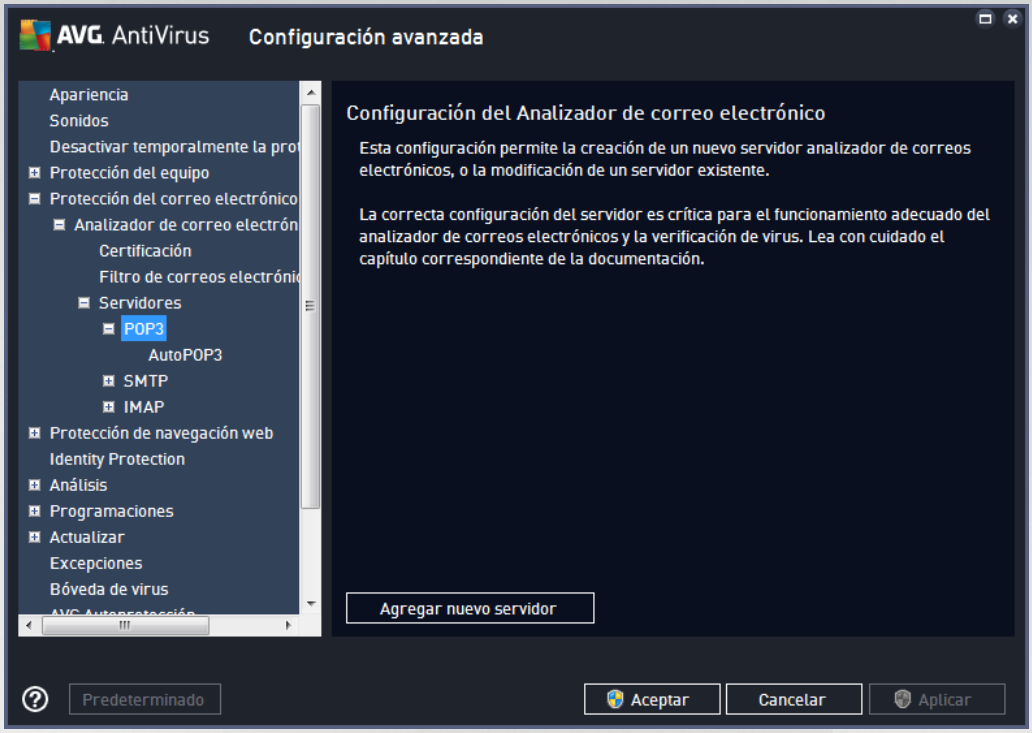
El cuadro de diálogo ***Filtro de archivos adjuntos*** le permite establecer los parámetros para el análisis de los archivos adjuntos de los mensajes de correo electrónico. De manera predeterminada, la opción ***Quitar archivos adjuntos*** está desactivada. Si decide activarla, todos los archivos adjuntos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

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

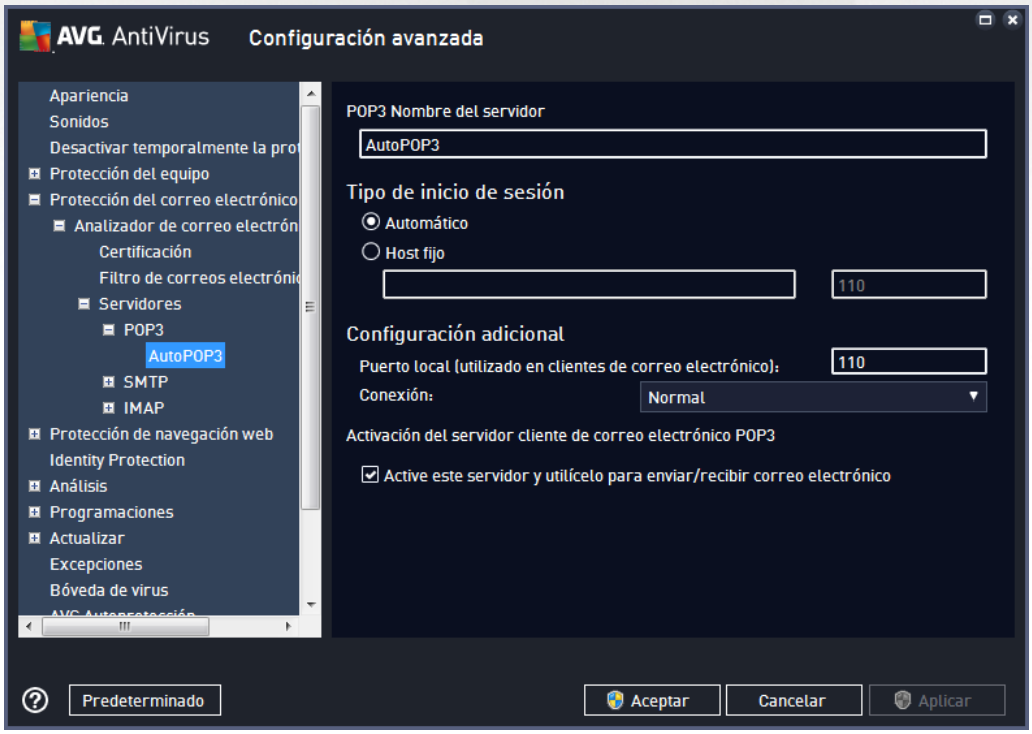
En la sección ***Servidores*** podrá editar parámetros para los servidores del Analizador de correos electrónicos:

- Servidor POP3
- Servidor SMTP
- Servidor IMAP

También puede definir nuevos servidores para correo entrante o saliente, utilizando el botón ***Agregar nuevo servidor***.



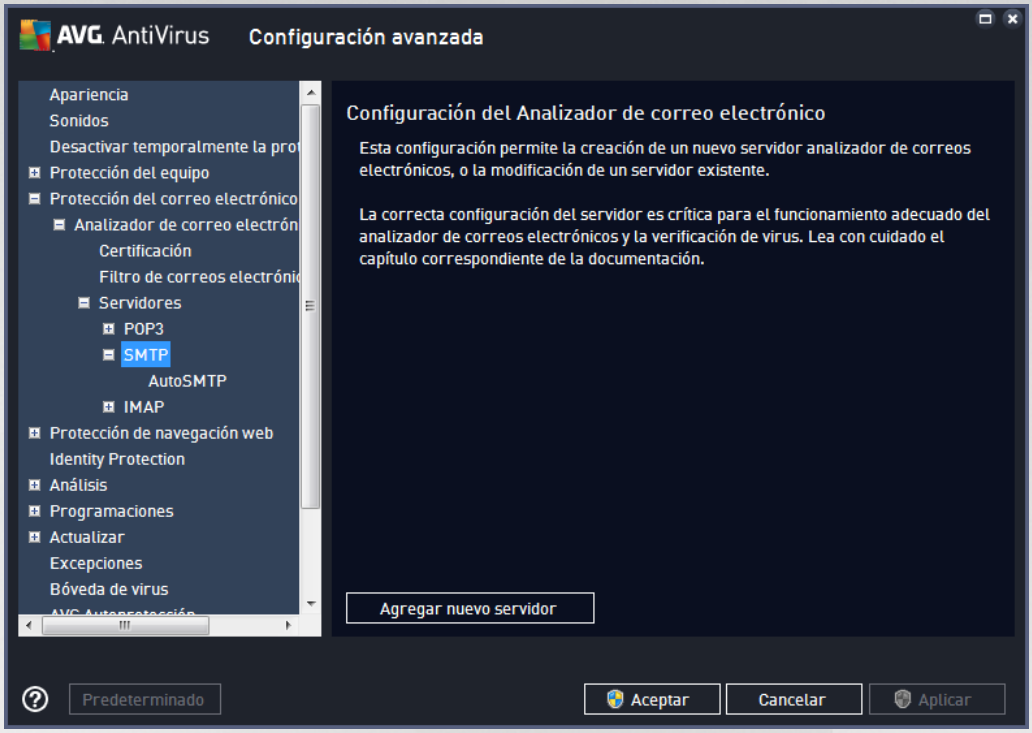
En este cuadro de diálogo puede configurar un nuevo servidor del Analizador de correos electrónicos usando el protocolo POP3 para el correo entrante:



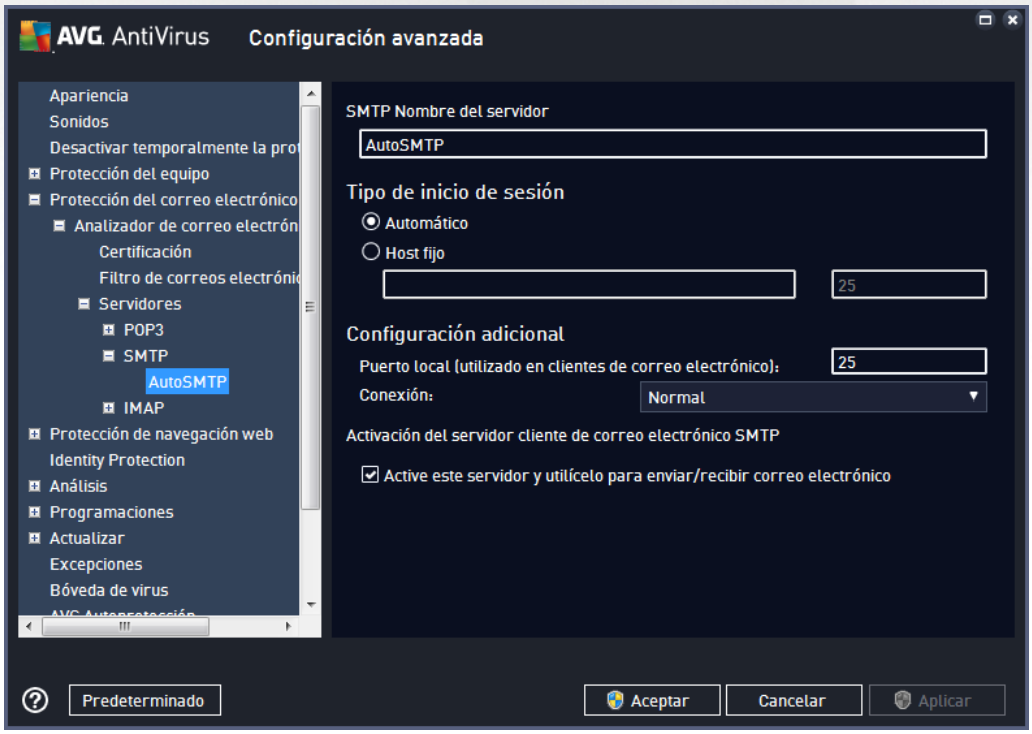
- ***Nombre del servidor POP3***: en este campo podrá especificar el nombre de

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*).

- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo entrante:
    - o ***Automático***: El inicio de sesión se realizará de manera automática, de acuerdo con la configuración del cliente de correo electrónico.
    - o ***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. El nombre de inicio de sesión permanece invariable. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, pop.acme.com*), así como una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (*por ejemplo, pop.acme.com:8200*). El puerto estándar para comunicaciones POP3 es 110.
- ***Configuración Adicional***: especifica los parámetros con mayor detalle:
    - o ***Puerto local***: especifica el puerto en el cual se espera recibir la comunicación de la aplicación de correo. Luego debe especificar en su aplicación de correo este puerto como el puerto para comunicaciones POP3.
    - o ***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



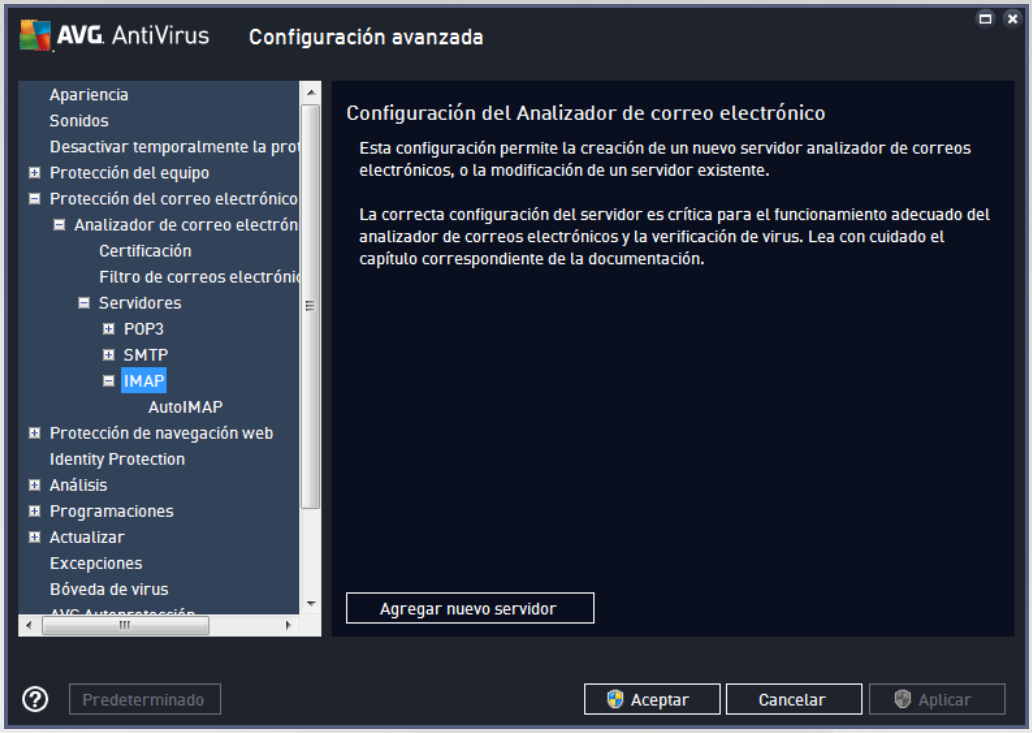
En este cuadro de diálogo puede configurar un nuevo servidor del Analizador de correos electrónicos usando el protocolo SMTP para el correo saliente:



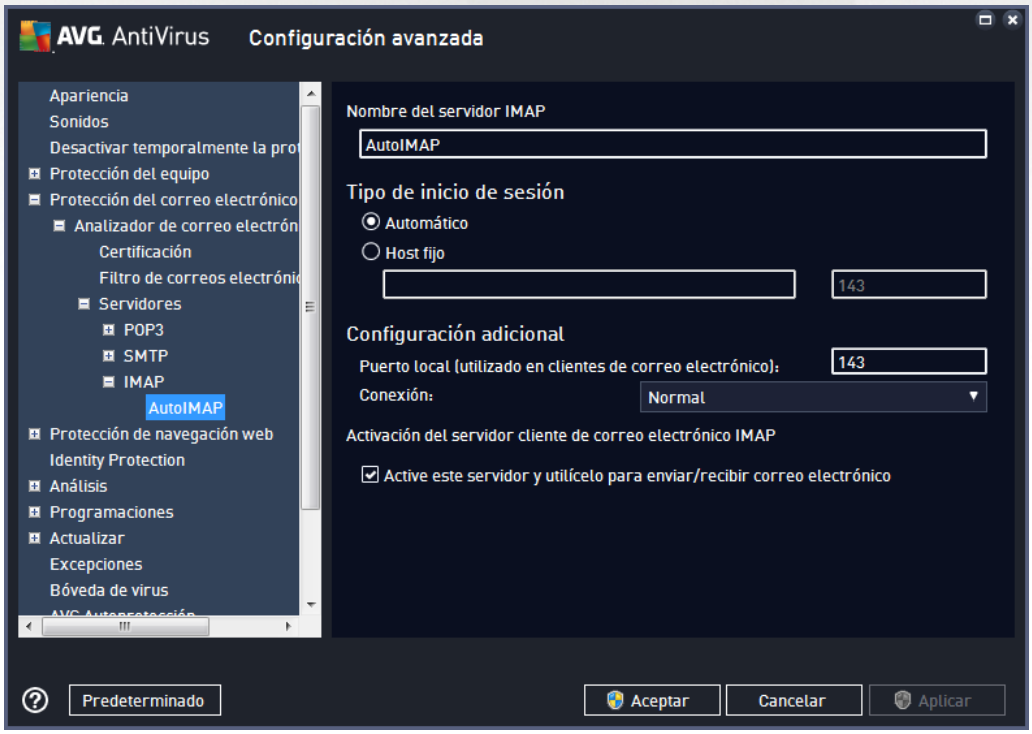
- ***Nombre del servidor SMTP***: en este campo podrá especificar el nombre de los servidores recién

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 los servidores "AutoSMTP" creados automáticamente, este campo está desactivado.

- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo saliente:
    - o ***Automático***: el inicio de sesión se efectuará automáticamente, según la configuración del cliente de correo electrónico.
    - o ***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:
    - o ***Puerto local***: especifica el puerto en el cual se espera recibir la comunicación de la aplicación de correo. Posteriormente deberá especificar en su aplicación de correo este puerto como puerto para la comunicación SMTP.
    - o ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/valor predeterminado de SSL*). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.
- ***Activación del Servidor SMTP de cliente de correo electrónico***: seleccione esta casilla o quite la marca de ella para activar o desactivar el servidor SMTP especificado anteriormente



En este cuadro de diálogo puede configurar un nuevo servidor del Analizador de correos electrónicos usando el protocolo IMAP para el correo saliente:



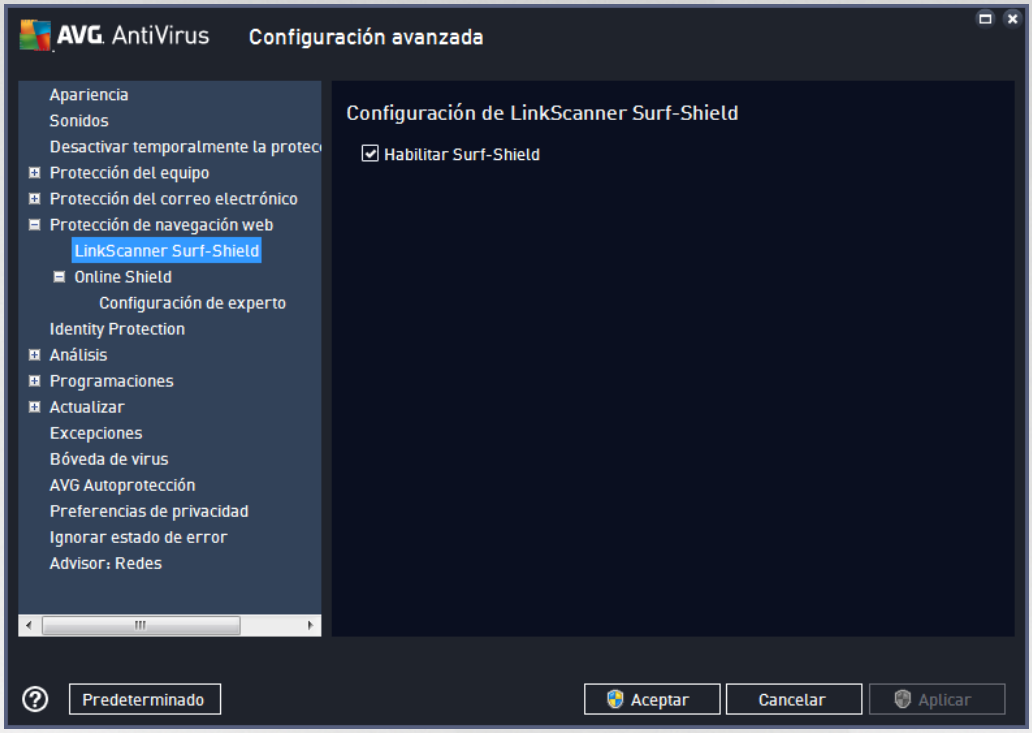
- ***Nombre del servidor IMAP***: en este campo podrá especificar el nombre de los servidores recién

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*).

- ***Tipo de Inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo saliente:
    - o ***Automático***: El inicio de sesión se efectuará automáticamente, según la configuración del cliente de correo electrónico.
    - o ***Host fijo***: En este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, smtp.acme.com*), así como una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (*por ejemplo, imap.acme.com:8200*). El puerto estándar para comunicaciones IMAP es el 143.
- ***Configuración Adicional***: especifica los parámetros con mayor detalle:
    - o ***Puerto local utilizado en***: 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.
    - o ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/valor predeterminado de SSL*). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.
- ***Activación del servidor IMAP en el cliente de correo electrónico***: seleccione esta casilla o quite la marca de ella para activar o desactivar el servidor IMAP especificado anteriormente

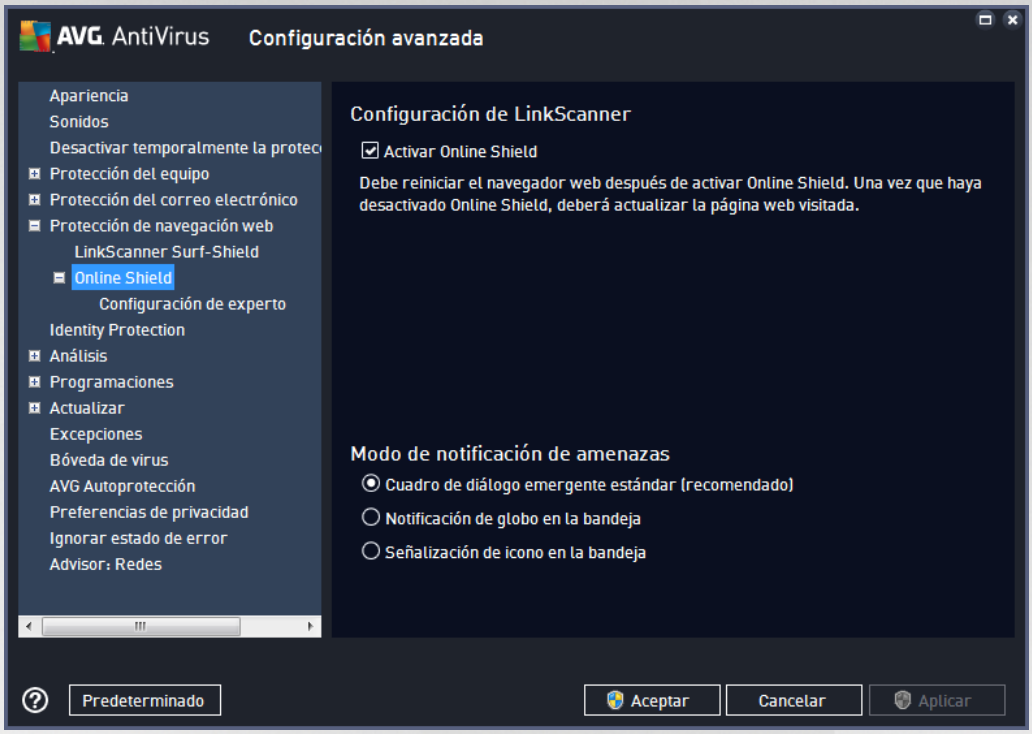
7.6. Protección de navegación web

El cuadro de diálogo ***Configuración de LinkScanner*** le permite marcar/desmarcar las siguientes funciones:



- ***Activar Surf-Shield*** (*activada de forma predeterminada*): protección (*en tiempo real*) activa contra sitios que amenazan la vulnerabilidad de la seguridad a medida que se accede a ellos. Las conexiones a los sitios maliciosos conocidos y el contenido que amenaza la vulnerabilidad se bloquean cuando el usuario accede a ellos a través de un navegador Web (*o cualquier otra aplicación que utilice HTTP*).

