AVG AntiVirus

Manual del usuario

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

Contenido

1. Introducción

Este manual del usuario proporciona documentación completa para el usuario sobre **AVG AntiVirus**.

AVG AntiVirus ofrece protección en tiempo real contra las amenazas actuales más sofisticadas. Puede chatear, descargar e intercambiar archivos con confianza; jugar y reproducir vídeos sin preocupaciones o interrupciones; descargar, compartir archivos y enviar mensajes de forma segura; disfrutar de su vida en redes sociales o navegar y realizar búsquedas con la protección en tiempo real.

También puede querer utilizar otras fuentes de información:

- ***Archivo de ayuda***: Hay una sección de *Resolución de problemas* disponible directamente en el archivo de ayuda incluido en **AVG AntiVirus** *(para abrir el archivo de ayuda, pulse la tecla F1 en cualquier cuadro de diálogo de la aplicación)*. Esta sección proporciona una lista de las situaciones que ocurren más frecuentemente cuando un usuario desea buscar ayuda profesional para un problema técnico. Seleccione la situación que mejor describa el problema y haga clic en ella para abrir instrucciones detalladas que llevan a su solución.

- ***Centro de soporte del sitio web de AVG***: También puede buscar la solución a su problema en el sitio web de AVG (*http://www.avg.com/*). En la sección de ***Asistencia*** puede encontrar información de grupos temáticos centrados en las ventas y los aspectos técnicos, una sección estructurada de preguntas más frecuentes y todos los contactos disponibles.

- ***AVG ThreatLabs***: Un sitio web específico relacionado con AVG (*http://www.avg.com/about-viruses*) se dedica a temas de virus, proporcionando información general estructurada sobre las amenazas en línea. También puede encontrar instrucciones sobre cómo quitar virus y spyware, además de consejos para mantenerse protegido.

- ***Foro de discusión***: También puede usar 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 se ha diseñado para proteger 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 probablemente los service packs superiores de los sistemas operativos especificados)

2.2. Requisitos de hardware mínimos y recomendados

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

- CPU Intel Pentium de 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 de 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 que está instalando una versión actualizada de **AVG AntiVirus**, se recomienda que descargue el archivo de instalación desde el sitio web de AVG (http://www.avg.com/). La sección ***Centro de soporte*** proporciona información estructurada sobre los archivos de instalación para cada edición de AVG. Una vez que haya descargado y guardado el archivo de instalación en el disco duro, podrá iniciar el proceso de instalación. La instalación es una secuencia de cuadros de diálogo simples y fáciles de entender. Cada uno describe brevemente qué se hace en cada paso del proceso de instalación. A continuación se ofrece una explicación detallada de cada ventana de diálogo:

3.1. Bienvenido

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

Selección de idioma

En este cuadro de diálogo puede seleccionar el idioma utilizado para el proceso de instalación. Haga clic en el cuadro combinado situado junto a la opción ***Idioma*** para desplazarse por el menú de idioma. Seleccione el idioma deseado y el proceso de instalación continuará en el idioma que haya elegido. La aplicación también se comunicará en el idioma seleccionado, con la opción de cambiar a inglés, que está siempre instalada de forma predeterminada.

Acuerdo de licencia de usuario final y Política de privacidad

Antes de continuar con el proceso de instalación, le recomendamos que se familiarice con el ***Acuerdo de licencia de usuario final*** y la ***Política de privacidad***. Se puede acceder a ambos documentos mediante los vínculos activos de la parte inferior del cuadro de diálogo. Haga clic en cualquiera de los hipervínculos para

abrir un nuevo cuadro de diálogo o una nueva ventana del navegador que contendrá el texto completo del documento respectivo. Lea detenidamente estos documentos vinculantes legalmente. Al hacer clic en el botón ***Continuar***, confirma que está de acuerdo con estos documentos.

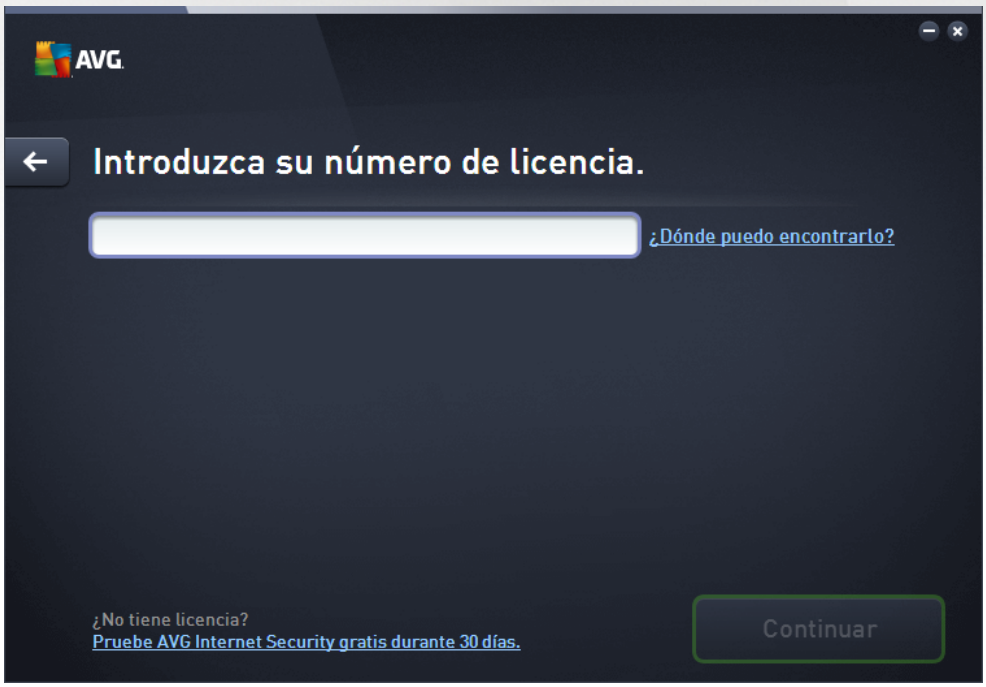
Continuar con la instalación

Para continuar con la instalación, simplemente haga clic en el botón ***Continuar***. Se le pedirá el número de licencia y, entonces, el proceso de instalación se ejecutará en modo automático. Se recomienda usar esta opción estándar para la mayoría de los usuarios al instalar **AVG AntiVirus**; tiene todos los ajustes de configuración predefinidos por el proveedor del programa. Esta configuración ofrece máxima seguridad con un uso óptimo de los recursos. En el futuro, si fuese necesario modificar la configuración, siempre tendrá la opción de hacerlo directamente desde la aplicación.

Si lo prefiere, existe la opción de ***Instalación personalizada***, disponible en forma de un hipervínculo ubicado en el botón ***Continuar***. La instalación personalizada solo la deberían realizar usuarios experimentados que tuvieran una buena razón para instalar la aplicación con una configuración no estándar, p. ej., para adaptarse a requisitos específicos del sistema. Si opta por este modo de instalación, al haber rellenado el número de licencia se le redirigirá al cuadro de diálogo ***Personalice su instalación***, donde puede especificar la configuración.

3.2. Introduzca su número de licencia

En el cuadro de diálogo ***Introducir su número de licencia*** se le invita a introducir su licencia escribiéndola *(o mediante el método de copiar y pegar)* en el campo de texto que se proporciona:



¿Dónde se encuentra el número de licencia?

Puede encontrar el número de venta en el paquete del CD, dentro de la caja de **AVG AntiVirus**. El número de

licencia se encontrará en el correo electrónico de confirmación que recibió después de haber comprado su **AVG AntiVirus** en línea. Debe introducir el número tal como figura. Si cuenta con el formato digital del número de licencia (*en el correo electrónico*), se recomienda usar el método copiar y pegar para insertarlo.

Cómo utilizar el método copiar y pegar

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

- Abra el correo electrónico que contiene su número de licencia.
- Haga clic en el botón izquierdo del ratón al principio del número de licencia, mantenga pulsado y arrastre el ratón hasta el final del número, y suelte el botón del ratón. El número aparece seleccionado.
- Pulse y mantenga pulsada la tecla ***Ctrl*** y luego pulse ***C***. Esto copia el número.
- Señale y haga clic en la posición donde le gustaría pegar el número copiado, es decir, en el campo de texto del cuadro de diálogo ***Introducir su número de licencia***.
- Pulse y mantenga pulsada la tecla ***Ctrl*** y luego pulse ***V***. Esto pega el número en el lugar seleccionado.

Continuar con la instalación

En la sección inferior del cuadro de diálogo puede encontrar el vínculo ***Instalar ahora***. El botón se activa introduciendo su número de licencia. Una vez activado, haga clic en el botón para iniciar el proceso de instalación. En caso de que no tenga un número de licencia válido y disponible, puede elegir instalar ***AVG AntiVirus Free Edition*** de la aplicación. Por desgracia, las ediciones gratuitas no admiten todas las funciones disponibles en la versión profesional completa. Por consiguiente, considere visitar el sitio web de AVG (http://www.avg.com/) para obtener información detallada sobre la compra y actualización de AVG.

3.3. Personalizar la instalación

El cuadro de diálogo ***Personalizar su instalación*** permite configurar parámetros detallados de la instalación:

¿Dónde quiere realizar la instalación?

Aquí puede especificar dónde le gustaría tener instalada la aplicación. La dirección del campo de texto muestra la ubicación sugerida en la carpeta Archivos de programa. Si prefiere otra ubicación, haga clic en el vínculo ***Cambiar ubicación*** para abrir una ventana nueva con la estructura de árbol de su disco.
A continuación, vaya a la ubicación deseada y confirme.

¿Qué componentes quiere instalar?

Esta sección contiene información general de todos los componentes que se pueden instalar. Si la configuración predeterminada no se ajusta a sus necesidades, puede quitar componentes específicos. Sin embargo, solo puede seleccionar entre los componentes que están incluidos en AVG AntiVirus. La única excepción es el componente ***Protección del equipo*** que no puede excluirse de la instalación. Cuando resalte cualquier elemento de esta sección, se mostrará una breve descripción del componente respectivo en el lateral derecho. Para obtener información detallada sobre la funcionalidad de cada componente, consulte el capítulo Información general de los componentes de esta documentación.

Continuar con la instalación

Para continuar con la instalación, simplemente haga clic en el botón ***Instalar ahora***. Como alternativa, en caso de que necesite cambiar o verificar la configuración de idioma, puede retroceder un paso al cuadro de diálogo anterior usando el botón de la flecha en la parte superior de este cuadro de diálogo.

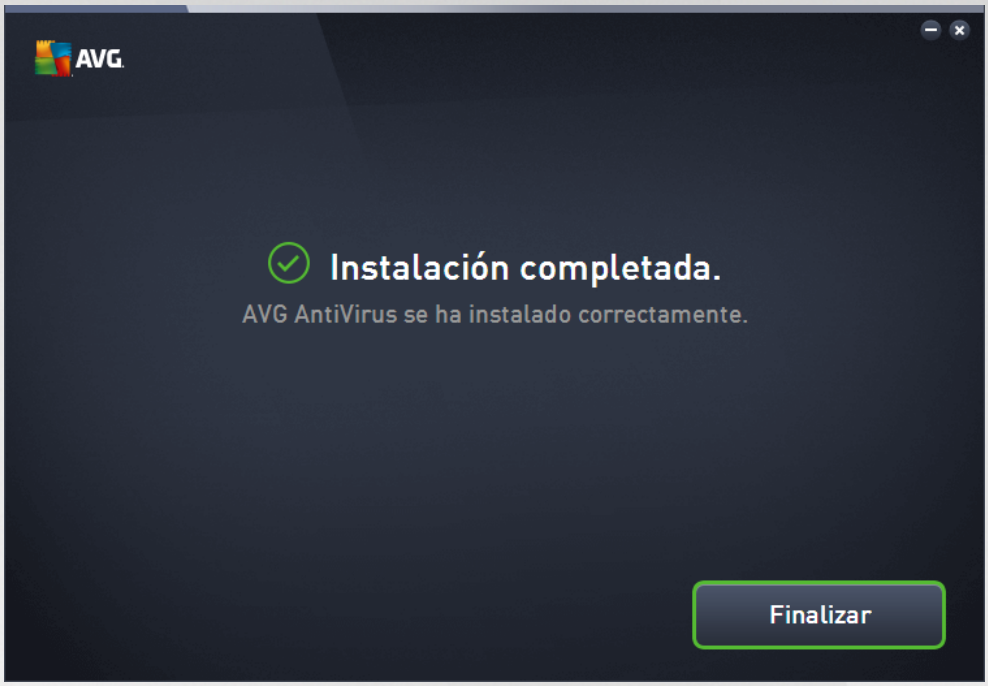
3.4. Instalación de AVG

Una vez confirmado el inicio de la instalación en el cuadro de diálogo anterior, el proceso de instalación se ejecuta de manera totalmente automática y no requiere ninguna intervención:

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

3.5. Instalación completada

El cuadro de diálogo ***Instalación completada*** confirma que AVG AntiVirus se ha instalado y configurado por completo:



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

4. Tras la instalación

4.1. Actualización de la base de datos de virus

Tenga en cuenta que tras la instalación *(y reinicio del equipo, si fuera necesario)* **AVG AntiVirus** actualiza automáticamente su base de datos de virus y todos los componentes para que estén en pleno funcionamiento, lo cual puede tardar unos minutos. Cuando el proceso de actualización esté en marcha, se le notificará mediante la información que aparece en el cuadro de diálogo principal. Espere un momento hasta que termine el proceso de actualización y tendrá su **AVG AntiVirus** completamente preparado y listo para protegerle.

4.2. Registro del producto

Cuando haya finalizado la instalación de **AVG AntiVirus**, registre el producto en línea en el sitio web de AVG (*http://www.avg.com/*). Después de registrar el producto, podrá obtener acceso total a su cuenta de usuario de AVG, al boletín de actualizaciones de AVG y a otros servicios que se ofrecen exclusivamente a los usuarios registrados. La forma más sencilla de registrarse es directamente a través de la interfaz de usuario de **AVG AntiVirus**. Seleccione el elemento línea superior de navegación / Opciones / Registrarse ahora. Se le redirigirá a la página ***Registro*** en el sitio web de AVG (*http://www.avg.com/*). Siga las instrucciones proporcionadas en dicha página.

4.3. Acceso a la interfaz de usuario

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

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

4.4. Análisis del equipo completo

Existe el riesgo potencial de que un virus informático se haya transmitido a su equipo antes de la instalación de **AVG AntiVirus**. Por esta razón, le recomendamos ejecutar un Análisis completo del equipo para asegurarse de que no haya infecciones en el equipo. Es probable que el primer análisis lleve algo de tiempo *(como una hora)*, pero se recomienda llevarlo a cabo para garantizar que el equipo no está en riesgo debido a una amenaza. Para obtener instrucciones sobre cómo ejecutar un análisis completo del equipo, consulte el capítulo Análisis de AVG.

4.5. Prueba Eicar

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

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

Intente descargar el archivo *eicar.com* y guárdelo en el disco local. De forma inmediata después de confirmar la descarga del archivo de prueba, **AVG AntiVirus** emitirá un aviso. Este aviso demuestra que AVG se ha instalado correctamente en el equipo.

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

4.6. Configuración predeterminada de AVG

La configuración predeterminada (*es decir, cómo está configurada la aplicación justamente después de la instalación*) de **AVG AntiVirus** la realiza el proveedor del software de manera que todos los componentes y funciones ofrezcan un rendimiento óptimo. ***A menos que tenga un buen motivo para hacerlo, no modifique la configuración de AVG. Los cambios de configuración debe realizarlos únicamente un usuario experimentado.*** Si desea cambiar la configuración de AVG para adaptarla mejor a sus necesidades, vaya a Configuración avanzada de AVG, seleccione el elemento de menú principal *Opciones/Configuración avanzada* y edite la configuración de AVG en el cuadro de diálogo Configuración avanzada de AVG que se acaba de abrir.

5. Interfaz de usuario de AVG

AVG AntiVirus se abre con la ventana principal:

La ventana principal se divide en varias secciones:

- ***La línea superior de navegación*** consta de cuatro vínculos activos alineados en la sección superior de la ventana principal *(más información de AVG, Informes, Soporte, Opciones)*. Detalles >>
- ***Información del estado de seguridad*** proporciona información básica sobre el estado actual de **AVG AntiVirus**. Detalles >>
- Se puede encontrar ***información general de los componentes instalados*** en una banda horizontal de bloques en la sección central de la ventana principal. Los componentes se muestran como bloques en verde claro con una etiqueta del correspondiente icono del componente, junto con la información de su estado. Detalles >>
- ***Mis aplicaciones*** están representadas gráficamente en la banda central inferior de la ventana principal y le ofrecen información general de aplicaciones complementarias a **AVG AntiVirus** que ya tiene instaladas en su equipo o que se recomienda instalar. Detalles >>
- Los ***vínculos rápidos de análisis / reparación / actualización*** se sitúan en la línea inferior de bloques en la ventana principal. Estos botones permiten un acceso inmediato a las funciones más importantes y de mayor uso de AVG. Detalles >>

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

- El ***icono de Bandeja del sistema*** se encuentra en la esquina inferior derecha de la pantalla *(en la bandeja del sistema)* e indica el estado actual de **AVG AntiVirus**. Detalles >>

5.1. Línea superior de navegación

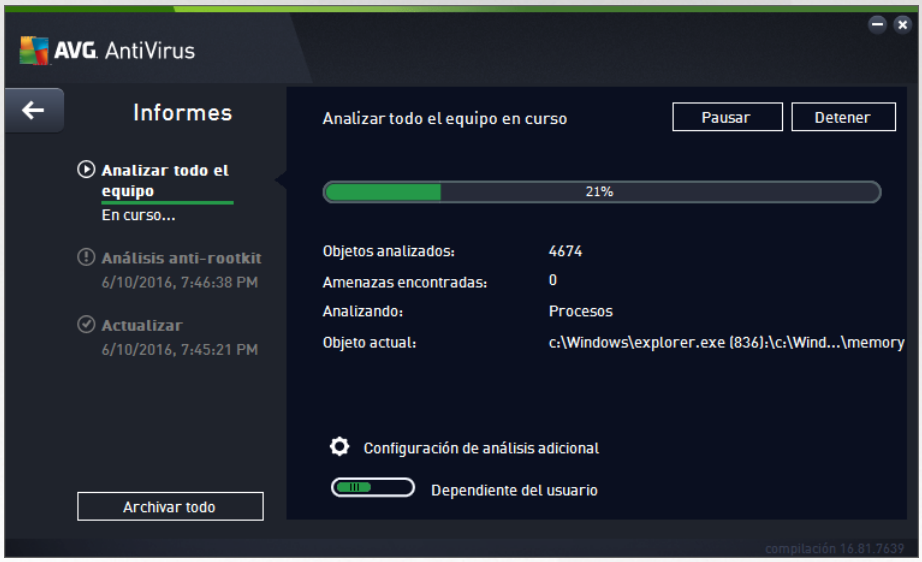
La ***línea superior de navegación*** consiste en varios vínculos activos alineados en la sección superior de la ventana principal. La navegación incluye los siguientes botones:

5.1.1. Más de AVG

Haga clic en el vínculo para conectarse al sitio web de AVG para consultar toda la información acerca de la protección de AVG para obtener una seguridad en Internet óptima.

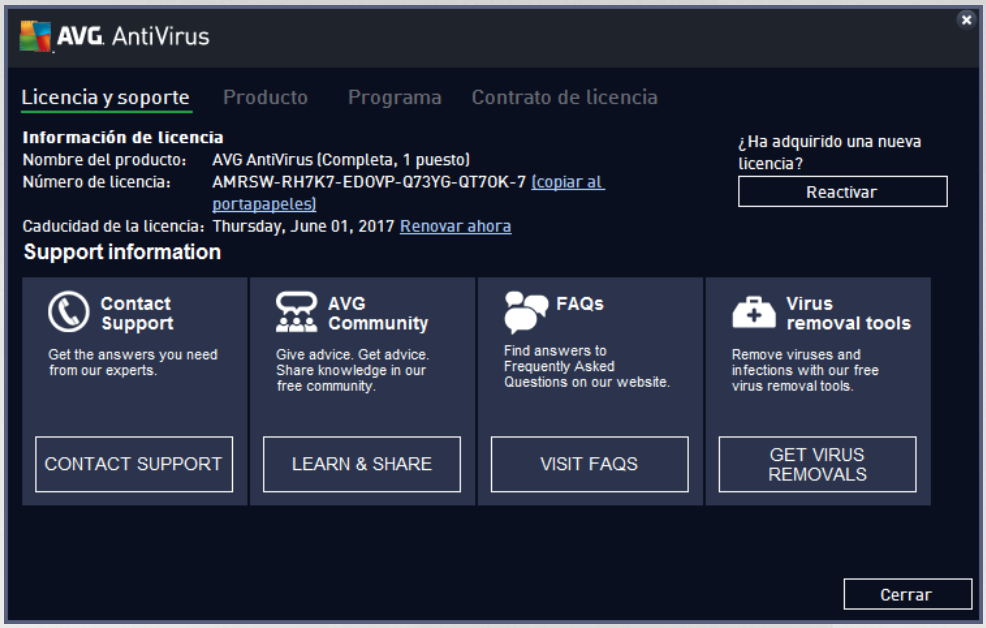
5.1.2. Informes

Abre un nuevo cuadro de diálogo ***Informes*** con información general de todos los informes relevantes sobre los procesos de análisis y actualización iniciados previamente. Si el análisis o actualización está en curso, se muestra un círculo rotando al lado del texto ***Informes*** en la navegación superior de la interfaz de usuario principal. Haga clic en el círculo para que se muestre en el cuadro de diálogo el progreso del proceso en curso:



5.1.3. Soporte

Abre un nuevo cuadro de diálogo estructurado en cuatro fichas donde puede encontrar toda la información relevante sobre **AVG AntiVirus**:



- ***Licencia y soporte***: la pestaña ofrece información sobre el nombre del producto, el número de licencia y la fecha de caducidad. En la sección inferior del cuadro de diálogo también puede encontrar información general de todos los contactos disponibles de atención al cliente. Los siguientes vínculos y botones activos están disponibles en la ficha:

  - *Reactivar*: haga clic para abrir el nuevo cuadro de diálogo ***Activar software de AVG***. Escriba su número de licencia en el campo respectivo para sustituir su número de venta *(el que utilizó durante la instalación de AVG AntiVirus)* o para cambiar su número de licencia actual por otro (*por ejemplo, si actualiza 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 se asegura de introducir el número de licencia correctamente.

  - *Renovar ahora*: recomendamos que obtenga la renovación de licencia de **AVG AntiVirus** con tiempo, por lo menos un mes antes de la caducidad de la licencia actual. Se le notificará cuando se aproxime la fecha de caducidad. Haga clic en este vínculo para ser redirigido al sitio web de AVG *(http://www.avg.com/)* donde encontrará información detallada sobre el estado de su licencia, la fecha de caducidad y la oferta de renovación o actualización.

- ***Producto***: la ficha proporciona información general de los datos técnicos más importantes de **AVG AntiVirus** con relación a la información del producto del AntiVirus, componentes instalados y protección de correo electrónico instalada.

- ***Programa***: en esta ficha puede encontrar información técnica detallada sobre los **AVG AntiVirus** instalados, como el número de la versión principal del producto y una lista de los números de versión de todos los productos correspondientes *(por ejemplo, Zen, PC TuneUp, ...)*. A continuación, esta ficha proporciona información general sobre los componentes instalados e información de seguridad específica *(números de las versiones de bases de datos de virus y LinkScanner)*.

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

5.1.4. Opciones

El mantenimiento de **AVG AntiVirus** está disponible desde el elemento ***Opciones***. Haga clic en la flecha para abrir el menú desplegable:

- ***Analizar equipo*** inicia un análisis de todo el equipo.
- ***Analizar carpeta seleccionada...***: pasa a la interfaz de análisis de AVG y permite definir, dentro de la estructura de árbol del equipo, qué archivos y carpetas deben analizarse.
- ***Analizar archivo...***: permite ejecutar un análisis bajo demanda en un solo archivo específico. Haga clic en esta opción para abrir una nueva ventana con la estructura de árbol del disco. Seleccione el archivo que desee y confirme el inicio del análisis.
- ***Actualizar***: inicia automáticamente el proceso de actualización de **AVG AntiVirus**.
- ***Actualizar desde directorio...***: ejecuta el proceso de actualización desde los archivos de actualización que se encuentran ubicados en una carpeta específica del disco local. No obstante, esta opción solo se recomienda en caso de emergencia, es decir, en situaciones en las que no hay conexión a Internet (por ejemplo, si el equipo está infectado y desconectado de Internet, o bien está conectado a una red que no tiene acceso a Internet, etc.). En la ventana recién abierta, seleccione la carpeta donde anteriormente se guardó el archivo de actualización e inicie el proceso de actualización.
- ***Almacén de virus***: abre la interfaz en el espacio de cuarentena, el Almacén de virus, donde AVG elimina todas las infecciones detectadas. Dentro de este espacio de cuarentena los archivos infectados están aislados, la seguridad del equipo está garantizada y, al mismo tiempo, los archivos infectados se almacenan para una posible reparación en el futuro.
- ***Historial***: ofrece más opciones de submenú específicas:
    - *Resultados del análisis*: abre un cuadro de diálogo que proporciona información general de los resultados del análisis.
    - *Resultados de Resident Shield*: abre un cuadro de diálogo con información general de las amenazas detectadas por Resident Shield.
    - *Resultados de Identity Protection*: abre un cuadro de diálogo con información general sobre las amenazas detectadas por el componente Identidad.
    - *Resultados de Protección del correo electrónico*: abre un cuadro de diálogo con información general de los archivos adjuntos de correo electrónico detectados como peligrosos por el componente Protección del correo electrónico.
    - *Resultados de Online Shield*: abre un cuadro de diálogo con información general de las amenazas detectadas por Online Shield.
    - *Registro del historial de eventos*: abre la interfaz del registro del historial con información general de todas las acciones de **AVG AntiVirus** registradas.

- ***Configuración avanzada...***: abre el cuadro de diálogo Configuración avanzada de AVG, donde puede editar la configuración de **AVG AntiVirus**. Por lo general, se recomienda mantener la configuración predeterminada de la aplicación definida por el proveedor del software.

- ***Contenido de la Ayuda***: abre los archivos de ayuda de AVG.

- ***Obtener ayuda***: abre el cuadro de ayuda que ofrece todos los contactos accesibles y la información de ayuda.

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

- ***Acerca de virus y amenazas***: abre la enciclopedia de virus en línea del sitio web de AVG (*http://www.avg.com/*) donde puede buscar información detallada sobre los virus identificados.

- ***Reactivar***: abre el cuadro de diálogo de activación con el número de licencia que proporcionó durante el proceso de instalación. En este cuadro de diálogo puede editar su número de licencia para reemplazar el número de venta (*con el que ha instalado AVG*) o sustituir el número de licencia antiguo (*por ejemplo, cuando actualice a un nuevo producto AVG*). Si utiliza la versión de prueba de **AVG AntiVirus**, los últimos dos elementos aparecen como ***Comprar ahora*** y ***Activar***, y le permiten adquirir de inmediato la versión completa del programa. Si **AVG AntiVirus** se ha instalado con un número de venta, se muestran los elementos ***Registrar*** y ***Activar***:

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

- ***Acerca de AVG***: abre un nuevo cuadro de diálogo con cuatro pestañas que proporcionan información sobre la licencia y el soporte, información del programa y el producto, y la versión completa del contrato de licencia. *(El mismo cuadro de diálogo se puede abrir desde el vínculo Soporte de la navegación principal).*

5.2. Información sobre el estado de seguridad

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

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

 - El icono amarillo advierte de que ***uno o más componentes no están configurados correctamente***, por lo que se recomienda revisar su configuración o propiedades. No significa que haya un problema crítico en **AVG AntiVirus**; quizás simplemente se trate de que decidió desactivar un componente de forma intencionada. Sigue estando protegido. Sin embargo, se recomienda revisar la configuración del componente que presenta el problema. Se mostrará el componente que está configurado incorrectamente con una banda naranja de advertencia en la interfaz de usuario.

El icono amarillo también aparece si, por alguna razón, decidió ignorar el estado de error de un componente. Se puede acceder a la opción ***Ignorar estado de error*** a través de Configuración avanzada / Ignorar estado de error. Aquí puede declarar que conoce el estado de error del componente

pero que, por alguna razón, desea que **AVG AntiVirus** siga así y no quiere que se le advierta sobre ello. Es posible que necesite utilizar esta opción en una situación específica, pero se recomienda encarecidamente que desactive la opción ***Ignorar estado error*** tan pronto como sea posible.

El icono amarillo también se mostrará si **AVG AntiVirus** requiere que el equipo se reinicie (***Es necesario reiniciar***). Preste atención a esta advertencia y reinicie el equipo.

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

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

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

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

5.3. Información general de los componentes

Se puede encontrar información general de los componentes instalados en una banda horizontal de bloques en la sección central de la ventana principal. Los componentes se muestran como bloques en verde claro etiquetados con el correspondiente icono del componente. Cada bloque proporciona información sobre el estado actual de protección. Si el componente está configurado de forma adecuada y funciona correctamente, la información se muestra en letras verdes. Si el componente se interrumpe, su funcionalidad es limitada o el componente se encuentra en estado de error, se le notificará con un texto de advertencia mostrado en un campo de texto naranja. ***Se recomienda encarecidamente que preste atención a la configuración del componente.***

Mueva el ratón hacia el componente para mostrar un breve texto al final de la ventana principal. El texto proporciona una introducción básica de la funcionalidad del componente. También informa de su estado actual y especifica qué servicios del componente no están bien configurados.

Lista de componentes instalados

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

- ***Equipo***: este componente contiene dos servicios: ***AntiVirus Shield***, que detecta virus, spyware, gusanos, troyanos, archivos ejecutables no deseados o catálogos en el sistema y le protege de adware malicioso, y ***Anti-Rootkit***, que analiza rootkits peligrosos ocultos en aplicaciones, controladores o catálogos. Detalles >>
- ***Navegación web***: le protege de ataques web mientras navega por Internet. Detalles >>

- ***Identidad***: El componente ejecuta el servicio ***Identity Shield***, que protege constantemente sus activos digitales contra las amenazas nuevas y desconocidas de Internet. Detalles >>

- ***Mensajes de correo electrónico***: comprueba sus mensajes de correo electrónico entrantes en busca de spam y bloquea virus, ataques de suplantación de identidad y otras amenazas. Detalles >>

Acciones accesibles

- ***Mueva el ratón sobre el icono*** de cualquier componente para resaltarlo en la información general de los componentes. Al mismo tiempo, en la parte inferior de la interfaz de usuario aparece una descripción de la funcionalidad básica del componente.

- ***Haga clic en el icono del componente*** para abrir la interfaz propia del componente con la información de su estado actual y acceder a la configuración e información estadística.

5.4. Mis aplicaciones

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

- ***Protección móvil*** es una aplicación que protege al teléfono móvil de virus y software malicioso. También ofrece la posibilidad de realizar un seguimiento remoto de su smartphone si no lo lleva encima.

- La aplicación ***PC Tuneup*** es una herramienta avanzada que permite realizar un análisis detallado del sistema y saber cómo pueden mejorarse la velocidad y el rendimiento general del equipo.

Para obtener información detallada de cualquiera de las aplicaciones de ***Mis aplicaciones***, haga clic en el bloque respectivo. Será redirigido a la página web de AVG, donde también puede descargar el componente de forma inmediata.

5.5. Vínculos rápidos Analizar/Actualizar

Los vínculos rápidos están situados en la línea inferior de los botones de la **AVG AntiVirus** interfaz de usuario. Estos vínculos le permiten acceder inmediatamente a las funciones más importantes y más utilizadas de la aplicación, como analizar y actualizar. Los vínculos rápidos son accesibles desde todos los cuadros de diálogo de la interfaz de usuario:

- ***Analizar ahora***: el botón está dividido gráficamente en dos secciones. Siga el vínculo ***Analizar ahora*** para iniciar el Análisis completo del equipo de forma inmediata y ver el progreso y los resultados en la ventana Informes, que se abrirá automáticamente. El botón ***Opciones*** abre el cuadro de diálogo ***Opciones de análisis***, donde puede gestionar análisis programados y editar los parámetros de Análisis completo del equipo / Analizar archivos o carpetas específicos. *(Consulte los detalles en el capítulo Análisis de AVG)*

- ***Reparar rendimiento****:* este botón le dirige al servicio ***Analizador de equipos***, una herramienta avanzada para el análisis detallado y la corrección del sistema para saber cómo se puede mejorar la velocidad y el rendimiento general del equipo.

- ***Actualizar ahora***: pulse el botón para iniciar la actualización del producto de forma inmediata. Se le informará sobre los resultados de la actualización en el cuadro de diálogo deslizante situado sobre el icono de bandeja del sistema de AVG. *(Consulte los detalles en el capítulo Actualizaciones de AVG).*

5.6. Icono de la bandeja del sistema

El ***icono de la bandeja del sistema de AVG*** *(en la barra de tareas de Windows, esquina inferior derecha del monitor)* indica el estado actual de **AVG AntiVirus**. Está visible en todo momento en la bandeja del sistema, sin importar si la interfaz de usuario de **AVG AntiVirus** está abierta o cerrada:

Apariencia del icono de la bandeja del sistema de AVG

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

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

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

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

Información sobre el icono de la bandeja del sistema de AVG

El ***icono de la bandeja del sistema de AVG*** informa también de las actividades en curso en su **AVG AntiVirus**, así como de posibles cambios de estado en el programa (*por ejemplo, inicio automático de un análisis o actualización programados, cambio de perfil de Firewall, cambio de estado de un componente, situación de estado de error, ...*) mediante una ventana emergente que se abre en el icono de la bandeja del sistema.

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

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

- ***Abrir AVG***: haga clic para abrir la interfaz de usuario de **AVG AntiVirus**.

- ***Deshabilitar la protección de AVG temporalmente***: esta opción permite desactivar toda la protección proporcionada por **AVG AntiVirus** de una vez. Recuerde que no debe utilizar esta opción a menos que sea absolutamente necesario. En la mayoría de los casos, no será necesario deshabilitar **AVG AntiVirus** antes de instalar un nuevo software o nuevos controladores, ni siquiera cuando el instalador o asistente del software sugiera cerrar primero los programas y aplicaciones que estén en ejecución para garantizar que no haya interrupciones indeseadas durante el proceso de instalación. Si tiene que deshabilitar temporalmente **AVG AntiVirus** para hacer algo, vuelva a habilitarlo tan pronto como termine. Si está conectado a Internet o a una red durante el tiempo en que el software antivirus se encuentra desactivado, el equipo está expuesto a sufrir ataques.

- ***Análisis***: haga clic para abrir el menú contextual de los análisis predefinidos (*Análisis completo del equipo* y *Analizar archivos o carpetas específicos*) y seleccione el análisis que necesite. Se iniciará de inmediato.

- ***Ejecutando análisis...***: este elemento aparece solo si hay algún análisis ejecutándose actualmente en el equipo. Puede establecer la prioridad de este análisis, detenerlo o pausarlo. También puede acceder a las siguientes acciones: *Establecer prioridad para todos los análisis, Pausar todos los análisis* o *Detener todos los análisis*.

- ***Reparar rendimiento***: haga clic para iniciar el componente Analizador de equipos.

- ***Iniciar sesión en AVG MyAccount***: abre la página de inicio de MyAccount, donde puede gestionar los productos a los que está suscrito, adquirir protección adicional, descargar archivos de instalación, comprobar facturas y pedidos anteriores y gestionar información personal.

- ***Actualizar ahora***: inicia una actualización inmediata.

- ***Ayuda***: abre el archivo de ayuda en la página de inicio.

5.7. Asesor AVG

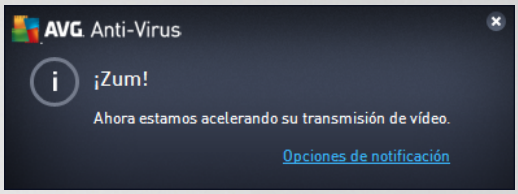
Asesor AVG se ha diseñado para detectar problemas que puedan poner su equipo en riesgo y para recomendar una acción que solucione la situación. ***AVG Advisor*** se muestra en forma de elemento emergente deslizante sobre la bandeja del sistema. El servicio detecta una posible ***red desconocida con un nombre conocido***. Esto suele aplicarse únicamente a usuarios que se conectan a varias redes, normalmente con equipos portátiles: Si una red nueva y desconocida tiene el mismo nombre que una red conocida y utilizada con frecuencia *(por ejemplo, Casa o MiWifi)*, es posible que se confunda y se conecte accidentalmente a una red totalmente desconocida y potencialmente insegura. ***Asesor AVG*** puede evitar esta situación al advertirle de que el nombre en realidad representa a otra red. Sobra decir que, si cree que la red desconocida es segura, puede guardarla en una lista de redes conocidas de ***Asesor AVG para que no se le vuelva a notificar en el futuro.***

Navegadores web compatibles

Esta característica funciona con los siguientes navegadores web: Internet Explorer, Chrome, Firefox, Opera y Safari.

5.8. Acelerador AVG

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



6. Componentes de AVG

6.1. Protección del equipo

El componente ***Equipo*** abarca dos servicios de seguridad principales: ***AntiVirus*** y ***Caja fuerte para datos***:

- ***AntiVirus*** consiste en un motor de análisis que protege todos los archivos, las áreas de sistema del equipo y dispositivos extraíbles *(disco flash, etc.)*, y analiza virus conocidos. Todos los virus detectados se bloquean para evitar que actúen y, a continuación, se borran o se ponen en cuarentena en el Almacén de virus. El usuario ni siquiera advierte el proceso, ya que la protección residente se ejecuta "en segundo plano". AntiVirus también usa el análisis heurístico, donde los archivos se analizan en busca de características típicas de virus. Esto significa que AntiVirus tiene la capacidad para detectar un virus nuevo y desconocido si este contiene algunas características típicas de los virus existentes. **AVG AntiVirus** también puede analizar y detectar aplicaciones ejecutables o catálogos DLL potencialmente no deseados en el sistema *(varios tipos de spyware, adware, etc.)*. Asimismo, AntiVirus analiza el registro del sistema en busca de entradas sospechosas y archivos temporales de Internet, y permite tratar todos los elementos potencialmente dañinos de la misma manera que cualquier otra infección.

- ***Caja fuerte para datos*** le permite crear almacenes virtuales seguros para guardar datos valiosos o sensibles. El contenido de una caja fuerte para datos está encriptado y protegido con una contraseña elegida por usted para que nadie pueda acceder sin autorización.

Controles del cuadro de diálogo

Para cambiar entre ambas secciones del cuadro de diálogo, haga clic en cualquier parte del correspondiente panel de servicio. El panel se resalta en una sombra más clara de azul. En ambas secciones del cuadro de diálogo puede encontrar los siguientes controles. La funcionalidad es la misma tanto si pertenecen a un servicio de seguridad como a otro *(AntiVirus o Anti-Rootkit)*:

 ***Habilitado / Deshabilitado***: el botón recuerda a un semáforo, tanto en apariencia como en funcionalidad. Haga clic para cambiar entre las dos posiciones. El color verde indica ***Habilitado***, es

decir, el servicio de seguridad AntiVirus está activo y funciona correctamente. El color rojo representa el estado ***Deshabilitado***, es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, le recomendamos encarecidamente que mantenga la configuración predeterminada de seguridad. La configuración predeterminada garantiza el funcionamiento óptimo de la aplicación y el nivel máximo de seguridad. Si, por alguna razón, desea desactivar el servicio, se le advertirá sobre el posible riesgo a través de una señal roja de ***Advertencia*** y la información de que no está completamente protegido. ***Tenga en cuenta que debe activar de nuevo el servicio lo antes posible.***

Configuración: haga clic en el botón para que se le redirija a la interfaz de Configuración avanzada. Se abre el cuadro de diálogo correspondiente, en el que puede configurar el servicio seleccionado, es decir, AntiVirus. En la interfaz de configuración avanzada puede editar todos los ajustes de cada servicio de seguridad de **AVG AntiVirus,** pero tenga en cuenta que esta configuración solo está recomendada para usuarios experimentados.

Flecha: use la flecha verde de la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal, en la que se muestra la información general de los componentes.

Como crear una caja fuerte para datos

En la sección ***Caja fuerte para datos*** del cuadro de diálogo ***Protección del equipo*** encontrará el botón ***Crear una caja fuerte***. Haga clic en el botón para abrir un nuevo cuadro de diálogo con el mismo nombre, en el que podrá especificar los parámetros de la caja fuerte que desea crear. Complete toda la información necesaria y siga las instrucciones de la aplicación:

En primer lugar, debe especificar el nombre de la caja fuerte y crear una contraseña segura:

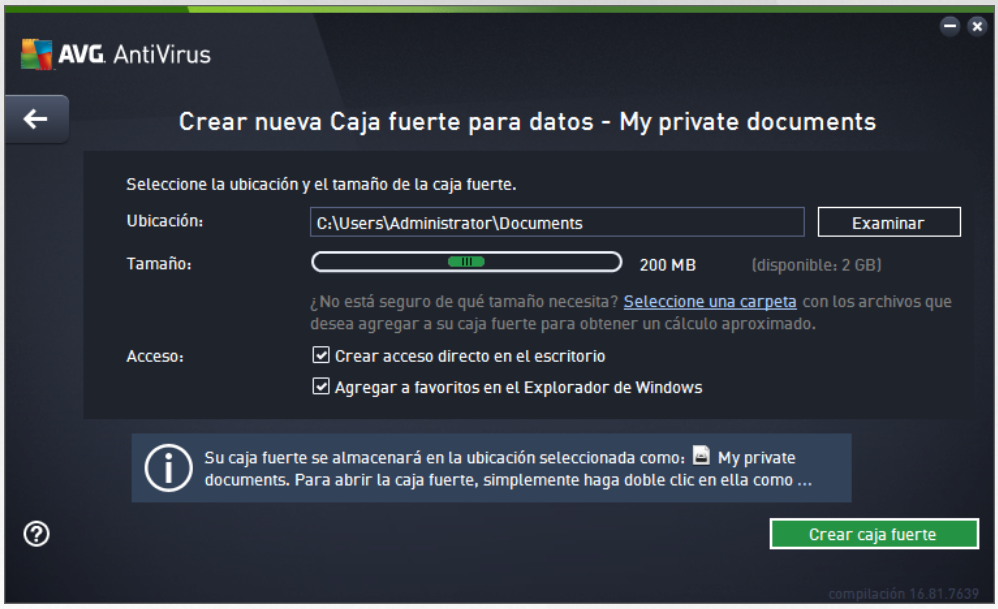
- ***Nombre de la caja fuerte***: para crear una caja fuerte para datos nueva, primero necesita un nombre adecuado para identificarla. Si comparte el equipo con otros miembros de su familia, quizás desee incluir su nombre e indicar el contenido de la caja fuerte, por ejemplo *Correos electrónicos de papá*.

- ***Crear contraseña / Confirmar contraseña***: cree una contraseña para mantener la seguridad de sus datos y escríbala en los campos de texto correspondientes. El indicador gráfico de la derecha le dirá

si su contraseña es débil *(relativamente fácil de descifrar con herramientas de software especiales)* o fuerte. Recomendamos seleccionar una contraseña con una seguridad media, como mínimo. Puede aumentar la seguridad de la contraseña incluyendo mayúsculas, números y otros caracteres como puntos, guiones, etc. Si desea asegurarse de que está escribiendo la contraseña correctamente, puede marcar la casilla ***Mostrar contraseña*** *(evidentemente, siempre que no haya nadie más delante)*.

- ***Sugerencia de contraseña***: le recomendamos que cree también una sugerencia de contraseña que le ayude a recordar la contraseña en caso de que la olvide. Recuerde que la caja fuerte para datos está diseñada para proteger los archivos con acceso exclusivo mediante contraseña, por lo tanto, hay que introducirla siempre y si la olvida, no podrá acceder a la caja fuerte para datos.

Una vez especificados todos los datos requeridos en los campos de texto, haga clic en el botón ***Siguiente*** para continuar con el siguiente paso:



Este cuadro de diálogo proporciona las siguientes opciones de configuración:

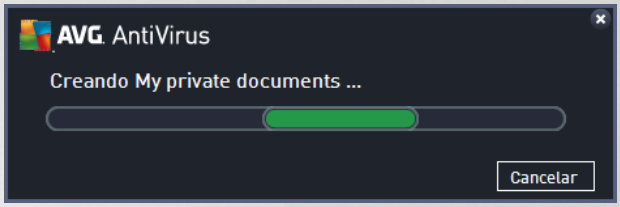
- ***Ubicación*** establece dónde se ubicará físicamente la caja fuerte para datos. Examine el disco duro para encontrar un destino adecuado o mantenga la ubicación predeterminada, que es la carpeta *Documentos*. Tenga en cuenta que una vez que haya creado la caja fuerte para datos, no podrá cambiar su ubicación.

- ***Tamaño***: puede predefinir el tamaño de la caja fuerte para datos, lo que reservará el espacio necesario en el disco. El valor establecido no debe ser demasiado pequeño *(insuficiente para sus necesidades)* ni demasiado grande *(que ocupe demasiado espacio de disco de forma innecesaria)*. Si ya sabe qué desea incluir en la caja fuerte para datos, puede colocar todos los archivos en una carpeta y, a continuación, utilizar el vínculo ***Seleccionar una carpeta*** para calcular automáticamente el tamaño total. Sin embargo, el tamaño se puede cambiar más adelante según sus necesidades.

- ***Acceso***: las casillas de verificación de esta sección le permiten crear accesos directos a la caja fuerte para datos.

Cómo utilizar la caja fuerte para datos

Cuando esté satisfecho con la configuración, haga clic en el botón ***Crear caja fuerte***. Aparecerá el cuadro de diálogo ***Su caja fuerte para datos ya está lista*** para anunciarle que la caja fuerte ya está disponible para guardar sus archivos. En este momento, la caja fuerte está abierta y puede acceder a ella de inmediato. Cada vez que intente acceder a ella, se le invitará a desbloquearla con la contraseña que haya definido:



Para usar la nueva caja fuerte para datos, primero debe abrirla. Para ello, haga clic en el botón ***Abrir ahora***. Una vez abierta, la caja fuerte para datos aparece en el equipo como un nuevo disco virtual. Asígnele la letra que desee en el menú desplegable (*solo se le permitirá seleccionar uno de los discos que haya libres en ese momento*). Por norma general, no podrá elegir C *(normalmente asignada al disco duro)*, A *(unidad de disquete)* ni D *(unidad de DVD)*. Tenga en cuenta que cada vez que desbloquee una caja fuerte para datos, puede elegir una letra diferente de unidad disponible.

Cómo desbloquear la caja fuerte para datos

La siguiente vez que intente acceder a la caja fuerte para datos, se le invitará a desbloquearla con la contraseña que haya definido:

En el campo de texto, escriba la contraseña para acreditarse y haga clic en el botón ***Desbloquear***. Si necesita ayuda para recordar la contraseña, haga clic en ***Sugerencia*** para que se muestre la sugerencia de contraseña que definió al crear la caja fuerte para datos. La caja fuerte para datos nueva aparecerá en la información general de sus cajas fuertes para datos como DESBLOQUEADA y podrá agregar o eliminar archivos según sea necesario.

6.2. Protección de la navegación web

La ***Protección de navegación web*** consiste en dos servicios: ***LinkScanner Surf-Shield*** y ***Online Shield***:

- ***LinkScanner Surf-Shield*** protege contra la creciente cantidad de amenazas existentes en la web que se actualizan constantemente. Estas amenazas pueden estar ocultas en cualquier tipo de sitio web, desde gubernamentales y de marcas grandes y reconocidas hasta sitios de empresas pequeñas, y rara vez permanecen en un mismo sitio por más de 24 horas. LinkScanner protege su equipo analizando las páginas web que se encuentran detrás de todos los vínculos de cualquier página que visite, comprobando que sean seguros en el único momento que importa: cuando se está a punto de hacer clic en ese vínculo. ***LinkScanner Surf Shield no ha sido diseñado para la protección de plataformas de servidor***

- ***Online Shield*** es un tipo de protección residente en tiempo real; analiza el contenido de las páginas web visitadas (y los posibles archivos incluidos en ellas) antes incluso de que aparezcan en el navegador web o se descarguen en el equipo. Online Shield detecta que la página que se dispone a visitar incluye algún javascript peligroso e impide que esta se abra. Asimismo, reconoce el software malicioso contenido en una página y detiene inmediatamente su descarga para que no entre en el equipo. Esta potente protección bloquea el contenido malicioso de cualquier página web que intente abrir e impide que se descargue en el equipo. Cuando esta característica está habilitada, si hace clic en un vínculo o escribe la URL de un sitio peligroso, impedirá automáticamente que abra la página web, protegiéndole de sufrir una infección involuntaria. Resulta importante recordar que las páginas web explotadas puede infectar al equipo simplemente visitando el sitio afectado. ***Online Shield no ha sido diseñado para plataformas de servidor***

Controles del cuadro de diálogo

Para cambiar entre ambas secciones del cuadro de diálogo, haga clic en cualquier parte del correspondiente panel de servicio. El panel se resalta en una sombra más clara de azul. En ambas secciones del cuadro de diálogo puede encontrar los siguientes controles. La funcionalidad es la misma que si pertenecen a un servicio de seguridad u otro *(LinkScanner Surf-Shield u Online Shield)*:

 ***Habilitado / Deshabilitado***: el botón recuerda a un semáforo, tanto en apariencia como en funcionalidad. Haga clic para cambiar entre las dos posiciones. El color verde pertenece a ***Habilitado***, lo que significa que el servicio de seguridad LinkScanner Surf-Shield / Online Shield está activo y funciona correctamente. El color rojo representa el estado ***Deshabilitado***, es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, le recomendamos encarecidamente que mantenga la configuración predeterminada de seguridad. La configuración predeterminada garantiza el funcionamiento óptimo de la aplicación y el nivel máximo de seguridad. Si, por alguna razón, desea desactivar el servicio, se le advertirá sobre el posible riesgo a través de una señal roja de ***Advertencia*** y la información de que no está completamente protegido. ***Tenga en cuenta que debe activar de nuevo el servicio lo antes posible.***

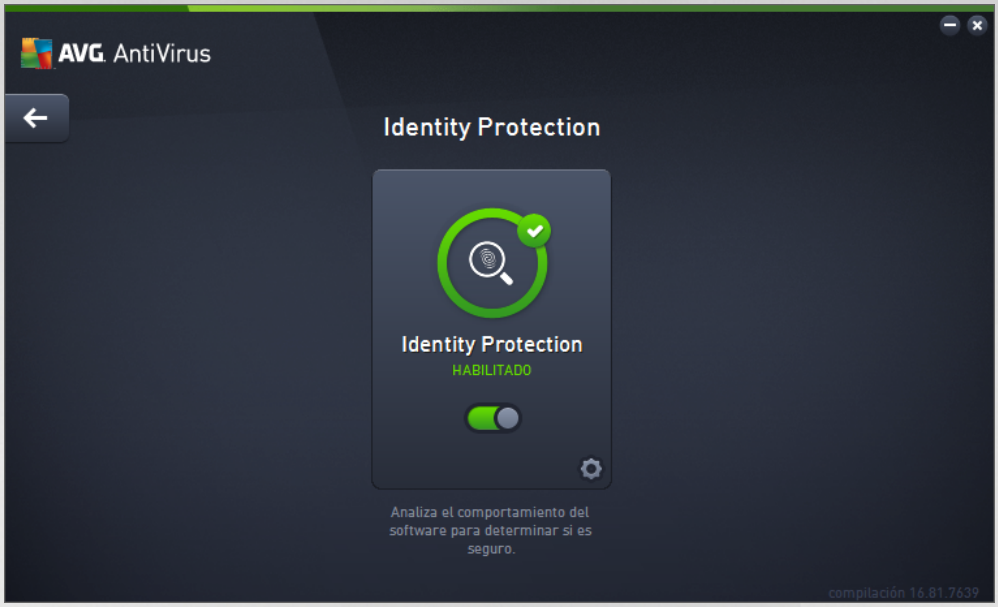
 ***Configuración***: haga clic en el botón para que se le redirija a la interfaz de Configuración avanzada. Precisamente, el respectivo cuadro de diálogo se abre y puede configurar el servicio seleccionado, es decir, LinkScanner Surf-Shield u Online Shield. En la interfaz de configuración avanzada puede editar todos los ajustes de cada servicio de seguridad de **AVG AntiVirus,** pero tenga en cuenta que esta configuración solo está recomendada para usuarios experimentados.

 ***Flecha***: use la flecha verde de la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal, en la que se muestra la información general de los componentes.

6.3. Identity Protection

El ***componente*** Identity Protection ejecuta el servicio ***Identity Shield***, que protege constantemente sus activos digitales contra las amenazas nuevas y desconocidas de Internet:

- ***Identity Protection*** es un servicio que le protege frente a todo tipo de software malicioso (*spyware, robots, robo de identidad, etc.*) utilizando tecnologías de comportamiento y ofreciendo protección ante los ataques de día cero de virus nuevos. Identity Protection se centra en impedir que los ladrones de identidad roben sus contraseñas, datos bancarios, números de tarjeta de crédito y otros activos digitales personales desde todo tipo de software malicioso *(malware)* que ataque a su equipo. Para ello, se asegura de que todos los programas que se ejecutan en el equipo o en la red compartida funcionan correctamente. Identity Protection detecta y bloquea constantemente los comportamientos sospechosos y protege el equipo frente a todo el software malicioso nuevo. Además, protege el equipo en tiempo real contra amenazas nuevas e incluso desconocidas. Monitoriza todos los procesos *(incluidos los ocultos)* y más de 285 patrones de comportamiento diferentes, y puede determinar si está ocurriendo algo malicioso en su sistema. De esta forma, puede revelar amenazas que aún no se han descrito en la base de datos de virus. Siempre que un fragmento desconocido de código entra en un equipo, se vigila y controla inmediatamente para buscar comportamientos maliciosos. Si se determina que el archivo es malicioso, Identity Protection mueve el código al Almacén de virus y deshace todos los cambios que se hayan hecho en el sistema *(inserción de código, cambios en el Registro, apertura de puertos, etc.)*. No es necesario iniciar un análisis para estar protegido. La tecnología es muy proactiva, prácticamente no necesita actualización y siempre está en guardia.



Controles del cuadro de diálogo

En el cuadro de diálogo puede encontrar los siguientes controles:

Habilitado / Deshabilitado: el botón recuerda a un semáforo, tanto en apariencia como en funcionalidad. Haga clic para cambiar entre las dos posiciones. El color verde indica ***Habilitado***, lo que significa que el servicio de seguridad Identity Protection está activo y funciona correctamente. El color rojo representa el estado ***Deshabilitado***, es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, le recomendamos encarecidamente que mantenga la configuración predeterminada de seguridad. La configuración predeterminada garantiza el funcionamiento óptimo de la aplicación y el nivel máximo de seguridad. Si, por alguna razón, desea desactivar el servicio, se le advertirá sobre el posible riesgo a través de una señal roja de ***Advertencia*** y la información de que no está completamente protegido. ***Tenga en cuenta que debe activar de nuevo el servicio lo antes posible.***

Configuración: haga clic en el botón para que se le redirija a la interfaz de Configuración avanzada. El cuadro de diálogo correspondiente se abre para que pueda configurar el servicio seleccionado, es decir, Identity Protection. En la interfaz de configuración avanzada puede editar todos los ajustes de cada servicio de seguridad de **AVG AntiVirus,** pero tenga en cuenta que esta configuración solo está recomendada para usuarios experimentados.

Flecha: use la flecha verde de la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal, en la que se muestra la información general de los componentes.

En **AVG AntiVirus** no se incluye el servicio Identity Alert. Si quiere usar este tipo de protección, pulse el botón ***Actualizar para activar*** para que se le redirija a la página web en la que puede comprar una licencia de Identity Alert.

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

6.4. Protección del correo electrónico

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

- ***Analizador de correo electrónico***: Uno de los focos más habituales de virus y troyanos es el correo electrónico. La suplantación de identidad y el spam aumentan el nivel de riesgo del correo electrónico. Las cuentas gratuitas de correo electrónico tienen mayor probabilidad de recibir correos electrónicos maliciosos *(ya que no suelen emplear tecnología anti-spam)*, y su uso entre los usuarios domésticos está muy extendido. Asimismo, los usuarios domésticos, al navegar por sitios desconocidos y facilitar sus datos personales en formularios en línea *(tales como su dirección de correo electrónico)*, aumentan su exposición a los ataques por correo electrónico. Las empresas generalmente utilizan cuentas corporativas de correo electrónico y emplean mecanismos como filtros anti-spam para reducir el riesgo. El componente Protección del correo electrónico es responsable de analizar cada mensaje de correo electrónico enviado o recibido; cuando se detecta un virus en un correo, se mueve al Almacén de virus inmediatamente. Este componente también puede filtrar ciertos tipos de adjuntos de correo electrónico y añadir un texto de certificación a los mensajes que no contengan infecciones. ***El Analizador de correo electrónico no ha sido diseñado para plataformas de servidor.***

- ***Anti-Spam*** verifica todos los mensajes de correo electrónico entrantes y marca los correos no deseados como spam *(por spam se entiende el correo electrónico no solicitado; la mayoría publicita un producto o servicio que se envía en masa a un gran número de direcciones de correo electrónico al mismo tiempo, y así se llena la cuenta de correo del destinatario. No se considera spam el correo comercial legítimo al que los consumidores dan su consentimiento).*. Anti-Spam puede modificar el asunto del correo electrónico *(que se ha identificado como spam)* añadiendo una cadena especial de texto. De esta manera puede filtrar fácilmente los mensajes en el cliente de correo electrónico. El componente Anti-Spam utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado. Anti-Spam emplea una base de datos constantemente actualizada para detectar el spam. También es posible utilizar servidores RBL *(bases de datos públicas de direcciones de correo electrónico de "spammers conocidos")* y agregar manualmente direcciones de correo electrónico a la Lista blanca *(nunca se marcan como spam)* y la Lista negra *(siempre se marcan como spam)*.

Controles del cuadro de diálogo

Para cambiar entre ambas secciones del cuadro de diálogo, haga clic en cualquier parte del correspondiente panel de servicio. El panel se resalta en una sombra más clara de azul. En ambas secciones del cuadro de diálogo puede encontrar los siguientes controles. La funcionalidad es la misma tanto si pertenecen a un servicio de seguridad como a otro *(Analizador de correo electrónico o Anti-Spam)*:

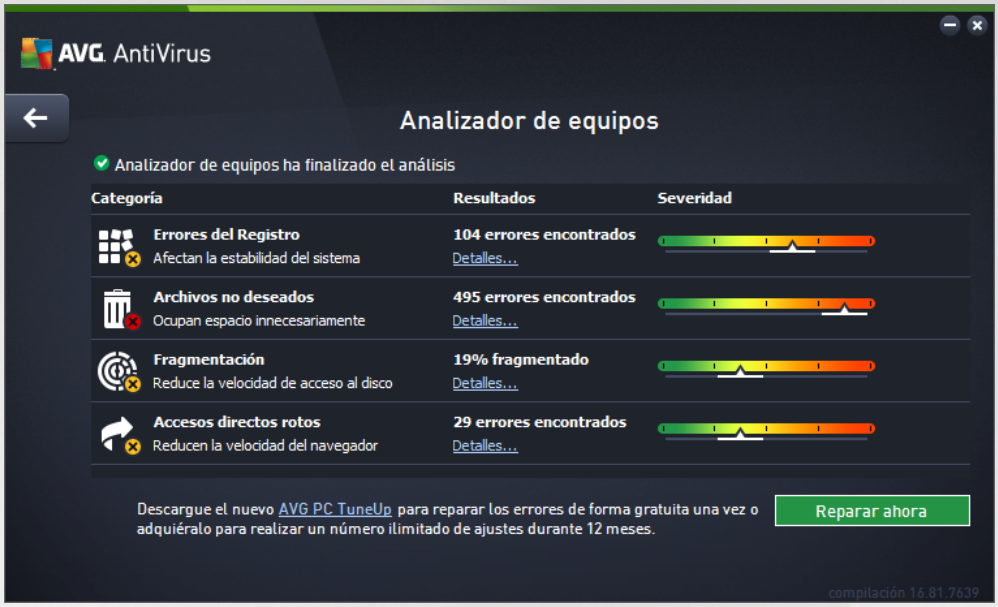
Habilitado / Deshabilitado: el botón recuerda a un semáforo, tanto en apariencia como en funcionalidad. Haga clic para cambiar entre las dos posiciones. El color verde pertenece a ***Habilitado***, lo cual significa que el servicio de seguridad está activo y funciona correctamente. El color rojo representa el estado ***Deshabilitado***, es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, le recomendamos encarecidamente que mantenga la configuración predeterminada de seguridad. La configuración predeterminada garantiza el funcionamiento óptimo de la aplicación y el nivel máximo de seguridad. Si, por alguna razón, desea desactivar el servicio, se le advertirá sobre el posible riesgo a través de una señal roja de ***Advertencia*** y la información de que no está completamente protegido. ***Tenga en cuenta que debe activar de nuevo el servicio lo antes posible.***

Configuración: haga clic en el botón para que se le redirija a la interfaz de Configuración avanzada. Precisamente, el cuadro de diálogo correspondiente se abre y podrá configurar el servicio seleccionado, es decir, Analizador de correo electrónico o Anti-Spam. En la interfaz de configuración avanzada puede editar todos los ajustes de cada servicio de seguridad de **AVG AntiVirus,** pero tenga en cuenta que esta configuración solo está recomendada para usuarios experimentados.