7.6.1. Online Shield

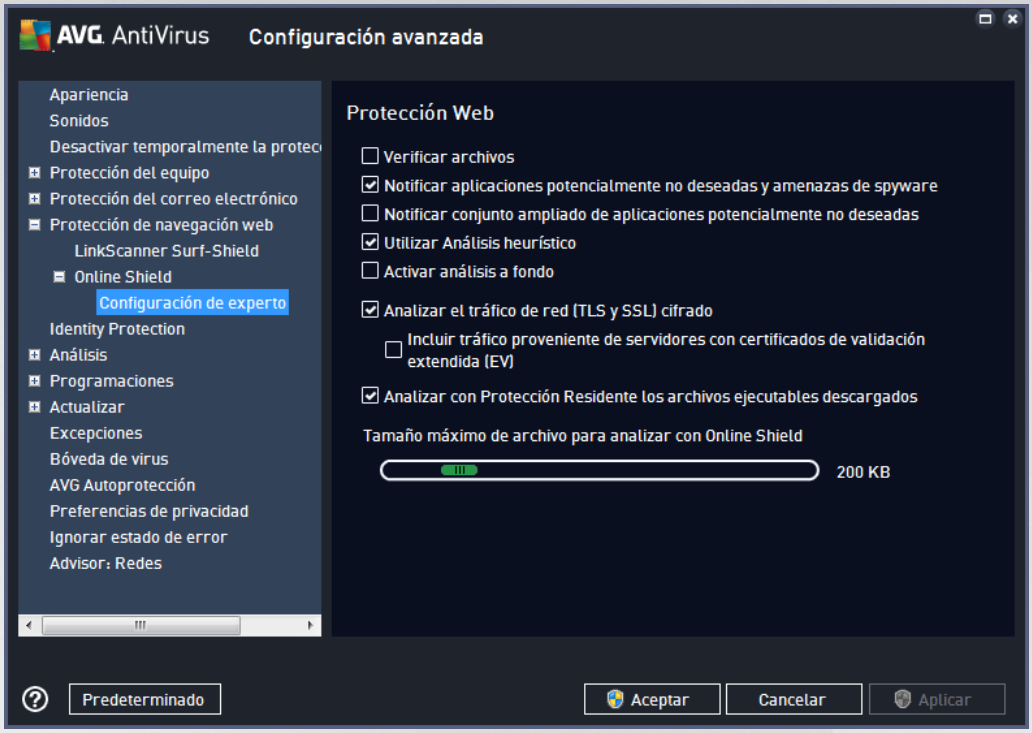


El cuadro de diálogo ***Online Shield*** ofrece las siguientes opciones:

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

Modo de notificación de amenazas

En la sección inferior del cuadro de diálogo, seleccione el método que desea utilizar para recibir información sobre una posible amenaza detectada: a través de un cuadro de diálogo emergente estándar, a través de notificación de balón de bandeja o a través de información del icono de la bandeja.



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:

- Verificar archivos (desactivada de forma predeterminada): Analiza el contenido de los archivos que pudieran existir en la página web que se visualizará.
- Analizar programas potencialmente no deseados y amenazas de Spyware (activada de forma predeterminada): Seleccionar para activar el análisis de spyware, además 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- Informar sobre conjunto mejorado de aplicaciones potencialmente no deseadas (desactivada de forma predeterminada): seleccione esta opción para detectar un paquete extendido de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- Utilizar heurística (activada de forma predeterminada): Analiza el contenido de la página que se visualizará utilizando el método de análisis heurístico (emulación dinámica de las instrucciones del objeto analizado en un entorno virtual).
- Activar análisis a fondo (desactivada de forma predeterminada): En determinadas situaciones (con sospechas de que el equipo está infectado) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro.

Pero recuerde que este método consume mucho tiempo.

- Analizar el tráfico de red (TLS y SSL) cifrado (activada por defecto): Deje marcada esta opción para permitir a AVG analizar también toda la comunicación de red cifrada, es decir, las conexiones sobre protocolos de seguridad (SSL y su versión más reciente, TLS). Esto se aplica a sitios web que utilizan HTTPS y conexiones de clientes de correo electrónico que utilizan TLS/SSL. El tráfico protegido se descifra, se analiza para detectar malware y se vuelve a cifrar para devolverlo protegido a su computadora. Dentro de esta opción puede decidir incluir el tráfico de servidores con certificados de validación extendida (EV) y analizar también la comunicación de red cifrada de servidores con certificado de validación extendida. La emisión de un certificado de validación extendida requiere la validación extensiva a través de la autoridad de certificación y los sitios web operados conforme al certificado, por lo tanto, son mucho más confiables (menos propensos a distribuir malware). Por este motivo, es posible que decida no analizar el tráfico proveniente de servidores con certificación de EV, lo cual hará que la comunicación cifrada sea moderadamente más rápida.

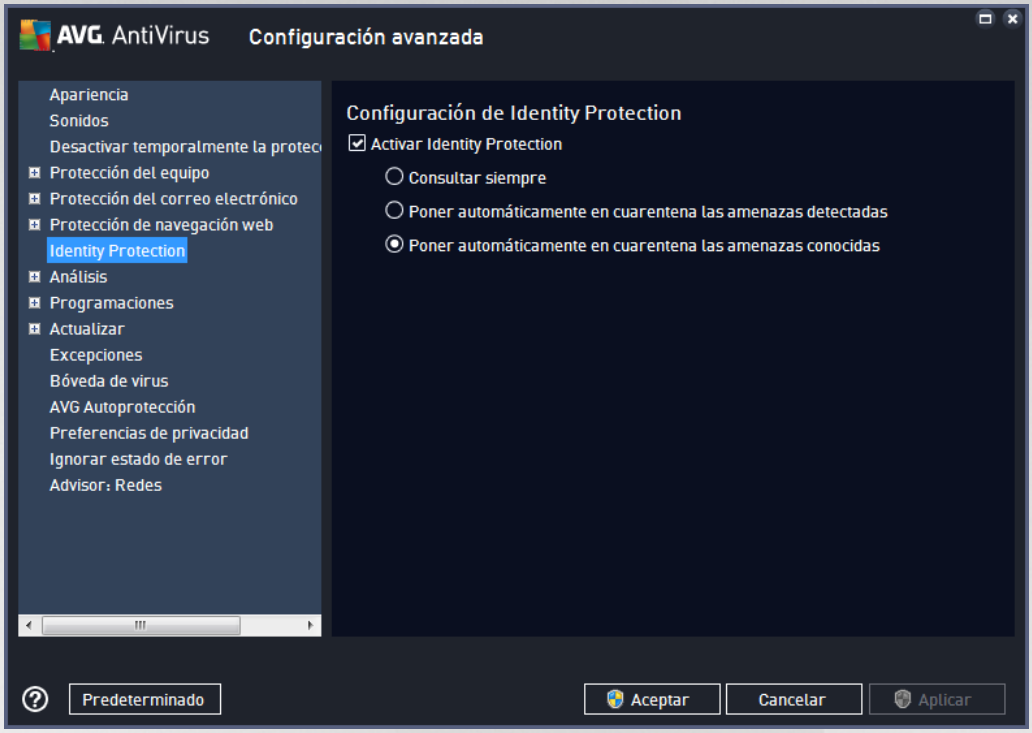
- Analizar archivos ejecutables descargados con Protección Residente (activada de forma predeterminada): Analice archivos ejecutables (generalmente archivos con extensiones exe, bat, com) después de haberlos descargado. La Protección Residente analiza archivos antes de descargar para garantizar que ningún código malicioso ingrese a su equipo. Sin embargo, este análisis está limitado por el Tamaño máximo de parte del archivo que se va a analizar: ver el siguiente elemento en este cuadro de diálogo. Por ello, los archivos grandes se analizan parte por parte, y esto también se aplica a la mayoría de los archivos ejecutables. Los archivos ejecutables pueden realizar diferentes tareas en su equipo, y es vital que sean 100 % seguros. Esto se puede asegurar analizando el archivo en partes antes de descargarlo y también inmediatamente después de completada la descarga del archivo. Le recomendamos mantener esta opción seleccionada. Si desactiva esta opción, de todas maneras puede tener la seguridad de que AVG encontrará cualquier código posiblemente peligroso. Sólo en ocasiones no podrá evaluar un archivo ejecutable como un complejo, por lo tanto puede producir algunos falsos positivos.

El control deslizante de abajo en el cuadro de diálogo le permite definir el Tamaño máximo de parte del archivo que se va a analizar: si los archivos incluidos están presentes en la página visualizada, también puede analizar su contenido incluso antes de que se descarguen en el equipo. Sin embargo, el análisis de archivos grandes toma bastante tiempo y es posible que la descarga de la página web se ralentice de modo notable. Puede emplear la barra deslizante para especificar el tamaño máximo de archivo que se analizará con Online Shield. Incluso si el archivo descargado es más grande de lo especificado y, por lo tanto, no se analizará con Online Shield, todavía estará protegido: si el archivo está infectado, la Protección Residente lo detectará de inmediato.

7.7. Identity Protection

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

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 Identidad. ***Es altamente recomendable 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***: 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 desea ejecutar.
- ***Poner automáticamente en cuarentena las amenazas detectadas***: seleccione esta casilla de verificación para especificar que desea mover inmediatamente todas las amenazas posibles detectadas al lugar seguro de la Bóveda de virus. Si se mantiene la configuración predeterminada, cuando se detecte una amenaza, se le preguntará si desea ponerla en cuarentena para tener la seguridad de que no se elimine ninguna de las aplicaciones que desea ejecutar.
- ***Poner automáticamente en cuarentena las amenazas conocidas*** (*activada de forma predeterminada*): mantenga este elemento marcado si desea que todas las aplicaciones detectadas como posible malware se muevan automáticamente y de inmediato a la Bóveda de virus.

7.8. 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:

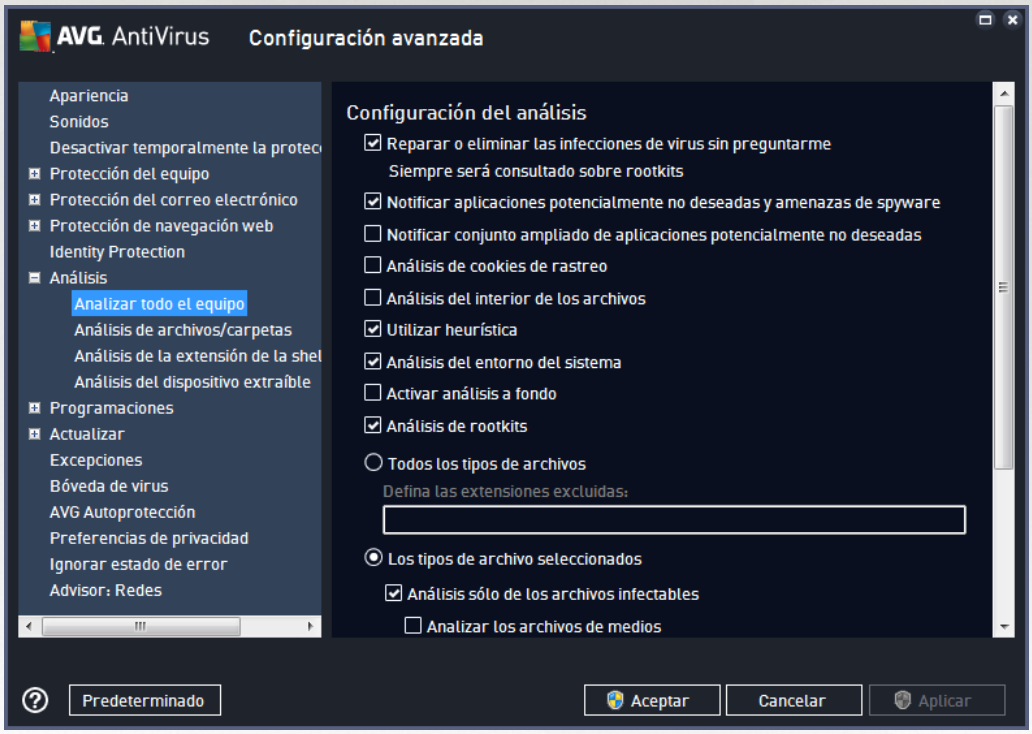
- Analizar todo el equipo: análisis predefinido estándar de todo el equipo
- Análisis de archivos/carpetas: análisis estándar predefinido de áreas seleccionadas del equipo

- Análisis de la extensión de la shell: análisis específico de un objeto seleccionado directamente del entorno del Explorador de Windows

- Análisis del dispositivo extraíble: análisis específico de dispositivos extraíbles conectados a su equipo

7.8.1. Analizar todo el equipo

La opción ***Análisis Completo del Equipo*** le permite editar los parámetros de uno de los análisis predefinidos por el proveedor de software, el Análisis Completo del Equipo:



Configuración del análisis

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

- ***Reparar o eliminar las infecciones de virus sin preguntarme*** (*activada de forma 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 aplicaciones potencialmente no deseadas y amenazas de Spyware*** (*activada de forma predeterminada*): Seleccione esta opción para activar el análisis de spyware y 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- ***Informar sobre conjunto mejorado de aplicaciones potencialmente no deseadas*** (*desactivada de*

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

- ***Análisis de cookies de rastreo*** (*desactivada de forma predeterminada*): Este parámetro estipula que se deben detectar las cookies; (*las cookies HTTP se utilizan para la autenticación, el rastreo y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de sus carritos de compras electrónicos*)

- ***Análisis del interior de los archivos*** (*desactivada de forma predeterminada*): Este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos, por ejemplo, ZIP, RAR etc.

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

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

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

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

También debe decidir si desea analizar

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

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

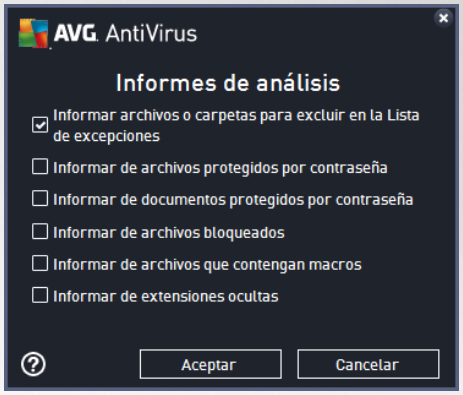
- De manera opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben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

Ajustar el tiempo que tarda el análisis en completarse

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

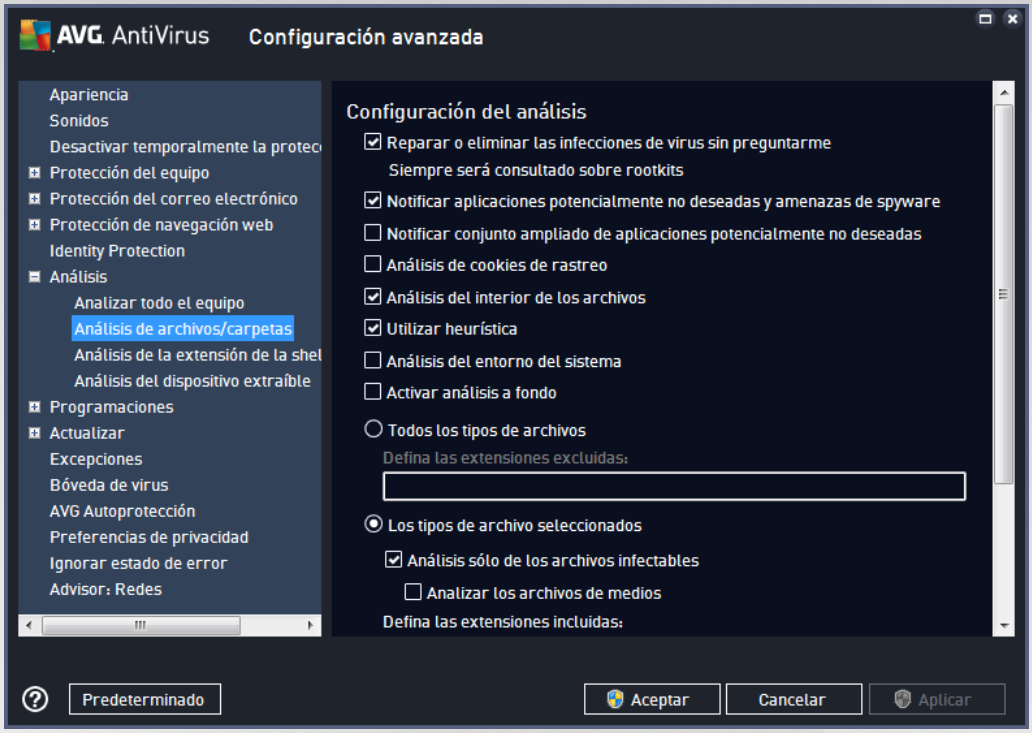
Configurar informes de análisis adicionales...

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



7.8.2. Análisis de archivos/carpetas

La interfaz de edición para el ***Análisis de archivos o carpetas específicos*** es casi idéntica al cuadro de diálogo de edición del Análisis de todo el equipo, sin embargo, la configuración predeterminada es más estricta para el Análisis de todo el equipo:

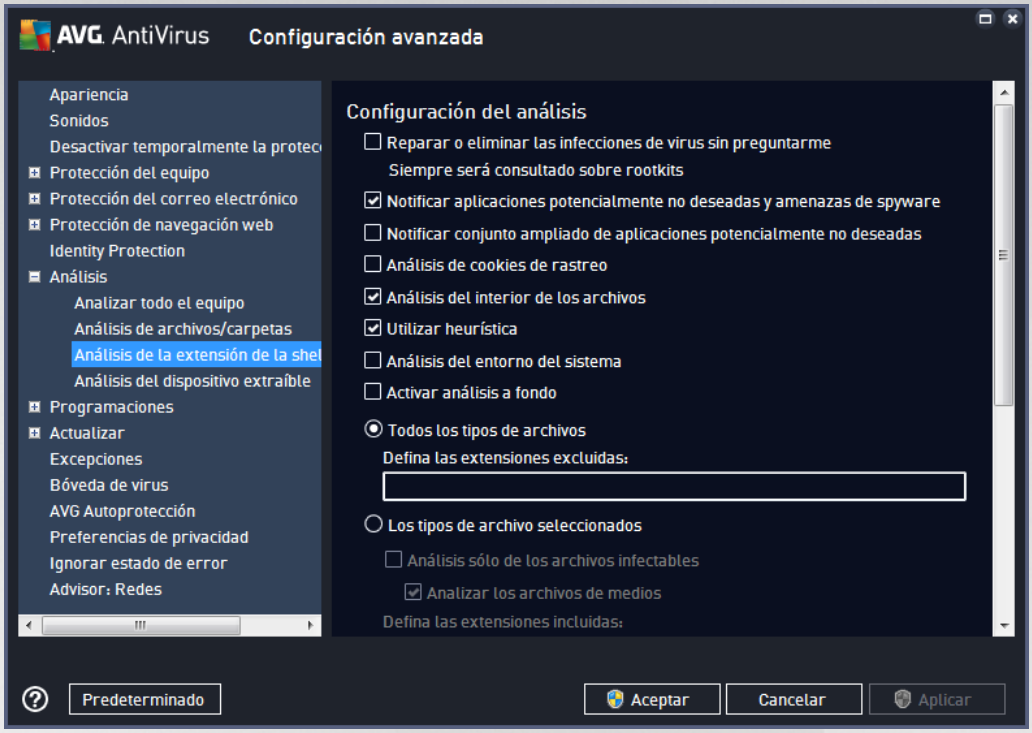


Todos los parámetros definidos en este diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con Análisis de archivos o carpetas específicos.

Nota: *Para obtener una descripción de los parámetros específicos, consulte el capítulo Configuración avanzada de AVG/Análisis/Análisis de toda la PC.*

7.8.3. Análisis de la extensión de la shell

De modo parecido al elemento anterior, Analizar 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 de Windows Explorer (*extensión de consola*), consulte el capítulo Análisis en Windows Explorer:



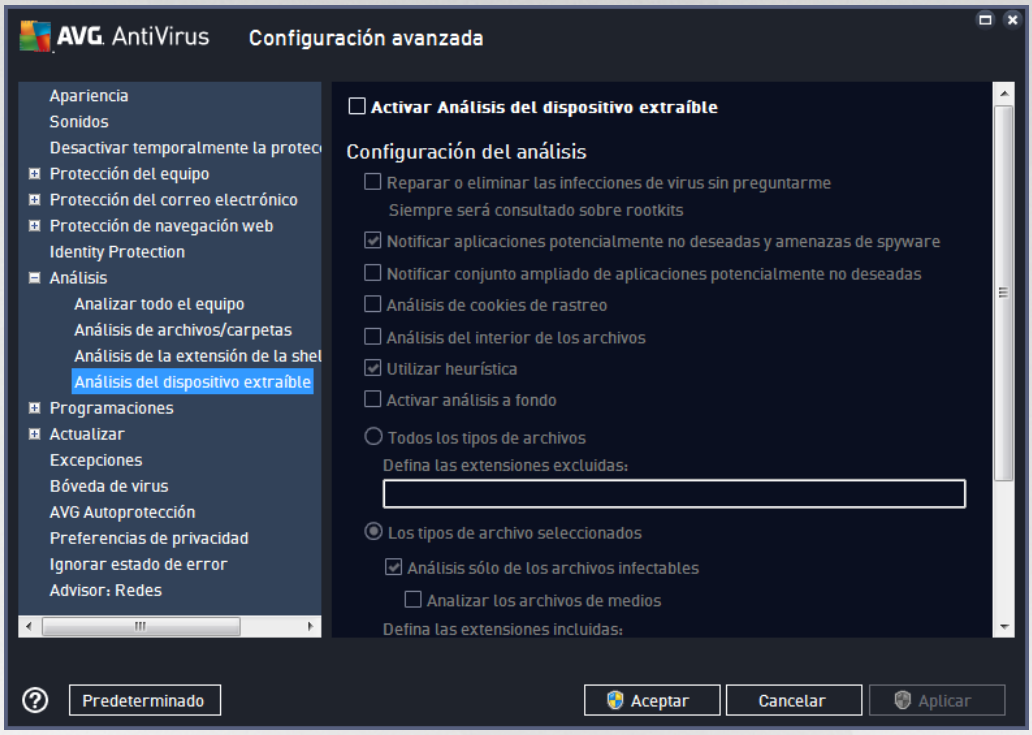
Las opciones de edición son casi idénticas a las disponibles para Analizar todo el equipo, sin embargo, la configuración predeterminada es diferente (*por ejemplo, el análisis de todo el equipo no comprueba de manera predeterminada los archivos, pero sí analiza el entorno del sistema, mientras que con el análisis de extensión de la shell es al revés*).