Flecha: use la flecha verde de la sección superior izquierda del cuadro de diálogo para volver a la interfaz de usuario principal, en la que se muestra la información general de los componentes.

6.5. Analizador de PC

El componente ***Analizador de equipos*** es una herramienta avanzada para el análisis detallado y la corrección que intenta mejorar la velocidad y el rendimiento general del equipo. Se abre pulsando el botón ***Reparar rendimiento***, situado en el cuadro de diálogo de la interfaz de usuario principal, o mediante la misma opción que aparece en el menú de contexto del icono de AVG de la bandeja del sistema. A continuación, podrá observar el avance del análisis y sus resultados directamente en el gráfico:



Se pueden analizar las siguientes categorías: errores del Registro, archivos no deseados, fragmentación y accesos directos rotos:

- ***Errores del Registro*** ofrece el número de errores en el Registro de Windows que podrían estar ralentizando el equipo o hacer que se muestren mensajes de error.
- ***Archivos no deseados*** ofrece el número de archivos que ocupan espacio en el disco y que lo más probable es que no sean necesarios. Por lo general, se trata de distintos tipos de archivos temporales y archivos que se encuentran en la Papelera de reciclaje.
- ***Fragmentación*** calculará el porcentaje del disco duro que se encuentra fragmentado; es decir, que ha estado en uso por mucho tiempo y en el que, por ello, la mayoría de los archivos se encuentran dispersos por diferentes partes.
- ***Accesos directos rotos*** detecta accesos directos que ya no funcionan, llevan a ubicaciones no existentes, etc.

La información general de los resultados muestra la cantidad de problemas del sistema detectados, clasificados según las diferentes categorías analizadas. Los resultados del análisis también se presentarán gráficamente sobre un eje en la columna ***Gravedad***.

Botones de control

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

inmediatamente el análisis del equipo.

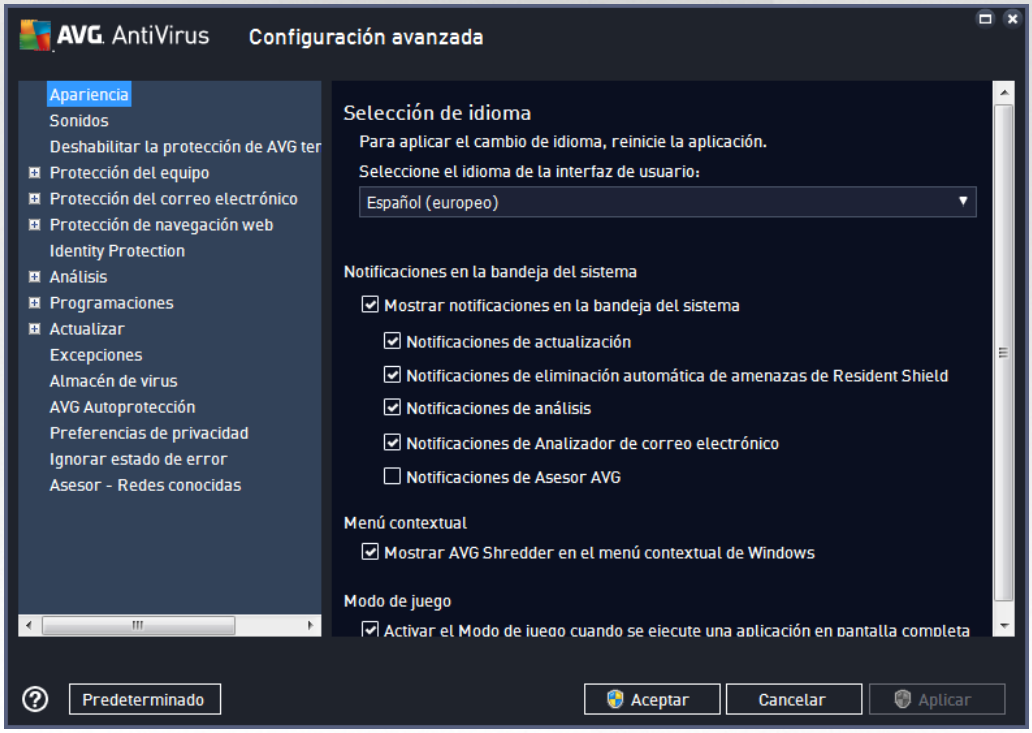
- ***Reparar ahora*** *(se muestra una vez que ha finalizado el análisis*): lamentablemente, la funcionalidad del Analizador de equipos en **AVG AntiVirus** se limita al análisis de estado actual de su equipo. Sin embargo, AVG proporciona una herramienta avanzada para el análisis detallado y la corrección que intenta mejorar la velocidad y el rendimiento general del equipo. Haga clic en el botón para que se le redirija al sitio web dedicado para obtener más información.

7. Configuración avanzada de AVG

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

7.1. Apariencia

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



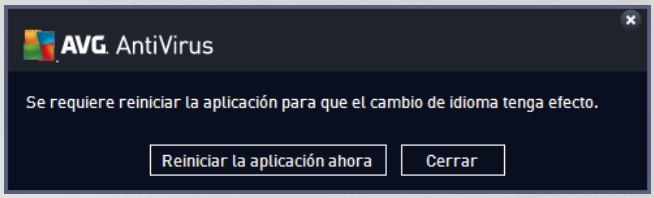
Selección de idioma

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

- En el menú desplegable, seleccione el idioma deseado de la aplicación
- Confirme su selección pulsando el botón ***Aplicar*** *(esquina inferior derecha del cuadro de diálogo)*
- Pulse el botón ***Aceptar*** para confirmar

- Aparece un nuevo cuadro de diálogo que le informa de que debe reiniciar **AVG AntiVirus para poder cambiar el idioma**

- Pulse el botón ***Reiniciar AVG ahora*** para confirmar el reinicio del programa y espere un segundo hasta que el cambio de idioma tenga efecto:



Notificaciones de la bandeja del sistema

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

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

- ***Mostrar notificaciones en la bandeja del sistema*** *(activado de manera predeterminada)*: se muestran todas las notificaciones por defecto. Desactive este elemento para deshabilitar completamente la visualización de todas las notificaciones. Cuando está activo, puede seleccionar las notificaciones específicas que deben mostrarse:

  - ***Notificaciones de actualización*** *(activada de manera predeterminada)*: decida si se debe mostrar la información relacionada con el inicio, progreso y finalización del proceso de actualización de **AVG AntiVirus**.

  - ***Notificaciones de eliminación automática de amenazas de Resident Shield*** *(activadas de manera predeterminada)*: decida si la información relacionada con los procesos de guardado, copia y apertura de archivos se debe mostrar o suprimir (*esta configuración solo se muestra si la opción de reparación automática de Resident Shield está activada*).

  - ***Notificaciones de análisis*** *(activada de manera predeterminada)*: decida si se debe mostrar información cuando se inicie automáticamente un análisis programado, su progreso y los resultados.

  - ***Notificaciones de Analizador de correo electrónico*** *(activada de manera predeterminada)*: decida si se debe mostrar información tras el análisis de todos los mensajes de correo electrónico entrantes y salientes.

  - ***Notificaciones estadísticas*** *(activada de manera predeterminada)*: mantenga la opción marcada para permitir que la notificación periódica de revisión estadística se muestre en la bandeja del sistema.

  - ***Notificaciones de Asesor AVG*** *(activada de manera predeterminada):* decida si desea que se

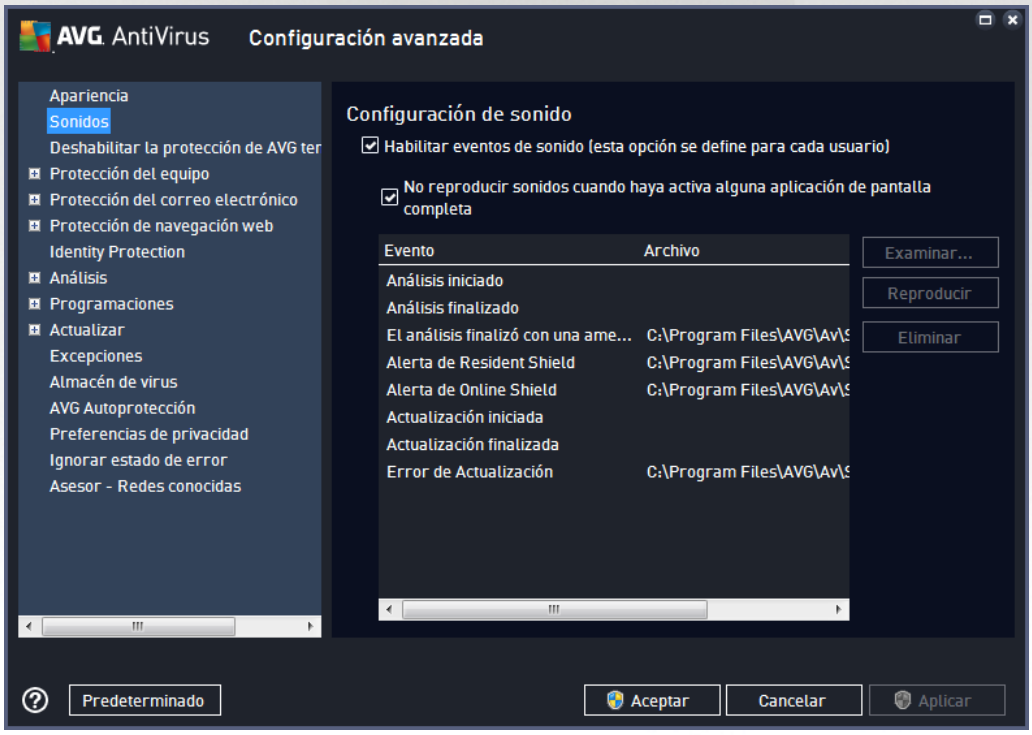
muestre información acerca de las actividades de Asesor AVG en el panel desplegable de la bandeja del sistema.

Modo de juego

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

7.2. Sonidos

En el cuadro de diálogo ***Configuración de sonido*** puede especificar si desea recibir información sobre acciones específicas de **AVG AntiVirus** mediante una notificación sonora:



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

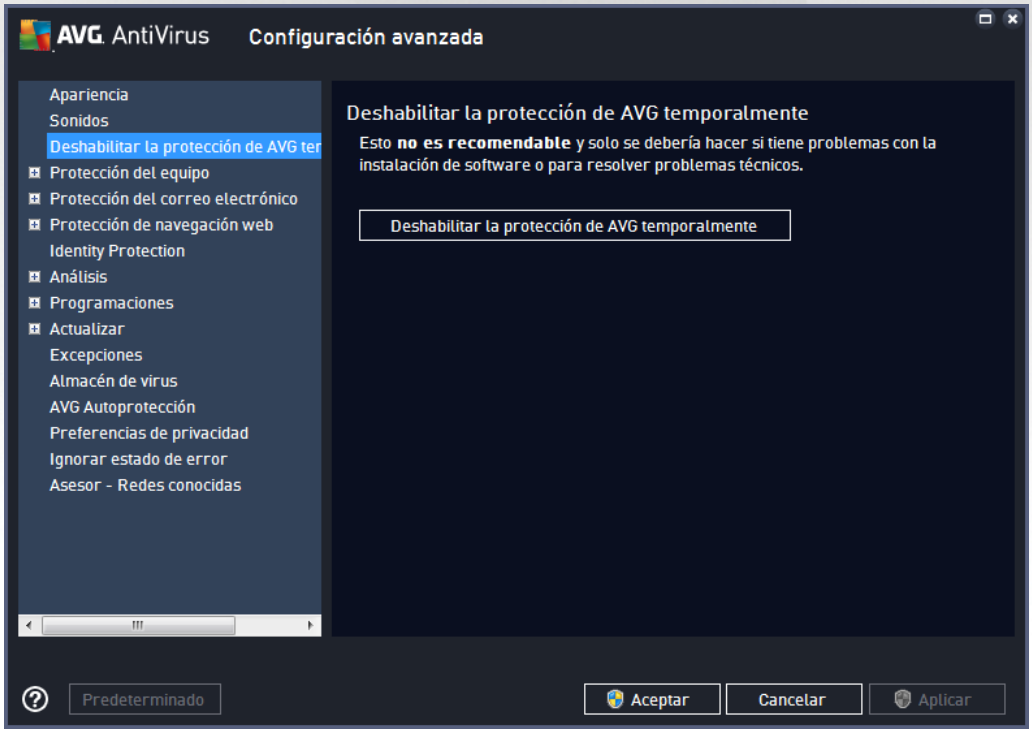
Botones de control

- ***Examinar...***: tras seleccionar el evento correspondiente de la lista, utilice el botón ***Examinar*** para buscar en el disco duro el archivo de sonido que desea asignarle. *(Tenga en cuenta que solo se admiten archivos de sonido *.wav en este momento)*
- ***Reproducir***: para escuchar el sonido seleccionado, resalte el elemento de la lista y pulse el botón ***Reproducir***.
- ***Eliminar***: utilice el botón ***Eliminar*** para quitar el sonido asignado a un evento específico.

7.3. Deshabilitar la protección de AVG temporalmente

En el cuadro de diálogo ***Deshabilitar la protección de AVG temporalmente*** tiene la opción de deshabilitar toda la protección otorgada por **AVG AntiVirus** a la vez.

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



En la mayoría de los casos, no ***será necesario*** deshabilitar **AVG AntiVirus** antes de instalar un nuevo software o nuevos controladores, ni siquiera cuando el instalador o asistente del software sugiera cerrar primero los programas y aplicaciones que estén en ejecución para garantizar que no haya interrupciones indeseadas durante el proceso de instalación. Si sufre problemas durante la instalación, pruebe a desactivar la protección residente *(en el cuadro de diálogo enlazado, desmarque el elemento **Permitir Resident Shield**)* primero. Si tiene que deshabilitar temporalmente **AVG AntiVirus** para hacer algo, vuelva a habilitarlo tan pronto como termine. Si está conectado a Internet o a una red cuando el software antivirus se encuentra desactivado, el equipo está expuesto a sufrir ataques.

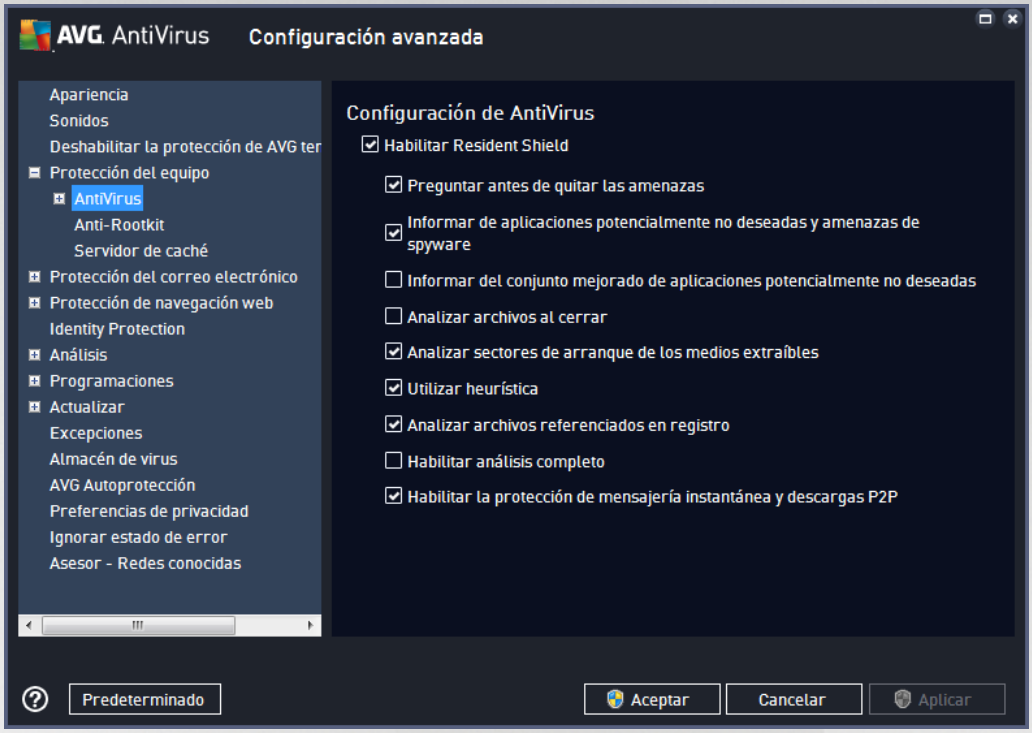
Cómo desactivar la protección de AVG

Marque la casilla de verificación ***Deshabilitar la protección de AVG temporalmente*** y confirme su elección con el botón ***Aplicar***. En el cuadro de diálogo recién abierto ***Deshabilitar protección de AVG temporalmente***, especifique durante cuánto tiempo desea deshabilitar **AVG AntiVirus**. De manera predeterminada, la protección se desactivará durante 10 minutos, que deberían ser suficientes para cualquier tarea normal como instalar software nuevo, etc. Puede elegir un período de tiempo superior; sin embargo, está opción no se recomienda si no es absolutamente necesario. A continuación, todos los componentes desactivados se activarán de nuevo automáticamente. Como mucho, puede deshabilitar la protección de AVG hasta el siguiente reinicio del equipo.

7.4. Protección del equipo

7.4.1. AntiVirus

AntiVirus junto con ***Resident Shield*** protege su equipo de forma continua de todos los tipos de virus conocidos, spyware y software malicioso en general *(incluidos los llamados programas maliciosos no activos y durmientes, es decir, los que se han descargado pero aún no se han activado)*.



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

- ***Preguntar antes de quitar las amenazas*** (*activada de forma predeterminada*): seleccione esta opción para garantizar que Resident Shield no lleve a cabo ninguna acción automáticamente, sino que, en su lugar, se abra un cuadro de diálogo en el que se describe la amenaza detectada y se permite decidir lo que hacer. Si deja la casilla desactivada, **AVG AntiVirus** eliminará la infección automáticamente. En caso contrario, el objeto se moverá al Almacén de virus.

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

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

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

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

marque esta opción para analizar los sectores de arranque de las unidades flash USB, unidades de disco externas y otros medios extraíbles en busca de amenazas.

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

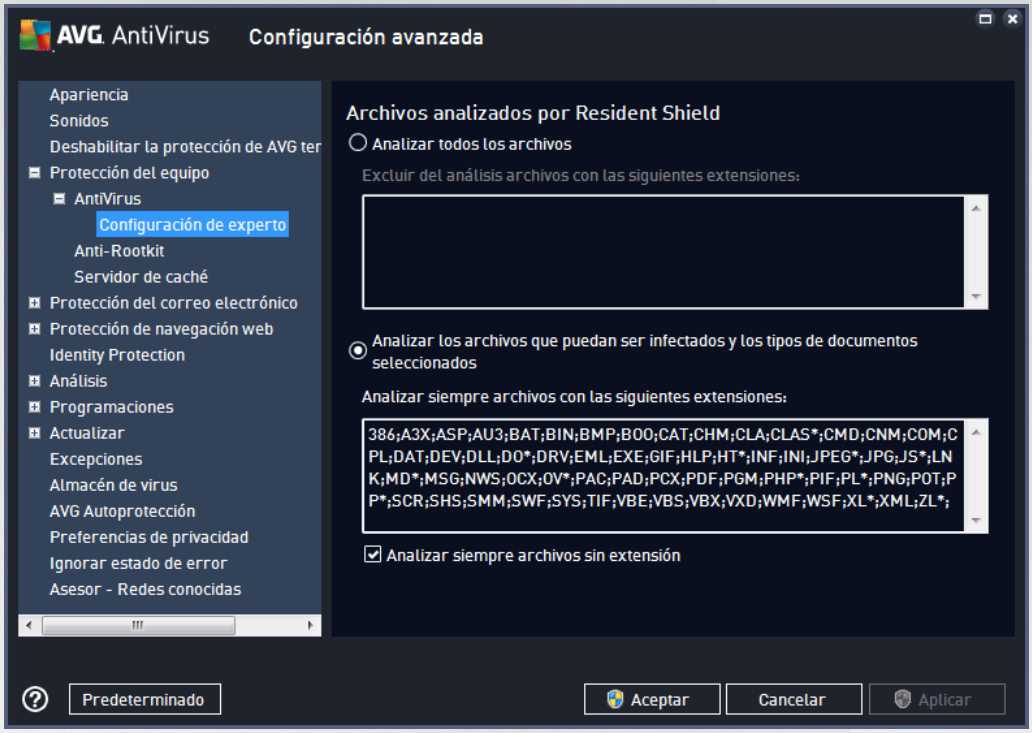
- ***Analizar archivos referenciados en registro*** (*activada de manera predeterminada*): este parámetro define que AVG analizará todos los archivos ejecutables añadidos al registro de inicio para evitar que una infección conocida se ejecute en el siguiente inicio del equipo.

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

- ***Habilitar la protección de mensajería instantánea y descargas P2P*** (*activada de manera predeterminada*): marque este elemento si desea verificar que la comunicación de mensajería instantánea (*por ejemplo, AIM, Yahoo!, ICQ, Skype, MSN Messenger, etc.*) y los datos descargados de redes punto a punto *(redes que permiten la conexión directa entre clientes, sin un servidor, que suponen un peligro potencial; usadas normalmente para compartir archivos de música)* no contienen virus.

Nota: *Si AVG está instalado en Windows 10, aparecerá un elemento llamado* ***Habilitar la Antimalware Scan Interface (AMSI) de Windows*** *en la lista. Esta característica mejora la protección antivirus, pues habilita la cooperación entre Windows y AVG para detectar código malicioso. Esto hace que la protección sea más confiable y reduce el número de falsos positivos.*

En el cuadro de diálogo ***Archivos analizados por Resident Shield*** se pueden configurar los archivos que serán analizados (*por extensiones específicas*):

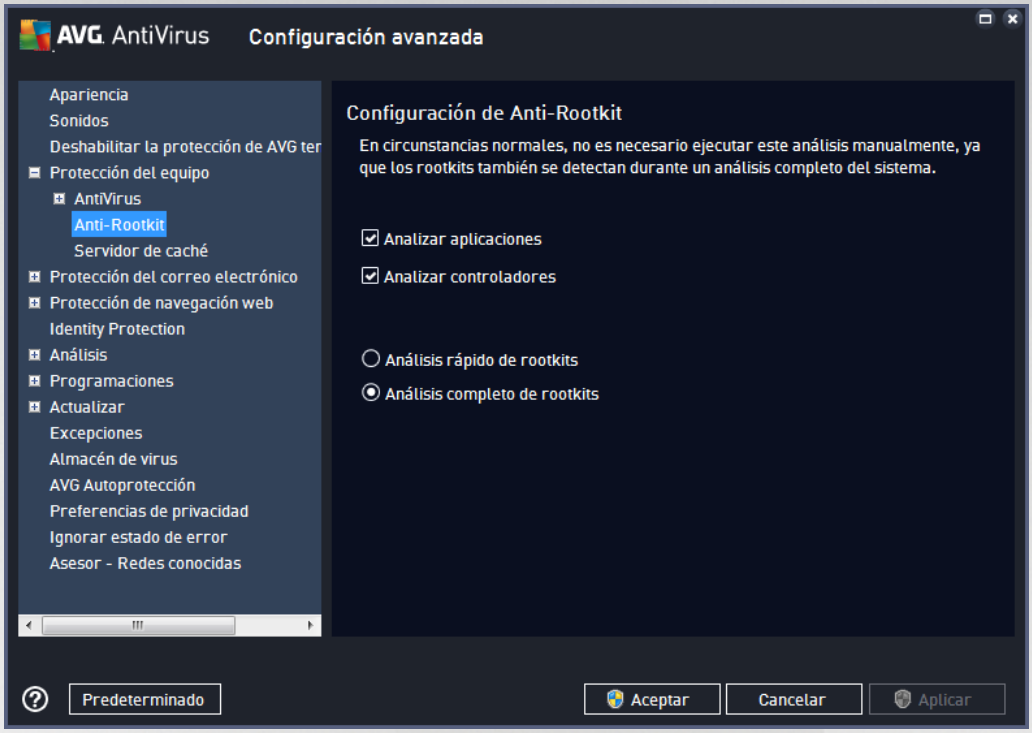


Marque la casilla de verificación respectiva para decidir si desea ***Analizar todos los archivos*** o ***Analizar los archivos que puedan ser infectados y los tipos de documentos seleccionados*** solamente. Para aumentar la velocidad de análisis y proporcionar el máximo nivel de protección al mismo tiempo, le recomendamos que mantenga la configuración predeterminada. De esta forma solo se analizarán los archivos que puedan estar infectados. En la sección correspondiente del cuadro de diálogo también puede encontrar una lista editable de extensiones de archivos que se incluyen en el análisis.

Seleccione la opción ***Analizar siempre archivos sin extensión*** (*activada de forma predeterminada*) para asegurarse de que Resident Shield analiza incluso los archivos sin extensión o con formato desconocido. Le recomendamos que mantenga esta característica activada, dado que los archivos sin extensión son sospechosos.

7.4.2. Anti-Rootkit

En el cuadro de diálogo ***Configuración de Anti-Rootkit*** se puede editar la configuración del servicio ***Anti-Rootkit***, así como parámetros concretos del análisis anti-rootkit. El análisis anti-rootkit consiste en un proceso predeterminado incluido en el análisis completo del equipo:

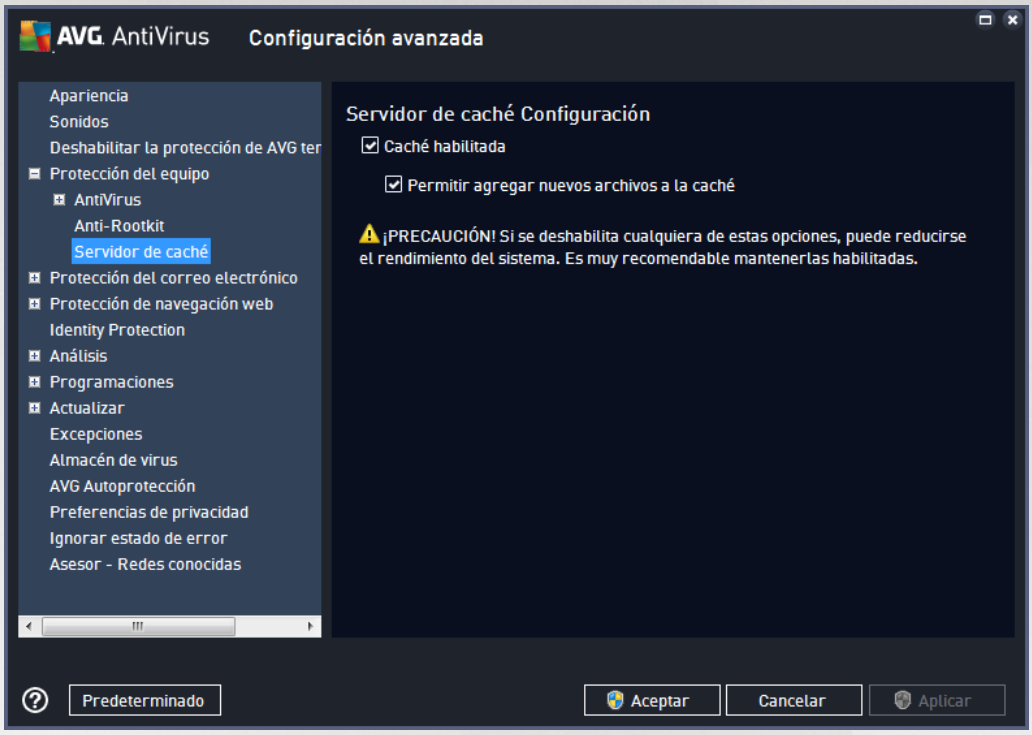


Analizar aplicaciones y ***Analizar controladores*** permiten especificar en detalle lo que debería incluir el análisis anti-rootkit. Estos ajustes están dirigidos a usuarios avanzados. Se recomienda mantener todas las opciones activadas. Además, puede seleccionar el modo de análisis de rootkits:

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

7.4.3. Servidor de caché

El cuadro de diálogo ***Servidor de caché*** hace referencia al proceso del servidor de caché destinado a agilizar todos los tipos de análisis de **AVG AntiVirus**:



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

El cuadro de diálogo ***Servidor de caché*** ofrece las siguientes opciones de configuración:

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

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

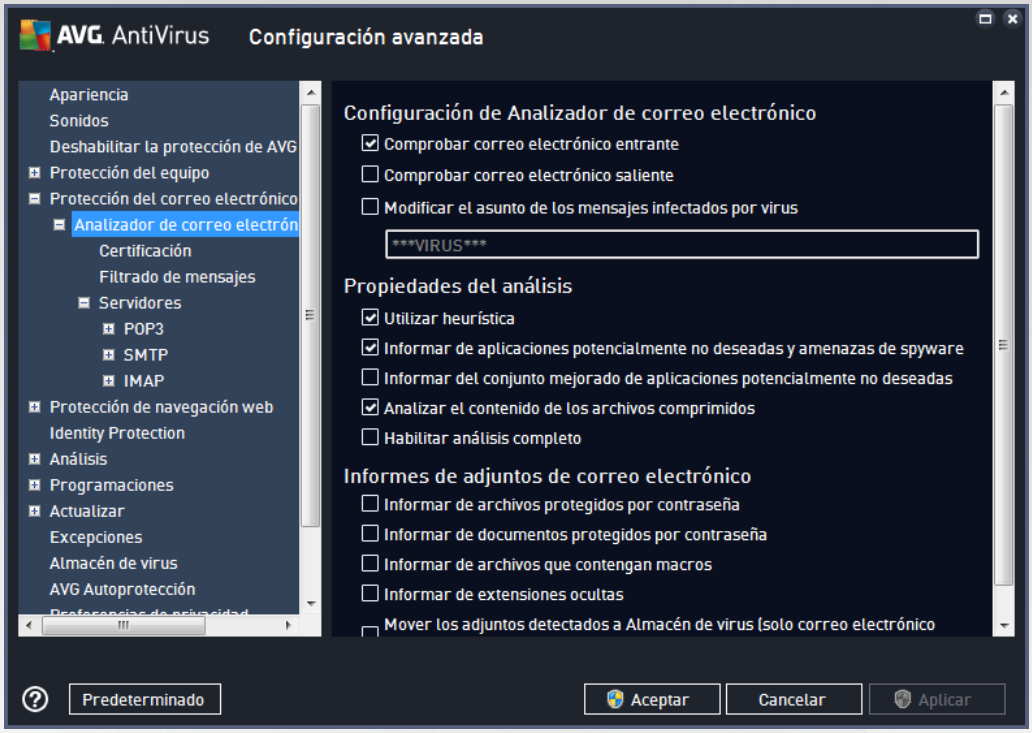
A no ser que tenga un buen motivo para desactivar el servidor de caché, recomendamos que mantenga la configuración predeterminada y deje la opción activada. De lo contrario, es posible que sufra una reducción importante de la velocidad y el rendimiento del sistema.

7.5. Analizador de correo electrónico

En esta sección puede editar la configuración detallada de Analizador de correo electrónico y Anti-Spam:

7.5.1. Analizador de correo electrónico

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



Análisis del correo electrónico

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

- ***Comprobar correo electrónico entrante*** (*activada de manera predeterminada*): marque esta opción para activar o desactivar el análisis de todos los mensajes entregados en su cliente de correo electrónico
- ***Comprobar correo electrónico saliente*** (*desactivada de manera predeterminada*): marque esta opción para activar o desactivar el análisis de todos los mensajes de correo electrónico enviados desde su cuenta
- ***Modificar el asunto de los mensajes infectados por virus*** (*desactivada de manera predeterminada*): si desea recibir avisos al detectar mensajes de correo electrónico infectados, marque esta opción e introduzca el texto que desee en el campo de texto. Este texto se añadirá al campo "Asunto" de cada mensaje de correo electrónico infectado para que resulte más fácil identificarlo y filtrarlo. El valor predeterminado es ***VIRUS***, el cual recomendamos mantener.

Propiedades del análisis

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

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

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

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

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

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

Informes de adjuntos de correo electrónico

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

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

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

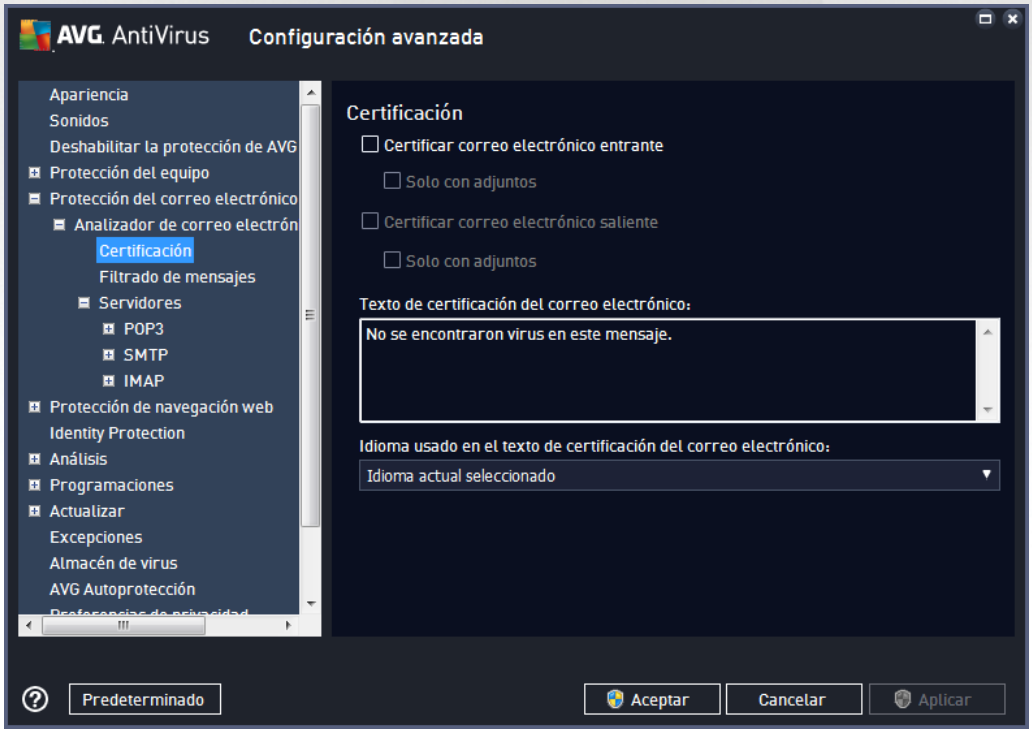
- ***Informar de archivos que contengan macros***: una macro es una secuencia predefinida de pasos que tiene como objetivo facilitar ciertas tareas al usuario (*las macros de MS Word son muy*

conocidas). Dada su naturaleza, una macro puede contener instrucciones posiblemente peligrosas, y quizás necesite marcar esta casilla de verificación para asegurarse de que el programa informe de los archivos con macros como sospechosos.

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

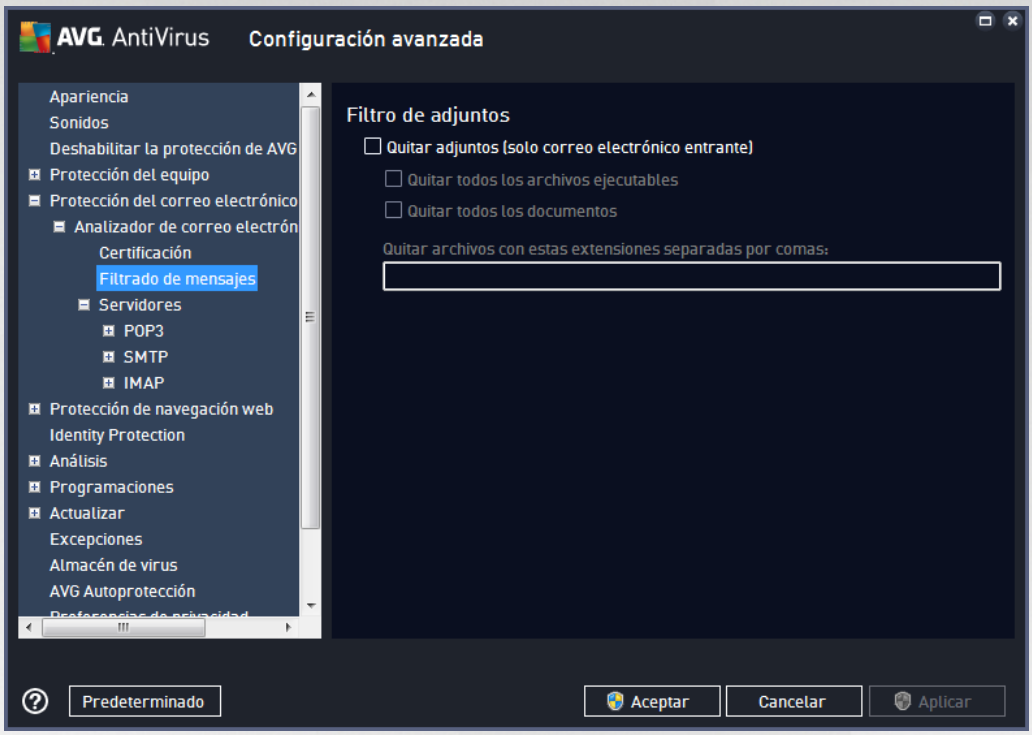
- ***Mover los adjuntos detectados a Almacén de virus***: indique si desea recibir notificaciones por correo electrónico sobre archivos comprimidos protegidos por contraseña, documentos protegidos por contraseña, archivos que contengan macros o archivos con extensiones ocultas detectados como datos adjuntos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

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



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

Nota: *Tenga en cuenta que solo el texto predeterminado se mostrará en el idioma establecido y que su texto personalizado no se traducirá automáticamente*



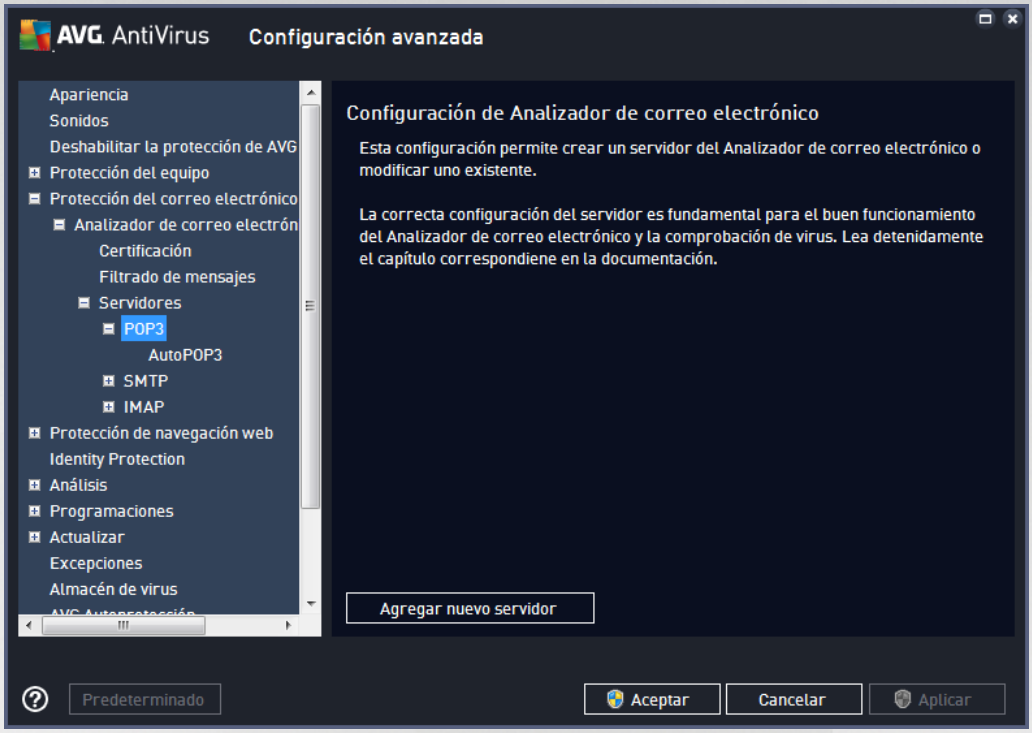
En el cuadro de diálogo ***Filtro de adjuntos***, puede configurar parámetros que se utilizarán para analizar los adjuntos al mensaje de correo electrónico. De manera predeterminada, la opción ***Quitar adjuntos*** se encuentra desactivada. Si decide activarla, todos los adjuntos a los mensajes de correo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

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

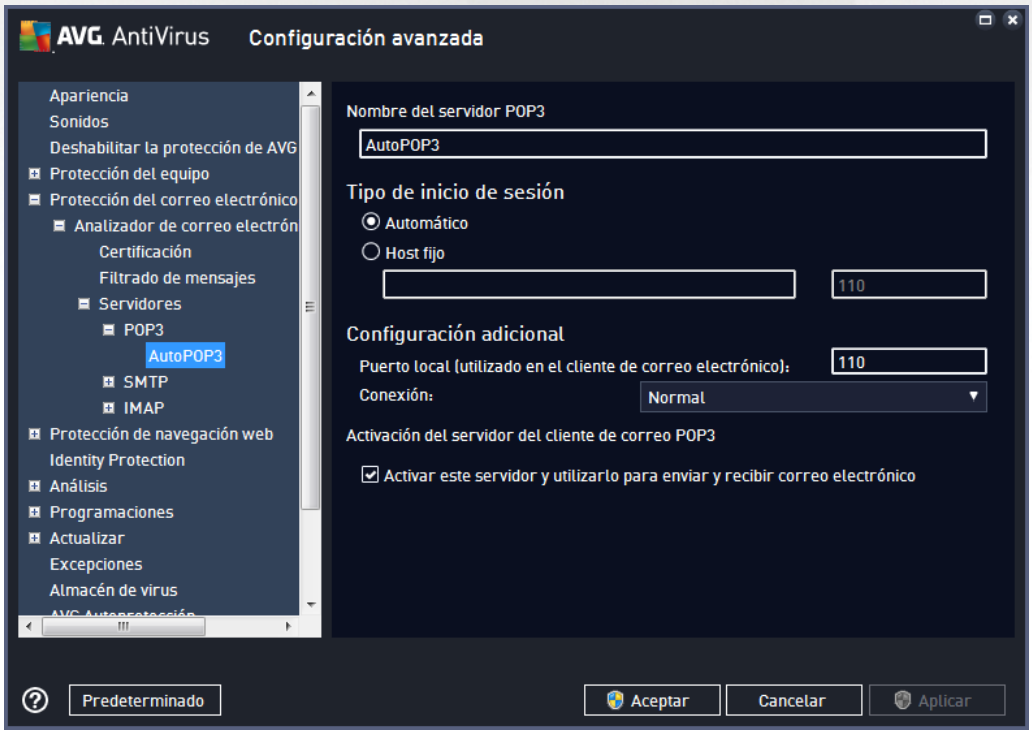
En la sección ***Servidores*** puede editar los parámetros de los servidores del Analizador de correo electrónico:

- Servidor POP3
- Servidor SMTP
- Servidor IMAP

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



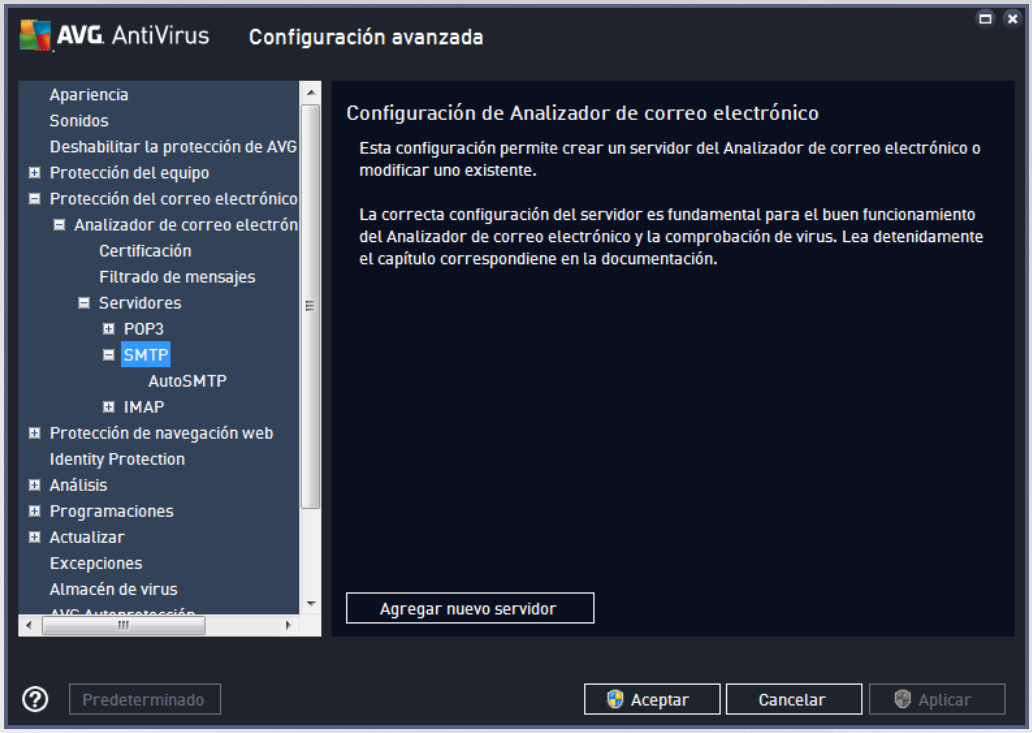
En este cuadro de diálogo puede configurar un nuevo servidor para el Analizador de correo electrónico mediante el protocolo POP3 para el correo electrónico entrante:



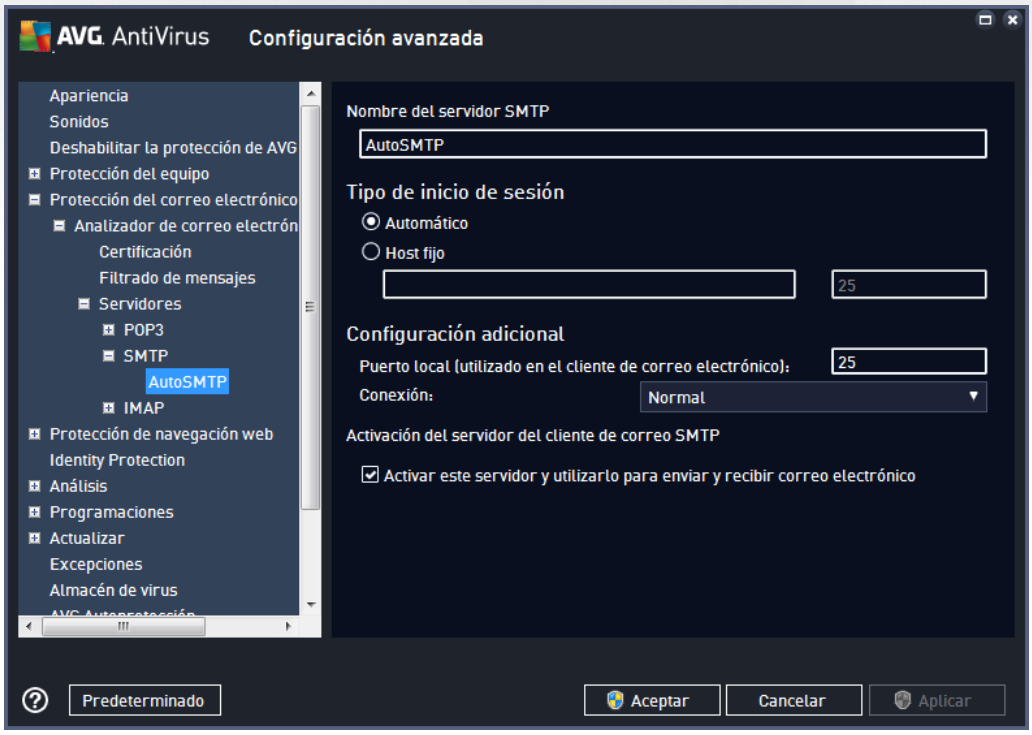
- ***Nombre de servidor POP3***: en este campo, puede especificar el nombre de servidores

recientemente añadidos (*para añadir un servidor POP3, haga clic con el botón secundario del ratón sobre el elemento POP3 del menú de navegación izquierdo*).

- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo que se usará para el correo electrónico entrante:
    - ***Automático***: el inicio de sesión se efectuará automáticamente en función de la configuración del cliente de correo electrónico.
    - ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. El nombre empleado para iniciar sesión permanece igual. Por ejemplo, puede usar un nombre de dominio (*como pop.acme.com*) o una dirección IP (*como 123.45.67.89*). Si el servidor de correo electrónico emplea un puerto no estándar, puede especificar este puerto después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, pop.acme.com:8200*). El puerto estándar para las comunicaciones POP3 es el 110.
- ***Configuración adicional***: permite especificar parámetros más detallados:
    - ***Puerto local***: especifica el puerto en que debería esperarse la comunicación de la aplicación de correo electrónico. Luego, debe indicar en la aplicación de correo electrónico este puerto como el puerto para la comunicación POP3.
    - ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos se envían cifrados sin riesgo de que otra persona pueda rastrearlos o supervisarlos. Esta característica también está disponible únicamente si el servidor de correo electrónico de destino la admite.
- ***Activación del servidor POP3 del cliente de correo***: marque o deje en blanco este elemento para activar o desactivar el servidor POP3 especificado



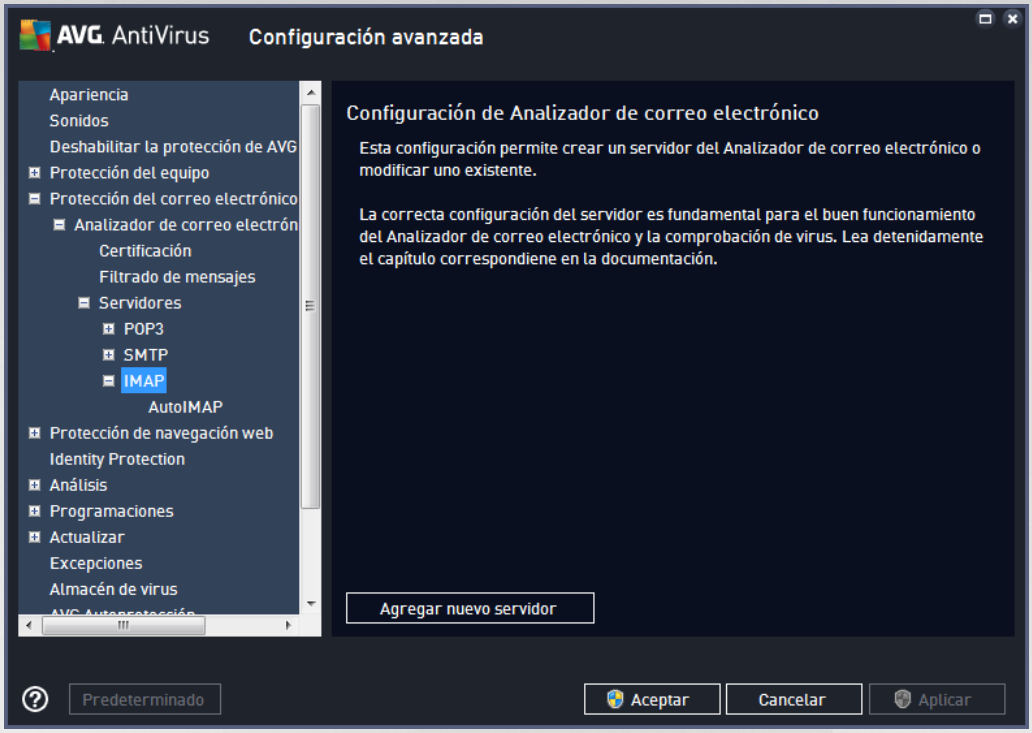
En este cuadro de diálogo puede configurar un nuevo servidor de Analizador de correo electrónico mediante el protocolo SMTP para el correo electrónico saliente:



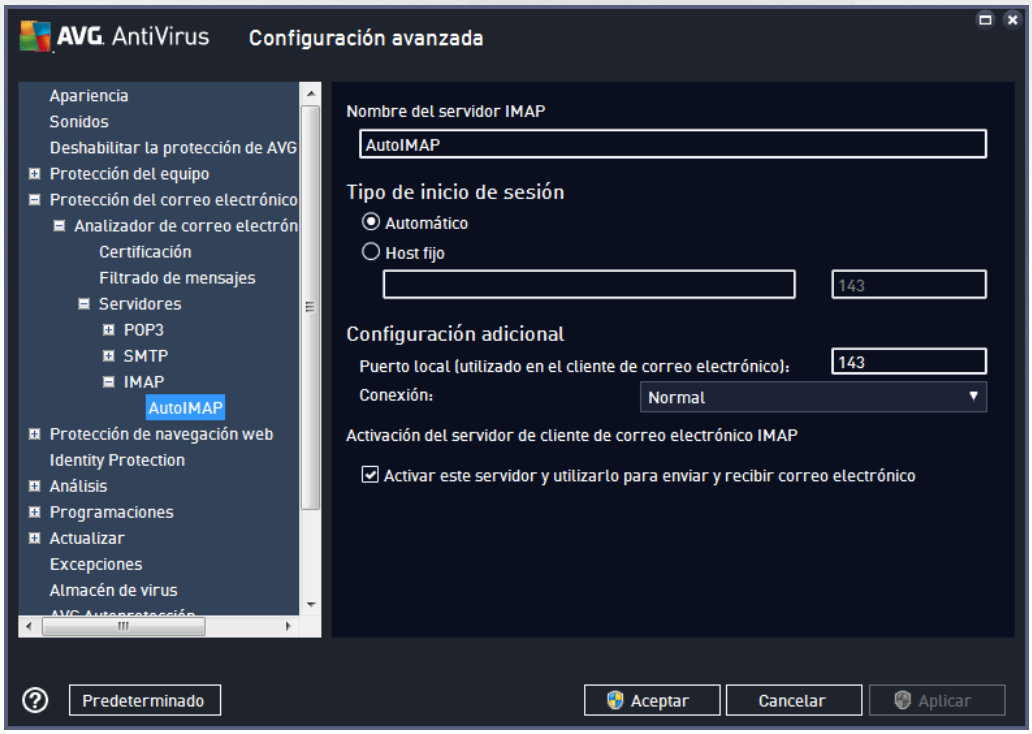
- ***Nombre de servidor SMTP***: en este campo, puede especificar el nombre de los servidores

agregados recientemente (*para añadir un servidor SMTP, haga clic con el botón secundario del ratón en el elemento SMTP del menú de navegación de la izquierda*). Para los servidores "AutoSMTP" creados automáticamente, este campo se encuentra desactivado.

- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo que se usará para el correo electrónico saliente:
    - o ***Automático***: el inicio de sesión se efectuará automáticamente en función de la configuración del cliente de correo electrónico
    - o ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. Como nombre puede usar un nombre de dominio (*por ejemplo, smtp.acme.com*) o una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo electrónico emplea un puerto no estándar, puede especificar este puerto después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, smtp.acme.com:8200*). El puerto estándar para la comunicación SMTP es el 25.
- ***Configuración adicional***: permite especificar parámetros más detallados:
    - o ***Puerto local***: especifica el puerto en que debería esperarse la comunicación de la aplicación de correo electrónico. A continuación, debe establecer este puerto como puerto para la comunicación SMTP en la aplicación de correo.
    - o ***Conexión***: en este menú desplegable, puede especificar el tipo de conexión a utilizar (*normal/ SSL/SSL predeterminado*). Si elige una conexión SSL, los datos se envían cifrados sin riesgo de que otra persona pueda rastrearlos o supervisarlos. Esta característica solo está disponible si el servidor de correo de destino la admite.
- ***Activación del servidor SMTP de cliente de correo electrónico***: marque o deje en blanco esta casilla para activar o desactivar el servidor SMTP indicado anteriormente



En este cuadro de diálogo puede configurar un nuevo servidor de Analizador de correo electrónico mediante el protocolo IMAP para el corriente saliente:



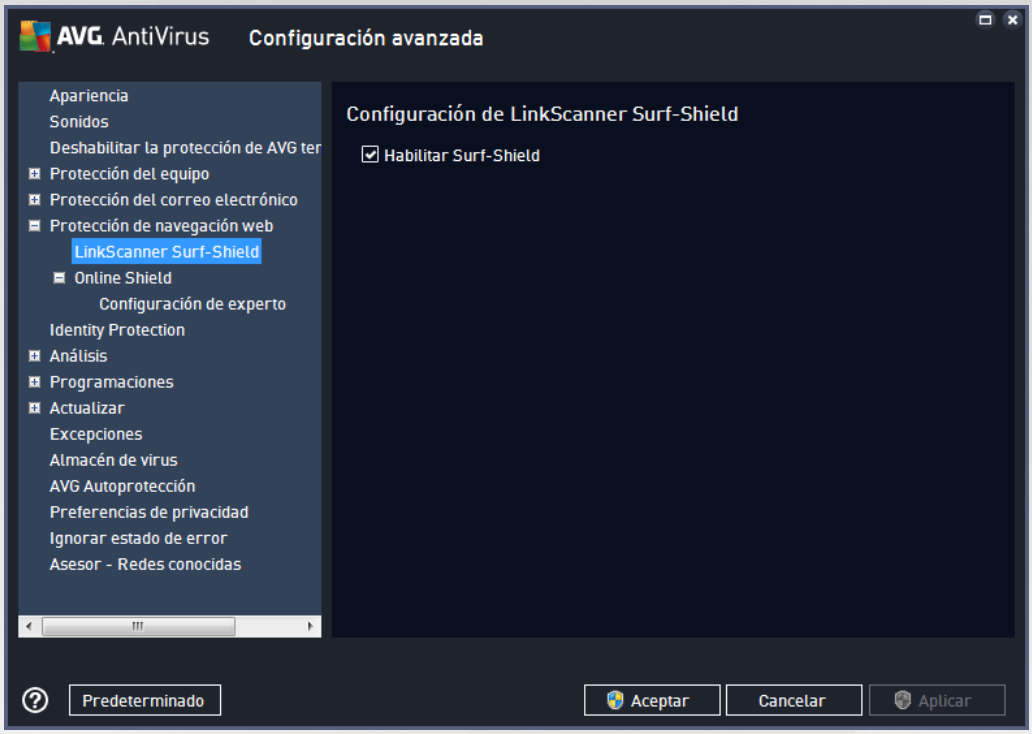
- ***Nombre de servidor IMAP***: en este campo, puede especificar el nombre de los servidores agregados

recientemente (*para añadir un servidor IMAP, haga clic con el botón secundario del ratón 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 que se usará para el correo electrónico saliente:
    - o ***Automático***: el inicio de sesión se efectuará automáticamente en función de la configuración del cliente de correo electrónico
    - o ***Host fijo***: en este caso, el programa siempre utilizará el servidor indicado aquí. Especifique la dirección o el nombre del servidor de correo. Como nombre puede usar un nombre de dominio (*por ejemplo, smtp.acme.com*) o una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo electrónico emplea un puerto no estándar, puede especificar este puerto después del nombre del servidor con el símbolo dos puntos a modo de delimitador (*por ejemplo, imap.acme.com:8200*). El puerto estándar para la comunicación IMAP es el 143.
- ***Configuración adicional***: permite especificar parámetros más detallados:
    - o ***Puerto local utilizado en***: especifica el puerto en que debería esperarse la comunicación de la aplicación de correo electrónico. A continuación, debe establecer este puerto como puerto para la comunicación IMAP en la aplicación de correo.
    - o ***Conexión***: en este menú desplegable, puede especificar el tipo de conexión a utilizar (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos se envían cifrados sin riesgo de que otra persona pueda rastrearlos o supervisarlos. Esta característica solo está disponible si el servidor de correo de destino la admite.
- ***Activación del servidor IMAP de cliente de correo electrónico***: marque o deje en blanco esta casilla para activar o desactivar el servidor IMAP indicado anteriormente

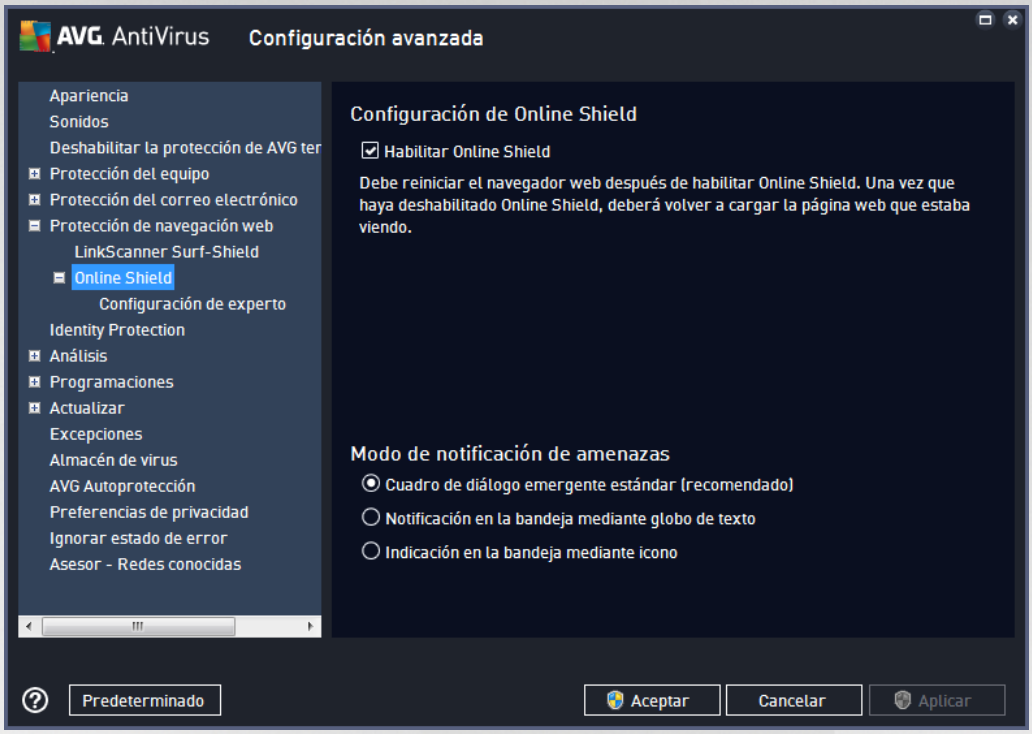
7.6. Protección de la navegación web

El cuadro de diálogo ***Configuración de LinkScanner*** le permite marcar o quitar la marca de las siguientes características:



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

7.6.1. Online Shield

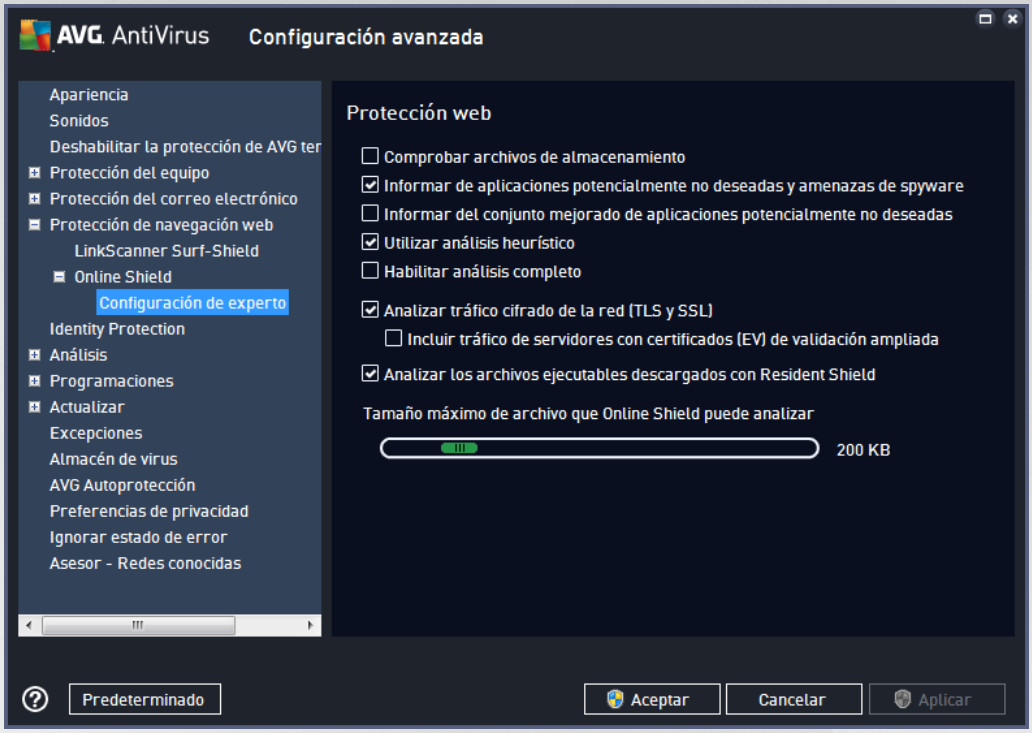


El cuadro de diálogo ***Online Shield*** ofrece las siguientes opciones:

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

Modo de notificación de amenazas

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



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

- ***Comprobar archivos de almacenamiento*** - (*desactivada de forma predeterminada*): al marcar esta opción se analiza el contenido de los archivos que posiblemente se incluyan en las páginas web que se muestren.
- ***Informar de programas potencialmente no deseados y amenazas de spyware*** - (*activada de manera predeterminada*): marque esta opción para activar el análisis en busca de spyware y virus. El spyware representa una categoría dudosa de software malicioso: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos que mantenga activada esta característica ya que aumenta la seguridad del equipo.
- ***Informar de conjunto mejorado de aplicaciones potencialmente no deseadas***: (*desactivado de manera predeterminada*): Marque para detectar paquetes extendidos de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.
- ***Utilizar heurística*** - (*activada de manera predeterminada*): se escanea el contenido de la página a mostrar mediante el método de análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).
- ***Habilitar análisis completo*** (*desactivada de manera predeterminada*): en determinadas

situaciones (*si sospecha que su equipo está infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados, que analizarán incluso las áreas del equipo que rara vez se infectan, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.