Nota: *Para obtener una descripción de los parámetros específicos, consulte el capítulo Configuración avanzada de AVG/Análisis/Análisis de toda la PC.*

En comparación con el cuadro de diálogo Analizar todo el equipo, el cuadro de diálogo ***Análisis de la extensión de la shell*** también incluye la sección denominada ***Visualización de progreso del análisis y sus resultados***, donde puede especificar si desea tener acceso al progreso del análisis y sus resultados desde la interfaz de 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.

7.8.4. Análisis del dispositivo extraíble

La interfaz de edición para el ***Análisis del Dispositivo Extraíble*** también es muy parecida al cuadro de diálogo de edición para el Análisis Completo del Equipo:



El ***Análisis del dispositivo extraíble*** se inicia automáticamente cada vez que conecta algún dispositivo extraíble a la PC. 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/Analizar toda la PC.*

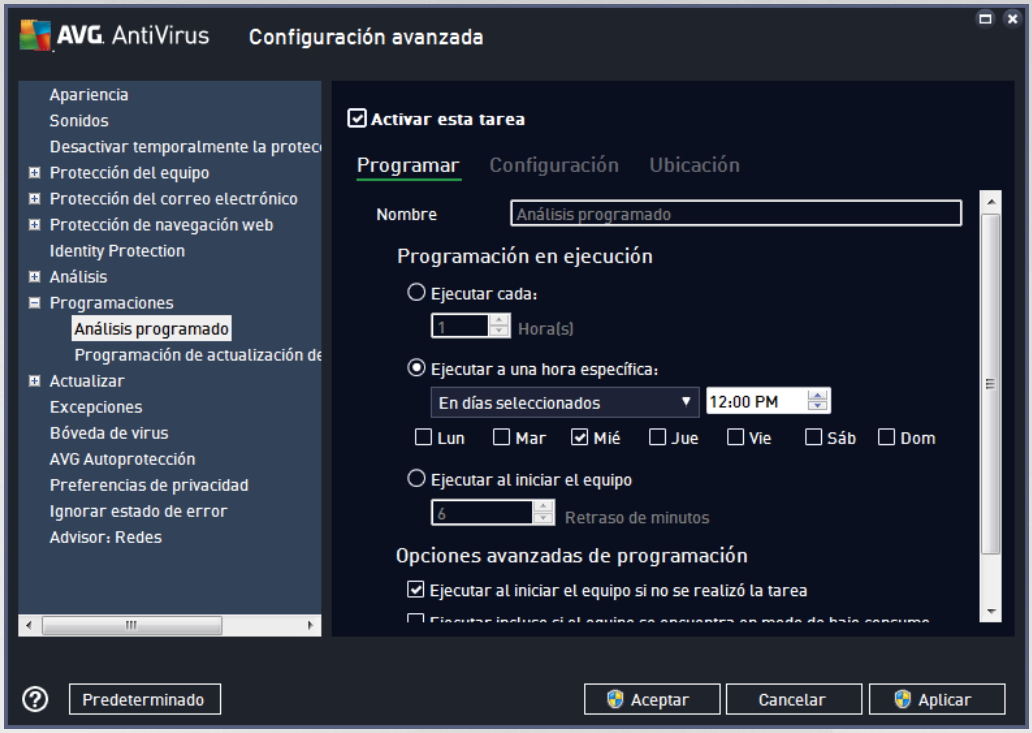
7.9. Programaciones

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

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

7.9.1. Análisis programado

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



A continuación, el campo de texto ***Nombre*** (*desactivado para todos los programas predeterminados*) indica el nombre asignado a este programa por proveedor de 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. Por otro lado, un ejemplo de un buen nombre descriptivo sería "Análisis de áreas del sistema", etc. Tampoco es necesario especificar en el nombre del análisis si se trata del análisis de toda la PC o solo un análisis de archivos o carpetas seleccionados. Sus propios análisis siempre serán una versión específica del análisis de los archivos o carpetas seleccionados.*

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

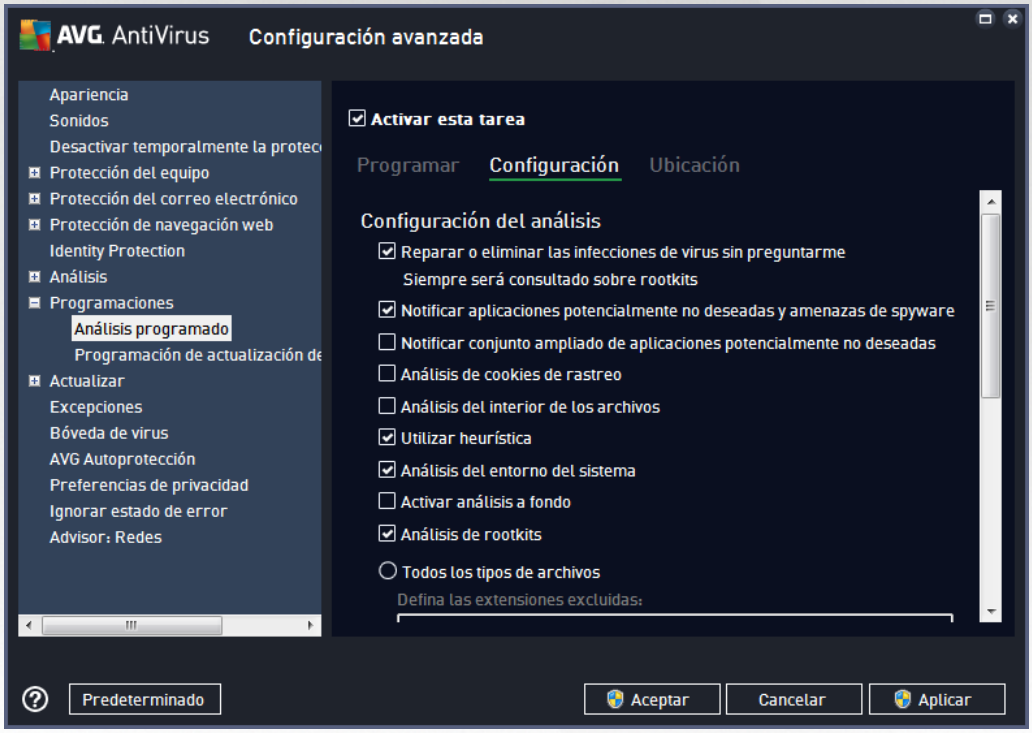
Programación en ejecución

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 período de tiempo determinado (***Ejecutar cada...***), estableciendo una fecha y una hora exactas (***Ejecutar en horas específicas***) o estableciendo un evento al que debe estar asociada la ejecución del análisis (***Ejecutar al iniciar el equipo***).

Opciones avanzadas de programación

- ***Ejecutar al iniciar la PC si no se realizó la tarea***: si programa la tarea para que se ejecute a una hora específica, esta opción le garantiza que el análisis se realizará posteriormente en caso de que la PC esté apagada en el horario programado.

- ***Ejecutar incluso si la PC se encuentra en modo de bajo consumo***: la tarea se debe llevar a cabo a la hora programada aun si la PC está funcionando con batería.



En la pestaña ***Configuración*** 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 / eliminar una infección de virus sin preguntarme*** *(activada de forma predeterminada):* Si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.

- ***Analizar aplicaciones potencialmente no deseadas y amenazas de Spyware*** *(activada de forma predeterminada):* Seleccione esta opción para activar el análisis de spyware, además 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- ***Informar sobre conjunto mejorado de aplicaciones potencialmente no deseadas*** (*desactivada de forma predeterminada*): Seleccione esta opción para detectar paquetes extendidos de spyware:

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

- ***Análisis de cookies de rastreo*** (*desactivada de forma predeterminada*): este parámetro especifica que se deben detectar cookies durante el análisis; (las cookies *HTTP se utilizan para la autenticación, el rastreo y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de sus carritos de compras electrónicos*).

- ***Análisis del interior de los archivos*** (*desactivado de forma predeterminada*): este parámetro especifica que el análisis debe comprobar todos los archivos, incluso si se almacenan dentro de un archivo, por ejemplo, ZIP, RAR, etc.

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

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

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

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

También debe decidir si desea analizar

- ***Todos los tipos de archivos***: además cuenta con la opción 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.

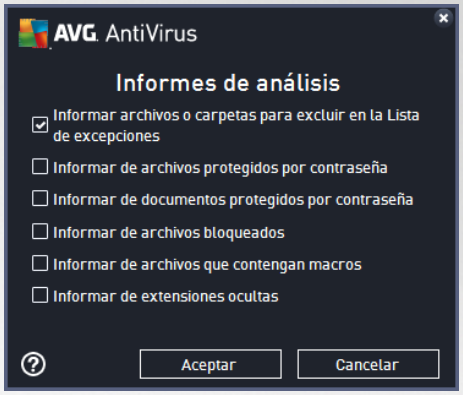
- De manera opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben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

Ajustar el tiempo que tarda el análisis en completarse

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

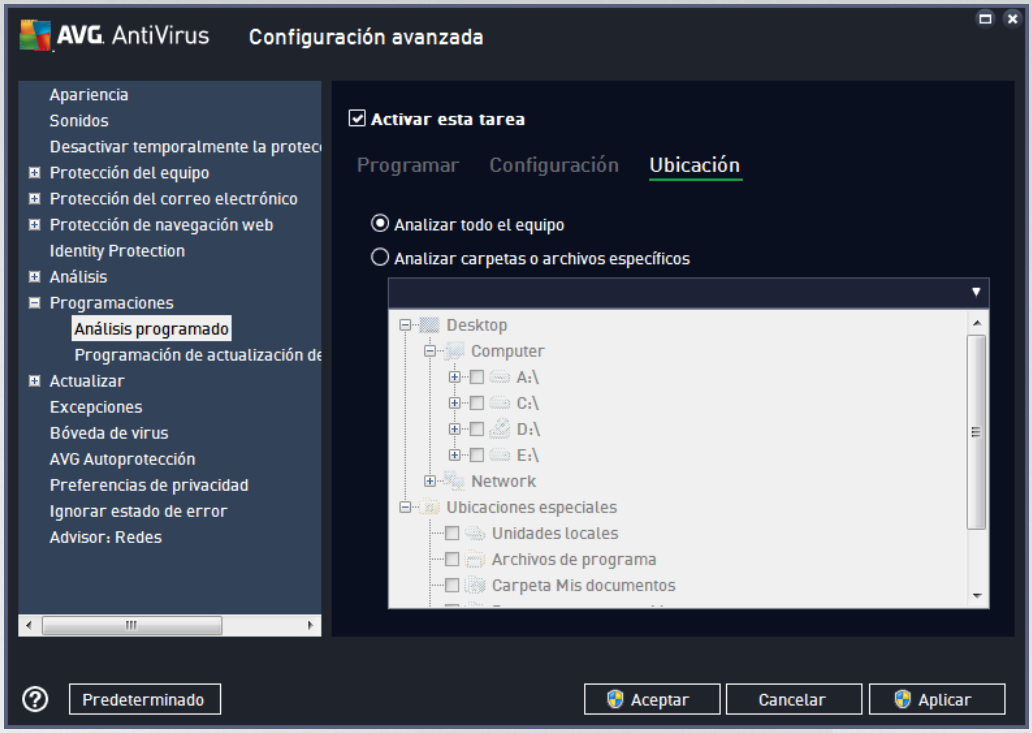
Configurar informes de análisis adicionales

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



Opciones de apagado del equipo

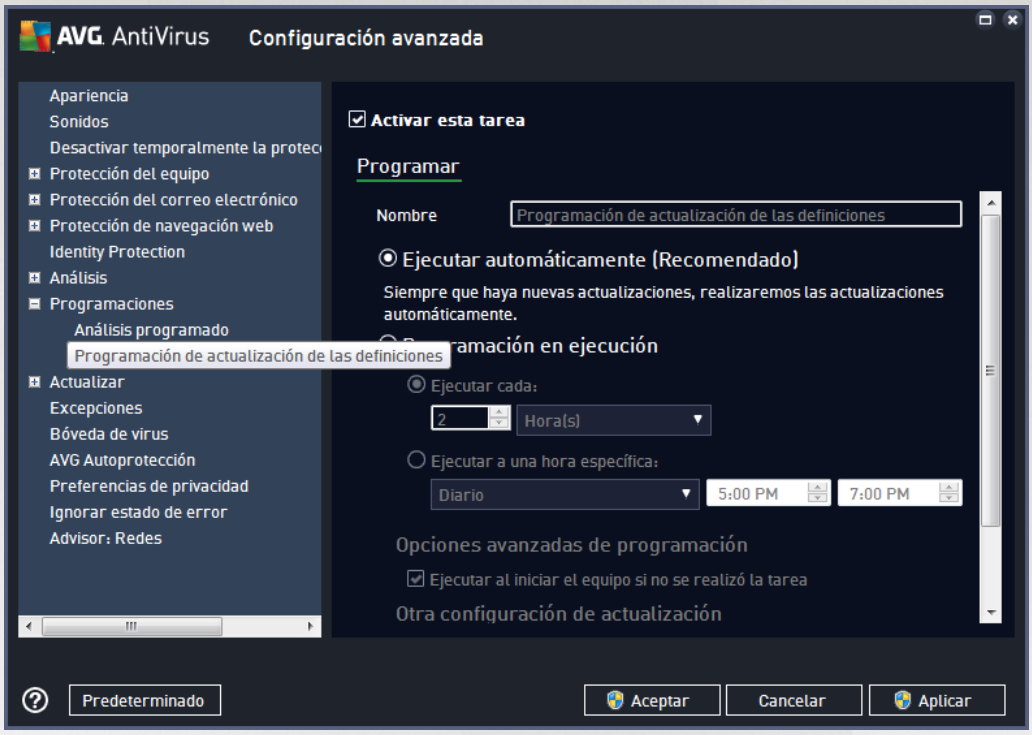
En la sección ***Opciones de apagado del equipo***: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite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



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

7.9.2. Programación de actualización de las definiciones

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



En este cuadro de diálogo puede configurar algunos parámetros detallados de la programación de actualización. El campo de texto ***Nombre*** (*desactivado para todos los programas predeterminados*) indica el nombre asignado a este programa por proveedor de programa.

Programación en ejecución

De manera predeterminada, la tarea se inicia automáticamente (***Ejecución automática***) tan pronto como esté disponible una nueva actualización de definiciones de virus. Le recomendamos que mantenga esta configuración, a menos que haya una buena razón para obrar de manera contraria. En este último caso, puede configurar el inicio de la tarea manualmente y especificar los intervalos de tiempo para la nueva programación de inicio de actualización de definiciones. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto período de tiempo (***Ejecutar cada...***) o definiendo una fecha y hora exactas (***Ejecutar en horas específicas***).

Opciones avanzadas de programación

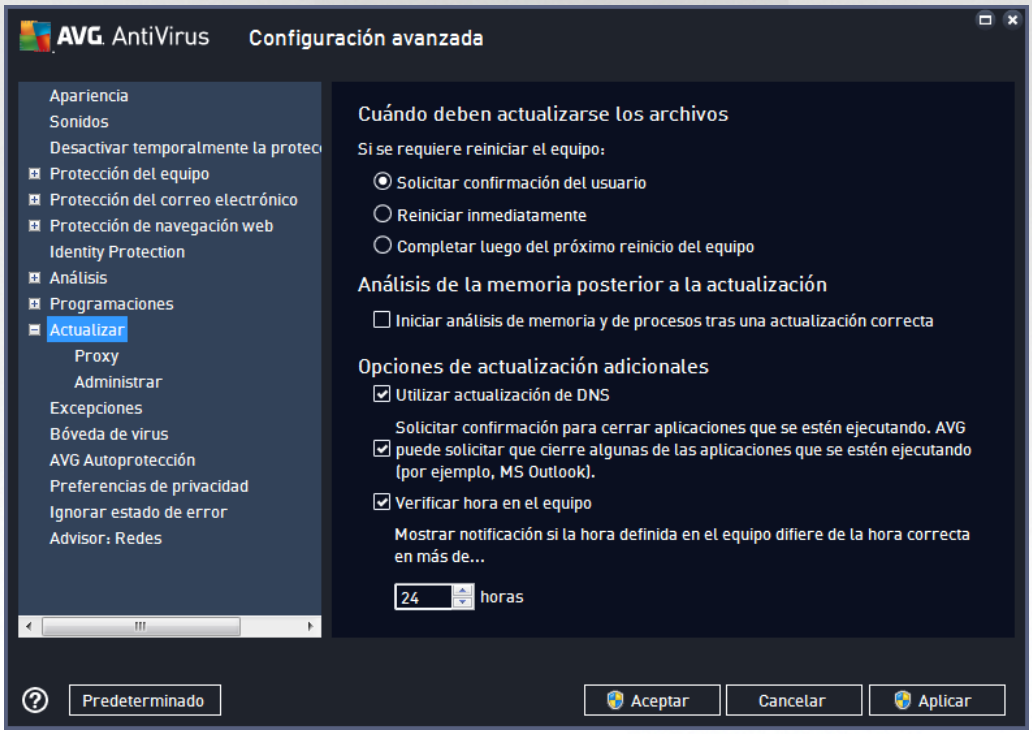
Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

Otra configuración de actualización

Finalmente, marque la opción ***Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet*** para asegurarse de que, si se interrumpe la conexión a Internet y el proceso de actualización de Anti-Spam falla, se iniciará otra vez inmediatamente después de restaurar la conexión a Internet. Una vez que se inicia 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)*.

7.10. Actualizar

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



Cuándo deben actualizarse los archivos

En esta sección, puede seleccionar entre tres opciones alternativas para utilizar en caso de que el proceso de actualización requiera un reinicio del equipo. Se puede programar la finalización de la actualización para el próximo reinicio del equipo, o bien se puede ejecutar el reinicio inmediatamente:

- ***Solicitar confirmación del usuario*** *(activada de forma predeterminada)*: se le pedirá que apruebe un reinicio de la PC, necesario para finalizar el proceso de actualización
- ***Reiniciar inmediatamente***: la PC se reiniciará inmediatamente de forma automática después de que el proceso de actualización haya finalizado, y no será necesaria la aprobación del usuario

- ***Completar luego del próximo reinicio de la PC***: la finalización del proceso de actualización se pospondrá hasta el próximo reinicio de la PC. Tenga en cuenta que esta opción sólo se recomienda si está seguro de que la PC 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

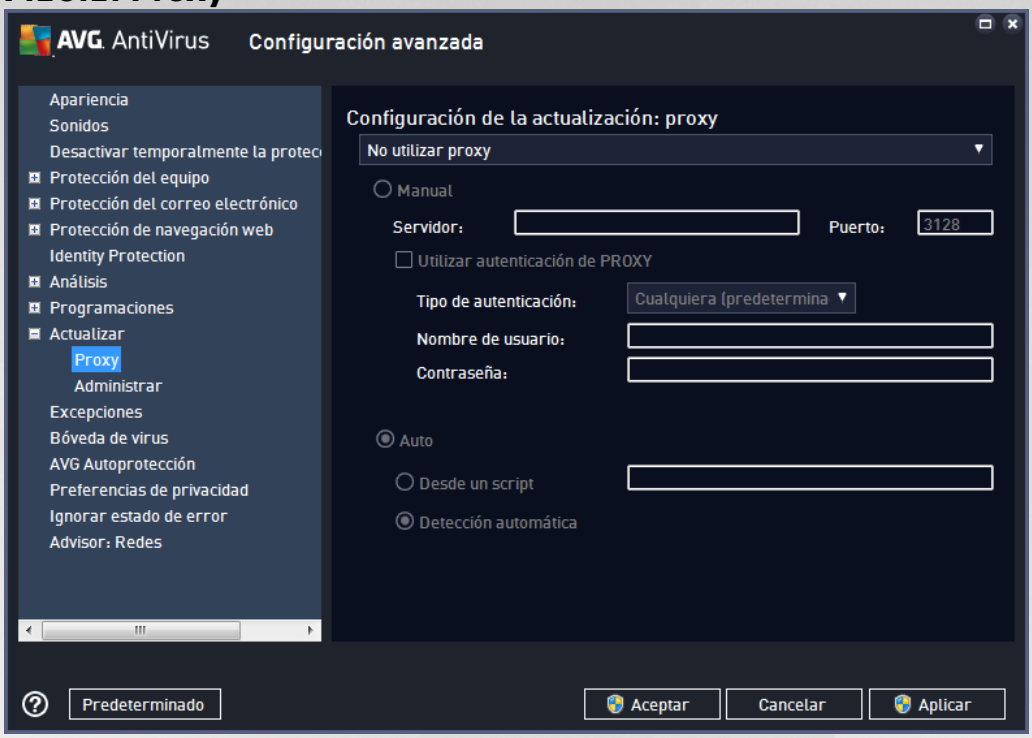
- ***Crear un punto de restauración del sistema nuevo en cada actualización del programa*** (*activada de forma predeterminada*): antes de iniciar cada actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, 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*** (*activada de forma predeterminada*): si este elemento está marcado, una vez que se inicia la actualización, su **AVG AntiVirus** busca la información sobre la última versión de la base de datos de virus y la última versión del programa en el servidor DNS. A continuación, sólo se descargan y aplican los archivos más pequeños e indispensables para la actualización. De esta manera, se minimiza la cantidad de datos que se deben descargar y el proceso de actualización se ejecuta con mayor rapidez.

- ***Solicitar confirmación para cerrar aplicaciones que se están ejecutando*** (*activada de forma predeterminada*): con este elemento tendrá la seguridad de que ninguna aplicación actualmente en ejecución se cerrará sin su permiso, si se requiere para que el proceso de actualización finalice.

- ***Verificar hora en la PC*** (*activada de forma predeterminada*): marque esta opción para declarar que desea recibir una notificación en caso de que la hora de la PC difiera por más horas de las especificadas de la hora correcta.

7.10.1. Proxy



El servidor proxy es un servidor independiente o un servicio que funciona en la PC que garantiza una conexión más segura a Internet. De acuerdo con las reglas especificadas de red puede acceder a Internet ya sea 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:

- ***No utilizar proxy***: configuración predeterminada
- ***Utilizar proxy***
- ***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.