- ***Analizar tráfico de red cifrado (TLS y SSL)***: (*activado de manera predeterminada*): deje activada esta opción para permitir que AVG cifre 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 los sitios web que usan HTTPS y a las conexiones de cliente de correo electrónico que emplean TLS/SSL. El tráfico protegido se descifra, se analiza en busca de malware y se vuelve a cifrar para entregarse de forma segura en el equipo. Dentro de esta opción, puede elegir ***Incluir tráfico de servidores con certificados de validación ampliada (EV)*** y analizar también la comunicación de red cifrada procedente de servidores que cuentan con un certificado EV. La emisión de un certificado EV exige una validación extensiva por parte de la entidad emisora de certificados. Por lo tanto, los sitios web que funcionan con el certificado son de mayor confianza *(menor probabilidad de que distribuyan malware)*. Por este motivo, puede optar por no analizar el tráfico de servidores certificados EV, lo que aceleraría moderadamente la comunicación cifrada.

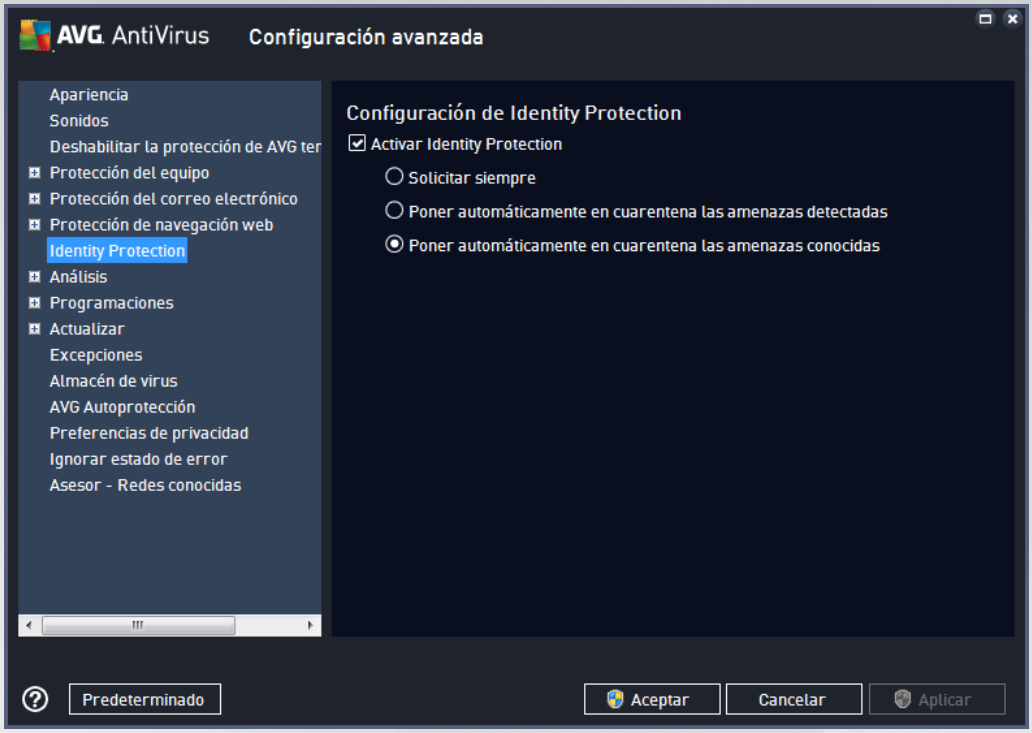
- ***Analizar archivos ejecutables descargados con Resident Shield*** - (*activada de manera predeterminada*): se analizan los archivos ejecutables *(normalmente archivos con las extensiones exe, bat, com)* una vez que han sido descargados. Resident Shield analiza los archivos antes de la descarga para garantizar que ningún archivo malicioso acceda a su equipo. Sin embargo, este análisis está limitado por la opción ***Tamaño parcial máximo de un archivo a analizar***, que se muestra a continuación en el mismo cuadro de diálogo. Por lo tanto, los archivos grandes se analizan por partes, incluidos la mayoría de los archivos ejecutables. Los archivos ejecutables pueden realizar diferentes tareas en su equipo, por lo que es crucial que sean completamente seguros. Para garantizar esto, se puede analizar el archivo por partes tanto antes de descargarlo como una vez finalizada la descarga. Le recomendamos que active esta opción. Aunque la desactive, puede tener la tranquilidad de que AVG detectará cualquier código potencialmente peligroso. No obstante, es posible que no pueda evaluar un archivo ejecutable como una unidad, por lo que puede detectar algunos falsos positivos.

Mediante el control deslizante de la parte inferior del cuadro de diálogo, puede definir el ***Tamaño parcial máximo de un archivo a analizar***: si la página mostrada incluye archivos, también es posible analizar su contenido incluso antes de que se descarguen en el equipo. Sin embargo, el análisis de archivos grandes lleva bastante tiempo y se puede ralentizar la descarga de la página web de forma significativa. Mediante el control deslizante se puede especificar el tamaño máximo de un archivo que se vaya a analizar con ***Online Shield***. Incluso si el archivo descargado es mayor de lo especificado y, por tanto, no se analizará con Online Shield, seguirá estando protegido: si el archivo está infectado, ***Resident Shield*** lo detectará inmediatamente.

7.7. Identity Protection

Identity Protection es un componente anti-malware que le protege frente a todo tipo de software malicioso (*spyware, robots, robo de identidad, etc.*) utilizando tecnologías de comportamiento y ofreciendo protección ante los ataques de día cero de virus nuevos *(para obtener una descripción detallada de la funcionalidad de este componente, consulte el capítulo Identidad)*.

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



Activar Identity Protection (*activada de forma predeterminada*): deje en blanco esta opción para desactivar el componente Identidad. ***Recomendamos encarecidamente no hacerlo a menos que sea necesario.*** Cuando Identity Protection está activo, puede especificar lo que desea hacer al detectarse una amenaza:

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

7.8. Análisis

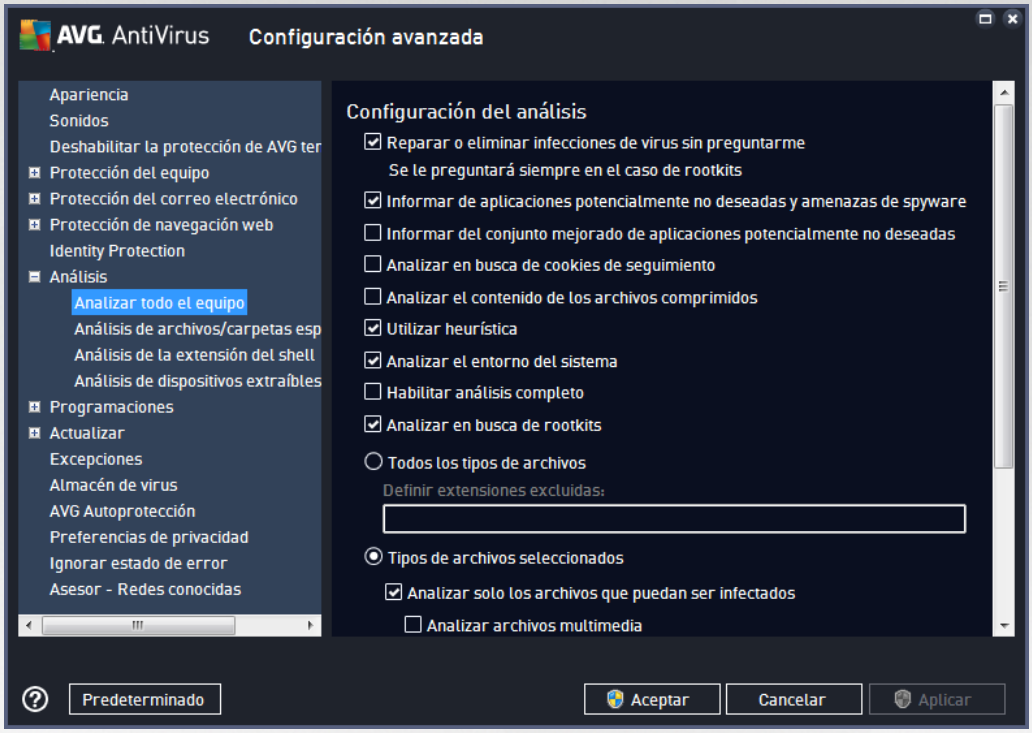
La configuración avanzada del análisis se divide en cuatro categorías que se refieren a tipos de análisis específicos tal y como los definió el proveedor del software:

- Análisis completo del equipo: análisis predefinido estándar de todo el equipo
- Análisis de archivos/carpetas específicos: análisis predefinido estándar de áreas seleccionadas del equipo
- Análisis de la extensión del shell: análisis específico de un objeto seleccionado directamente en el entorno del Explorador de Windows

- Análisis de dispositivos extraíbles: análisis específico de los dispositivos extraíbles conectados al equipo

7.8.1. Análisis completo del equipo

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



Configuración del análisis

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

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

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

- ***Informar de conjunto mejorado de aplicaciones potencialmente no deseadas*** (*desactivado de manera predeterminada*): marque esta opción para detectar paquetes extendidos de spyware, es decir, programas correctos e inofensivos si proceden directamente del fabricante, pero que pueden ser utilizados posteriormente con propósitos maliciosos. Se trata de una medida adicional que

aumenta aún más la seguridad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada.

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

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

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

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

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

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

También debería decidir qué desea analizar

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

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

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

Ajustar la velocidad del análisis

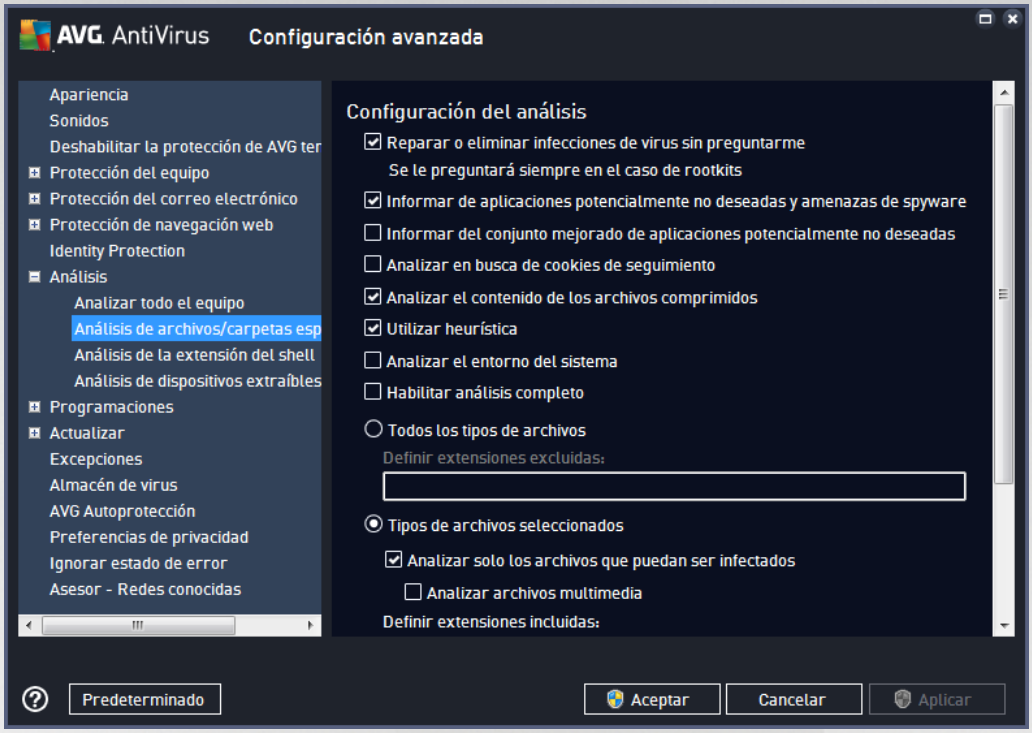
En la sección ***Ajustar la velocidad del análisis*** puede especificar la rapidez con que desea que se ejecute el análisis, según el uso de los recursos del sistema. De manera predeterminada, el valor de esta opción se encuentra ajustado al nivel *dependiente del usuario* de utilización de los recursos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

Establecer informes de análisis adicionales...

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

7.8.2. Análisis de archivos o carpetas específicos

La interfaz de edición de ***Analizar archivos o carpetas específicos*** es casi idéntica al cuadro de diálogo de edición de Análisis completo del equipo; no obstante, la configuración predeterminada es más estricta en el Análisis del equipo completo:

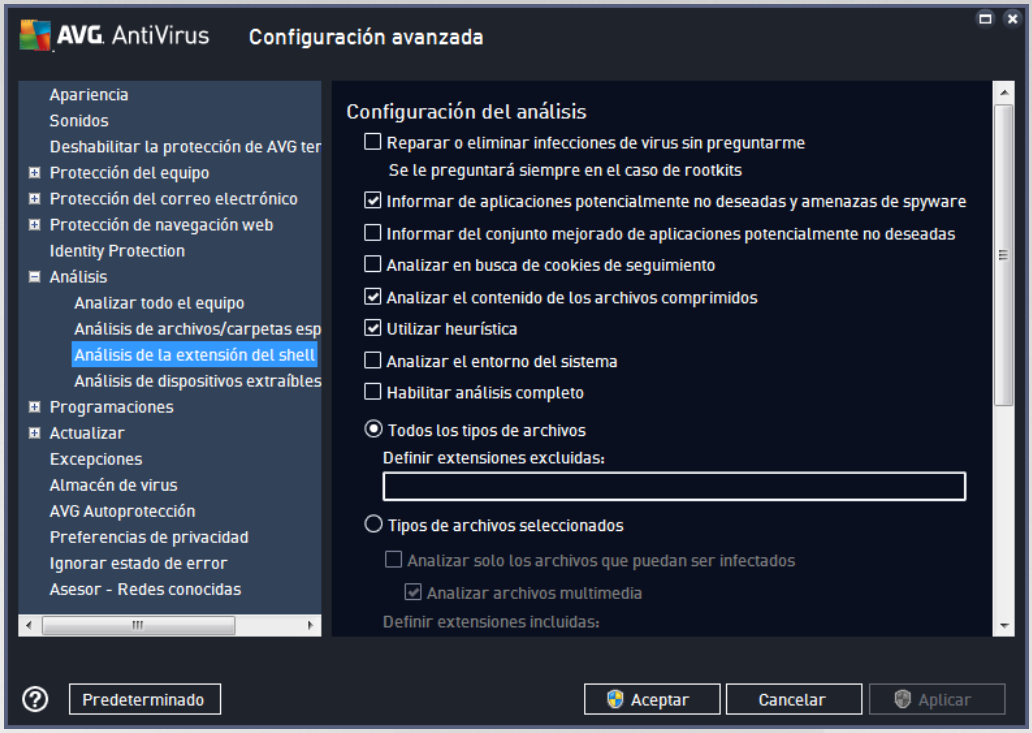


Todos los parámetros definidos en este cuadro de diálogo de configuración se aplican únicamente a las áreas seleccionadas para ser analizadas mediante Analizar archivos o carpetas específicos.

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

7.8.3. Análisis de la extensión del shell

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



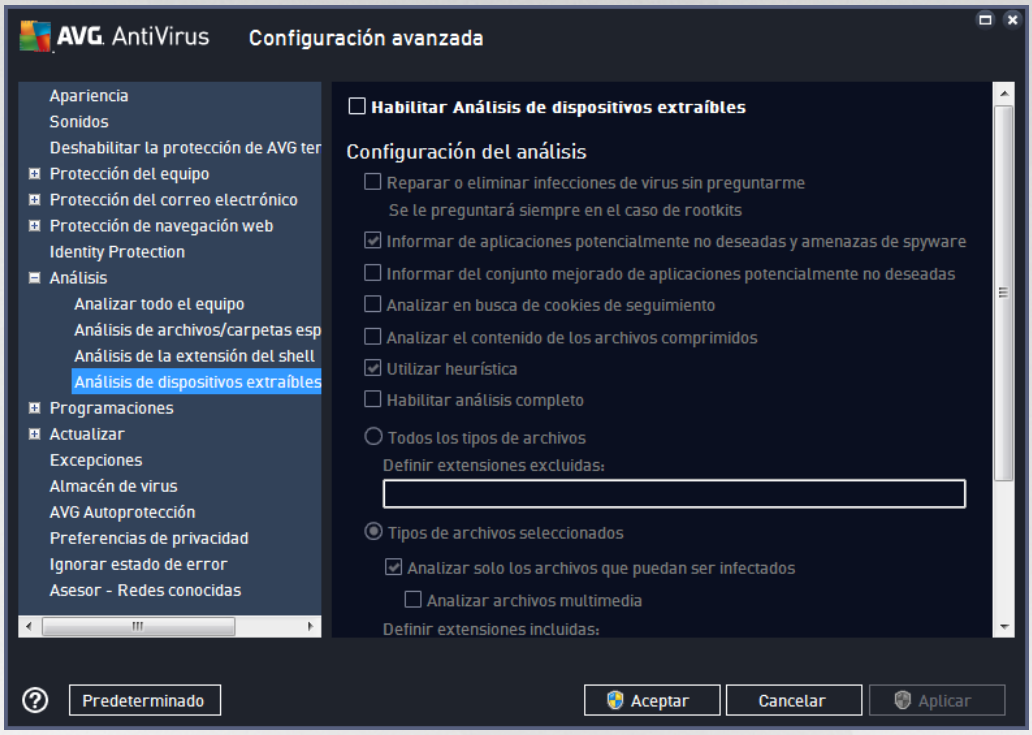
Las opciones de edición son casi idénticas a las opciones disponibles para el Análisis del equipo completo; sin embargo, la configuración predeterminada es distinta (*por ejemplo, el Análisis completo del equipo no comprueba de manera predeterminada los archivos, sino que escanea el entorno del sistema; al revés que con el Análisis de la extensión del shell*).

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

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

7.8.4. Análisis de dispositivos extraíbles

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



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

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

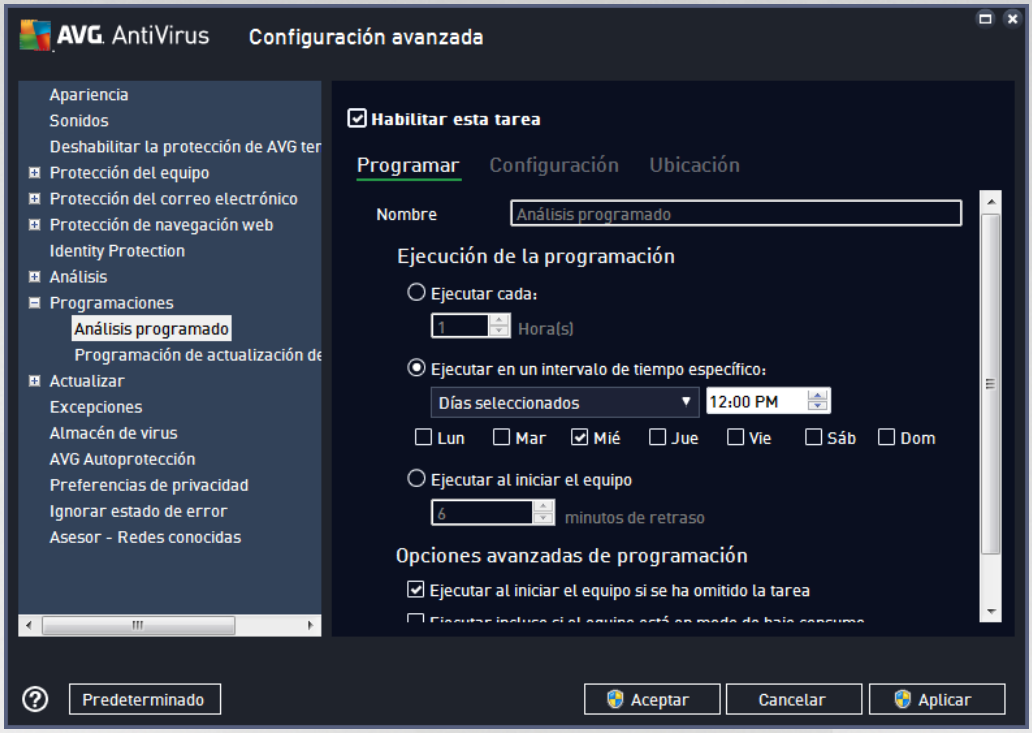
7.9. Programaciones

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

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

7.9.1. Análisis programado

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



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

Ejemplo: *No resulta apropiado llamar al análisis "Análisis nuevo" o "Mi análisis" puesto que estos nombres no hacen referencia a lo que realmente se comprueba en el análisis. Por otro lado, un ejemplo de un buen nombre descriptivo sería "Análisis del área de sistema" etc. Tampoco es necesario especificar en el nombre del análisis si se trata del análisis del equipo completa o solo el análisis de archivos o carpetas seleccionados; sus propios análisis siempre serán una versión específica del análisis de archivos o carpetas seleccionados.*

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

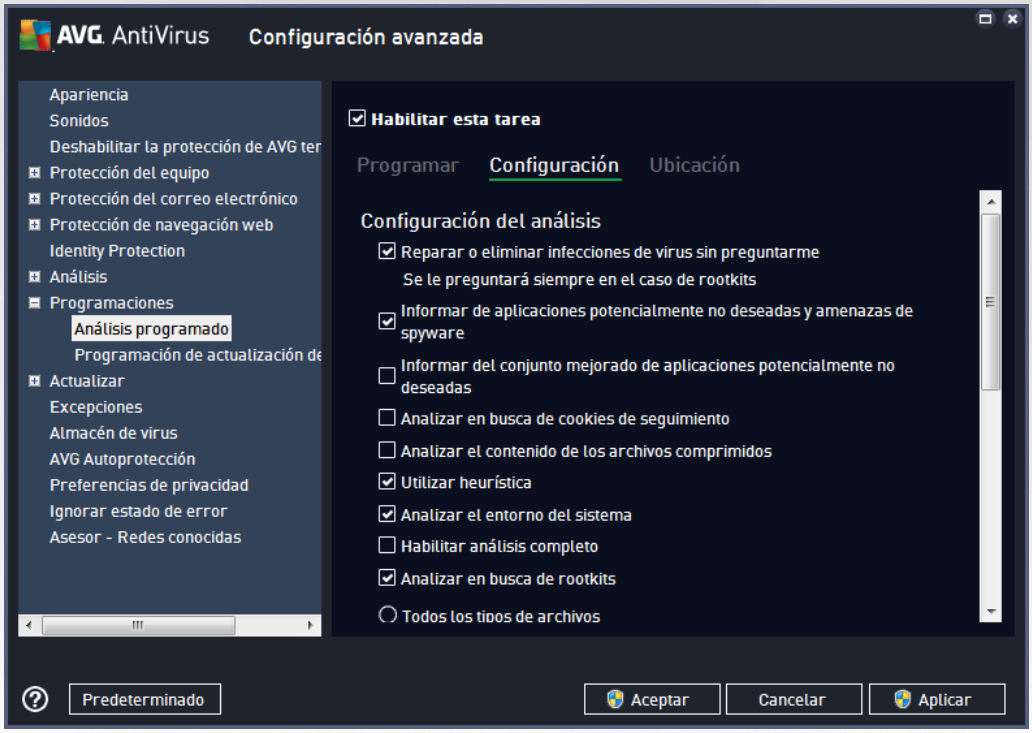
Ejecución de la programación

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

Opciones avanzadas de programación

- ***Ejecutar al iniciar el equipo si se ha omitido la tarea***: si programa la tarea para que se ejecute en un momento determinado, esta opción garantizará que el análisis se ejecutará posteriormente si el equipo se apaga a la hora programada.

- ***Ejecutar incluso si el equipo está en modo de bajo consumo***: la tarea debe ejecutarse aunque el equipo esté funcionando con la batería a la hora programada.



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

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

- ***Informar de aplicaciones potencialmente no deseadas y amenazas de spyware*** *(activado de manera predeterminada):* marque esta opción para activar el análisis en busca de spyware y de virus. El spyware representa una categoría dudosa de software malicioso: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos que mantenga activada esta característica ya que aumenta la seguridad del equipo.