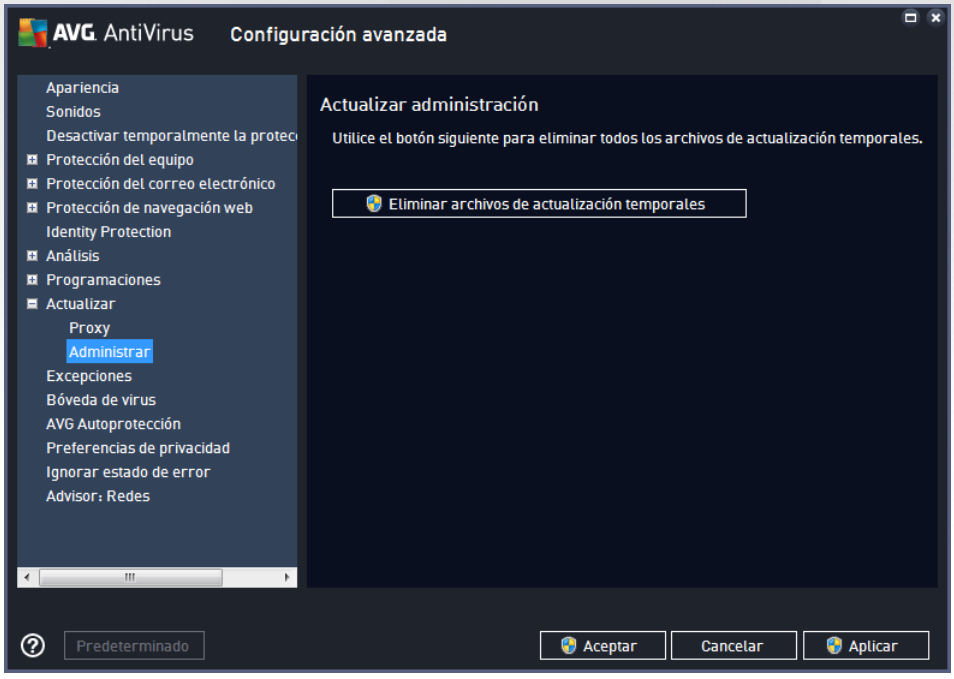
Configuración automática

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 leerá desde el navegador de internet predeterminado
- ***Desde un 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

7.10.2. Administrar

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

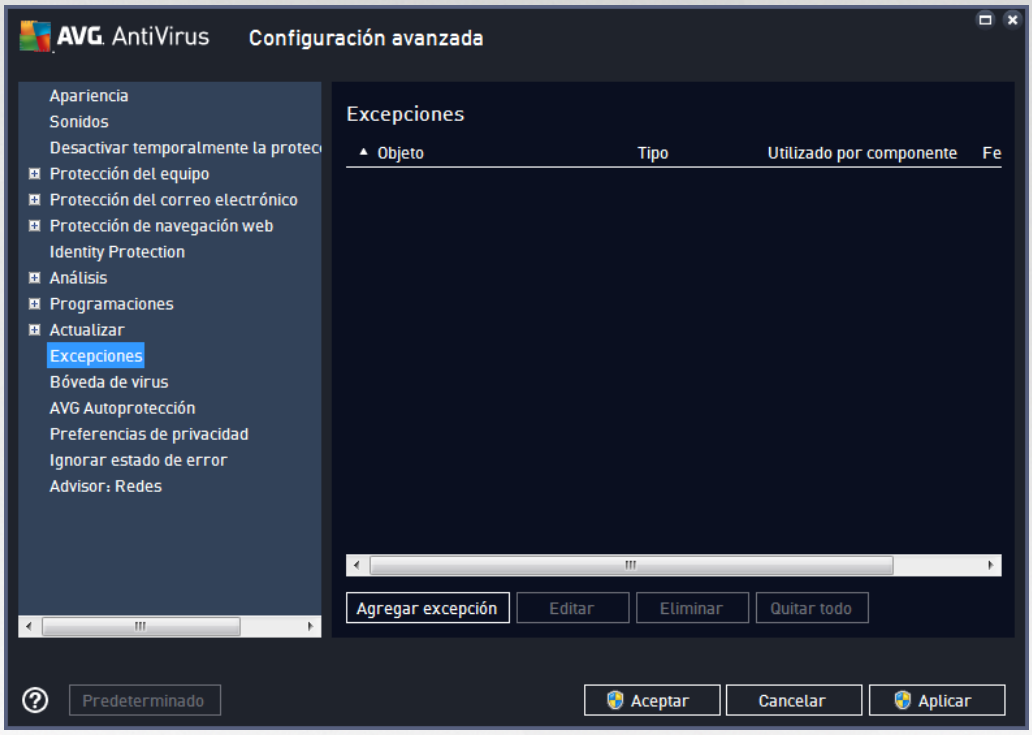


- ***Eliminar archivos de actualización temporales***: presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada estos archivos se guardan durante 30 días*)
- ***Revertir la base de datos de virus a la versión anterior***: presione este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

7.11. Excepciones

En el cuadro de diálogo ***Excepciones*** puede definir excepciones, es decir, elementos que **AVG AntiVirus** ignorará. Generalmente, deberá definir una excepción si AVG continúa detectando un programa o archivo como amenaza, o bloqueando un sitio web seguro como peligroso. Agregue ese archivo o sitio web a esta lista de excepciones, y AVG no le informará sobre él ni lo bloqueará más.

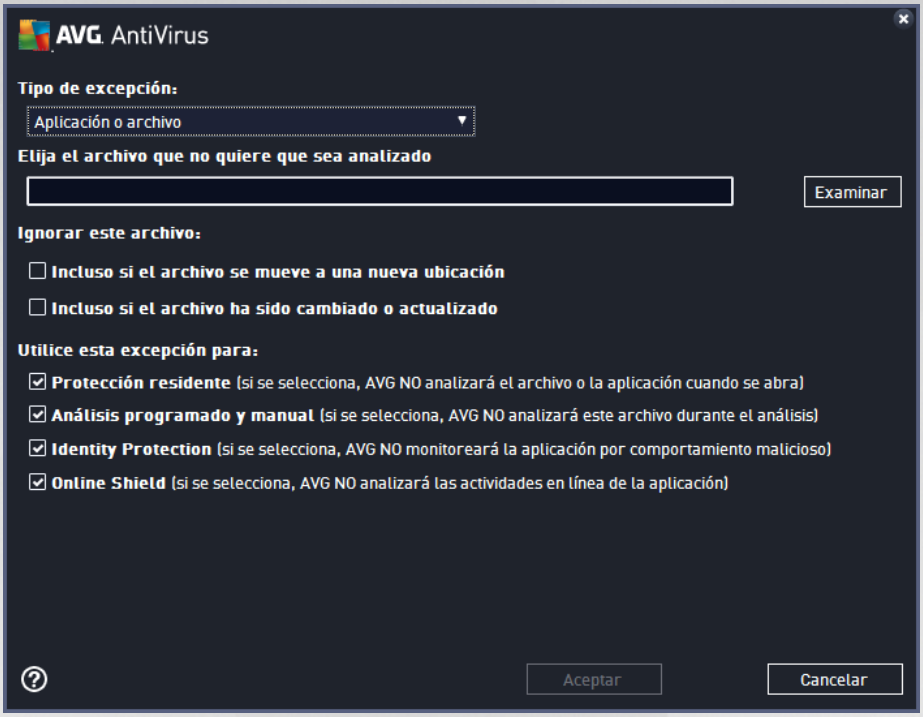
¡Siempre asegúrese de que el archivo, programa o sitio web en cuestión realmente es seguro!



La tabla en el cuadro de diálogo muestra una lista de excepciones, si ya se definió alguna. Cada elemento tiene una casilla de verificación a su lado. Si la casilla de verificación está marcada, la excepción está en vigor; en caso contrario, la excepción está definida, pero no se utiliza. Al hacer clic en un encabezado de columna, puede ordenar los elementos permitidos según sus criterios respectivos.

Botones de control

- ***Agregar excepción***: haga clic para abrir un nuevo cuadro de diálogo donde puede especificar el elemento que debe excluirse del análisis de AVG.



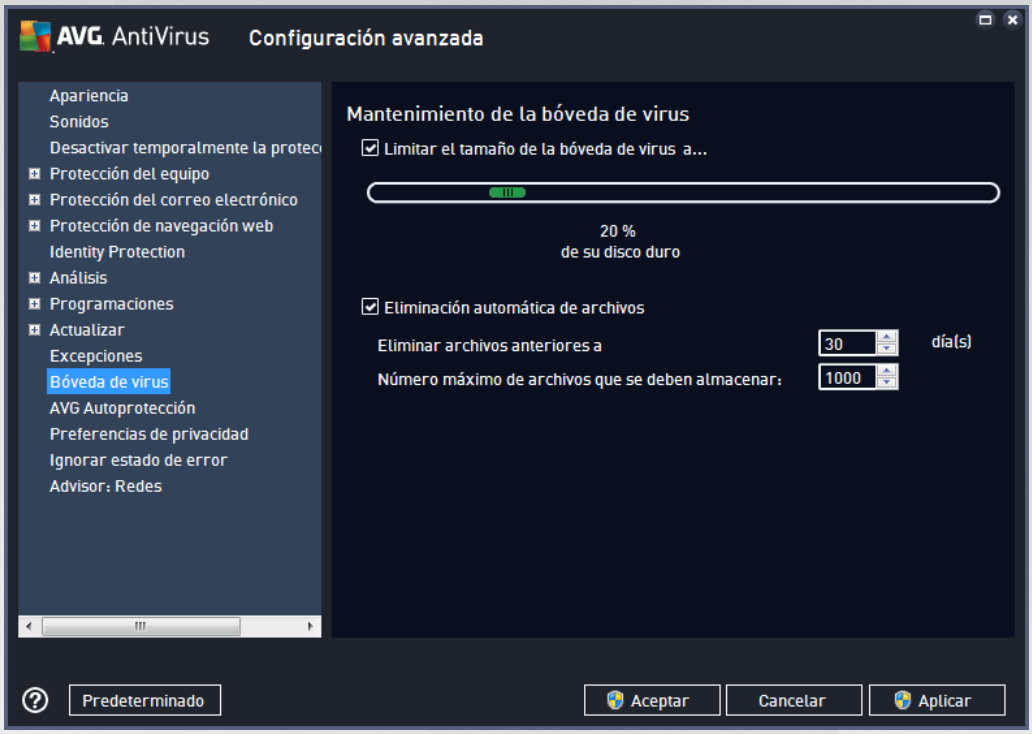
En primer lugar, se lo invitará a definir el tipo de objeto, es decir, si se trata de una aplicación, un archivo, una carpeta, una URL o un certificado. A continuación, deberá examinar su disco para proporcionar la ruta de acceso al objeto respectivo o escribir la URL. Finalmente, puede seleccionar las funciones de AVG que deben ignorar el objeto seleccionado *(Protección Residente, Identity Protection, Análisis)*.

- ***Editar***: este botón solamente está activo si ya se han definido algunas excepciones y se enumeran en la tabla. Luego, puede usar el botón para abrir el cuadro de diálogo de edición sobre una excepción seleccionada y configurar los parámetros de la excepción.

- ***Eliminar***: utilice este botón para cancelar una excepción previamente definida. Puede eliminarlas una por una, o resaltar un bloque de excepciones en la lista y cancelar las excepciones definidas. Después de cancelar la excepción, el archivo, carpeta o URL respectivo será comprobado por AVG otra vez. Tenga en cuenta que sólo se quitará la excepción, no el archivo ni la carpeta.

- ***Eliminar todo***: use este botón para borrar todas las excepciones definidas en la lista.

7.12. Bóveda de virus

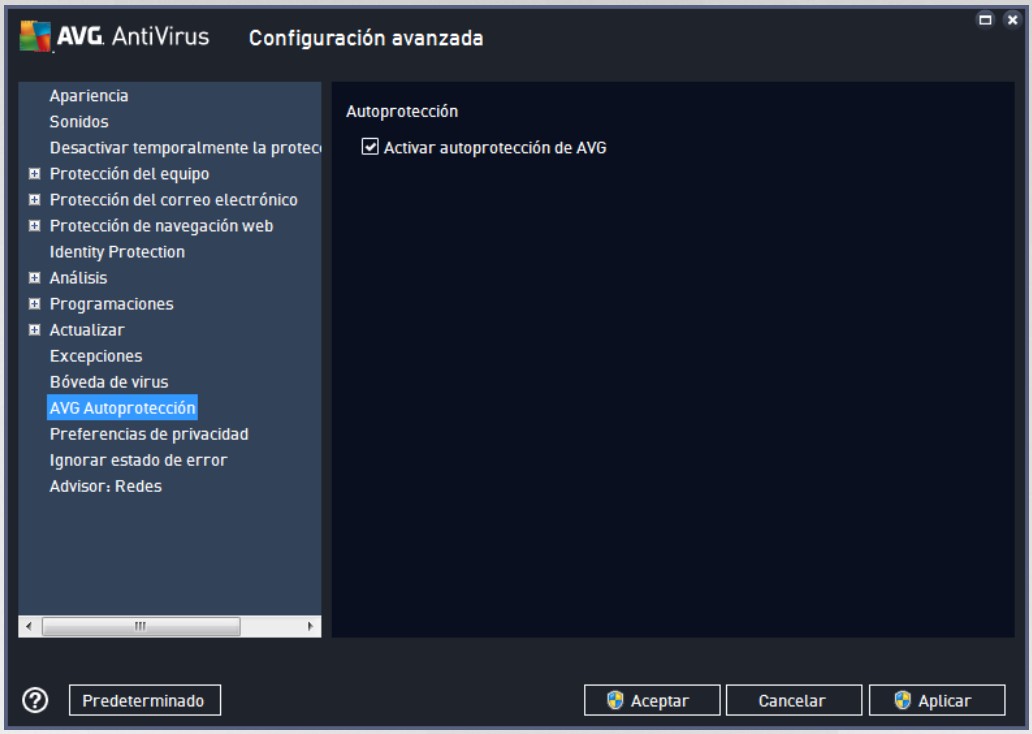


El cuadro de diálogo ***Mantenimiento de la Bóveda de Virus*** permite definir varios parámetros relacionados con la administración de objetos almacenados en la Bóveda de Virus:

- ***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 se define la longitud máxima de tiempo que los objetos deben almacenarse en la Bóveda de virus (***Eliminar archivos después de los... días***) y la cantidad máxima de archivos que se almacenará en la Bóveda de virus (***Número máximo de archivos que se deben almacenar***).

7.13. Autoprotección AVG

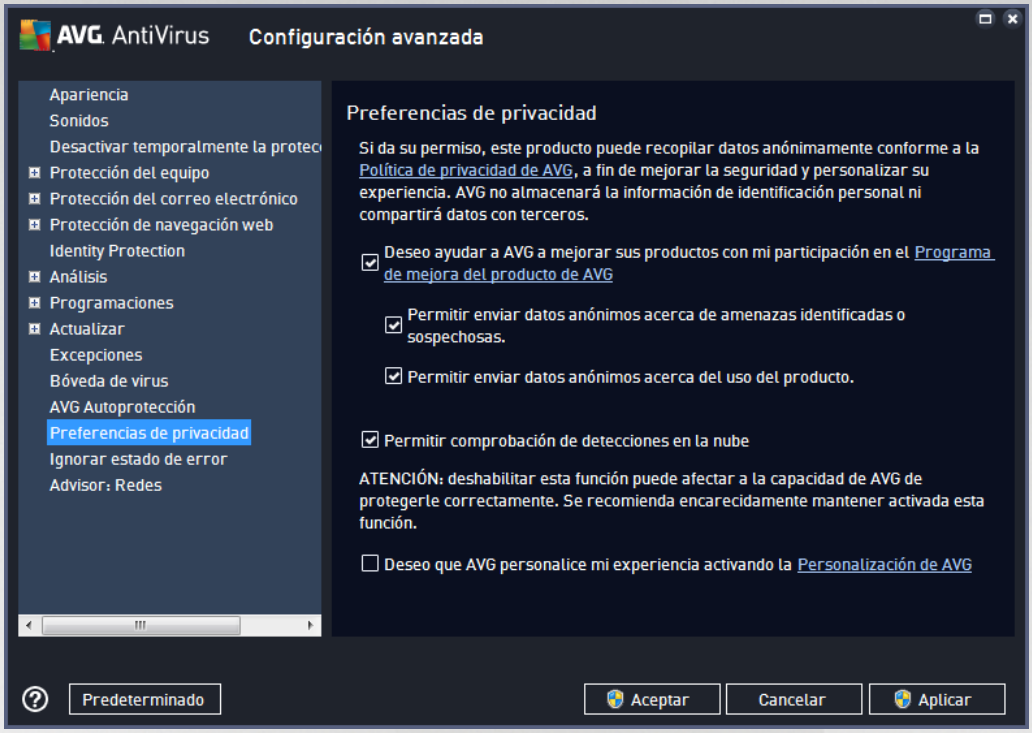


El elemento ***Autoprotección AVG*** permite **AVG AntiVirus** proteger sus propios procesos, archivos, claves de registro y controladores para que no se modifiquen ni desactiven. La razón principal para esta clase de protección es que algunas amenazas sofisticadas intentan desactivar la protección antivirus y luego causan daño a la PC libremente.

Recomendamos que esta función se mantenga activada.

7.14. Preferencias de privacidad

Este ***cuadro de diálogo*** le invita a participar en la mejora del producto AVG, así como a ayudarnos a aumentar el nivel de seguridad global de Internet. Sus informes nos permiten recopilar información actualizada sobre las últimas amenazas de participantes de todo el mundo y, a cambio, podemos mejorar la protección para todos. Los informes se crean de manera automática y, por lo tanto, no ocasiona inconvenientes. No se incluyen datos personales en los informes. Aunque el envío de informes de las amenazas detectadas es opcional, le pedimos que mantenga activada esta opción puesto que nos ayuda a mejorar la protección para los usuarios de AVG.



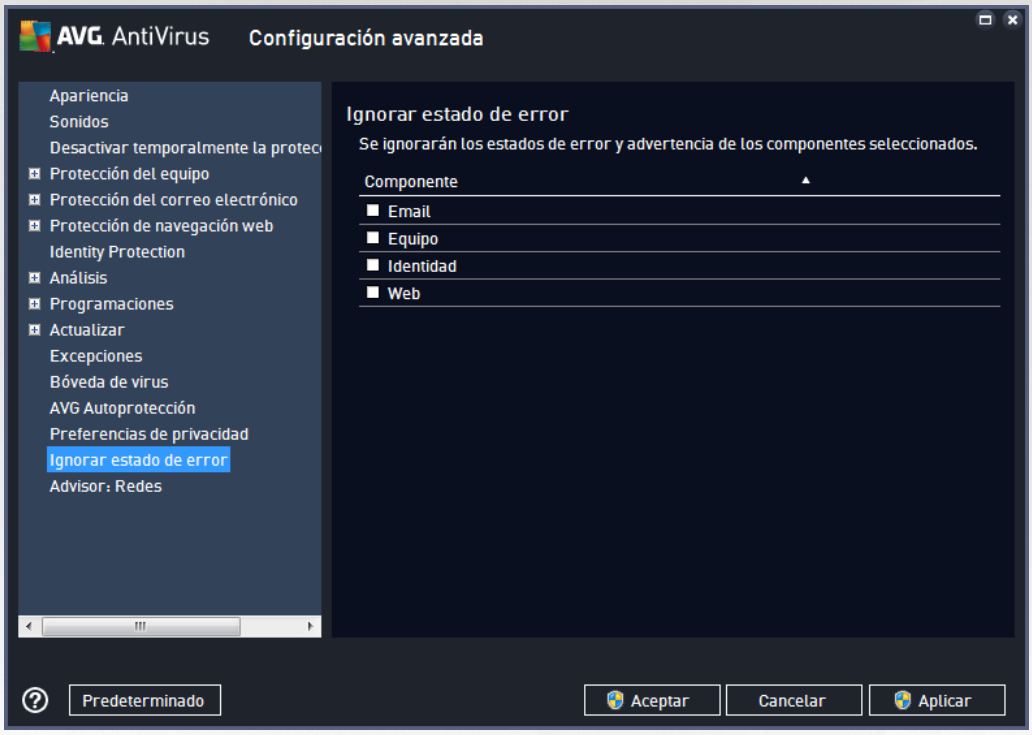
En el cuadro de diálogo, están disponibles las siguientes opciones de configuración:

- ***Deseo ayudar a AVG a mejorar los productos a través de la participación en el Programa de mejora del producto AVG*** *(activada de forma predeterminada)*: si desea ayudarnos a mejorar **AVG AntiVirus**, deje marcada la casilla de verificación. De este modo, se podrán notificar todas las amenazas encontradas a AVG, por lo que podremos recopilar información actualizada sobre malware de todos los participantes repartidos por el mundo y, a cambio, mejorar la protección de todos. El informe se realiza automáticamente, por lo que no le causa ninguna molestia, y no incluye ningún dato de identificación personal.
    - ***Permitir enviar datos acerca de correo electrónico mal identificado, previa autorización del usuario*** *(activada de forma predeterminada)*: envíe información sobre mensajes de correo electrónico identificados incorrectamente como spam o sobre mensajes de spam no detectados por el servicio Anti-Spam. Al enviar este tipo de información, se solicitará su confirmación.
    - ***Permitir enviar datos anónimos acerca de amenazas identificadas o sospechosas*** *(activada de forma predeterminada)*: envíe información sobre cualquier código o patrón de conducta sospechoso o definitivamente peligroso *(ya sea un virus, spyware o una página web maliciosa a la que intenta obtener acceso)* detectado en la PC.
    - ***Permitir enviar datos anónimos acerca del uso del producto*** *(activada de forma predeterminada)*: envíe datos estadísticos básicos sobre el uso de la aplicación, como el número de detecciones, análisis ejecutados, actualizaciones exitosas o no exitosas, etc.
- ***Permitir la comprobación de las detecciones en la nube*** *(activada de forma predeterminada)*: se comprobará si las amenazas detectadas están realmente infectadas, con el fin de descartar falsos positivos.

- ***Deseo que AVG personalice mi experiencia activando la Personalización de AVG*** *(desactivada de manera predeterminada)*: esta función analiza de forma anónima el comportamiento de los programas y las aplicaciones instalados en la PC. En función de esto, AVG puede ofrecerle servicios orientados a sus necesidades, para garantizarle la máxima seguridad.

7.15. Ignorar estado de error

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



De manera predeterminada, ningún componente está seleccionado en esta lista. Esto significa que, si algún componente se coloca en un estado de error, se le informará de inmediato por alguna de las siguientes vías:

- Icono del sistema: Mientras todas las partes de AVG funcionen correctamente, el icono se mostrará en cuatro colores; sin embargo, si ocurre un error, el icono aparece con un signo de admiración amarillo.

- Se muestra una descripción de texto del problema en la sección Información del estado de seguridad de la ventana principal de AVG.

Posiblemente surja una situación en la que por algún motivo necesite desactivar un componente temporalmente. Esta acción no se recomienda, debe intentar mantener todos los componentes activados de forma permanente y en la configuración predeterminada, pero puede suceder. En este caso el icono del sistema informa automáticamente el 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.