- ***Informar de conjunto mejorado de aplicaciones potencialmente no deseadas*** (*desactivado de manera predeterminada*): marque esta opción para detectar paquetes extendidos de spyware, es

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

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

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

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

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

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

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

También debería decidir qué desea analizar

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

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

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

Ajustar la velocidad del análisis

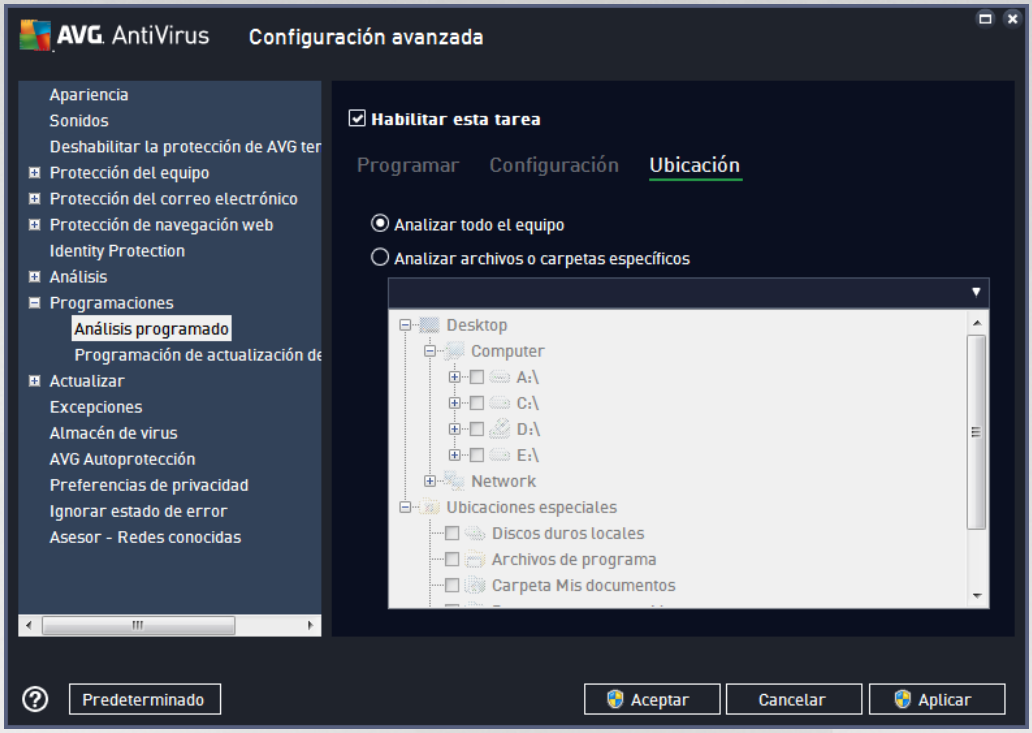
En esta sección puede especificar la velocidad de análisis deseada dependiendo del uso de recursos del sistema. De manera predeterminada, el valor de esta opción está establecido en el nivel automático *dependiente del usuario* de uso de recursos. Si desea que el análisis se ejecute más rápido, llevará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

Establecer informes de análisis adicionales

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

Opciones de apagado del equipo

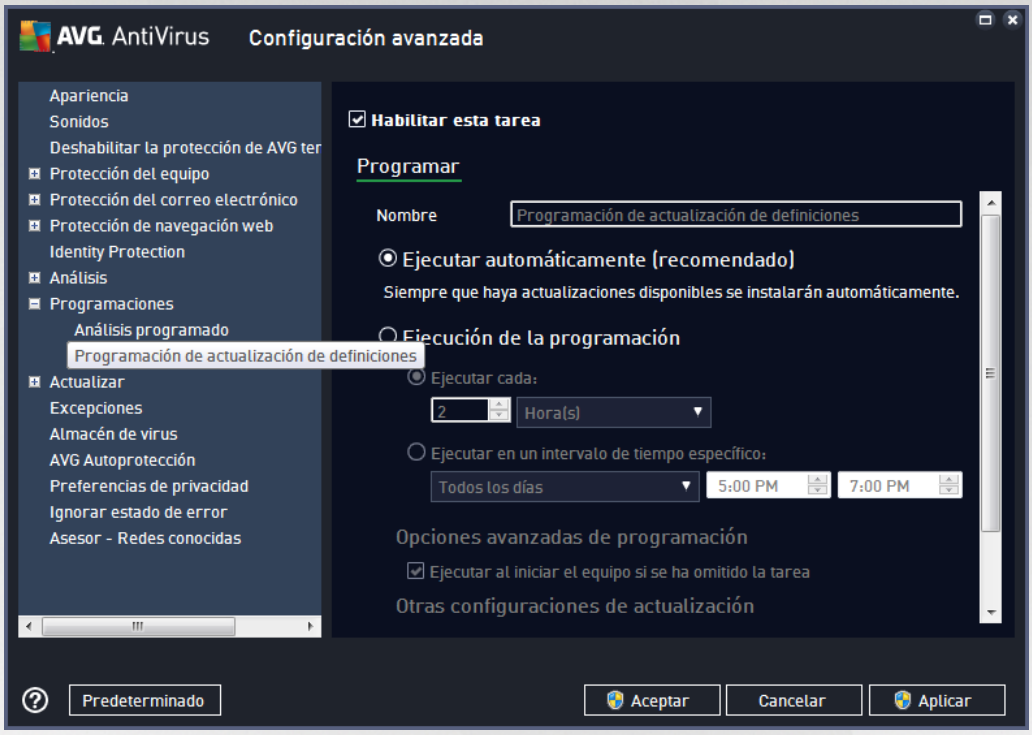
En la sección ***Opciones de apagado del equipo*** puede decidir si el equipo debe cerrarse automáticamente al finalizar la ejecución del proceso de análisis. Una vez confirmada esta opción (***Cerrar el equipo al terminar el análisis***), se activa una nueva opción que permite apagar el equipo aunque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



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

7.9.2. Programación de actualización de definiciones

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



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

Ejecución de la programación

De forma predeterminada, la tarea se inicia automáticamente (***Ejecutar automáticamente***) cuando hay una nueva actualización de definición de virus disponible. A excepción de que tenga un buen motivo para no hacerlo, le recomendamos que siga esta configuración. A continuación, puede configurar el inicio de la tarea manualmente, así como especificar los intervalos temporales del inicio de la actualización de definiciones recién programadas. Los intervalos se pueden definir mediante el inicio repetido de la actualización tras un período de tiempo (***Ejecutar cada...***) o indicando una fecha y hora exactas (***Ejecutar en un intervalo...***).

Opciones avanzadas de programación

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

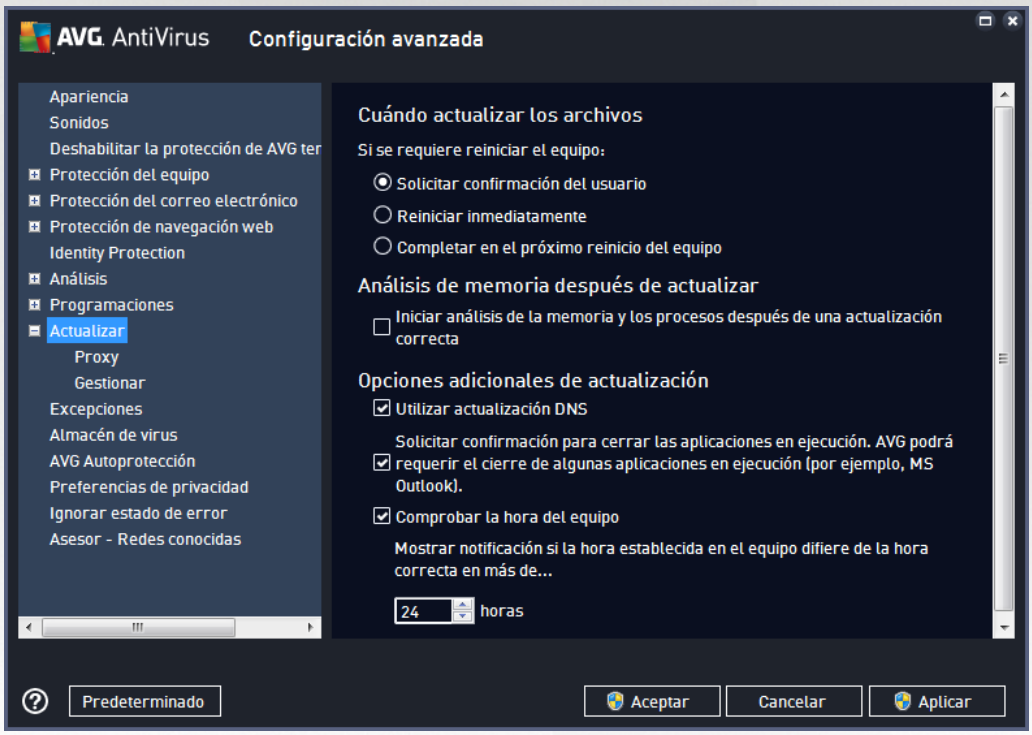
Otras configuraciones de actualización

Finalmente, marque la opción ***Ejecutar de nuevo la actualización cuando la conexión a Internet vuelva***

a estar disponible para asegurarse de que si la conexión a Internet se interrumpe y falla el proceso de actualización, se iniciará automáticamente de nuevo cuando la conexión de Internet se restablezca. Cuando la actualización programada se inicie a la hora especificada, se le informará de este hecho por medio de una ventana emergente que se abrirá encima del icono de la bandeja del sistema de AVG (*siempre que haya mantenido 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 se pueden especificar los parámetros generales de la actualización de AVG:



Cuándo actualizar los archivos

En esta sección se pueden seleccionar tres opciones alternativas que se utilizarán en caso de que el proceso de actualización requiera reiniciar el equipo. Es posible programar la finalización de la actualización para el siguiente reinicio del equipo, o bien reiniciar inmediatamente:

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

Análisis de memoria después de actualizar

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

Opciones adicionales de actualización

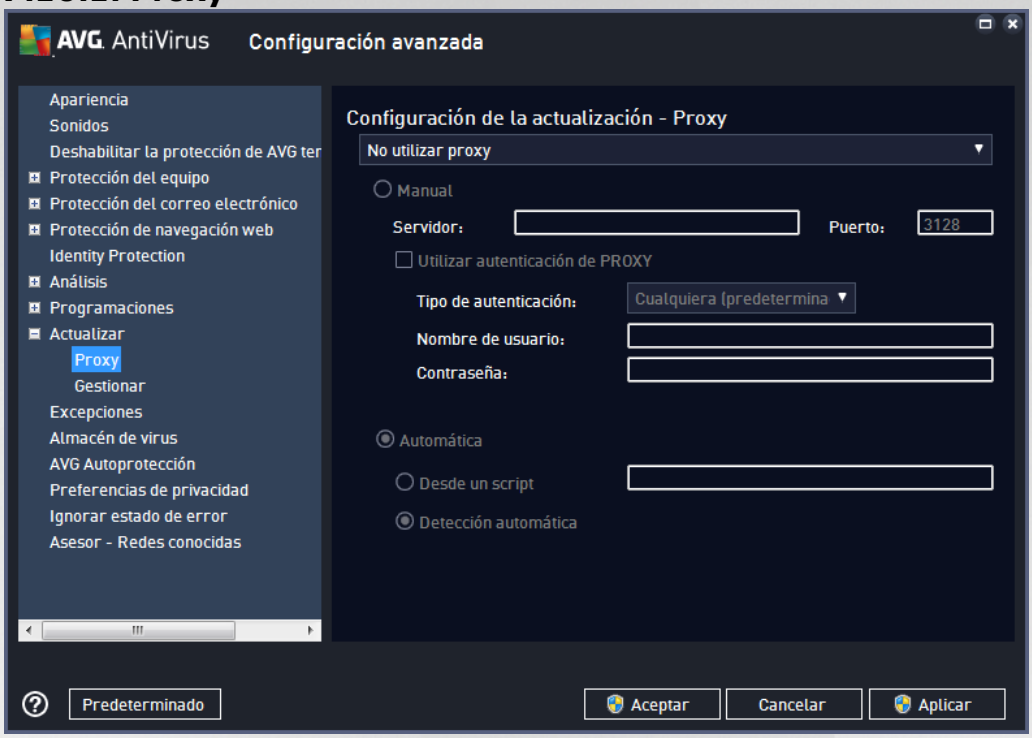
- ***Crear un nuevo punto de restauración del sistema en cada actualización del programa*** (*activada de manera predeterminada*): antes de iniciar cada actualización del programa AVG, se creará un punto de restauración del sistema. En caso de que falle el proceso de actualización y se bloquee el sistema operativo, este último siempre se podrá restaurar a la configuración original desde este punto. Se puede acceder a esta opción a través de Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema, pero se recomienda que solo realicen cambios los usuarios experimentados. Mantenga marcada esta casilla de verificación si desea utilizar esta funcionalidad.

- ***Utilizar actualización DNS*** (*activado de forma predeterminada*): si se marca este elemento, cuando se inicia la actualización,**AVG AntiVirus** busca información acerca de la versión más reciente de la base de datos de virus y del programa en el servidor DNS. Luego solo se descargará y se aplicará el número mínimo de archivos indispensables. De esta forma se minimiza la cantidad total de datos descargados y se agiliza el proceso de actualización.

- ***Solicitar confirmación para cerrar las aplicaciones en ejecución*** (*activada de manera predeterminada*): esto le permitirá asegurarse de que no se cerrará ninguna aplicación en ejecución sin autorización del usuario, en caso de que fuese necesario para finalizar el proceso de actualización.

- ***Comprobar la hora del equipo*** (*activada de manera predeterminada*): marque esta opción para indicar que desea recibir notificaciones visuales en caso de que la hora del equipo difiera de la hora correcta en un número de horas especificado.

7.10.1. Proxy



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

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

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

Configuración manual

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

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

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

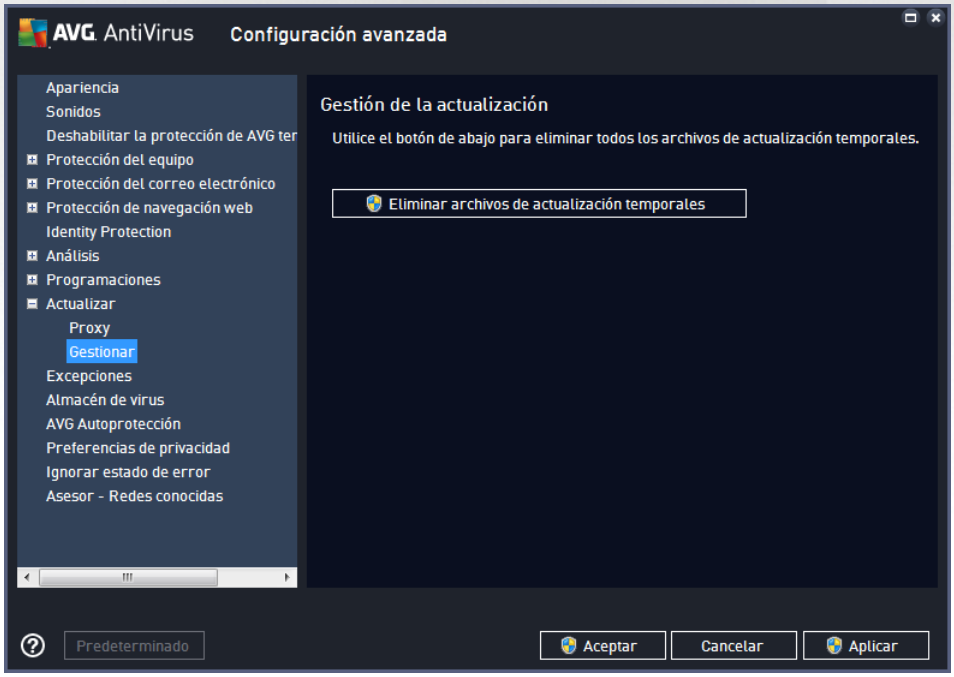
Configuración automática

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

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

7.10.2. Gestionar

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

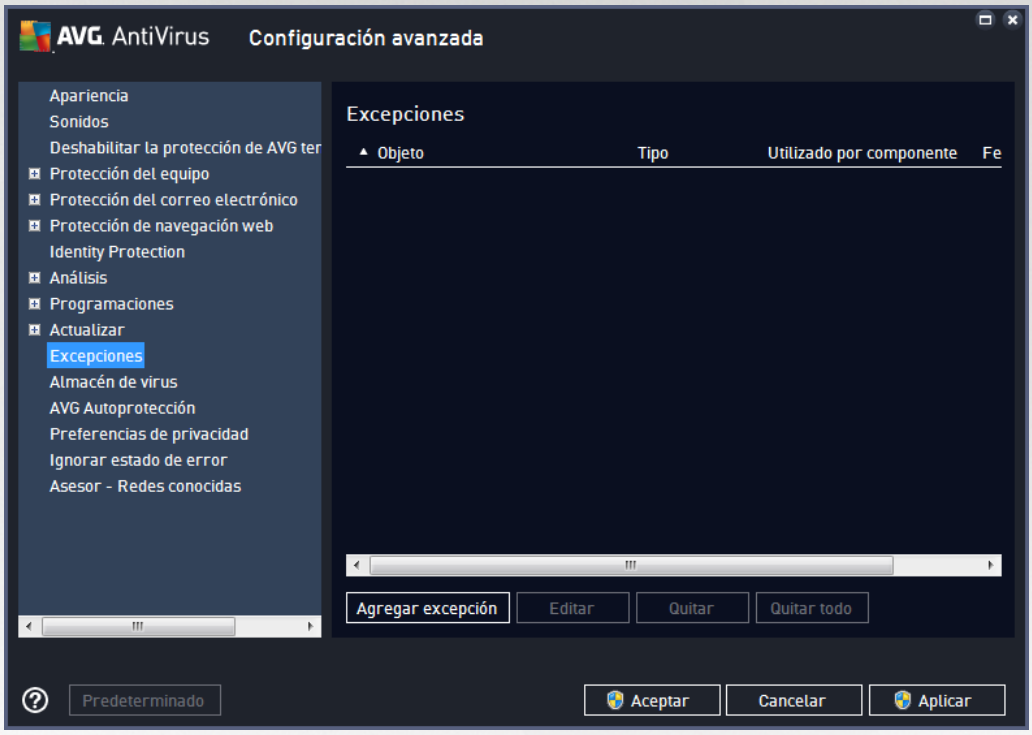


- ***Eliminar archivos de actualización temporales***: presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada, permanecen almacenados allí durante 30 días*)
- ***Restaurar la versión anterior de la base de datos de virus***: presione este botón para eliminar la última versión de la base de datos de virus del disco duro y recuperar la versión guardada anteriormente (*la nueva versión de la base de datos de virus formará parte de la actualización siguiente*)

7.11. Excepciones

En el cuadro de diálogo ***Excepciones*** puede definir excepciones, es decir, elementos que **AVG AntiVirus** ignorará. Normalmente, tendrá que definir una excepción si AVG sigue detectando un programa o un archivo como amenaza, o bloqueando un sitio web seguro al considerarlo peligroso. Agregue el archivo o el sitio web a esta lista de excepciones y AVG no lo notificará ni lo bloqueará más.

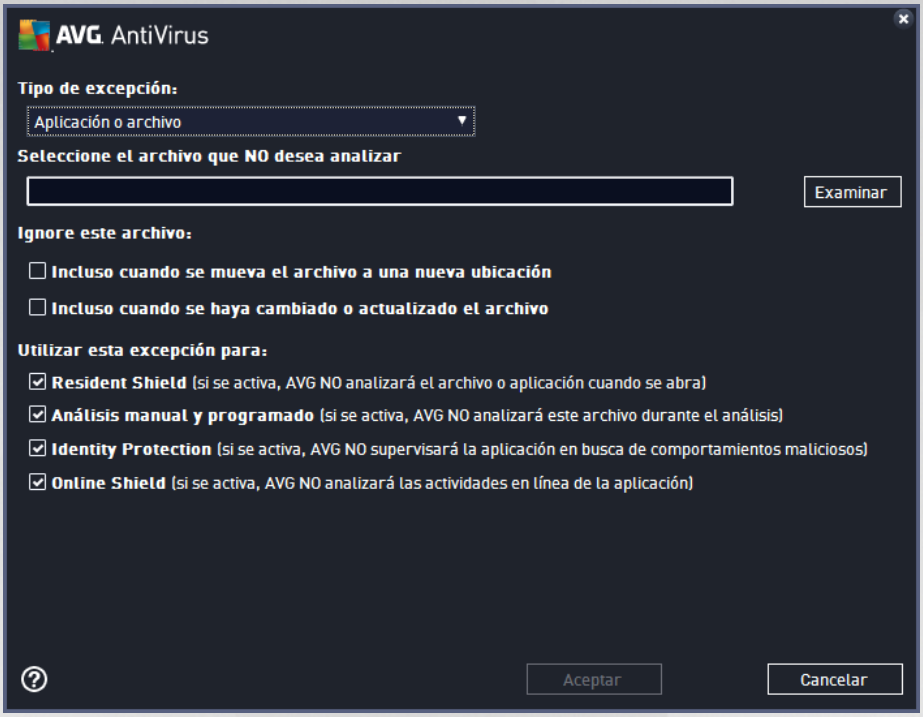
Asegúrese siempre de que el archivo, el programa o el sitio web en cuestión sea realmente seguro.



La tabla del cuadro de diálogo muestra una lista de excepciones, si estas se han definido. Cada elemento tiene a su lado una casilla de verificación. Si la casilla de verificación está marcada, la exclusión tiene efecto; en caso contrario, estará definida, pero no se utilizará. Si hace clic en el encabezado de una columna podrá ordenar los elementos permitidos en función de los criterios respectivos.

Botones de control

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



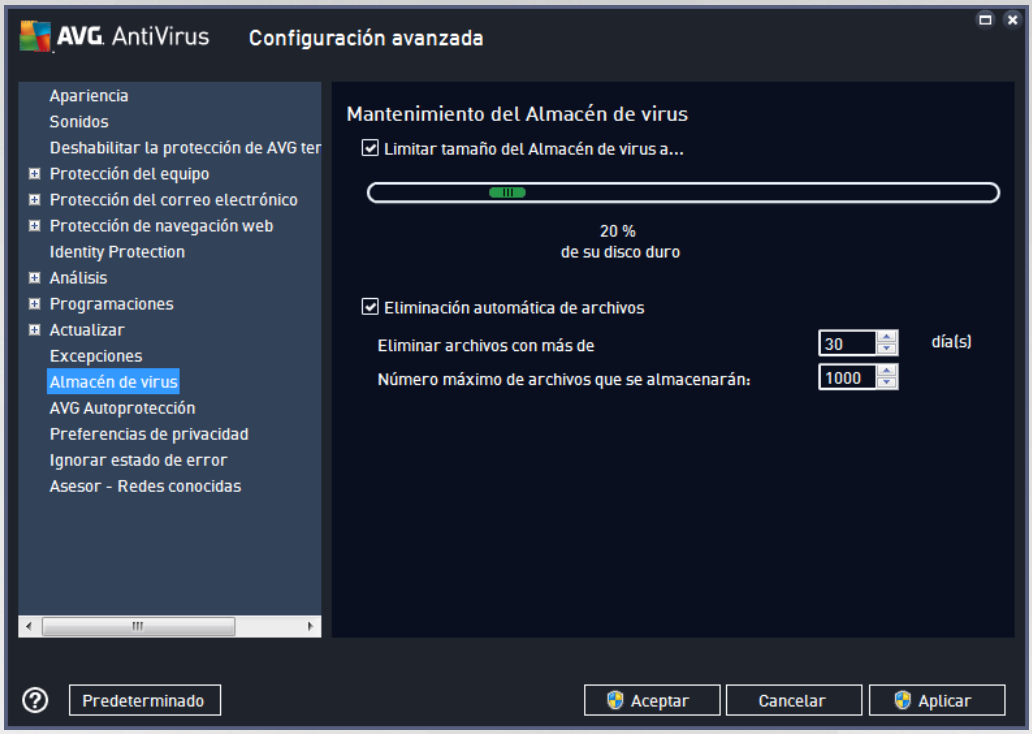
Primero, se le pedirá que defina el tipo de objeto, es decir, si se trata de una aplicación o un archivo, una carpeta, una URL o un certificado. A continuación, tendrá que examinar el disco para proporcionar la ruta del objeto correspondiente o introducir la URL. Por último, puede seleccionar qué características de AVG deberían ignorar el objeto seleccionado *(Resident Shield, Identity Protection, Analizar)*.

- ***Editar***: este botón solo está activo en caso de que se haya definido alguna excepción y ésta aparece en la tabla. En este caso, puede utilizar el botón para abrir el cuadro de diálogo de edición de la excepción seleccionada y configurar los parámetros de la misma.

- ***Quitar***: use este botón para cancelar una excepción definida con anterioridad. Puede eliminarlas una a una o resaltar un bloque de excepciones de la lista y cancelar las excepciones elegidas. Al cancelar la excepción, AVG verificará el archivo, carpeta o URL correspondientes. Tenga en cuenta que solo se quitará la excepción y no el archivo o la carpeta.

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

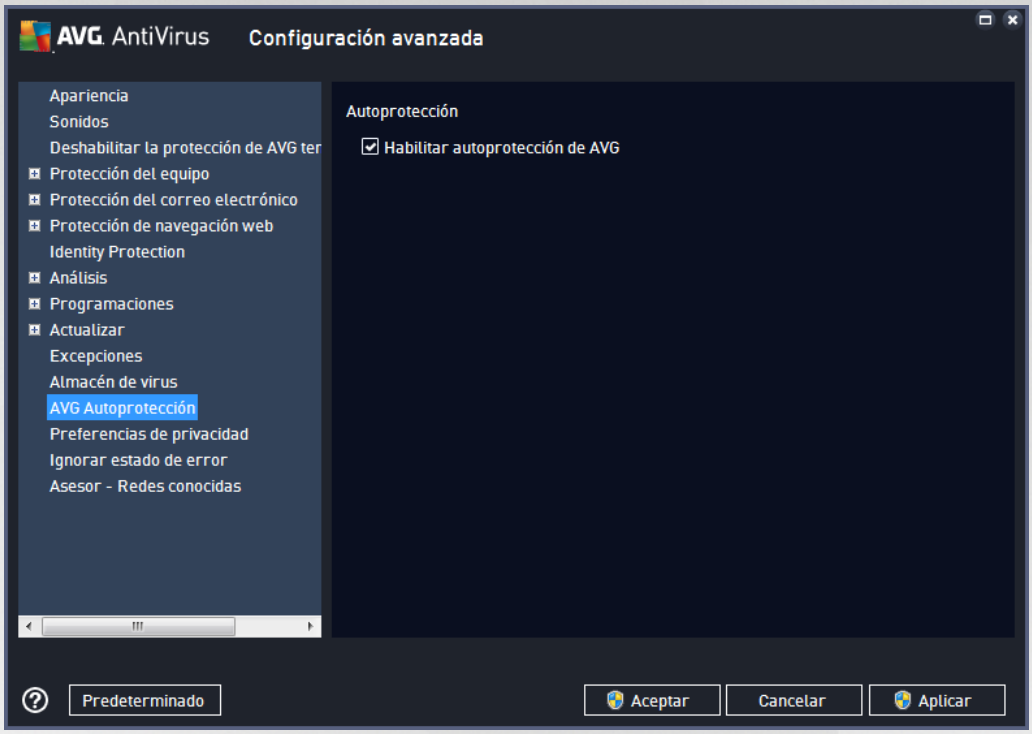
7.12. Almacén de virus



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

- ***Limitar tamaño del Almacén de virus***: utilice el control deslizante para configurar el tamaño máximo del Almacén de virus. El tamaño se especifica en proporción al tamaño del disco duro local.
- ***Eliminación automática de archivos***: defina en esta sección el tiempo máximo que los objetos deben permanecer guardados en el Almacén de virus (***Eliminar archivos con más de ... días***) y el número máximo de archivos que se guardarán en el Almacén de virus (***Número máximo de archivos que se almacenarán***).

7.13. Autoprotección de AVG

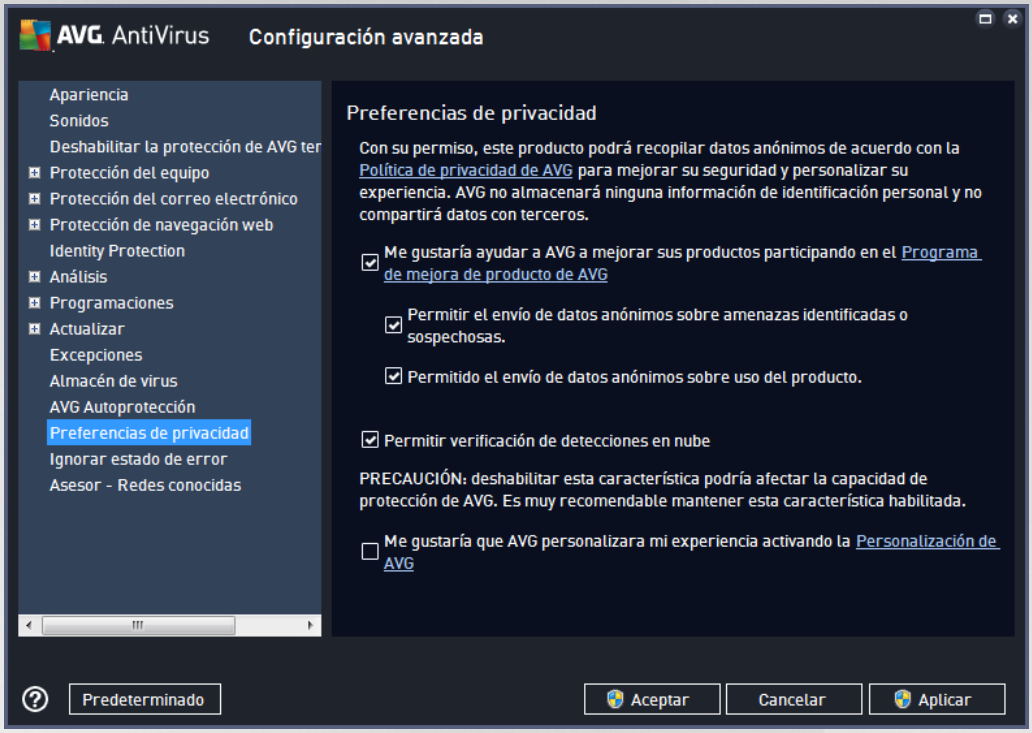


La ***Autoprotección de AVG*** permite que **AVG AntiVirus** proteja sus propios procesos, archivos, claves de registro y controladores evitando que sufran cambios o se desactiven. El principal motivo para aplicar este tipo de protección es que algunas amenazas complejas intentan desmontar la protección antivirus para después causar daños sin problemas al equipo.

Recomendamos mantener activada esta característica.

7.14. Preferencias de privacidad

El cuadro de diálogo ***Preferencias de privacidad*** le invita a participar en la mejora de productos AVG y a ayudarnos a incrementar el nivel de seguridad general en Internet. Sus informes nos ayudan a recopilar información actualizada sobre las amenazas más recientes de parte de personas del mundo entero, lo cual nos permite ofrecer una mejor protección a todos nuestros usuarios. El informe se realiza de forma automática y, por lo tanto, no le causa ninguna molestia. No se incluye ningún dato personal en los informes. El envío de informes de amenazas detectadas es opcional, aunque recomendamos mantener esta opción activada. Nos ayuda a mejorar su protección y la de otros usuarios de AVG.



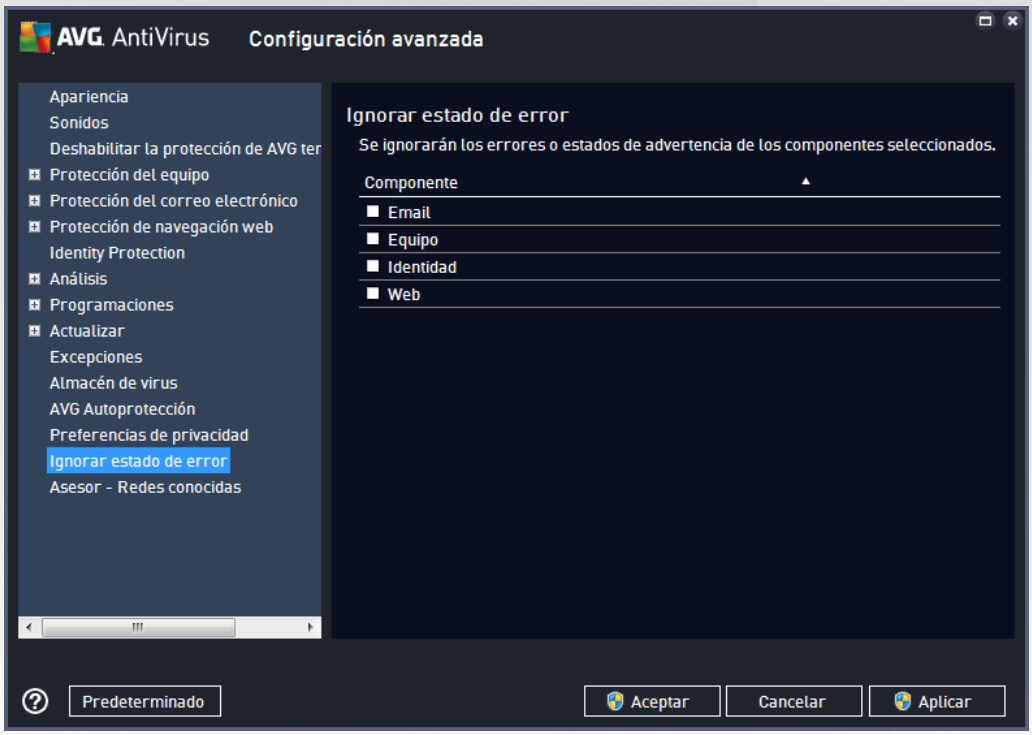
En el cuadro de diálogo dispone de las siguientes opciones de configuración:

- ***Me gustaría ayudar a AVG a mejorar sus productos participando en el Programa de mejora de producto de AVG*** *(activado de manera predeterminada)*: si desea ayudarnos a mejorar **AVG AntiVirus**, mantenga marcada la casilla de verificación. Esto permite el envío de informes de todas las amenazas encontradas a AVG, a fin de que podamos recopilar información actualizada sobre software malicioso de usuarios de todo el mundo y, a cambio, ofrecer una protección mejorada para todos. El informe se procesa automáticamente, por lo que no le provocará ningún inconveniente. Los informes no incluyen datos personales.
    - ***Permitir el envío tras confirmación por parte del usuario de datos sobre correos electrónicos mal identificados*** *(activada de forma predeterminada)*: se envía información sobre mensajes de correo electrónico incorrectamente identificados como spam, o sobre mensajes de spam que no han sido detectados por el servicio Anti-Spam. Al enviar este tipo de información, se le solicitará confirmación.
    - ***Permitir el envío de datos anónimos sobre amenazas identificadas o sospechosas*** *(activada de forma predeterminada)*: se envía información sobre cualquier código o patrón de comportamiento sospechoso o potencialmente peligroso *(puede ser un virus, spyware o una página web maliciosa a la que está intentando acceder)* detectado en su equipo.
    - ***Permitir el envío de datos anónimos sobre uso del producto*** *(activada de forma predeterminada)*: se envían estadísticas básicas sobre el uso de la aplicación, tales como el número de detecciones, los análisis ejecutados, las actualizaciones correctas/incorrectas, etc.
- ***Permitir la verificación de detecciones en la nube*** *(activada de forma predeterminada)*: se comprobarán las amenazas detectadas para ver si están realmente infectadas, a fin de descartar falsos positivos.

- ***Me gustaría que AVG personalizara mi experiencia activando la Personalización de AVG*** *(desactivada de manera predeterminada)*: esta característica analiza de forma anónima el comportamiento de los programas y las aplicaciones instalados en el PC. En función de este análisis, AVG puede ofrecerle servicios destinados directamente a sus necesidades para garantizarle la máxima seguridad.

7.15. Omitir el estado de error

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



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

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

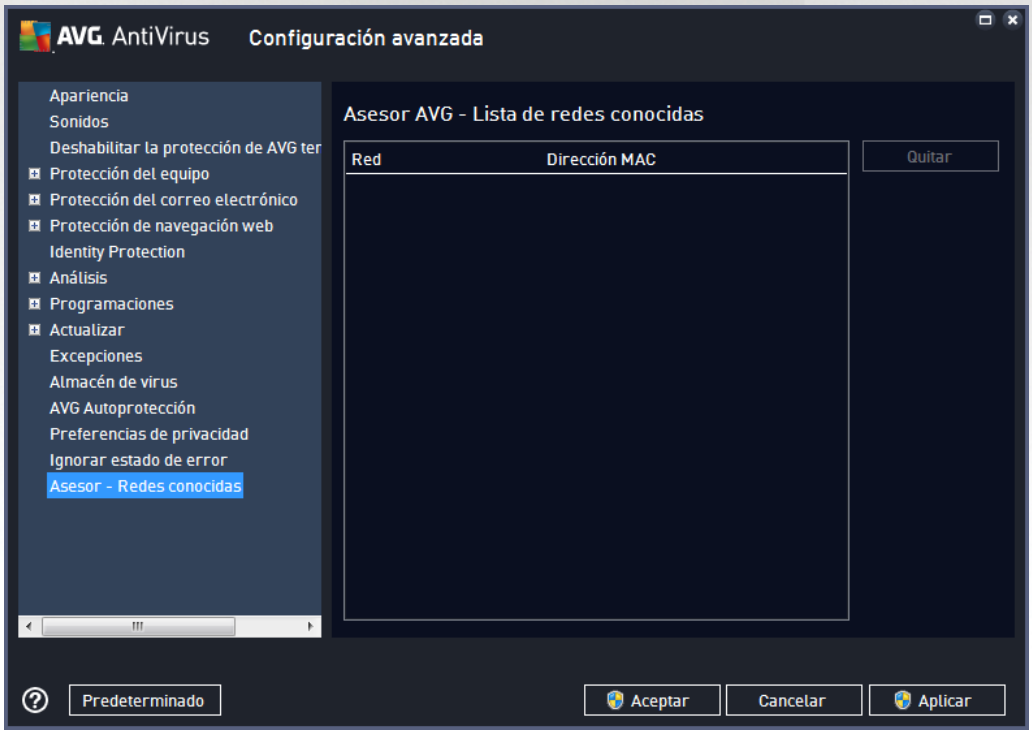
Pudiera darse una situación en la que, por algún motivo, necesite desactivar el componente de forma temporal. ***Esta acción no está recomendada, debería intentar mantener activos todos los componentes y con su configuración predeterminada***, pero puede suceder. En este caso, el icono de la bandeja del sistema informará automáticamente sobre el estado de error del componente. Sin embargo, en este caso en concreto no podemos hablar de error propiamente, ya que ha sido provocado deliberadamente por usted y es consciente del posible riesgo. Al mismo tiempo, una vez adquiere color gris, el icono no puede informar sobre ningún posible error posterior que pueda aparecer.

En dicha situación, en el cuadro de diálogo superior puede seleccionar los componentes que pueden encontrarse en ***estado de error*** (*o desactivados*) y sobre los que no desea recibir información. Pulse el botón ***Aceptar*** para confirmar.

7.16. Asesor - Redes conocidas

El Asesor AVG incluye una característica con la que se supervisan las redes a las que se conecta y, en caso de detectar una red nueva *(con un nombre de red que ya se haya usado, lo que puede generar confusión)*, le informará de ello y le recomendará que compruebe la seguridad de dicha red. Si decide que la nueva red es segura para conectarse, también puede guardarla en esta lista *(a través del vínculo proporcionado en la bandeja de notificación del Asesor AVG que se desliza sobre la bandeja del sistema una vez que se detecta una red desconocida. Para más información, consulte el capítulo sobre Asesor AVG)* Asesor AVG recordará los atributos únicos de la red *(concretamente la dirección MAC)* y no mostrará la notificación la próxima vez. Cada red a la que se conecte se considerará automáticamente la red conocida y se añadirá a la lista. Puede eliminar entradas individuales pulsando el botón ***Quitar***. La red correspondiente pasará a considerarse de nuevo como desconocida y potencialmente no segura.

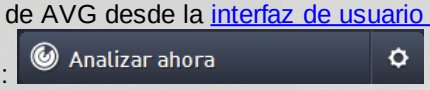
En esta ventana de diálogo puede verificar las redes que se consideran conocidas:



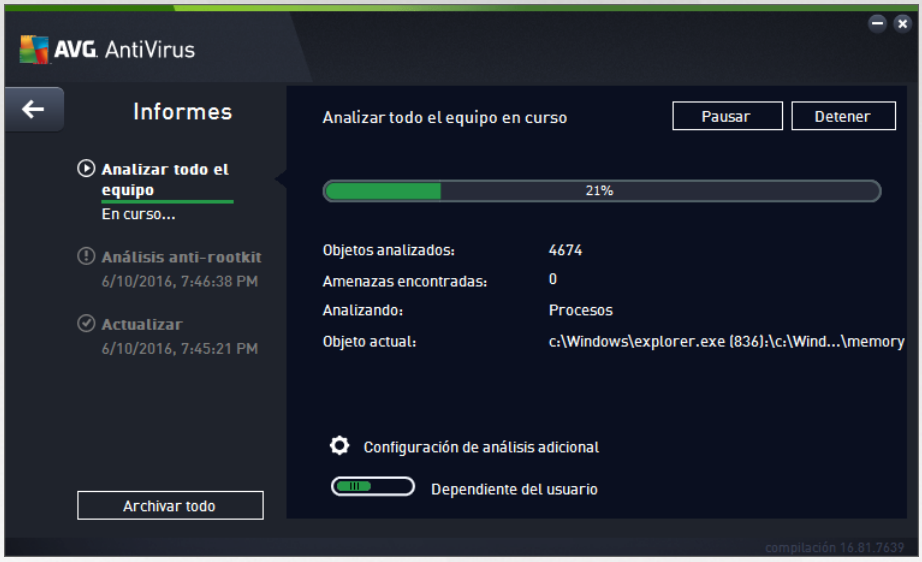
Nota: *El componente de redes conocidas de Asesor AVG no es compatible con Windows XP de 64 bits.*

8. Análisis de AVG

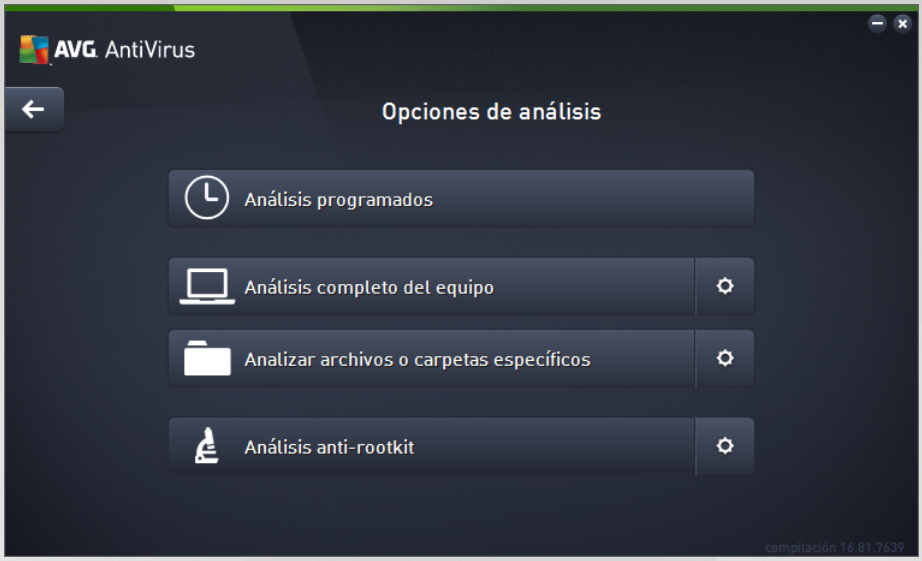
De manera predeterminada, **AVG AntiVirus** no ejecuta ningún análisis, ya que desde el análisis inicial *(que se le invitará a ejecutar*), quedará perfectamente protegido por los componentes residentes de **AVG AntiVirus**, que siempre están en guardia y no permiten que ningún código malicioso se introduzca en su equipo. Por supuesto, puede programar un análisis para que se ejecute a intervalos regulares o iniciar manualmente un análisis según sus necesidades en cualquier momento.

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

- ***Analizar ahora***: presione el botón para iniciar el Análisis completo del equipo de manera inmediata y ver el progreso y los resultados en la ventana Informes, que se abrirá automáticamente:



- ***Opciones***: seleccione este botón *(que se muestra gráficamente como tres líneas horizontales en un campo verde)* para abrir el cuadro de diálogo ***Opciones de análisis***, en el que puede gestionar análisis programados y editar parámetros de Análisis completo del equipo / Analizar archivos o carpetas específicos.



En el cuadro de diálogo ***Opciones de análisis***, puede ver tres secciones principales de configuración de análisis:

- ***Gestionar análisis programados***: haga clic en esta opción para abrir un nuevo cuadro de diálogo con información general de todas las programaciones de análisis. Antes de definir sus propios análisis, solo podrá ver un análisis programado predefinido por el fabricante del programa mostrado en la tabla. El análisis está deshabilitado de manera predeterminada. Para habilitarlo, haga clic con el botón derecho en la opción *Habilitar tarea* del menú contextual. Una vez que se ha habilitado un análisis programado, puede editar la configuración con el botón *Editar análisis programado*. También puede hacer clic en el botón *Programar análisis* para crear una nueva programación de análisis propia.

- ***Análisis completo del equipo / Configuración***: el botón se divide en dos secciones. Haga clic en la opción *Análisis completo del equipo* para iniciar al momento el análisis de todo el equipo *(para más detalles sobre el análisis de todo el equipo, consulte el capítulo correspondiente llamado Análisis predefinidos / Análisis completo del equipo)*. Haga clic en la sección *Configuración* para acceder al cuadro de diálogo de configuración del análisis completo del equipo.

- ***Analizar archivos o carpetas específicos / Configuración***: de nuevo, el botón está dividido en dos secciones. Haga clic en la opción *Analizar archivos o carpetas específicos* para iniciar de inmediato el análisis de las áreas seleccionadas de su equipo *(para más detalles sobre el análisis de los archivos o carpetas seleccionados, consulte el capítulo correspondiente llamado Análisis predefinidos / Analizar archivos o carpetas específicos)*. Haga clic en la sección *Configuración* para acceder al cuadro de diálogo de configuración del análisis de archivos o carpetas específicos.

- ***Analizar equipo en busca de rootkits / Configuración***: la sección izquierda del botón *Analizar equipo en busca de rootkits* inicia el análisis anti-rootkit inmediato *(para obtener más información sobre el análisis de rootkits, consulte el capítulo correspondiente, Análisis predefinidos / Analizar equipo en busca de rootkits)*. Haga clic en la sección *Configuración* para acceder al cuadro de diálogo de configuración del análisis de rootkits.

8.1. Análisis predefinidos

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

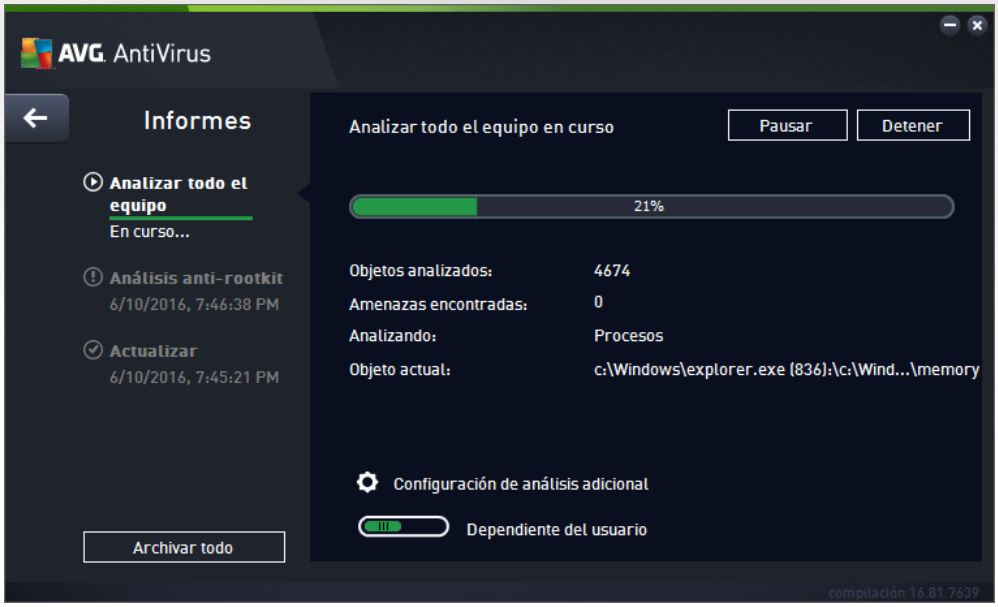
En **AVG AntiVirus**, encontrará los siguientes tipos de análisis predefinidos por el proveedor de software:

8.1.1. Analizar todo el equipo

Análisis completo del equipo analiza todo el equipo en busca de posibles infecciones o programas potencialmente no deseados. En este análisis se comprueban todos los discos duros del equipo, se detectan y reparan los virus encontrados o se mueven las infecciones detectadas al Almacén de virus. El análisis completo del equipo debería programarse en el equipo al menos una vez a la semana.

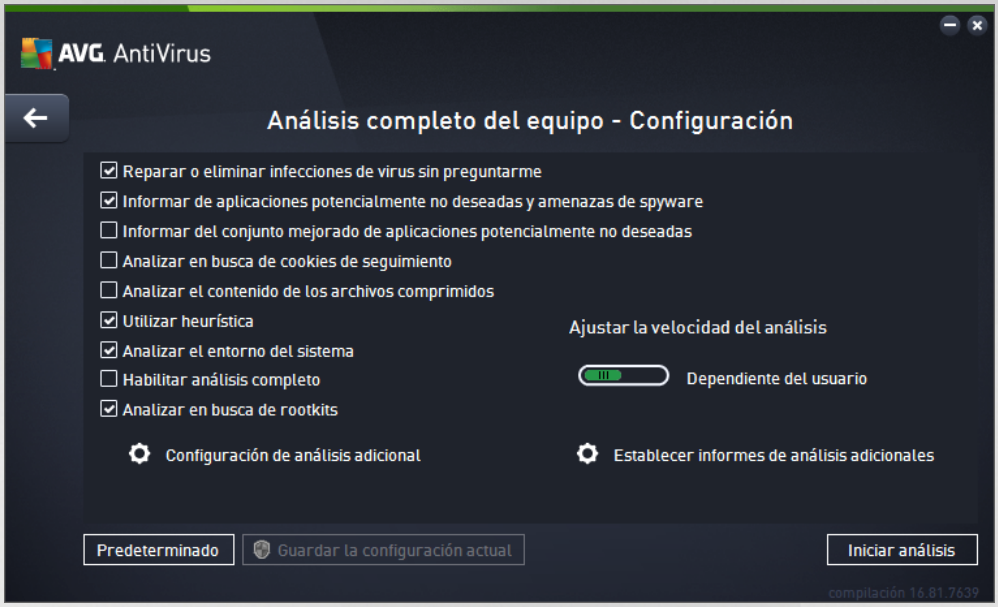
Inicio del análisis

El ***Análisis completo del equipo*** puede iniciarse directamente desde la interfaz de usuario principal haciendo clic en el botón ***Analizar ahora***. No es necesario realizar más configuraciones para este tipo de análisis; el análisis se iniciará inmediatamente. En el cuadro de diálogo ***Análisis completo del equipo en curso*** (*consulte imagen*) puede ver el progreso y los resultados. En caso necesario, el análisis se puede interrumpir temporalmente (***Pausar***) o cancelar (***Detener***).



Edición de la configuración del análisis

Puede editar la configuración de ***Análisis completo del equipo*** en el cuadro de diálogo ***Análisis completo del equipo - Configuración*** *(el cuadro de diálogo está disponible a través del vínculo de configuración de Análisis completo del equipo en el cuadro de diálogo Opciones de análisis).* ***Se recomienda que mantenga la configuración predeterminada a menos que tenga un buen motivo para modificarla.***



En la lista de parámetros de análisis, puede activar o desactivar parámetros específicos según sea necesario:

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

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

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

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

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

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

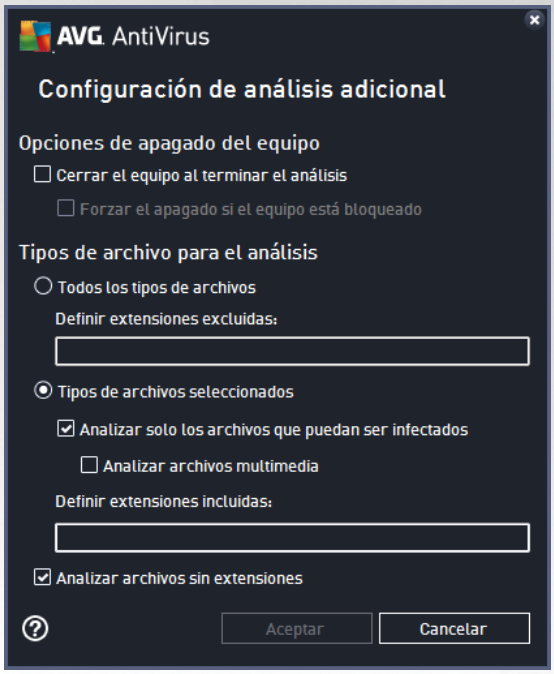
- ***Analizar el entorno del sistema****(activada de manera predeterminada)*: el análisis también

comprobará las áreas del sistema del equipo.

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

- ***Analizar en busca de rootkits*** *(activada de manera predeterminada)*: incluye un análisis anti-rootkit en el análisis del equipo completo. El análisis anti-rootkit también se puede iniciar de forma separada.

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



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

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

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

    - ➢ ***Tipos de archivos seleccionados***: puede especificar que desea analizar solamente los archivos que puedan estar infectados (*no se analizarán los archivos que no se pueden infectar, por ejemplo, algunos archivos de texto sin formato u otro tipo de archivos no ejecutables*), incluidos archivos multimedia (*archivos de vídeo y audio - si deja esta casilla en blanco, se reducirá aún más el tiempo del análisis, ya que estos archivos suelen ser*

grandes y no es demasiado probable que estén infectados por un virus). Del mismo modo, puede especificar las extensiones de los archivos que se deberían analizar siempre.

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

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

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

Advertencia *Advertencia: esta configuración de análisis es idéntica a la que se emplea para un análisis recién definido, tal como se describe en el capítulo Análisis de AVG / Programación de análisis / Cómo analizar. Si decide cambiar la configuración predeterminada de* ***Análisis completo del equipo****, puede guardar la nueva configuración como predeterminada para que la utilicen todos los análisis del equipo completo que se realicen en el futuro.*

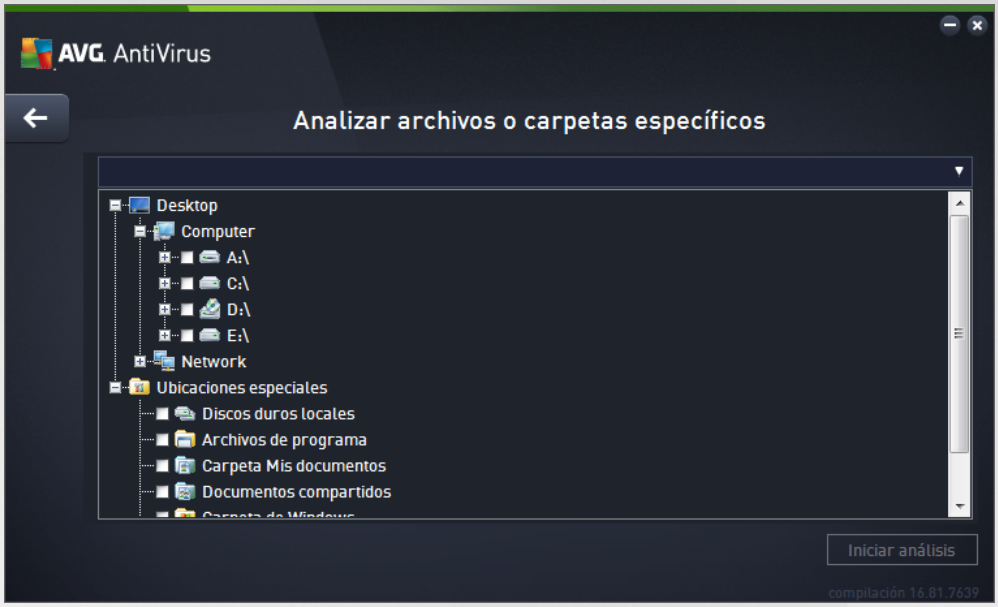
8.1.2. Analizar archivos o carpetas específicos

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

Inicio del análisis

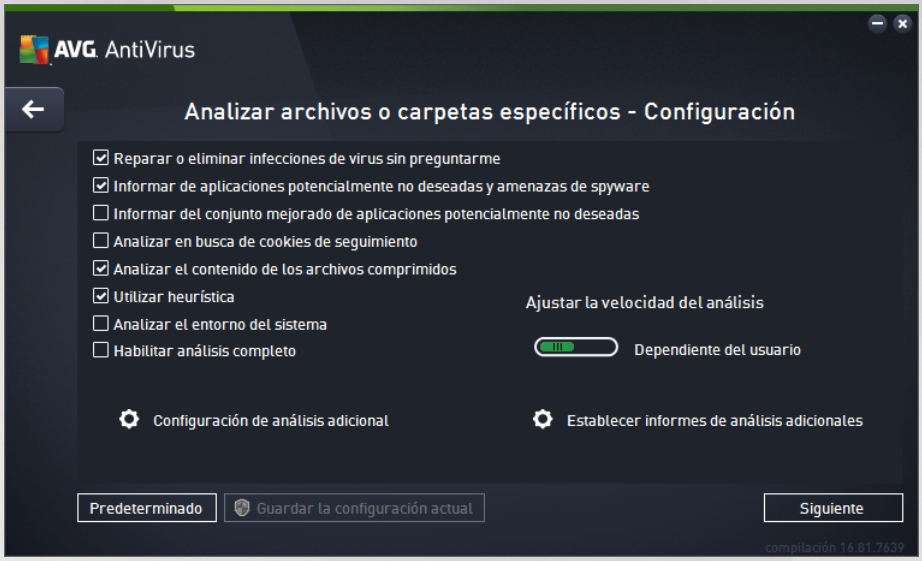
La opción ***Análisis de archivos o carpetas específicos*** se puede iniciar directamente desde el cuadro de diálogo Opciones de análisis haciendo clic en el botón **Analizar archivos o carpetas específicos**. Se abrirá un nuevo cuadro de diálogo llamado ***Seleccione los archivos o carpetas específicos para analizar***. En la

estructura de árbol del equipo, seleccione las carpetas que desea analizar. La ruta a cada carpeta seleccionada se generará automáticamente y se mostrará en el cuadro de texto ubicado en la parte superior de este cuadro de diálogo. También existe la opción de analizar una carpeta específica excluyendo del análisis todas sus subcarpetas. Para ello, escriba un signo menos "**-**" delante de la ruta que se genera de manera automática (*consulte la captura de pantalla*). Para excluir del análisis toda la carpeta, utilice el parámetro "!". Por último, para iniciar el análisis, pulse el botón ***Iniciar análisis***; el proceso de análisis en sí es básicamente idéntico al Análisis completo del equipo.



Edición de la configuración del análisis

Puede editar la configuración de ***Analizar archivos o carpetas específicos*** en el cuadro de diálogo ***Analizar archivos o carpetas específicos - Configuración*** *(se accede al cuadro de diálogo a través del vínculo Configuración de Analizar archivos o carpetas específicos en el cuadro de diálogo Opciones de análisis).* ***Se recomienda que mantenga la configuración predeterminada a menos que tenga un buen motivo para modificarla.***



En la lista de parámetros de análisis puede activar o desactivar los parámetros específicos según sus necesidades:

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

- ***Informar de aplicaciones potencialmente no deseadas y amenazas de spyware*** *(activada de manera predeterminada)*: Marque esta opción para activar el análisis en busca de spyware y de virus. El spyware representa una categoría dudosa de software malicioso: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos que mantenga activada esta característica ya que aumenta la seguridad del equipo.

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

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

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

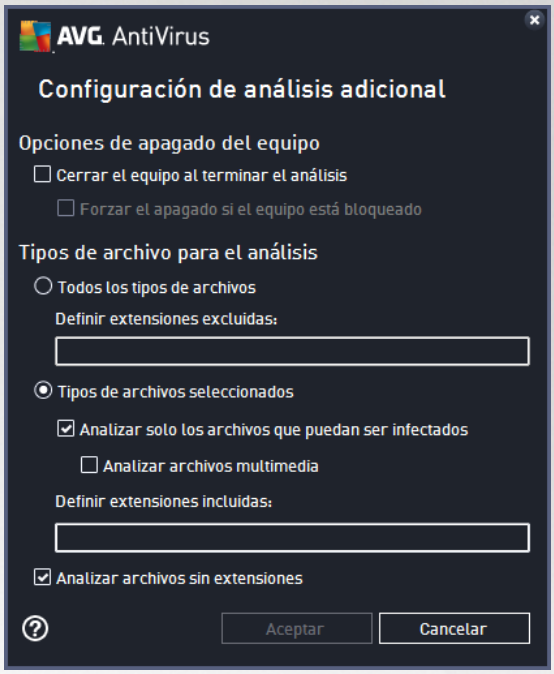
- ***Utilizar heurística*** *(activado de manera predeterminada)*: el análisis heurístico *(emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual)* será uno de los métodos utilizados para detectar virus durante el análisis.

- ***Analizar el entorno del sistema*** *(desactivado de manera predeterminada)*: el análisis también

comprobará las áreas del sistema del equipo.

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

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



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

  - ***Tipos de archivo para el análisis***: también debería decidir que desea analizar:

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

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

    - Opcionalmente, puede decidir ***Analizar archivos sin extensiones***: esta opción está

activada de manera predeterminada y se recomienda mantenerla a menos que tenga un buen motivo para modificarla. Los archivos sin extensión son bastante sospechosos y deberían analizarse siempre.

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

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

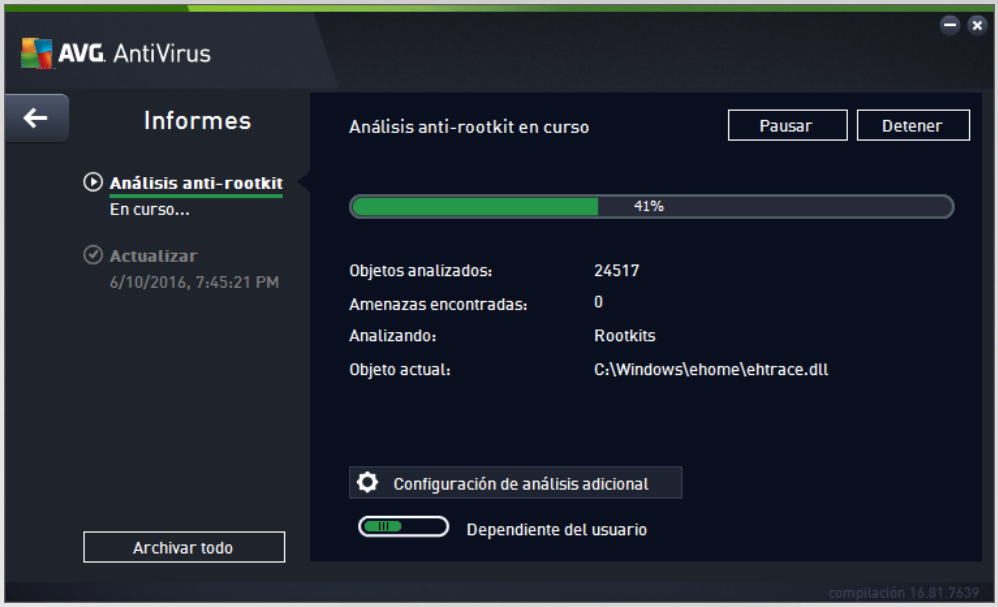
Advertencia *Advertencia: esta configuración de análisis es idéntica a la que se emplea para un análisis recién definido, tal como se describe en el capítulo Análisis de AVG / Programación de análisis / Cómo analizar. Si decide cambiar la configuración predeterminada de la opción* ***Analizar archivos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

8.1.3. Analizar equipo en busca de rootkits

Analizar equipo en busca de rootkits detecta y elimina eficazmente rootkits peligrosos, es decir, programas y tecnologías que pueden enmascarar la presencia de software malicioso en el equipo. Un rootkit está diseñado para asumir el control de un equipo sin autorización de los propietarios y los administradores legítimos del sistema. El análisis es capaz de detectar rootkits basándose en un conjunto predefinido de reglas. Encontrar un rootkit no implica necesariamente que esté infectado. Algunas veces, los rootkits se utilizan como controladores o forman parte de aplicaciones correctas.