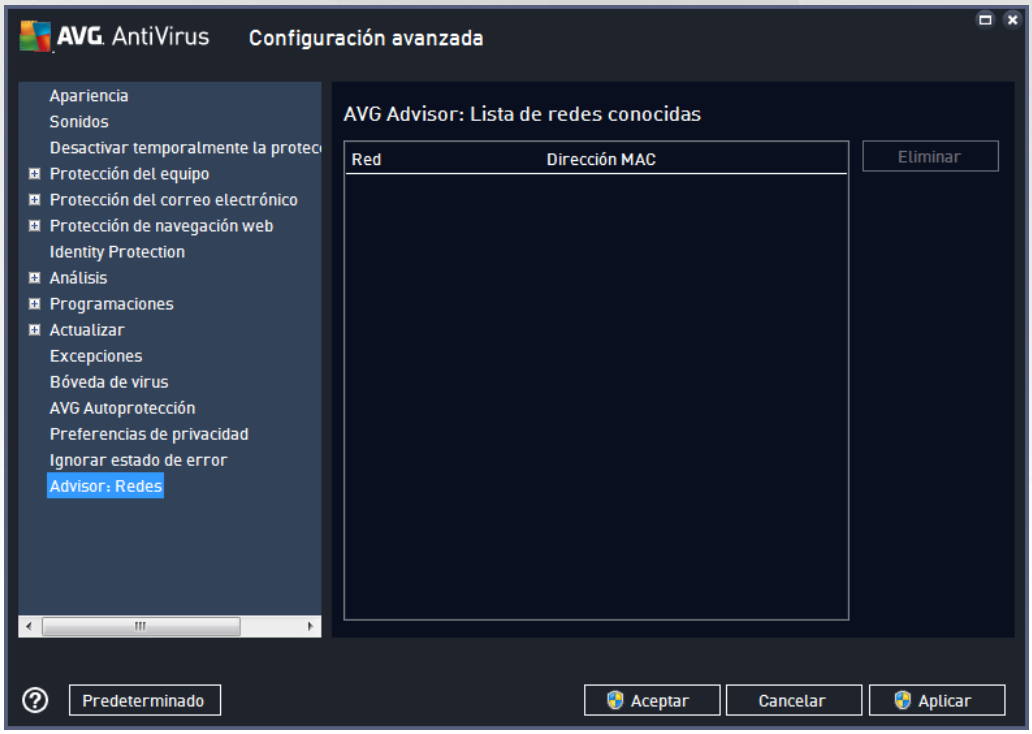
Para esta situación, dentro del cuadro de diálogo Ignorar estado de error puede seleccionar componentes que

pueden estar en un estado de error (o desactivado) y de los cuales no desee recibir información. Presione el botón Aceptar para confirmar.

7.16. Advisor: Redes conocidas

AVG Advisor incluye una función que monitorea redes a las cuales se conecta y, si detecta una red nueva (con el nombre de una red ya utilizada, lo cual puede generar confusión), lo notificará y le recomendará que verifique la seguridad de la red. Si decide que es seguro conectarse a la nueva red, también puede guardarla en esta lista (a través del vínculo proporcionado en la notificación de la bandeja de AVG Advisor que se desliza sobre la bandeja del sistema una vez que se detecta una red desconocida. Para obtener detalles, consulte el capítulo sobre AVG Advisor). AVG Advisor recordará luego los atributos únicos de la red (específicamente la dirección MAC) y no mostrará la notificación la próxima vez. Cada red a la que se conecte se considerará de forma automática la red conocida y se agregará a la lista. Puede eliminar entradas individuales presionando el botón Eliminar; la red respectiva se considerará como desconocida y potencialmente insegura nuevamente.

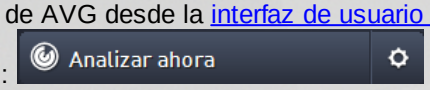
En esta ventana de diálogo, puede consultar qué redes se consideran conocidas:



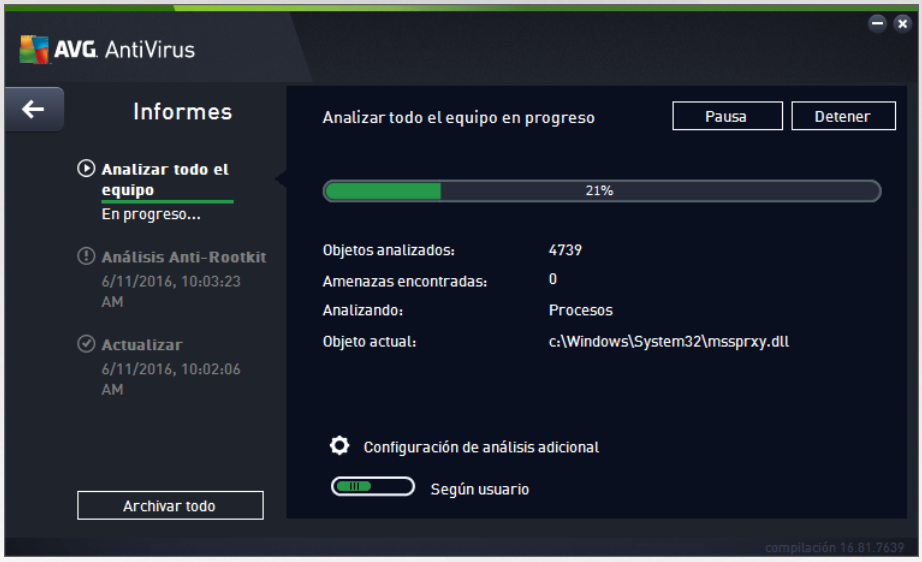
Nota: La función de redes conocidas dentro de AVG Advisor no se admite en Windows XP de 64 bits.

8. Análisis de AVG

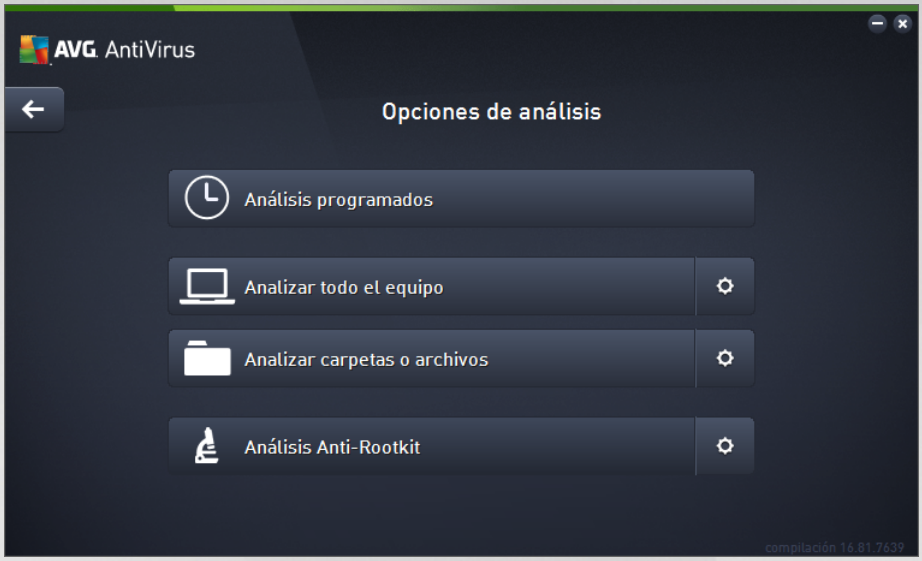
De forma predeterminada, **AVG AntiVirus** no ejecuta ningún análisis, dado que, después del análisis inicial *(al que se lo invitará a iniciar*), debería estar totalmente protegido mediante los componentes residentes de **AVG AntiVirus**, que están siempre en guardia y no permiten que ningún código malicioso ingrese en su equipo. Por supuesto, puede programar un análisis para que se ejecute a intervalos regulares, o ejecutar manualmente un análisis según sus necesidades en cualquier momento.

Puede acceder a la interfaz de análisis de AVG desde la interfaz de usuario principal a través del botón dividido gráficamente en dos secciones: 

- ***Analizar ahora***: presione el botón para iniciar Analizar toda la PC de inmediato y supervisar el progreso y los resultados en la ventana Informes, que se abre automáticamente:



- ***Opciones***: seleccione este botón *(se muestra gráficamente como tres líneas horizontales en un campo verde)* para abrir el cuadro de diálogo ***Opciones de análisis***, donde puede administrar análisis programados y editar parámetros de Analizar toda la PC / Analizar carpetas o archivos.



En el cuadro de diálogo ***Opciones de análisis*** se incluyen tres secciones de configuración de análisis principales:

- ***Administrar análisis programados***: Haga clic en esta opción para abrir un nuevo cuadro de diálogo con una descripción general de todas las programaciones de análisis. Antes de definir sus propios análisis, solamente podrá ver en la tabla un análisis programado predefinido por el proveedor del software. El análisis está desactivado de manera predeterminada. Para encenderlo, haga clic con el botón derecho y seleccione la opción *Activar tarea* en el menú contextual. Una vez que se active el análisis programado, puede editar su configuración a través del botón *Editar análisis programado*. También puede hacer clic en el botón *Agregar análisis programado* para crear una nueva programación de análisis propia.

- ***Analizar todo el equipo / Configuración***: El botón está dividido en dos secciones. Haga clic en la opción *Analizar todo el equipo* para iniciar de inmediato el análisis de todo el equipo *(para ver detalles sobre el análisis de todo el equipo, consulte el capítulo respectivo llamado Análisis predefinidos / Analizar todo el equipo)*. Si hace clic en la sección *Configuración*, irá al cuadro de diálogo de configuración del análisis de todo el equipo.

- ***Analizar carpetas o archivos / Configuración***: Nuevamente, el botón está dividido en dos secciones. Haga clic en la opción *Analizar carpetas o archivos* para iniciar de inmediato el análisis de áreas seleccionadas del equipo *(para ver detalles sobre el análisis de los archivos o carpetas seleccionados, consulte el capítulo llamado Análisis predefinidos / Analizar carpetas o archivos)*. Si hace clic en la sección *Configuración*, irá al cuadro de diálogo de análisis de archivos o carpetas específicos.

- ***Analizar el equipo en busca de rootkits / Configuración***: La sección izquierda del botón denominado *Analizar el equipo en busca de rootkits* ejecuta el análisis anti-rootkit inmediato *(para ver detalles sobre el análisis de rootkits, consulte el capítulo respectivo llamado Análisis predefinidos / Analizar el equipo en busca de rootkits)*. Si hace clic en la sección *Configuración*, irá al cuadro de diálogo de configuración del análisis de rootkits.

8.1. Análisis predefinidos

Una de las funciones principales de **AVG AntiVirus** es el análisis a pedido. Los análisis a pedido se diseñaron para analizar varias partes de la PC cuando existen sospechas de una posible infección de virus. De todas formas, se recomienda llevar a cabo estos análisis con regularidad aun si no cree que se vayan a detectar virus en la PC.

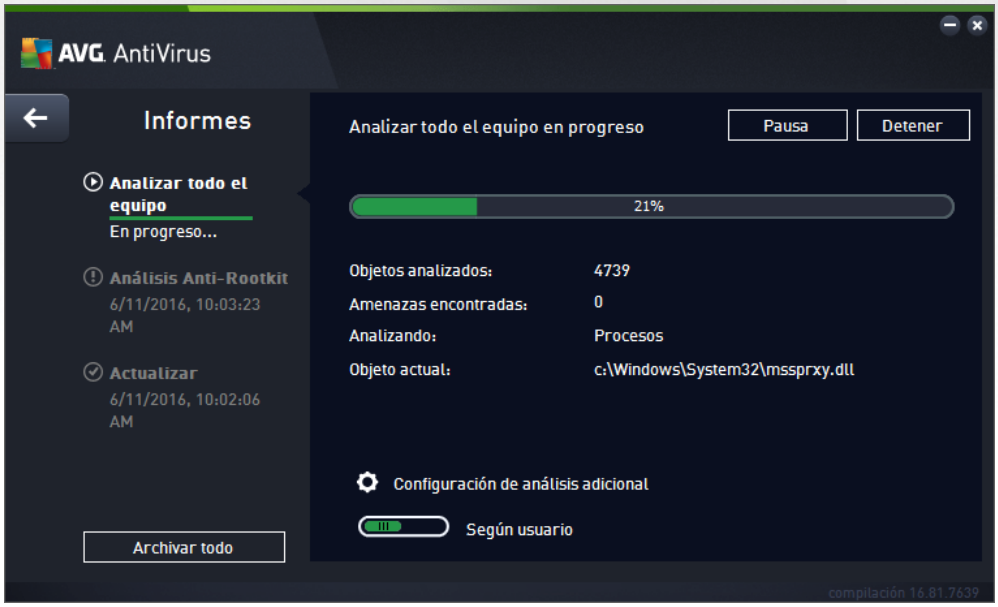
En **AVG AntiVirus** encontrará los siguientes tipos de análisis predefinidos por el proveedor del software:

8.1.1. Analizar todo el equipo

Analizar todo el equipo: analiza todo el equipo en busca de posibles infecciones o aplicaciones potencialmente no deseadas. Este análisis analizará todos los discos duros del equipo y detectará y reparará los virus encontrados, o eliminará la infección detectada enviándola a la Bóveda de virus. Se recomienda programar el análisis de todo el equipo en un equipo al menos una vez a la semana.

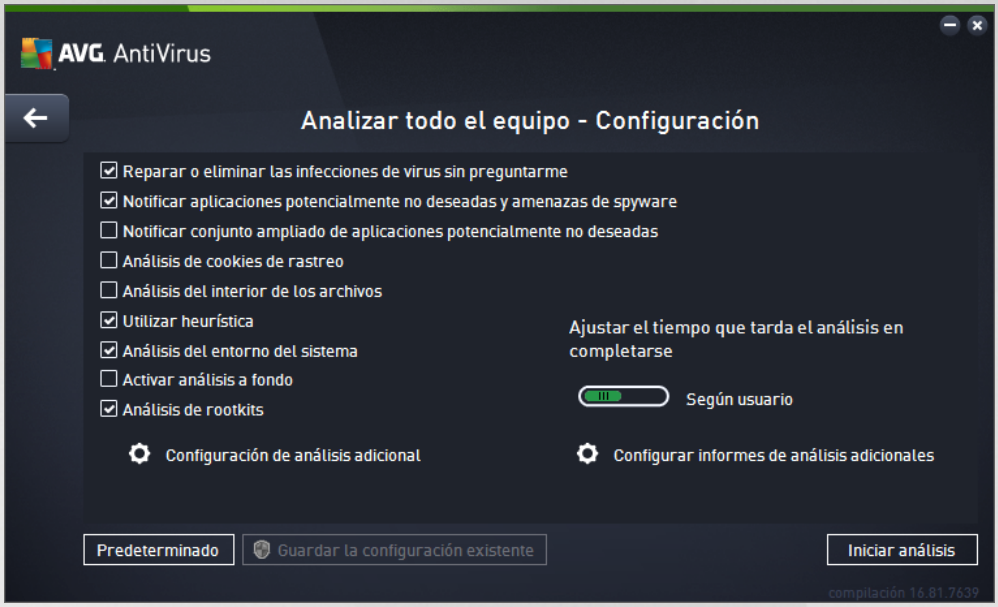
Ejecución del análisis

Analizar todo el equipo se puede iniciar directamente desde la interfaz de usuario principal haciendo clic en el botón ***Analizar ahora***. No se requieren ajustes específicos adicionales para este tipo de análisis; el análisis se iniciará de inmediato. En el cuadro de diálogo ***Análisis de toda la PC en progreso*** (*vea la captura de pantalla*) podrá mirar su progreso y resultados. El análisis puede interrumpirse temporalmente (***Pausa***) o se puede cancelar (***Detener***) si es necesario.



Edición de la configuración de análisis

Puede editar la configuración de ***Analizar todo el equipo*** en el cuadro de diálogo ***Analizar todo el equipo - Configuración*** *(el cuadro de diálogo está disponible a través del vínculo Configuración para Analizar todo el equipo dentro del cuadro de diálogo Opciones de análisis).* ***Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.***



En los parámetros de análisis, puede activar o desactivar parámetros según sea necesario.

- ***Reparar o eliminar las infecciones de virus sin preguntarme*** *(activada de forma predeterminada)*: si se identifica un virus durante el análisis, este 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.

- ***Informar aplicaciones potencialmente no deseadas y amenazas de Spyware*** *(activada de forma predeterminada)*: seleccione esta opción para activar el análisis de spyware y 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

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

- ***Análisis de cookies de rastreo*** *(desactivada de forma predeterminada)*: este parámetro estipula que se deben detectar las cookies *(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 del carrito de compras electrónico)*.

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

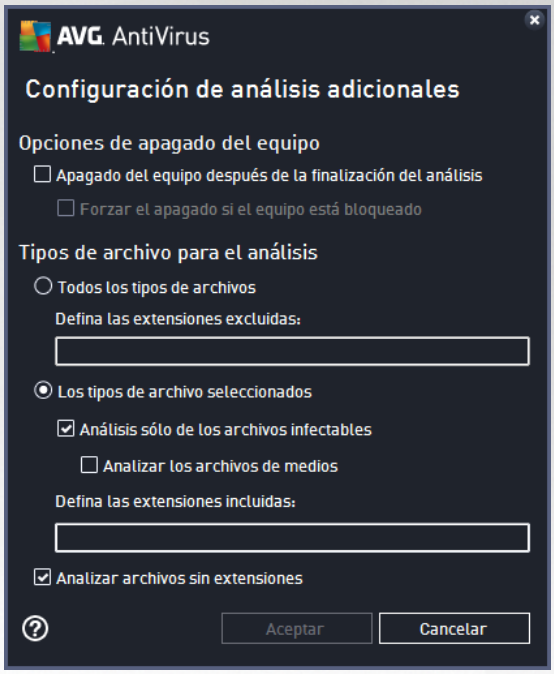
- ***Utilizar heurística*** *(activada de forma predeterminada)*: el análisis heurístico *(la emulación dinámica de las instrucciones del objeto analizado en un entorno de PC virtual)* será uno de los métodos empleados para la detección de virus durante el análisis.

- ***Análisis del entorno del sistema*** *(activada de forma predeterminada)*: el análisis también comprobará las áreas del sistema de la PC.

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

- ***Analizar en busca de rootkits*** *(activada de forma predeterminada)*: incluye análisis anti-rootkit en el análisis de todo el equipo. El análisis anti-rootkit también se puede ejecutar por separado.

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



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

  - ***Tipos de archivo para el análisis***: además debe decidir si desea que se analicen:

    - ***Todos los tipos de archivos***: cuenta además con la opción de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas.

    - ***Tipos de archivos seleccionados***: Puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de*

análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

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

- ***Ajustar el tiempo que tarda el análisis en completarse***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción se establece en el nivel *según usuario* de empleo automático de recursos. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se reducirá al mínimo (*útil cuando se tiene que trabajar en la PC sin importar la duración del análisis*) o más rápido con mayores requerimientos de recursos del sistema (*p. ej., cuando la PC está temporalmente desatendida*).

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

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

8.1.2. Analizar carpetas o archivos específicos

Analizar carpetas o archivos específicos: analiza únicamente las áreas de la PC seleccionadas para el análisis (carpetas, discos duros, discos flexibles, CD seleccionados, etc.). El progreso de análisis en el caso de detección de virus y su tratamiento es similar al del análisis de todo el equipo: cualquier virus encontrado se repara o coloca en la Bóveda de virus. Puede emplear el análisis de archivos/ carpetas para configurar sus propios análisis y programas en función de sus necesidades.

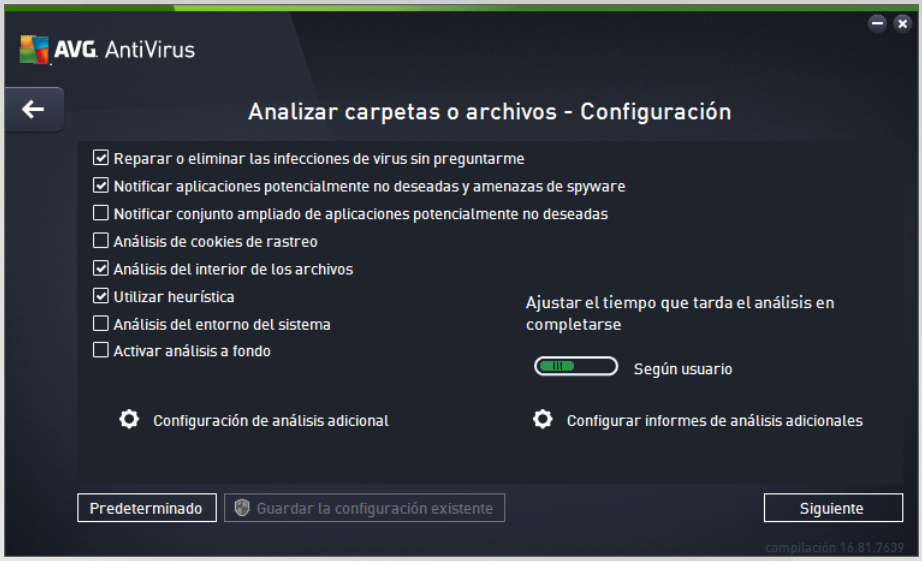
Ejecución del análisis

El análisis de archivos o carpetas se puede ejecutar directamente desde el cuadro de diálogo Opciones de análisis haciendo clic en el botón **Analizar carpetas o archivos**. Se abre un nuevo cuadro de diálogo denominado Seleccione archivos o carpetas específicos para el análisis. En la estructura de árbol del

equipo, seleccione aquellas carpetas que desea analizar. La ruta a cada carpeta seleccionada se genera automáticamente y aparece en el cuadro de texto de la parte superior de este cuadro de diálogo. También existe la opción 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 de 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

Puede editar la configuración de Analizar Archivos o Carpetas Específicos en el cuadro de diálogo Analizar Archivos o Carpetas Específicos - Configuración (el cuadro de diálogo está disponible a través del vínculo Configuración para Analizar archivos o carpetas específicos dentro del cuadro de diálogo Opciones de análisis). Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.



En los parámetros de análisis, puede activar o desactivar parámetros según sea necesario:

- Reparar / eliminar una infección de virus sin preguntarme (activada de forma predeterminada): Si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible una reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.

- Analizar aplicaciones potencialmente no deseadas y amenazas de Spyware (activado de forma predeterminada): Marcar para activar el análisis de spyware, además 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

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

- Análisis de cookies de rastreo (desactivada de forma predeterminada): Este parámetro especifica que se deben detectar cookies (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 del carrito de compras electrónico).

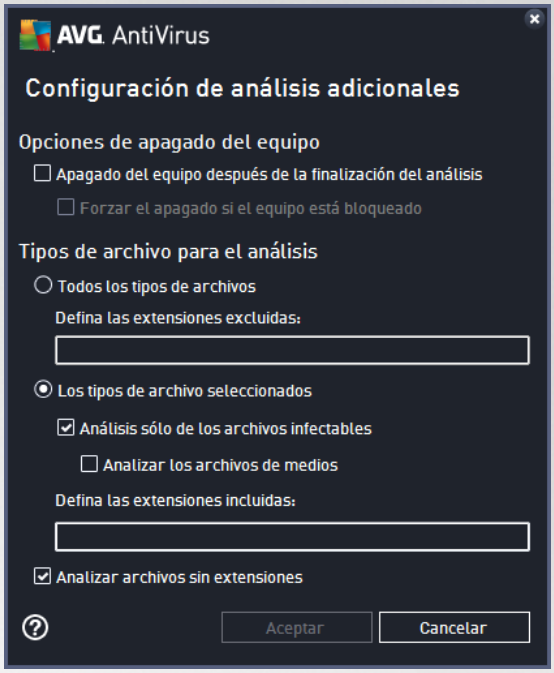
- Análisis del interior de los archivos (activada de forma predeterminada): Este parámetro define que el análisis debe comprobar todos los archivos almacenados dentro de archivos, por ej., ZIP, RAR, etc.

- Utilizar heurística (activada de forma predeterminada): 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.

- Análisis del entorno del sistema (desactivada de forma predeterminada): El análisis también comprobará áreas del sistema de su equipo.

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

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



  - o 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).

  - o Tipos de archivo para el análisis: además debe decidir si desea que se analicen:

    - ➢ Todos los tipos de archivos: cuenta además con la opción de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;

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

    - ➢ De manera opcional, puede decidir si desea Analizar archivos sin extensiones: esta opción

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

- Ajustar el tiempo que tarda el análisis en completarse: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De manera predeterminada, el valor de esta opción se establece en el nivel según usuario de empleo automático de recursos. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se reducirá al mínimo (útil cuando se tiene que trabajar en la PC sin importar la duración del análisis) o más rápido con mayores requerimientos de recursos del sistema (p. ej., cuando la PC está temporalmente desatendida).

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

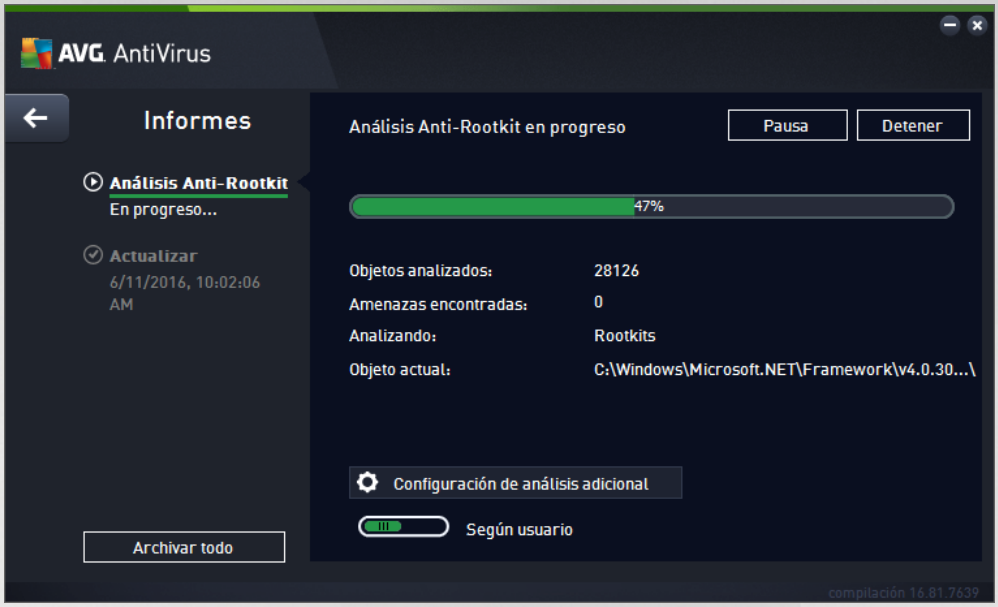
Advertencia: Estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo Análisis de AVG / Programación de análisis / Cómo analizar. Si decide cambiar la configuración predeterminada de Analizar carpetas o archivos específicos puede guardar la nueva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

8.1.3. Análisis del equipo en busca de rootkits

Analizar la PC en busca de rootkits detecta y elimina con eficacia los rootkits peligrosos; es decir, los programas y las tecnologías que pueden camuflar la presencia de software malicioso en la PC. Los rootkits se diseñaron para tomar el control fundamental de los sistemas de las PC sin la autorización de los propietarios ni de los administradores legítimos de los sistemas. El análisis puede detectar rootkits según un conjunto de reglas predefinido. Si se detecta un rootkit, no significa necesariamente que la PC esté infectada. En ocasiones, los rootkits se utilizan como controladores o forman parte de aplicaciones correctas.

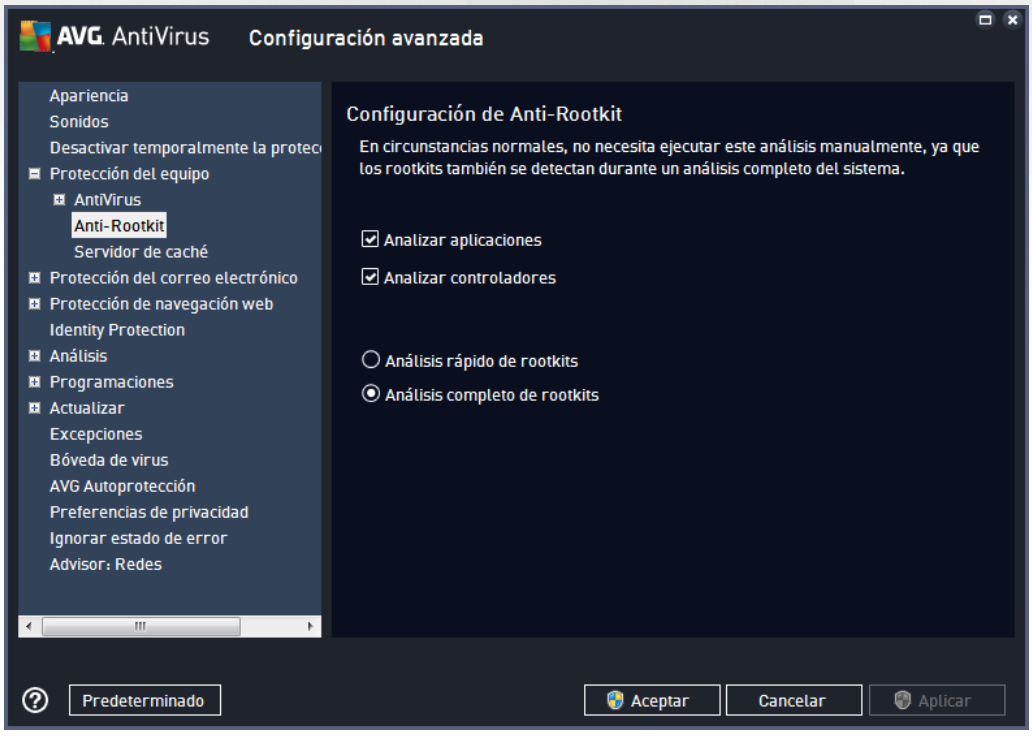
Ejecución del análisis

Analizar la PC en busca de rootkits puede ejecutarse directamente desde el cuadro de diálogo Opciones de análisis haciendo clic en el botón ***Analizar la PC en busca de rootkits***. Se abre un nuevo cuadro de diálogo denominado ***Análisis Anti-Rootkit en curso*** que muestra el progreso del análisis ejecutado:



Edición de la configuración de análisis

Puede editar la configuración del análisis Anti-Rootkit en el cuadro de diálogo ***Configuración Anti-Rootkit*** *(el cuadro de diálogo está disponible a través del vínculo Configuración para el análisis Analizar la PC en busca de rootkits dentro del cuadro de diálogo Opciones de análisis).* ***Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.***



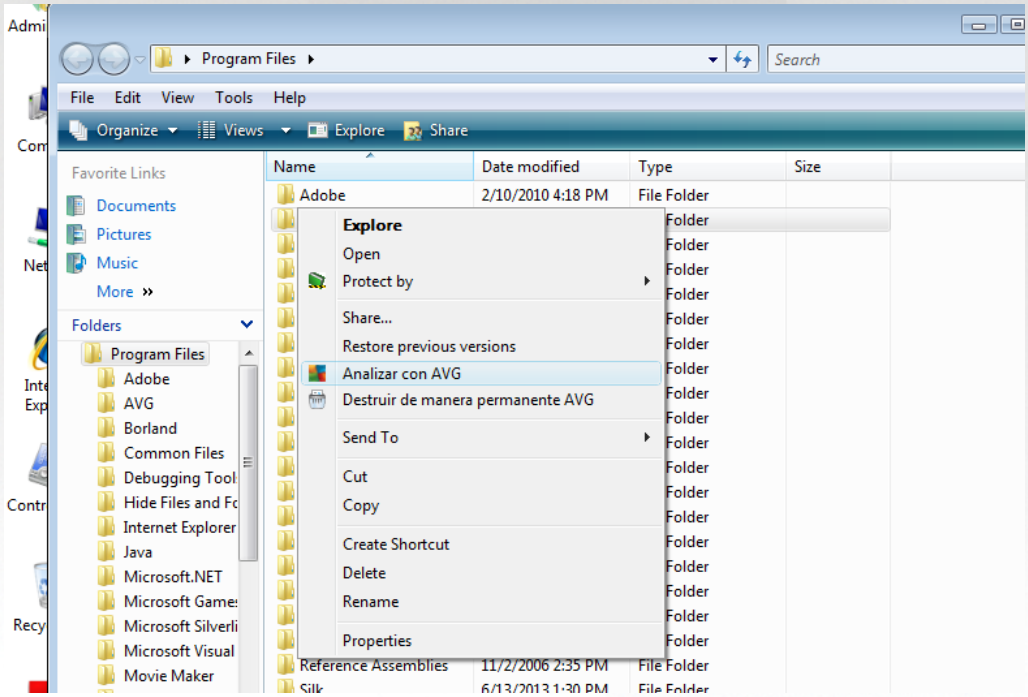
Analizar aplicaciones y ***Analizar controladores*** le permiten especificar en detalle qué debe incluirse en el análisis anti-rootkit. Esta configuración está diseñada para usuarios avanzados; le recomendamos mantener

todas las opciones activadas. También puede seleccionar el modo de análisis de rootkits:

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

8.2. Análisis en el Explorador de Windows

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



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

8.3. Análisis desde línea de comandos

En **AVG AntiVirus** existe la opción de ejecutar el análisis desde la línea de comandos. Puede utilizar esta opción en servidores, por ejemplo, o bien al crear un script por lotes que se ejecutará automáticamente una vez reiniciada la PC. 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 OS de 32 bits
- ***avgscana*** para OS de 64 bits

8.3.1. Sintaxis del comando

La sintaxis del comando es la siguiente:

- ***avgscanx /parámetro*** ... p. ej., ***avgscanx /comp*** para analizar toda la PC
- ***avgscanx /parámetro /parámetro*** .. con varios parámetros, estos deben alinearse en una fila y separarse mediante un espacio y un signo de barra
- si un parámetro requiere que se proporcione un valor específico (p. ej., el parámetro ***/scan*** requiere información sobre qué áreas seleccionadas de la PC 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:***

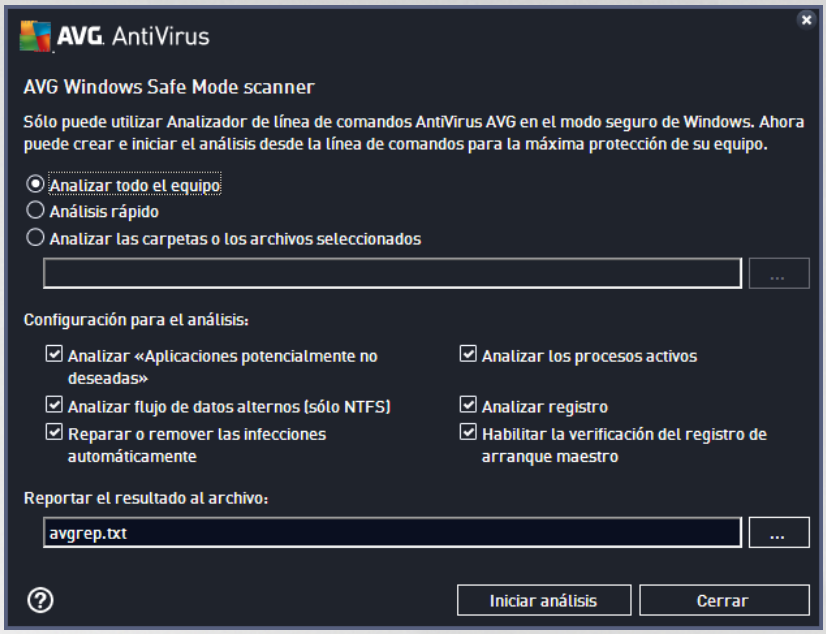
8.3.2. Parámetros del análisis

Para mostrar una descripción completa de los parámetros disponibles, escriba el comando respectivo junto con el parámetro/? o /AYUDA (p. ej., ***avgscanx /?***). El único parámetro obligatorio es /SCAN para especificar qué áreas de la PC 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***.

8.3.3. Análisis desde CMD iniciado desde la interfaz gráfica

Cuando ejecuta la PC en el modo seguro de Windows, existe también una opción de iniciar el análisis desde la línea de comandos en la interfaz gráfica de usuario:



En modo Seguro, el análisis en sí se ejecutará desde la línea de comandos. Este cuadro de diálogo solo le permite especificar los parámetros de análisis en la interfaz gráfica cómoda.

Primero, seleccione las áreas de la PC que desea analizar. Puede optar por la opción predeterminada ***Analizar toda la PC*** o la opción ***Analizar la carpeta o archivos seleccionados***.
La tercera opción, ***Análisis rápido***, inicia un análisis específico diseñado para el uso en modo seguro que inspecciona todas las áreas críticas de la PC necesarias para arrancar.

La configuración del análisis en la próxima sección le permite especificar parámetros de análisis detallados. Todo aparece seleccionado de forma predeterminada, y se sugiere que mantenga todo de esta manera y que sólo anule la selección de un parámetro si tiene alguna razón en particular para hacerlo.

- ***Analizar "aplicaciones potencialmente no deseadas"***: analizar spyware aparte de los virus
- ***Analizar flujos de datos alternos (sólo para NTFS)***: análisis de los flujos de datos alternos de NTFS; es decir, una función de Windows que puede emplearse con fines maliciosos por hackers para esconder datos, especialmente código malicioso
- ***Reparar o quitar infecciones automáticamente***: se cuidarán bien y se repararán/quitarán todas las detecciones posibles de la PC automáticamente
- ***Analizar los procesos activos***: análisis de los procesos y las aplicaciones cargados en la memoria de la PC
- ***Analizar registro***: análisis del registro de Windows
- ***Habilitar la verificación del registro de arranque maestro***: analiza la tabla de partición y el sector de arranque

Finalmente, en la parte inferior de este cuadro de diálogo puede especificar el nombre y el tipo de informe de análisis.

8.3.4. Parámetros del análisis de CMD

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

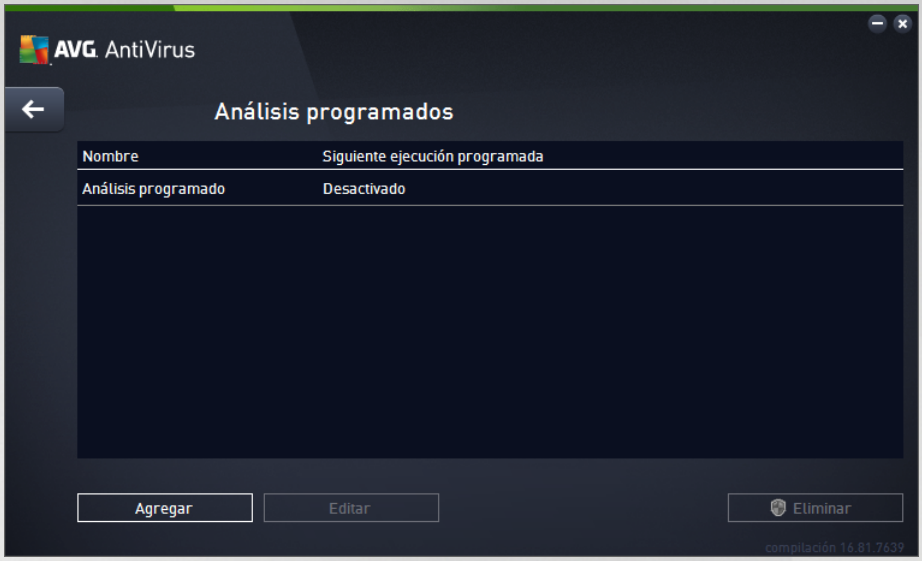
- /? Mostrar ayuda sobre este tema
- /@ Archivo de comandos /nombre de archivo/
- /ADS Analizar flujo de datos alternos *(sólo NTFS)*
- /ARC Analizar archivos
- /ARCBOMBSW Informar sobre archivos recomprimidos
- /ARCBOMBSW Informar sobre bombas de archivo *(archivos comprimidos reiteradas veces)*
- /BOOT Activar la comprobación de MBR/BOOT
- /BOOTPATH Iniciar QuickScan
- /CLEAN Borrar automáticamente
- /CLOUDCHECK Verificar falsos positivos
- /COMP Análisis de toda la PC
- /COO Analizar cookies
- /EXCLUDE Excluir ruta de acceso o archivos del análisis
- /EXT Analizar estas extensiones *(por ejemplo EXT=EXE,DLL)*
- /FORCESHUTDOWN Forzar el apagado de la PC después de la finalización del análisis
- /HELP Visualizar ayuda sobre este tema
- /HEUR Utilizar análisis heurístico
- /HIDDEN Informar sobre archivos con extensión oculta
- /IGNLOCKED Omitir archivos bloqueados
- /INFECTABLEONLY Analizar los archivos con extensiones infectables únicamente
- /LOG Generar un archivo de los resultados del análisis
- /MACROW Notificar macros
- /NOBREAK No permitir la anulación mediante CTRL-BREAK

- /NOEXT — No analizar estas extensiones *(por ejemplo, NOEXT=JPG)*
- /PRIORITY — Establecer prioridad de análisis *(Baja, Automática, Alta; consulte Configuración avanzada / Análisis)*
- /PROC — Analizar los procesos activos
- /PUP — Informar sobre aplicaciones potencialmente no deseadas
- /PUPEXT — Informar sobre conjunto mejorado de aplicaciones potencialmente no deseados
- /PWDW — Notificar archivos protegidos por contraseña
- /QT — Análisis rápido
- /REG — Analizar el registro
- /REPAPPEND — Anexar al archivo de reporte
- /REPOK — Notificar archivos no infectados como correctos
- /REPORT — Informar a archivo *(nombre de archivo)*
- /SCAN — Analizar carpetas o archivos específicos *(SCAN=ruta de acceso;ruta de acceso - p. ej. /SCAN=C:\;D:\)*
- /SHUTDOWN — Apagado de la PC después de la finalización del análisis
- /THOROUGHSCAN — Activar análisis a fondo
- /TRASH — Mover los archivos infectados a la Bóveda de virus

8.4. Programación de análisis

Con **AVG AntiVirus** puede ejecutar el análisis a pedido *(por ejemplo, cuando sospecha que una infección penetró en a la PC)* o según un plan programado. Se recomienda especialmente que ejecute los análisis en función de una programación: de esta forma puede asegurarse de que la PC esté protegida contra posibles infecciones, y no tendrá que preocuparse por la necesidad y el momento de iniciar el análisis. Se debe ejecutar Analizar toda la PC periódicamente, al menos una vez a la semana. Sin embargo, si es posible, ejecute el análisis de toda la PC diariamente, como está establecido en la configuración predeterminada de programación del análisis. Si la PC "siempre está encendido", se pueden programar los análisis fuera del horario de trabajo. Si la PC algunas veces está apagada, se puede programar que los análisis ocurran durante un arranque de la PC, cuando no se haya ejecutado la tarea.

Se puede crear/editar un análisis programado en el cuadro de diálogo ***Análisis programados*** disponible a través del botón ***Administrar análisis programados*** dentro del cuadro de diálogo Opciones de análisis. En el nuevo cuadro de diálogo ***Análisis programados*** podrá ver una descripción general completa de todos los análisis programados actualmente:

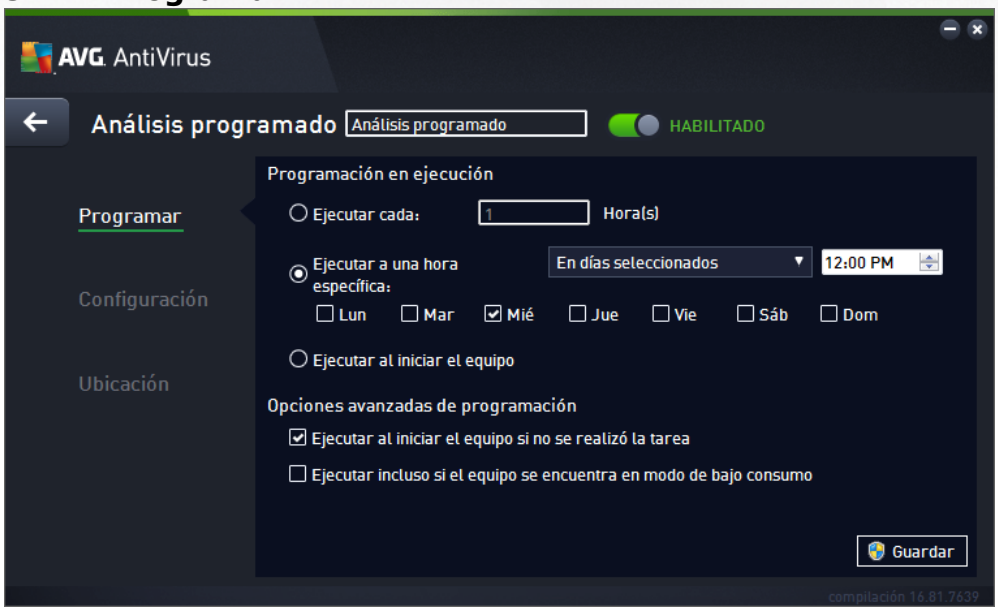


En el cuadro de diálogo puede especificar sus propios análisis. Utilice el botón ***Agregar análisis programado*** para crear una nueva programación de análisis propia. Los parámetros del análisis programado se pueden editar (*o se puede configurar una nueva programación*) en tres pestañas:

- Programación
- Configuración
- Ubicación

En cualquier pestaña, puede alternar la función del botón "semáforo"  para desactivar la prueba programada temporalmente y activarlo nuevamente según sea necesario.

8.4.1. Programar



En la parte superior de la pestaña ***Programar*** puede encontrar el campo de texto en el que especificar el nombre de la programación del análisis actualmente definido. Intente utilizar nombres cortos, descriptivos y adecuados para los análisis a fin de distinguirlos después fácilmente. Por ejemplo, no es adecuado llamar al análisis por el nombre "Nuevo análisis" o "Mi análisis", ya que estos nombres no hacen referencia a lo que el análisis realmente verifica. En cambio, un ejemplo de un buen nombre descriptivo sería "Análisis de áreas del sistema", etc.

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

- ***Ejecución de programación***: aquí puede especificar los intervalos de tiempo para la ejecución del análisis programado recientemente. El tiempo puede definirse con la ejecución repetida tras un período de tiempo determinado *(Ejecutar cada ...)*, estableciendo una fecha y una hora exactas *(Ejecutar en horas específicas)* o también mediante la definición de un evento con el que esté asociada la ejecución del análisis *(Ejecutar al iniciar la PC)*.

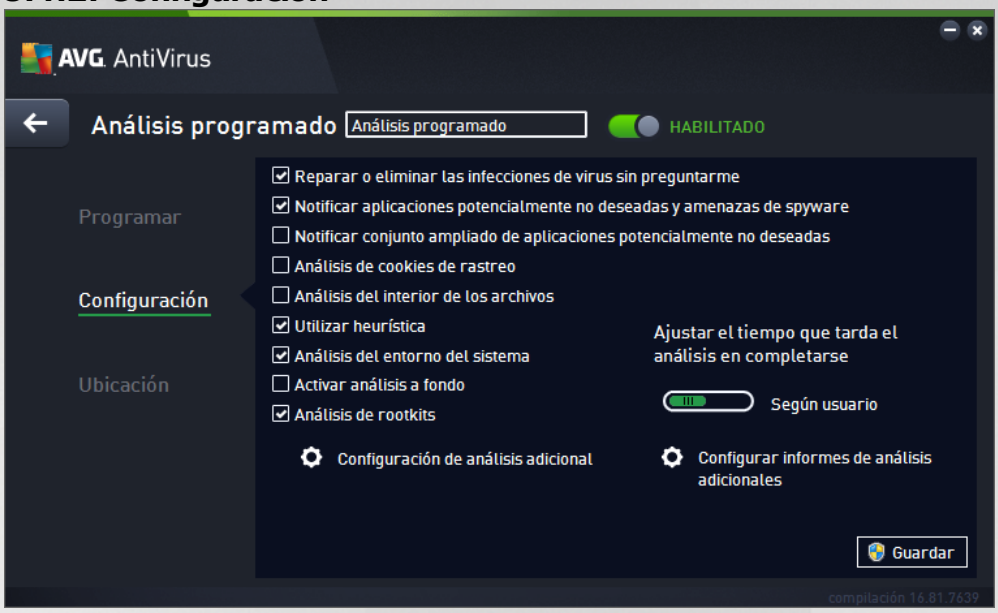
- ***Opciones de programación avanzada***: esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si la PC se encuentra en modo de alimentación baja o totalmente apagada. Una vez que se inicia el análisis programado a la hora que se especificó, se le informará este hecho mediante una ventana emergente que se abre sobre el icono del sistema AVG. A continuación aparece un nuevo icono de la bandeja del sistema AVG (a todo color y brillante) informando de que se está ejecutando un análisis programado. Haga clic con el botón secundario en el icono de ejecución del análisis AVG para abrir un menú contextual donde puede decidir pausar o detener la ejecución del análisis, y también cambiar la prioridad del análisis que se está ejecutando en ese momento.

Controles del cuadro de diálogo

- ***Guardar***: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y cambia a la descripción general de los análisis programados. 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.

-  - Utilice la flecha verde de la sección superior izquierda del diálogo para volver a la descripción general de los análisis programados.

8.4.2. Configuración



En la parte superior de la pestaña Configuración puede encontrar el campo de texto en el que especificar el nombre de la programación del análisis actualmente definido. Intente utilizar nombres cortos, descriptivos y adecuados para los análisis a fin de distinguirlos después fácilmente. Por ejemplo, no es adecuado llamar al análisis por el nombre "Nuevo análisis" o "Mi análisis", ya que estos nombres no hacen referencia a lo que el análisis realmente verifica. En cambio, un ejemplo de un buen nombre descriptivo sería "Análisis de áreas del sistema", etc.

En la pestaña Configuración se encontrará una lista de parámetros de análisis que de manera opcional se pueden activar o desactivar. A menos que se cuente con una razón válida para cambiar esta configuración recomendamos mantenerla:

- Reparar / eliminar una infección de virus sin preguntarme (activada de forma predeterminada): si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la Bóveda de virus.

- Analizar aplicaciones potencialmente no deseadas y amenazas de spyware (activada de forma predeterminada): seleccione esta opción para activar el análisis de spyware, además del 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 intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

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

- Análisis de cookies de rastreo (desactivada de forma predeterminada): este parámetro especifica que se deben detectar cookies durante el análisis; (las cookies HTTP se utilizan para la autenticación, el rastreo y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de sus carritos de compras electrónicos).

- Análisis del interior de los archivos (desactivado de forma predeterminada): este parámetro especifica que el análisis debe comprobar todos los archivos, incluso si se almacenan dentro de un archivo, por ejemplo, ZIP, RAR, etc.

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

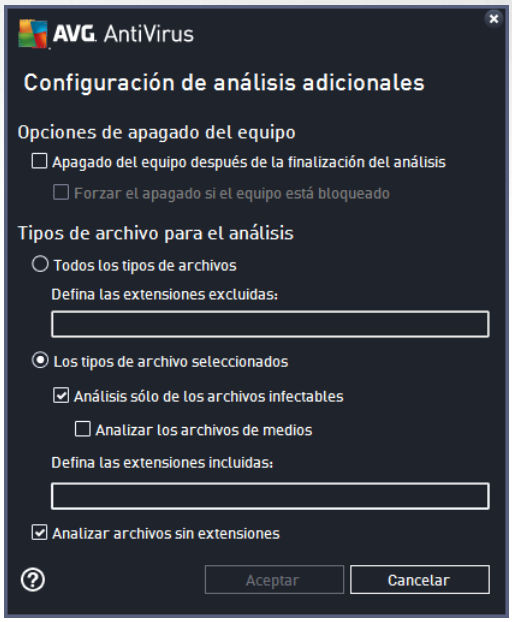
- Análisis del entorno del sistema (activada de forma predeterminada): el análisis también comprobará las áreas del sistema del equipo.

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

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

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

- Tipos de archivo para el análisis: además debe decidir si desea que se analicen:
    - Todos los tipos de archivos: Cuenta además con la opción 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), incluidos 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 esta sección puede especificar de manera adicional la velocidad de análisis deseada dependiendo del empleo de recursos del sistema. De manera predeterminada, el valor de esta opción está establecido en el nivel según usuario de empleo automático de recursos. Si desea que el análisis se realice a más velocidad, tardará menos tiempo, pero el uso de recursos del sistema aumentará de modo notable durante el análisis y el resto de actividades del equipo se ralentizará (esta opción se puede emplear cuando el equipo está encendido pero no hay nadie trabajando en él). Por otro lado, puede reducir el uso de recursos del sistema prolongando la duración del análisis.

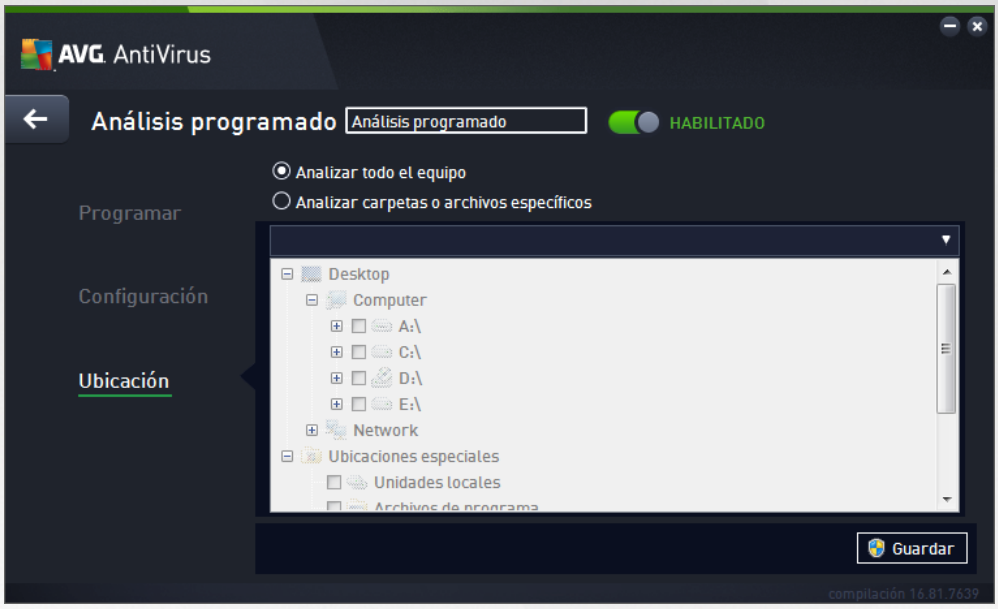
Configurar informes de análisis adicionales

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

Controles del cuadro de diálogo

- Guardar: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y cambia a la descripción general de los análisis programados. 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.
- ← - Utilice la flecha verde de la sección superior izquierda del diálogo para volver a la descripción general de los análisis programados.

8.4.3. Ubicación



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

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

- ***Discos duros locales***: todos los discos duros de la PC
- ***Archivos de programa***
    - C:\Program Files\

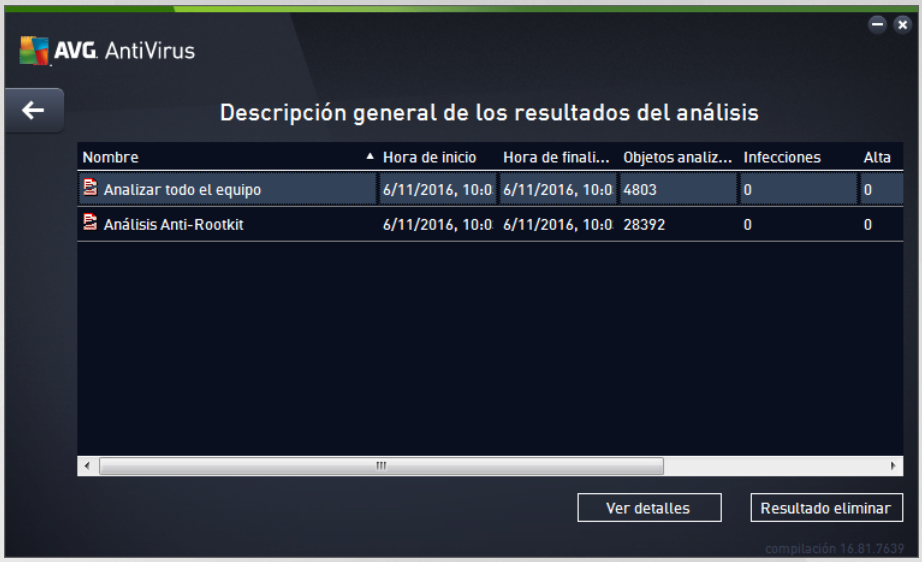
- *en la versión de 64 bits* C:\Program Files (x86)

- ***Carpeta Mis documentos***
  - *para Win XP:* C:\Documents and Settings\Default User\My Documents\
  - *para Windows Vista/7*: C:\Users\user\Documents\
- ***Documentos compartidos***
  - *para Win XP*: C:\Documents and Settings\All Users\Documents\
  - *para Windows Vista/7*: C:\Users\Public\Documents\
- ***Carpeta de Windows***: C:\Windows\
- ***Otro***
  - *Disco duro del sistema*: el disco duro en el cual se instaló el sistema operativo (normalmente C:)
  - *Carpeta del sistema*: C:\Windows\System32\
  - *Carpeta de archivos temporales*: C:\Documents and Settings\User\Local\ (*Windows XP*); o C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Archivos temporales de internet*: C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); o C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Controles del cuadro de diálogo

- ***Guardar***: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y cambia a la descripción general de los análisis programados. 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.
- - Utilice la flecha verde de la sección superior izquierda del diálogo para volver a la descripción general de los análisis programados.

8.5. Resultados del análisis



El cuadro de diálogo ***Descripción general de los resultados del análisis*** ofrece una lista de resultados de todos los análisis realizados. En la tabla se proporciona la siguiente información acerca de cada resultado de análisis:

- ***Icono***: la primera columna muestra un icono de información que describe el estado del análisis:
  - o No se encontraron infecciones; análisis finalizado
  - o No se encontraron infecciones; análisis interrumpido antes de finalizar
  - o Se encontraron infecciones, pero no se repararon; análisis finalizado
  - o Se encontraron infecciones, pero no se repararon; análisis interrumpido antes de finalizar
  - o Se encontraron infecciones que se repararon o eliminaron; análisis finalizado
  - o Se encontraron infecciones que se repararon o eliminaron; análisis interrumpido antes de finalizar
- ***Nombre***: la columna incluye el nombre del análisis correspondiente. Se trata de un análisis predefinido o su propio análisis programado.
- ***Hora de inicio***: proporciona la fecha y la hora exactas de inicio del análisis.
- ***Hora de finalización***: proporciona la fecha y la hora exactas de finalización, detenimiento o interrupción del análisis.
- ***Objetos analizados***: proporciona la cantidad total de todos los objetos analizados.
- ***Infecciones***: proporciona el número de infecciones eliminadas o totales encontradas.

- ***Alta / media / baja***: las tres columnas siguientes proporcionan la cantidad de infecciones encontradas de gravedad alta, media y baja, respectivamente.
- ***Rootkits***: proporciona la cantidad total de rootkits encontrados durante el análisis.

Controles de diálogo

Ver detalles: haga clic en el botón para ver información detallada sobre un análisis seleccionado *(resaltado en la tabla anterior)*.

Eliminar resultados: haga clic en el botón para eliminar un resultado de análisis seleccionado de la tabla.

 : utilice la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal con la descripción general de los componentes.

8.6. Detalles de los resultados del análisis

Para abrir una descripción general de información detallada sobre un resultado de análisis seleccionado, haga clic en el botón ***Ver detalles***, disponible en el cuadro de diálogo Descripción general de resultados de análisis. Se lo dirigirá a la misma interfaz de cuadro de diálogo que describe en detalle la información sobre un resultado de análisis respectivo. La información está dividida en tres pestañas:

- ***Resumen***: La pestaña ofrece información básica sobre el análisis: Si se completó exitosamente, si se encontraron amenazas y qué se hizo al respecto.
- ***Detalles***: La pestaña muestra toda la información sobre el análisis, incluidos los detalles sobre cualquier amenaza detectada. Exportar descripción general a archivo le permite guardarlo como archivo .csv.
- ***Detecciones***: Esta pestaña solo se muestra si se detectaron amenazas durante el análisis, y brinda información detallada sobre ellas:

   ***Severidad de información***: Incluye información o advertencias, no amenazas reales. Generalmente son documentos que contienen macros, documentos o archivos protegidos por una contraseña, archivos bloqueados, etc.

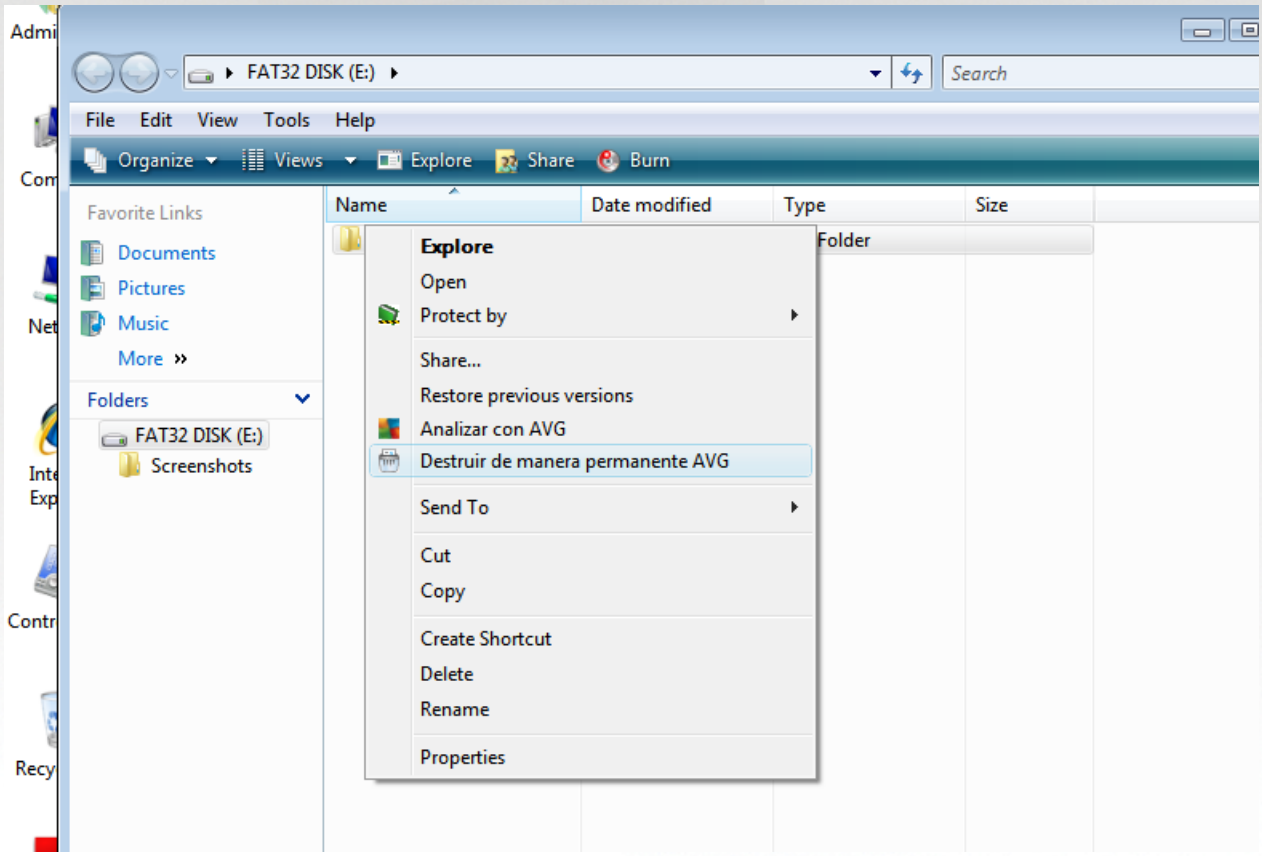
   ***Severidad media***: Generalmente son aplicaciones potencialmente no deseadas *(como adware)* o cookies de rastreo.

   ***Severidad alta***: Incluye amenazas serias como virus, Troyanos, vulnerabilidades, etc. También objetos detectados por el método de detección Heurística, es decir, amenazas aún no descritas en la base de datos de los virus.

9. AVG File Shredder

AVG File Shredder se diseñó para eliminar archivos de forma absolutamente segura; es decir, sin ninguna posibilidad de recuperarlos, ni siquiera con las herramientas de software avanzadas para este propósito.

Para destruir un archivo o una carpeta, haga clic derecho sobre un administrador de archivos *(Windows Explorer, Total Commander, etc.)* y seleccione ***Destruir de manera permanente con AVG*** en el menú contextual. Los archivos que se encuentran en la Papelera de Reciclaje también se pueden destruir. Si un archivo específico en una ubicación específica *(p. ej., CD-ROM)* no se puede destruir de manera confiable, recibirá una notificación, o bien, la opción en el menú contextual no estará disponible en absoluto.



Recuerde: Si destruye un archivo, lo perderá de forma permanente.

10. Bóveda de virus

La ***Bóveda de virus*** es un entorno seguro para administrar los objetos sospechosos o infectados que se han detectado durante los análisis de AVG. Una vez que se detecta un objeto infectado durante el análisis, y AVG no puede repararlo de inmediato, se le pide que decida qué hacer con el objeto sospechoso. La solución recomendada es mover el objeto a la ***Bóveda de virus*** para tratarlo allí. El objetivo principal de la ***Bóveda de virus*** es conservar cualquier archivo eliminado durante un cierto periodo de tiempo, para que pueda asegurarse de que ya no necesita el archivo en la ubicación original. Si la ausencia de un archivo provoca problemas, puede enviarlo a análisis o bien restaurarlo a la ubicación original.

La interfaz de la ***Bóveda de virus*** se abre en una ventana aparte y ofrece una visión general de información sobre los objetos infectados en cuarentena:

- ***Fecha de adición***: proporciona la fecha y la hora en que el archivo sospechoso se detectó y transfirió a la Bóveda de Virus.
- ***Amenaza***: si decide instalar el componente Identidad dentro de su **AVG AntiVirus**, se proporcionará una identificación gráfica de la gravedad de la detección en esta sección: desde inobjetable *(tres puntos verdes)* hasta muy peligrosa *(tres puntos rojos)*. También encontrará información sobre el tipo de infección y su ubicación original. El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Fuente***: especifica qué componente de **AVG AntiVirus** detectó la amenaza en cuestión.
- ***Notificaciones***: en una situación inusual, pueden proporcionarse notas en esta columna con comentarios detallados de la amenaza en cuestión.

Botones de control

Se puede tener acceso a los botones de control siguientes desde la interfaz de la ***Bóveda de Virus***:

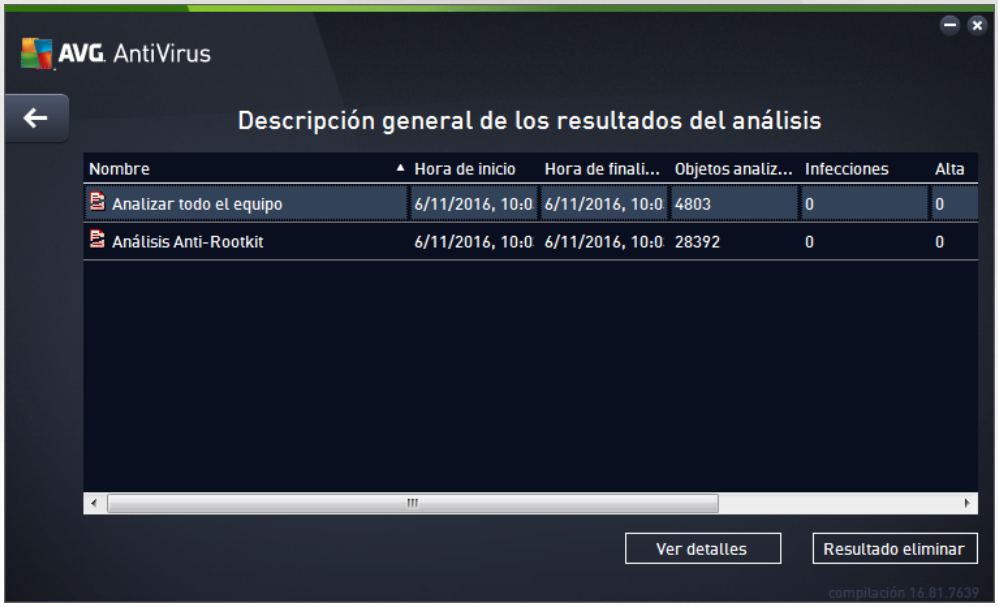
- ***Restaurar***: devuelve el archivo infectado a la ubicación original en el disco.
- ***Restaurar como***: mueve el archivo infectado a una carpeta seleccionada.
- ***Enviar para análisis***: el botón está activo sólo cuando se resalta un objeto en la lista de detecciones ubicada más arriba. En tal caso, tiene la opción de enviar la detección seleccionada a los laboratorios de virus de AVG en busca de análisis más detallados. Tenga en cuenta que esta característica debería servir principalmente para enviar falsos positivos; es decir, archivos que AVG detectó como infectados o sospechosos, pero que en realidad son inofensivos.
- ***Detalles***: para obtener información detallada sobre la cuarentena de amenazas específicas en la ***Bóveda de virus***, resalte el elemento seleccionado en la lista y haga clic en el botón ***Detalles*** para que aparezca un nuevo cuadro de diálogo con una descripción de la amenaza detectada.
- ***Eliminar***: elimina el archivo infectado de la ***Bóveda de virus*** de forma total e irreversible.
- ***Vaciar la Bóveda de virus***: elimina todo el ***contenido de la*** Bóveda de virus por completo. 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*).

11. Historial

La sección ***Historial*** incluye información sobre todos los eventos pasados *(tales como actualizaciones, análisis, detecciones, etc.)* e informes acerca de estos eventos. Puede acceder a esta sección desde la interfaz de usuario principal a través del elemento ***Opciones / Historial***. Además, el historial de todos los eventos registrados está dividido en las siguientes partes:

- Resultados del análisis
- Resultados de la Protección Residente
- Resultados de la Protección del correo electrónico
- Configuración de Online Shield
- Historial de eventos

11.1. Resultados del análisis



Se puede acceder al cuadro de diálogo Descripción general de los resultados del análisis a través del elemento de menú Opciones / Historial / Resultados del análisis en la navegación superior de la ventana principal de **AVG AntiVirus**. 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 acerca de cada análisis, consulte el cuadro de diálogo Resultados del análisis disponible a través del botón Ver detalles (en la parte inferior de este cuadro de diálogo).

- Hora de inicio: fecha y hora en que se inició el análisis
- Hora de finalización: fecha y hora en que finalizó el análisis
- Objetos analizados: número de objetos que se verificaron durante el análisis
- Infecciones: número de infecciones de virus detectadas/eliminadas
- Alta / Media: estas columnas proporcionan la cantidad de infecciones eliminadas/ totales encontradas de severidad alta y media, respectivamente
- Información: información relacionada con el curso y el resultado del análisis (normalmente en la finalización o la interrupción)
- Rootkits: número de rootkits detectados

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 y ver información detallada sobre el análisis seleccionado
- Eliminar resultado: presione este botón para eliminar el elemento seleccionado de la descripción general de los resultados del análisis
- : para regresar al cuadro de diálogo principal de AVG predeterminado (descripción general de los componentes), utilice la flecha de la esquina superior izquierda de este cuadro de diálogo

11.2. Resultados de la Protección Residente

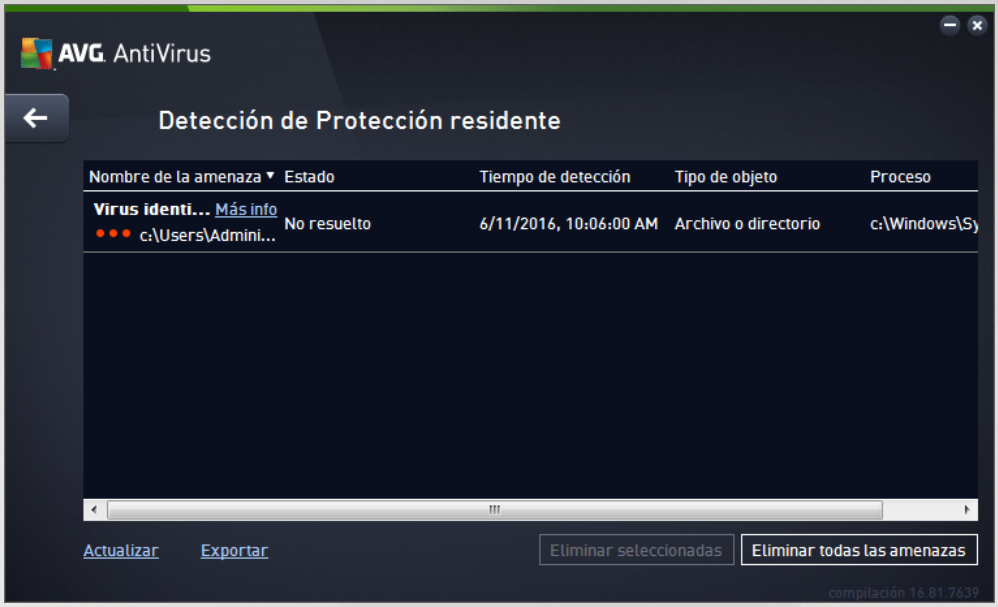
El servicio ***Protección Residente*** forma parte del componente ***PC*** y analiza archivos a medida que se copian, abren o guardan. Cuando se detecte una amenaza de virus o de cualquier tipo, se le advertirá inmediatamente mediante este cuadro de diálogo:

Dentro de este cuadro de diálogo de advertencia encontrará información sobre el objeto detectado y asignado al estado infectado (*Amenaza*), y algunos datos descriptivos sobre la infección reconocida (*Descripción*). El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea si es una amenaza conocida. En el cuadro de diálogo, también verá una descripción general de las soluciones disponibles sobre cómo tratar la amenaza detectada. Una de las alternativas se etiquetará como recomendada: ***Protegerme (recomendado). De ser posible, siempre debe marcar esta opción.***

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

En la sección inferior del cuadro de diálogo puede encontrar el vínculo ***Mostrar detalles***. Haga clic en él para abrir una nueva ventana con información detallada sobre el proceso en ejecución al momento de detectar la infección y la identificación del proceso.

Dentro el cuadro de diálogo ***Detección de Protección residente*** hay una lista de todas las detecciones de Protección residente de las que se puede obtener una descripción general. Este cuadro de diálogo está disponible a través del elemento de menú ***Opciones / Historial / Detección de Protección Residente*** en la navegación superior de la ventana principal de **AVG AntiVirus. El cuadro de diálogo ofrece una descripción general de los objetos que se detectaron mediante la protección residente evaluados como peligrosos y reparados o movidos a la** Bóveda de virus.



Para cada objeto detectado se proporciona la siguiente información:

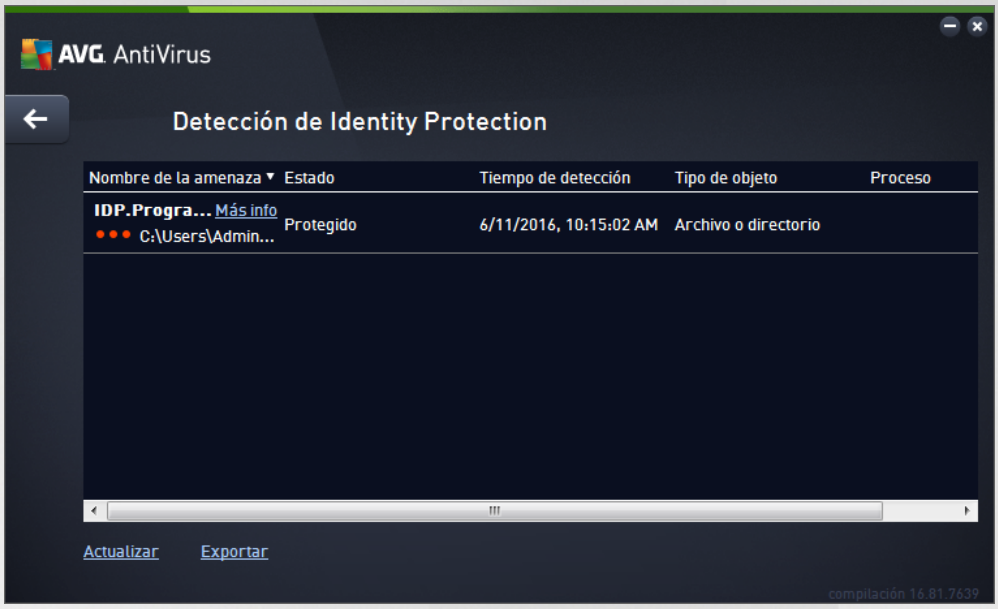
- ***Nombre de la amenaza***: descripción (*posiblemente incluso el nombre preciso*) del objeto detectado y la ubicación. El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Estado***: acción 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 realizó para que el objeto potencialmente peligroso se presente en pantalla de manera que se pueda detectar

Botones de control

- ***Actualizar***: actualice la lista de hallazgos detectados por ***Online Shield***
- ***Exportar***: exporte la lista entera de objetos detectados a un archivo
- ***Quitar seleccionados***: puede resaltar registros seleccionados en la lista y utilizar este botón para eliminar sólo esos elementos
- ***Eliminar todas las amenazas***: utilice el botón para eliminar todos los registros mencionados en este cuadro de diálogo
- : para regresar al cuadro de diálogo principal de AVG *predeterminado (descripción general de los componentes),* utilice la flecha de la esquina superior izquierda de este cuadro de diálogo

11.3. Resultados de Identity Protection

Se puede acceder al cuadro de diálogo ***Resultados de Identity Protection*** a través del elemento de menú ***Opciones /Historial / Resultados de Identity Protection*** en la línea de navegación superior de la ventana principal de **AVG AntiVirus**.



El cuadro de diálogo proporciona una lista de todos los hallazgos detectados por el componente Identity Protection. Para cada objeto detectado se proporciona la siguiente información:

- ***Nombre de la amenaza***: descripción *(posiblemente el nombre preciso)* del objeto detectado y la ubicación. El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Estado***: 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 realizó para que el objeto potencialmente peligroso se presente en pantalla de manera que se pueda detectar

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

Botones de control

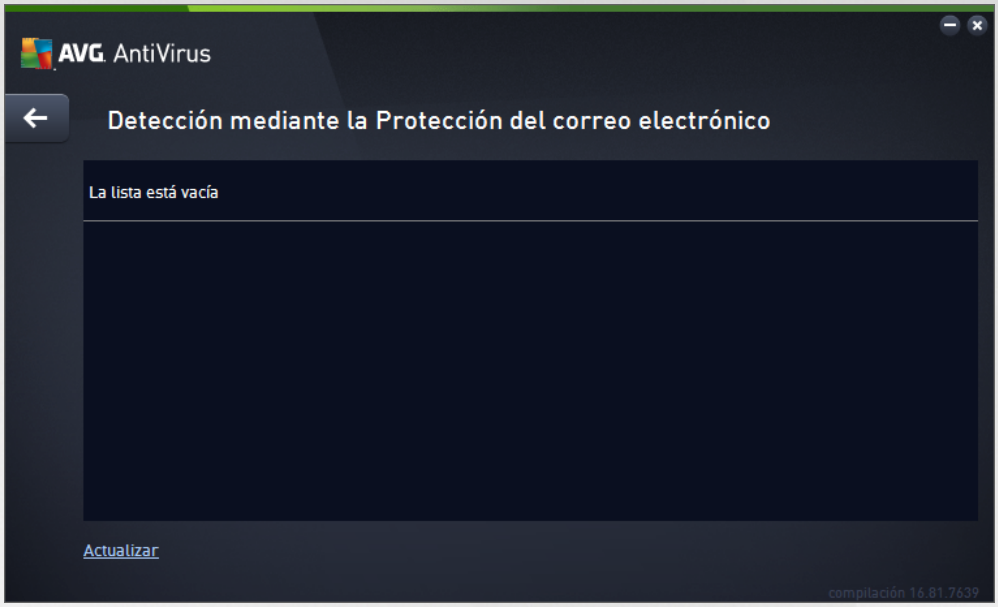
Los botones de control disponibles dentro de la interfaz de ***Resultados de Identity Protection*** son:

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

- : para regresar al cuadro de diálogo principal de AVG *predeterminado (descripción general de los componentes),* utilice la flecha en la esquina superior izquierda de este cuadro de diálogo

11.4. Resultados de Protección del correo electrónico

Se puede acceder al cuadro de diálogo ***Resultados de la Protección del correo electrónico*** a través del elemento de menú ***Opciones / Historial / Resultados de la protección del correo electrónico*** en la línea de navegación superior de la ventana principal de **AVG AntiVirus**.



El cuadro de diálogo proporciona una lista de todos los hallazgos detectados por el componente Analizador de correo electrónico. Para cada objeto detectado se proporciona la siguiente información:

- ***Nombre de la detección***: descripción *(posiblemente el nombre preciso)* del objeto detectado y su ubicación
- ***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
- ***Proceso***: qué acción se realizó para que el objeto potencialmente peligroso de manera que se pueda detectar

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

Botones de control

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

- ***Actualizar lista***: actualiza la lista de amenazas detectadas
- ←: para regresar al cuadro de diálogo principal de AVG *predeterminado (descripción general de los componentes),* utilice la flecha de la esquina superior izquierda de este cuadro de diálogo

11.5. Configuración 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 la PC. Si se detecta una amenaza, se le avisará de forma inmediata mediante el siguiente cuadro de diálogo:

Dentro de este cuadro de diálogo de advertencia encontrará información sobre el objeto detectado y asignado como infectado (*Amenaza*), y algunos datos descriptivos sobre la infección reconocida (*Nombre de objeto*). El vínculo *Más información* lo dirigirá a la enciclopedia de virus en línea, donde puede encontrar información detallada sobre la infección detectada si es conocida. El cuadro de diálogo proporciona los siguientes elementos de control:

- ***Mostrar detalles***: haga clic en el vínculo 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 cuadro de diálogo de advertencia.

No se abrirá la página web sospechosa, y la detección de la amenaza se registrará en la lista de los ***hallazgos de Online Shield***. Esta descripción general de amenazas detectadas está disponible a través del elemento de menú ***Opciones / Historial / Hallazgos de Online Shield*** en la navegación superior de la ventana principal de **AVG AntiVirus**.

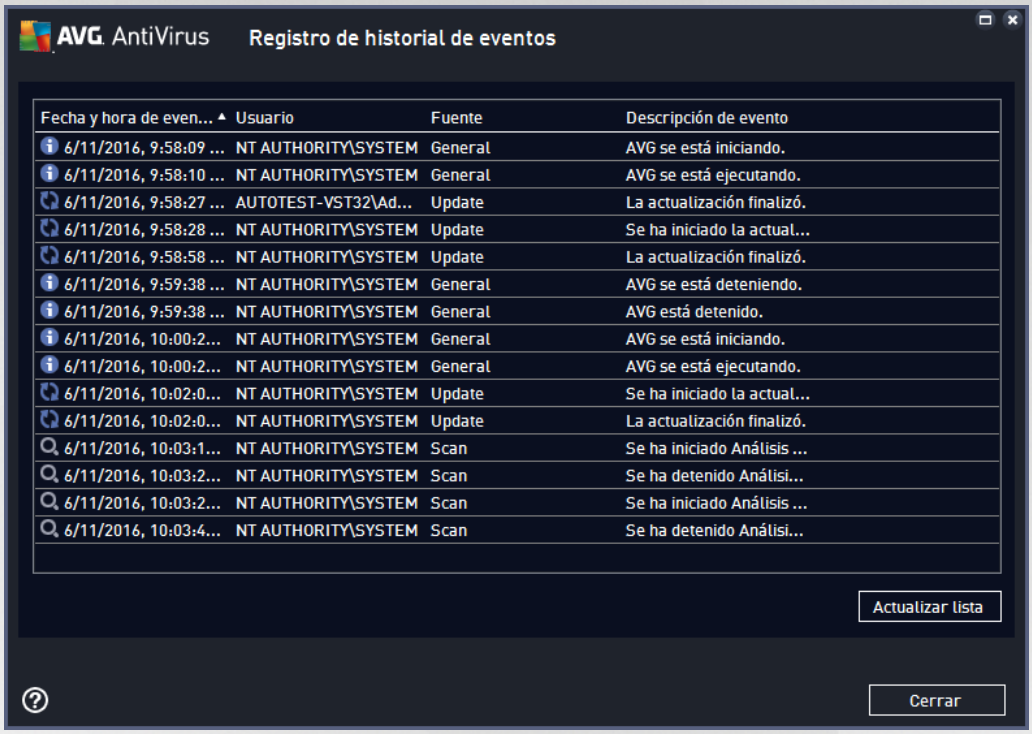
Para cada objeto detectado se proporciona la siguiente información:

- ***Nombre de la amenaza***: descripción (*posiblemente incluso el nombre*) del objeto detectado y el origen (*página web*); el vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Estado***: 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

Botones de control

- ***Actualizar***: actualice la lista de hallazgos detectados por ***Online Shield***
- ***Exportar***: exporte la lista entera de objetos detectados a un archivo
- ←: para regresar al cuadro de diálogo principal de AVG *predeterminado (descripción general de los componentes),* utilice la flecha en la esquina superior izquierda de este cuadro de diálogo

11.6. Historial de eventos



Se puede acceder al cuadro de diálogo Historial de eventos a través del elemento de menú Opciones / Historial / Historial de eventos en la línea de navegación superior de la ventana principal de **AVG AntiVirus**. En este cuadro de diálogo, puede encontrar un resumen de los eventos importantes que se han producido durante el funcionamiento de **AVG AntiVirus**. El cuadro de diálogo proporciona registros de los siguientes tipos de eventos: información sobre actualizaciones de la aplicación AVG; información sobre el inicio, finalización o interrupción del análisis (incluidas las pruebas realizadas automáticamente); información sobre eventos relacionados con la detección de virus (mediante la protección residente o el análisis) incluida la ubicación de ocurrencia; y otros eventos importantes.

Para cada evento, se muestra la información siguiente:

- Fecha y hora de eventos ofrece la fecha y la hora exactas en que ocurrió el evento.
- Usuario indica el nombre del usuario que había iniciado sesión a la hora en que ocurrió el evento.
- Fuente proporciona información sobre un componente de origen u otra parte del sistema AVG que desencadenó el evento.
- Descripción de evento proporciona un breve resumen de lo que sucedió realmente.

Botones de control

- Actualizar lista: presione este botón para actualizar todas las entradas de la lista de eventos
- Cerrar: presione el botón para regresar a la ventana principal de **AVG AntiVirus**

12. Actualizaciones de AVG

Ningún software de seguridad puede garantizar una verdadera protección ante los diversos tipos de amenazas si no se actualiza periódicamente. Los desarrolladores de virus siempre buscan nuevas fallas que vulneren en el software y el sistema operativo. Diariamente aparecen nuevos virus, nuevo malware y nuevos ataques de hackers. Por ello, los proveedores de software generan constantes actualizaciones y parches de seguridad, con objeto de corregir las deficiencias de seguridad descubiertas. Teniendo en cuenta la cantidad de nuevas amenazas para la PC que surgen cada día y la velocidad a la que se propagan, es absolutamente esencial actualizar su **AVG AntiVirus** de manera periódica. La mejor solución consiste en mantener la configuración predeterminada del programa donde está configurada la actualización automática. Tenga en cuenta que si la base de datos de virus de su **AVG AntiVirus** no está actualizada, el programa no podrá detectar las amenazas más recientes.

Es fundamental actualizar el programa AVG periódicamente. Las actualizaciones de definiciones de virus esenciales deben ser diarias si es posible. Las actualizaciones del programa menos urgentes pueden efectuarse semanalmente.

Para proporcionar la seguridad máxima disponible, **AVG AntiVirus** está programado de forma predeterminado para buscar nuevas actualizaciones de la base de datos de virus cada pocas horas. Dado que las actualizaciones de AVG no se lanzan de acuerdo a una programación fija, sino que en respuesta a la cantidad y severidad de nuevas amenazas, este control resulta de alta importancia para asegurarse de que su base de datos de virus de AVG se mantenga actualizada en todo momento.

Si desea comprobar si hay nuevos archivos de actualización de inmediato, utilice el vínculo rápido Actualizar ahora en la interfaz de usuario principal. Este vínculo está disponible en todo momento desde cualquier cuadro de diálogo de la interfaz de usuario. Una vez que se inicia la actualización, AVG verificará primero si hay nuevos archivos de actualización disponibles. Si es así, **AVG AntiVirus** iniciará la descarga y ejecutará el proceso de actualización en sí. Se le informará de los resultados de la actualización en el cuadro de diálogo deslizante situado sobre el icono del sistema AVG.

Si desea reducir el número de ejecuciones de actualizaciones, puede configurar sus propios parámetros de ejecución de actualizaciones. No obstante, ***es muy recomendable ejecutar la actualización al menos una vez por día.*** La configuración se puede editar en la sección Configuración avanzada/ Programaciones, en concreto en los siguientes cuadros de diálogo:

- Programación de actualización de las definiciones

13. Preguntas frecuentes y asistencia técnica

Si tiene algún problema técnico o referente a la compra de la aplicación **AVG AntiVirus**, existen varios modos de buscar ayuda. Elija una de las opciones siguientes:

- ***Obtener soporte***: En la aplicación de AVG usted puede obtener una página dedicada al soporte al cliente en el sitio web de AVG (http://www.avg.com/). Seleccione el elemento del menú principal ***Ayuda / Obtener soporte*** para acceder al sitio web de AVG con métodos de soporte disponibles. Para continuar, siga las instrucciones de la página web.

- ***Soporte*** *(vínculo del menú principal)*: el menú de la aplicación AVG (*en la parte superior de la interfaz del usuario principal*) incluye el vínculo ***Soporte***, que abre un cuadro de diálogo nuevo con todos los tipos de información que puede necesitar cuando intente encontrar ayuda. El cuadro de diálogo incluye datos básicos sobre el programa AVG instalado (*versión del programa/base de datos*), detalles de la licencia y una lista de vínculos de soporte rápidos.

- ***Resolución de problemas en el archivo de ayuda***: Está disponible una sección de ***Resolución de problemas*** incluida en el archivo de ayuda **AVG AntiVirus** *(para abrir el archivo de ayuda, presione la tecla F1 en cualquier diálogo en la aplicación)*. Esta sección proporciona una lista de las situaciones que se producen con más frecuencia cuando un usuario desea obtener ayuda profesional sobre una cuestión técnica. Seleccione la situación que mejor describa su problema y haga clic en ella para abrir instrucciones detalladas que le permitan solucionarlo.

- ***Centro de soporte del sitio web de AVG***: Como alternativa, puede buscar la solución a su problema en el sitio web de AVG (http://www.avg.com/). En la sección ***Soporte*** puede encontrar un resumen de los grupos temáticos vinculados con cuestiones técnicas y de ventas, una sección estructurada de preguntas frecuentes y todos los contactos disponibles.

- ***AVG ThreatLabs***: un sitio web específico relacionado con AVG (http://www.avg.com/about-viruses) está dirigido a cuestiones de virus y brinda una descripción general estructurada de la información relacionada con amenazas en línea. También encontrará instrucciones sobre cómo eliminar virus y spyware y cómo mantenerse protegido.

- ***Foro de discusión***: También puede utilizar el foro de discusión de usuarios de AVG en http://community.avg.com/.