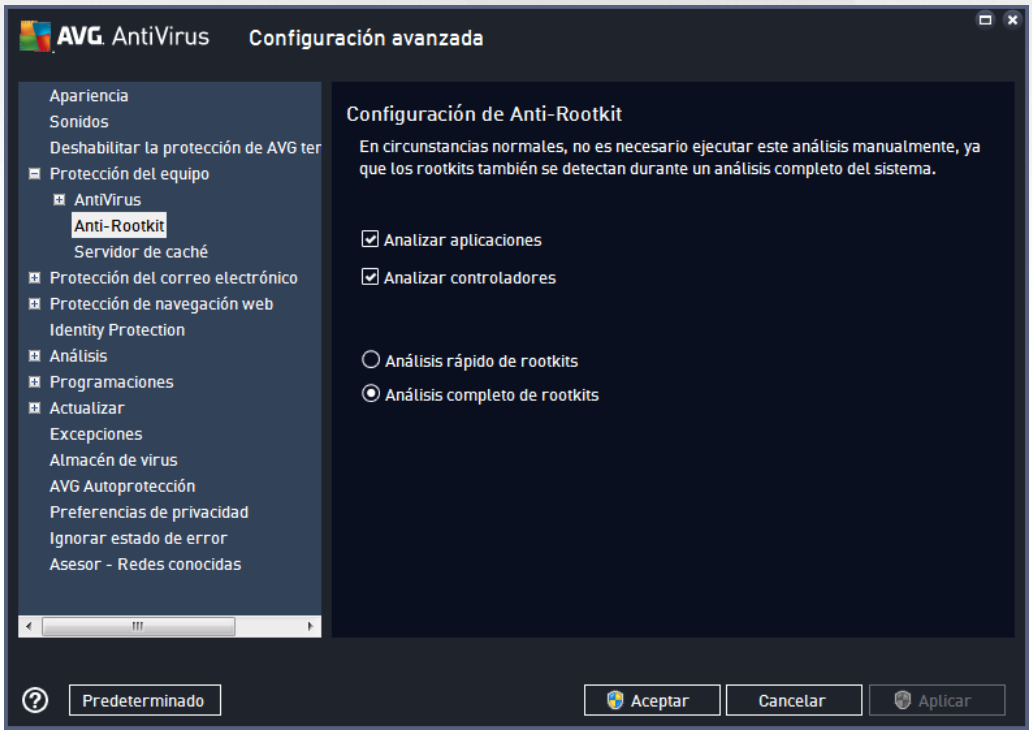
Inicio del análisis

Se puede iniciar ***Analizar equipo en busca de rootkits*** directamente desde el cuadro de diálogo Opciones de análisis haciendo clic en el botón ***Analizar equipo en busca de rootkits***. Se abre un nuevo cuadro de diálogo llamado ***Análisis anti-rootkit en curso***, que muestra el progreso del análisis iniciado:



Edición de la configuración del análisis

Puede editar la configuración del Análisis anti-rootkit en el cuadro de diálogo ***Configuración de Anti-Rootkit*** *(el cuadro de diálogo está disponible a través del vínculo Configuración del análisis Analizar equipo en busca de rootkits del cuadro de diálogo Opciones de análisis).* ***Se recomienda que mantenga la configuración predeterminada a menos que tenga un buen motivo para modificarla.***



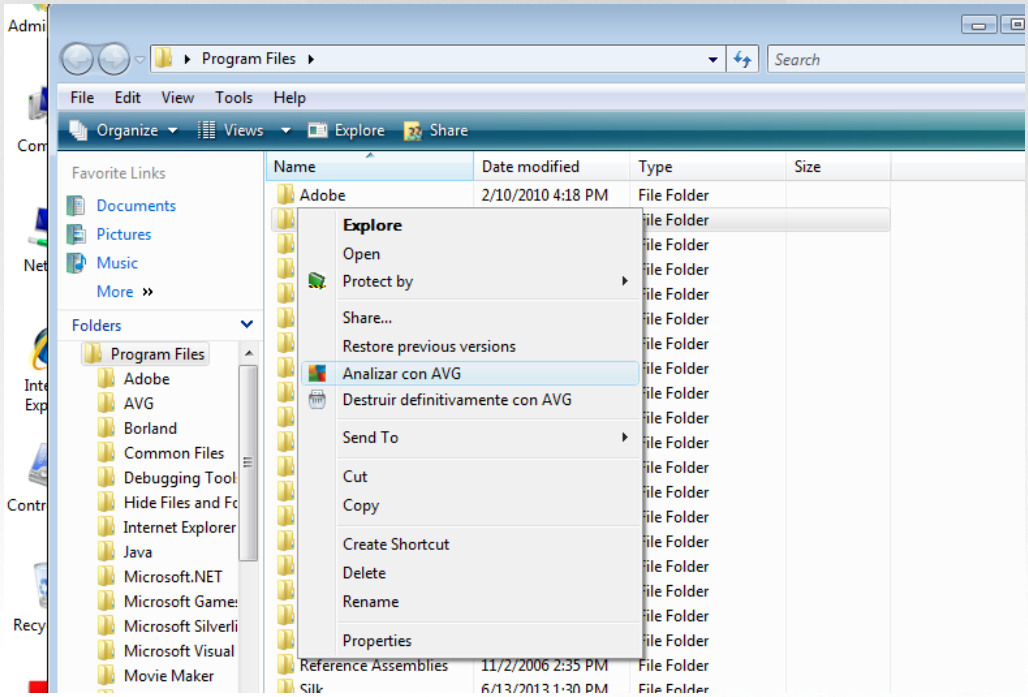
Analizar aplicaciones y ***Analizar controladores*** permiten especificar en detalle lo que debería incluir el análisis anti-rootkit. Estos ajustes están dirigidos a usuarios avanzados. Se recomienda mantener todas las

opciones activadas. Además, puede seleccionar el modo de análisis de rootkits:

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

8.2. Análisis en el Explorador de Windows

Además de los análisis predefinidos que comprueban el equipo entero o solo áreas seleccionadas, **AVG AntiVirus** también ofrece la opción de realizar un análisis rápido de un objeto específico directamente en el entorno del Explorador de Windows. Si desea abrir un archivo desconocido y no está seguro de su contenido, puede analizarlo bajo demanda. Siga estos pasos:



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

8.3. Análisis desde la línea de comandos

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

Para iniciar el análisis de AVG desde la línea de comandos, ejecute el siguiente comando en la carpeta donde

AVG esté instalado:

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

8.3.1. Sintaxis del comando

La sintaxis del comando es la siguiente:

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

8.3.2. Parámetros de análisis

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

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

8.3.3. Análisis desde CMD iniciado desde la interfaz gráfica

Si se ejecuta el equipo en el modo seguro de Windows, también existe la opción de iniciar el análisis desde la línea de comandos en la interfaz gráfica de usuario.

En el modo seguro, el propio análisis puede iniciarse desde la línea de comandos. El cuadro de diálogo solo le permite especificar los parámetros de análisis en la cómoda interfaz gráfica.

Primero, seleccione las áreas de su equipo que le gustaría escanear. Puede decidir entre el ***Análisis completo del equipo*** predeterminado o la opción ***Analizar carpetas o archivos seleccionados***. La tercera opción, el ***Análisis rápido***, inicia un análisis específico diseñado para el uso en modo seguro que inspecciona todas las áreas críticas de su equipo necesarias para el arranque.

La configuración de análisis de la siguiente sección le permite especificar los parámetros de análisis detallados. Todos están marcados de manera predeterminada y le recomendamos que lo mantenga así y solo anule la selección de un parámetro si tiene un motivo específico para hacerlo:

- ***Analizar "Aplicaciones potencialmente no deseadas"***: analizar spyware además de virus
- ***Analizar secuencias de datos alternativas (Solo NTFS)***: analizar las secuencias de datos alternativas en NTFS, es decir, una característica de Windows que puede usarse indebidamente por los hackers para ocultar datos, especialmente códigos maliciosos
- ***Reparar o eliminar infecciones automáticamente***: todas las detecciones posibles se procesan y se reparan o eliminan de su equipo automáticamente
- ***Analizar procesos activos***: analizar procesos y aplicaciones cargadas en la memoria del equipo
- ***Registro de análisis***: analizar el registro de Windows
- ***Habilitar comprobación Master Boot Record***: analizar la tabla de partición y el sector de arranque

Por último, en la parte inferior de este cuadro de diálogo puede especificar el nombre y el tipo de archivo para el informe de análisis.

8.3.4. Parámetros del análisis desde CMD

La lista que se presenta a continuación contiene todos los parámetros disponibles de análisis desde la línea de comandos:

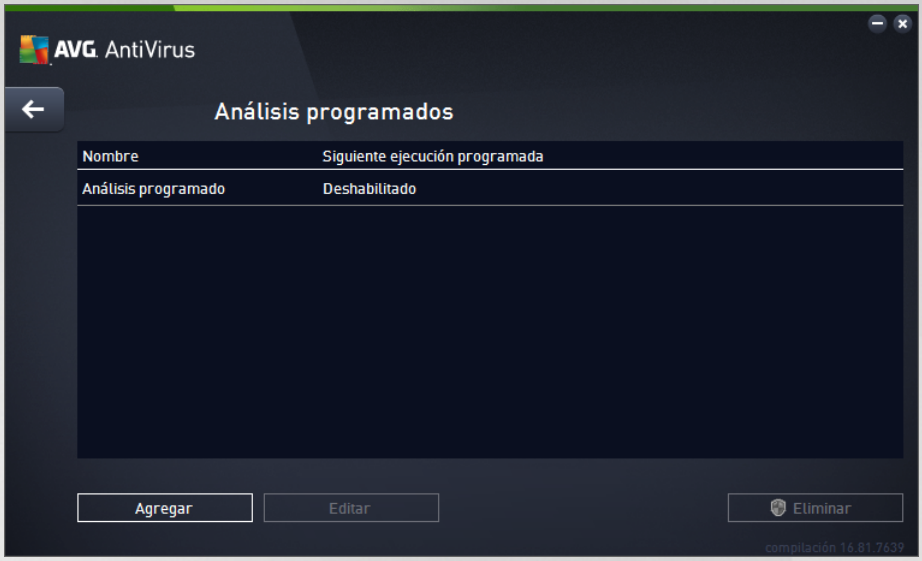
- /? Mostrar ayuda sobre este tema
- /@ Archivo de comando /nombre de archivo/
- /ADS Analizar secuencias de datos alternativas *(solo NTFS)*
- /ARC Analizar archivos comprimidos
- /ARCBOMBSW Informar de archivos repetidamente comprimidos
- /ARCBOMBSW Informar de bombas de archivos *(repetidamente comprimidos)*
- /BOOT Habilitar comprobación MBR/BOOT
- /BOOTPATH Iniciar QuickScan
- /CLEAN Limpiar automáticamente
- /CLOUDCHECK Comprobar si hay falsos positivos
- /COMP Análisis del equipo completo
- /COO Analizar cookies
- /EXCLUDE Excluir ruta o archivos del análisis
- /EXT Analizar estas extensiones *(por ejemplo, EXT=EXE,DLL)*
- /FORCESHUTDOWN Forzar el cierre del equipo al terminar el análisis
- /HELP Mostrar ayuda sobre este tema
- /HEUR Usar análisis heurístico
- /HIDDEN Informar de los archivos con extensión oculta
- /IGNLOCKED Ignorar archivos bloqueados
- /INFECTABLEONLY Analizar archivos con extensiones que puedan ser infectadas
- /LOG Generar un archivo de resultado del análisis
- /MACROW Informar de macros
- /NOBREAK No permitir CTRL-BREAK para anular

- /NOEXT No analizar estas extensiones *(por ejemplo, NOEXT=JPG)*
- /PRIORITY Establecer la prioridad del análisis *(Baja, Automática, Alta - consulte Configuración avanzada / Análisis)*
- /PROC Analizar procesos activos
- /PUP Informar de aplicaciones potencialmente no deseadas
- /PUPEXT Informar de conjunto mejorado de programas potencialmente no deseados
- /PWDW Informar de archivos protegidos por contraseña
- /QT Análisis rápido
- /REG Analizar el registro
- /REPAPPEND Añadir al archivo de informe
- /REPOK Informar de archivos no infectados como correctos
- /REPORT Informar en archivo *(nombre de archivo)*
- /SCAN Analizar archivos o carpetas específicos *(SCAN=path;path -e.g. /SCAN=C:\;D:\)*
- /SHUTDOWN Cerrar el equipo al terminar el análisis
- /THOROUGHSCAN Habilitar análisis completo
- /TRASH Mover archivos infectados al Almacén de virus

8.4. Programación de análisis

Con **AVG AntiVirus**, puede ejecutar análisis bajo demanda *(por ejemplo, si sospecha que puede haber una infección en el equipo)* o según una programación definida. Se recomienda encarecidamente que ejecute los análisis de manera programada; así podrá asegurarse de que el equipo está protegido contra cualquier posibilidad de infección y no tendrá que preocuparse por el análisis ni cuándo realizarlo. El Análisis completo del equipo debería ejecutarse regularmente, al menos una vez por semana. Sin embargo, de ser posible, lo ideal es realizar el análisis del equipo completo a diario, tal como lo establece la configuración predeterminada de la programación de análisis. Si el equipo está continuamente encendido, los análisis se pueden programar para que se realicen fuera de las horas de trabajo. Si el equipo se apaga en ocasiones, entonces programe que los análisis se realicen al iniciar el equipo cuando se haya pasado por alto dicha tarea.

Se puede crear o editar un análisis programado en el cuadro de diálogo ***Análisis programados*** al que se accede a través del botón ***Gestionar análisis programados*** en el cuadro de diálogo Opciones de análisis. En el nuevo cuadro de diálogo ***Análisis programados*** puede ver información general completa de todos los análisis programados actualmente:

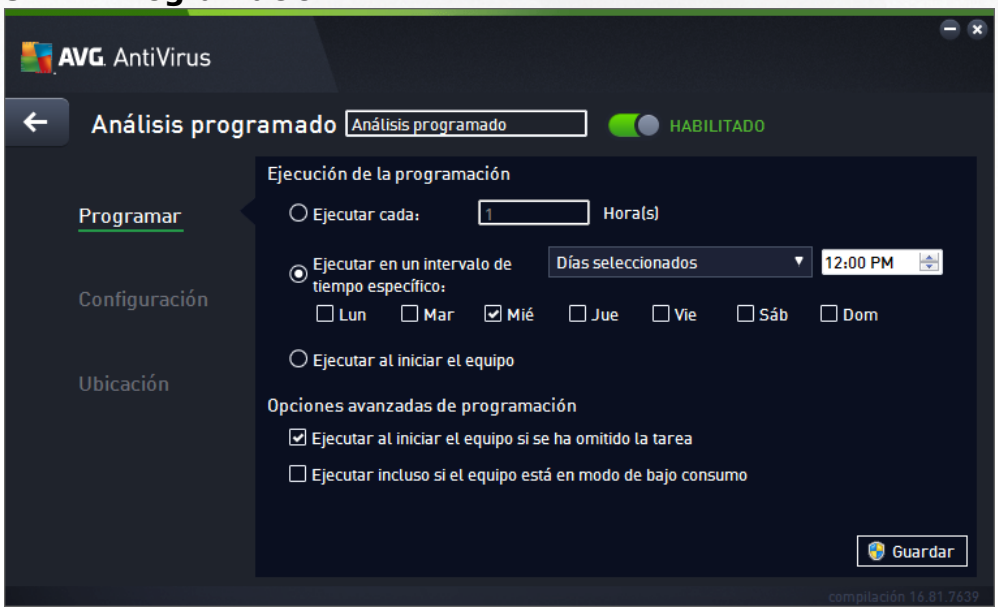


En el cuadro de diálogo puede especificar sus propios análisis. Utilice el botón ***Programar análisis*** para crear una nueva programación de análisis propia. Es posible editar los parámetros del análisis programado (*o configurar una nueva programación*) en tres fichas:

- Programación
- Configuración
- Ubicación

En cada ficha puede cambiar fácilmente el botón de "semáforo"  para desactivar el análisis programado de forma temporal y activarlo de nuevo cuando sea necesario.

8.4.1. Programación



En la parte superior de la ficha ***Programaciones*** puede encontrar el campo de texto donde puede especificar el nombre del análisis programado definido actualmente. Trate de usar siempre nombres breves, descriptivos y adecuados para los análisis con el objeto de facilitar su reconocimiento posterior. Por ejemplo: no resulta apropiado llamar al análisis "Análisis nuevo" o "Mi análisis" puesto que estos nombres no hacen referencia a lo que realmente se comprueba en el análisis. En cambio, un ejemplo de un buen nombre descriptivo podría ser "Análisis del área del sistema", etc.

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

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

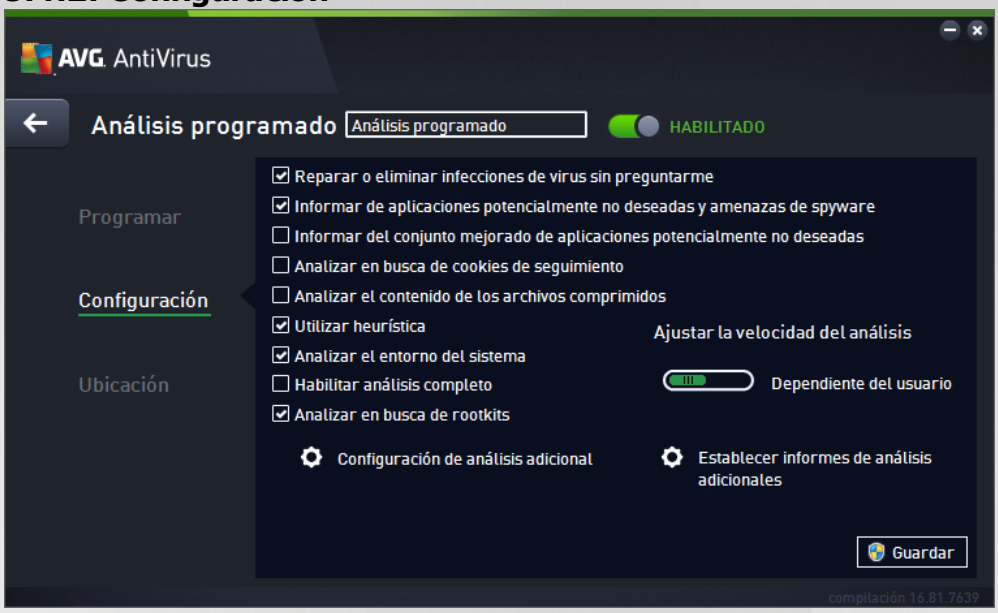
- ***Opciones avanzadas de programación***: esta sección permite definir bajo qué condiciones deberá iniciarse o no el análisis si el equipo está en modo de bajo consumo o apagado completamente. Cuando se inicie el análisis programado en el momento especificado, se informará de este hecho mediante una ventana emergente que se abrirá sobre el icono de AVG en la bandeja del sistema. Aparecerá un nuevo icono de AVG en la bandeja del sistema (a todo color con una luz intermitente) que le informa de que se está ejecutando un análisis programado. Haga clic con el botón secundario sobre el icono de AVG del análisis que se está ejecutando para abrir un menú contextual en el que puede poner en pausa el análisis en curso e incluso detenerlo por completo, pudiendo también cambiar su prioridad.

Controles en el cuadro de diálogo

- ***Guardar***: guarda todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve a la vista genera de Análisis programados. Por ello, si desea configurar los parámetros del análisis en todas las fichas, pulse el botón para guardarlos únicamente después de haber especificado todos sus requisitos.

- **:** Use la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la vista general de Análisis programados.

8.4.2. Configuración



En la parte superior de la ficha ***Configuración*** puede encontrar el campo de texto donde puede especificar el nombre de la programación de análisis actualmente definida. Trate de usar siempre nombres breves, descriptivos y adecuados para los análisis con el objeto de facilitar su reconocimiento posterior. Por ejemplo: no resulta apropiado llamar al análisis "Análisis nuevo" o "Mi análisis" puesto que estos nombres no hacen referencia a lo que realmente se comprueba en el análisis. En cambio, un ejemplo de un buen nombre descriptivo podría ser "Análisis del área del sistema", etc.

En la ficha ***Configuración*** encontrará una lista de parámetros de análisis que pueden activarse o desactivarse de manera opcional. ***A menos que tenga un buen motivo para modificarla, se recomienda mantener la configuración predefinida***:

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

- ***Informar de aplicaciones potencialmente no deseadas y amenazas de spyware*** *(activado de manera predeterminada):* marque esta opción para activar el análisis en busca de spyware y de virus. El spyware representa una categoría dudosa de software malicioso: aunque generalmente supone un riesgo de seguridad, algunos de estos programas se pueden instalar voluntariamente. Recomendamos que mantenga activada esta característica ya que aumenta la seguridad del equipo.

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

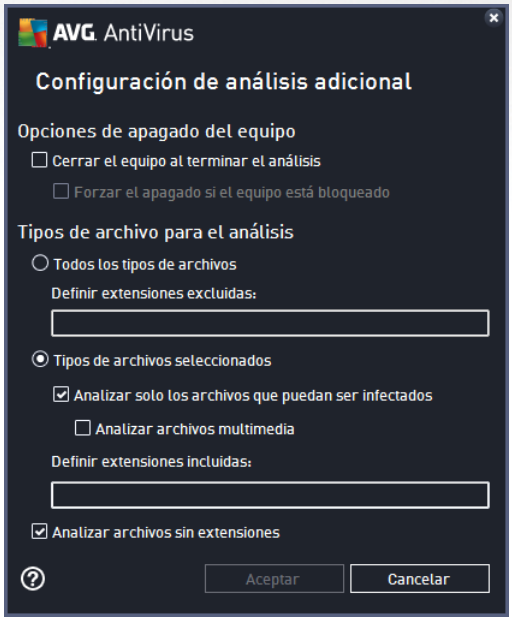
- ***Analizar en busca de cookies de seguimiento*** (*desactivado de manera predeterminada*): este parámetro especifica que deben detectarse cookies durante el análisis; (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica sobre los usuarios, como sus*

preferencias de Internet o el contenido de sus carros de compra electrónicos).

- ***Analizar el contenido de los archivos comprimidos*** (*desactivado de manera predeterminada*): este parámetro especifica que se deben analizar todos los archivos, incluso si se encuentran dentro de archivos comprimidos, por ejemplo, ZIP, RAR, etc.
- ***Utilizar heurística*** (*activado de manera predeterminada*): el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos utilizados para detectar virus durante el análisis.
- ***Analizar el entorno del sistema*** (*activado de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- ***Habilitar análisis completo*** (*desactivado de manera predeterminada):* en determinadas situaciones (*si sospecha que su equipo está infectado*), puede marcar esta opción para activar los algoritmos de análisis más detallados, que analizarán incluso las áreas del equipo que rara vez se infectan, simplemente para estar absolutamente seguro. Recuerde, sin embargo, que este método tiene una duración considerable.
- ***Analizar en busca de rootkits*** *(activado de manera predeterminada):* el análisis anti-rootkit busca posibles rootkits en el equipo (por ejemplo, programas y tecnologías que pueden encubrir una actividad de software malicioso en el sistema). Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, determinados controladores o secciones de aplicaciones normales se pueden detectar erróneamente como rootkits.

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***: indique si el equipo debe cerrarse automáticamente al finalizar la ejecución del proceso de análisis. Una vez confirmada esta opción *(Cerrar el equipo al terminar el*

análisis), se activa una nueva opción que permite apagar el equipo aunque esté bloqueado *(Forzar el apagado si el equipo está bloqueado)*.

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

Ajustar la velocidad del análisis

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

Establecer informes de análisis adicionales

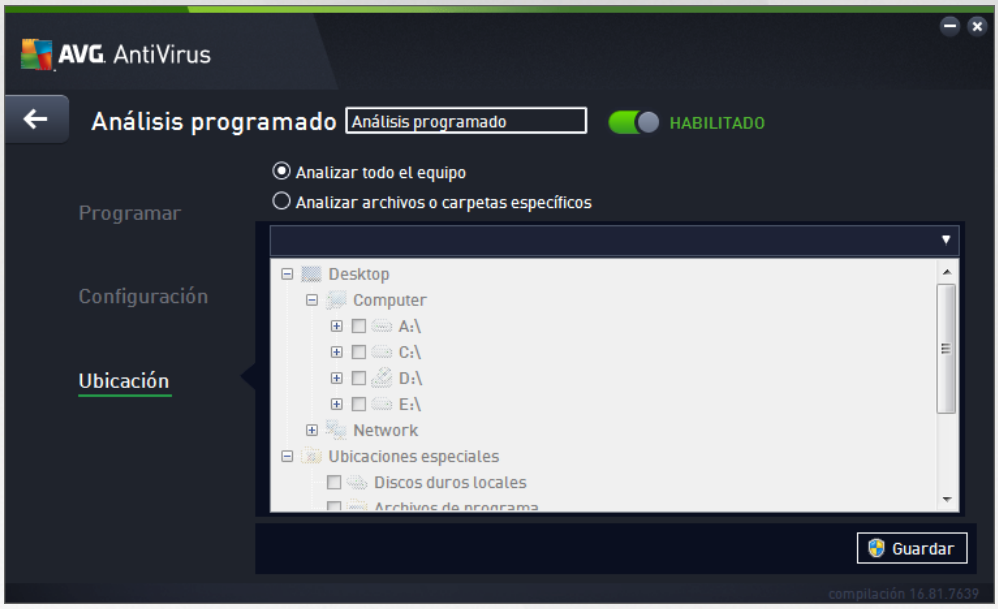
Haga clic en el vínculo ***Establecer informes de análisis adicionales...*** para abrir una nueva ventana de cuadro de diálogo independiente llamada ***Informes de análisis***, en la que puede marcar diferentes elementos para definir qué resultados del análisis deben incluirse en el informe:

Controles en el cuadro de diálogo

- ***Guardar***: guarda todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve a la vista genera de Análisis programados. Por ello, si desea configurar los parámetros del análisis en todas las fichas, pulse el botón para guardarlos únicamente después de haber especificado todos sus requisitos.

- : Use la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la vista general de Análisis programados.

8.4.3. Ubicación



En la ficha ***Ubicación*** se puede definir si se desea programar el análisis del equipo completo o el análisis de archivos o carpetas específicos. En caso de que se seleccione el análisis de archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activa la estructura de árbol mostrada, pudiéndose especificar las carpetas a analizar (*expanda los elementos haciendo clic en el nodo con el signo más hasta que encuentre la carpeta que desea analizar*). Puede seleccionar varias carpetas activando sus casillas correspondientes. Las carpetas seleccionadas aparecerán en el campo de texto, en la parte superior del cuadro de diálogo, y el menú desplegable conservará el historial del análisis seleccionado para su posterior uso. Como alternativa, puede introducir manualmente la ruta completa de la carpeta deseada (*si introduce varias rutas, es necesario separarlas con punto y coma, sin espacios adicionales*).

En la estructura del árbol también existe una rama denominada ***Ubicaciones especiales***. A continuación se ofrece una lista de ubicaciones que se analizarán cuando se marque la correspondiente casilla de verificación:

- ***Discos duros locales***: todos los discos duros del equipo

- ***Archivos de programa***

    - C:\Archivos de programa\

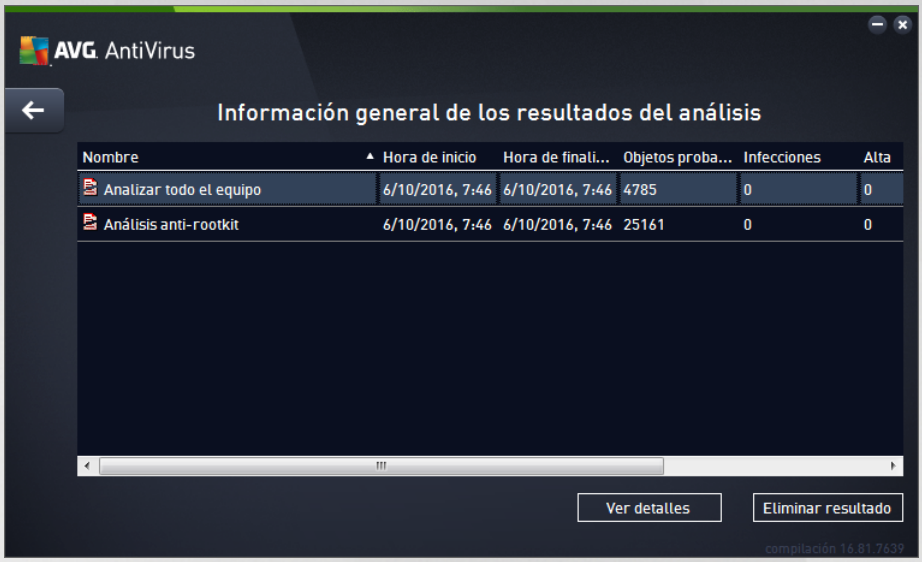
    - *en versiones de 64 bits* C:\Archivos de programa (x86)

- ***Carpeta Mis documentos***
    - *para Windows XP:* C:\Documents and Settings\Default User\Mis documentos\
    - *para Windows Vista/7*: C:\Usuarios\usuario\Documentos\
- ***Documentos compartidos***
    - *para Windows XP*: C:\Documents and Settings\All Users\Documentos compartidos\
    - *para Windows Vista/7*: C:\Usuarios\Acceso público\Documentos públicos\
- ***Carpeta de Windows***: C:\Windows\
- ***Otros***
    - *Unidad del sistema*: la unidad de disco duro en la que está instalado el sistema operativo (generalmente C:)
    - *Carpeta del sistema*: C:\Windows\System32\
    - *Carpeta de archivos temporales*: C:\Documents and Settings\usuario\Configuración local\ (*Windows XP*) o C:\Usuarios\usuario\AppData\Local\Temp\ (*Windows Vista/7*)
    - *Archivos temporales de Internet*: C:\Documents and Settings\usuario\Configuración local \Archivos temporales de Internet\ (*Windows XP*) o C:\Usuarios\usuario\AppData\Local \Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Controles en el cuadro de diálogo

- ***Guardar***: guarda todos los cambios efectuados en esta ficha o en cualquier otra ficha de este cuadro de diálogo y vuelve a la vista genera de Análisis programados. Por ello, si desea configurar los parámetros del análisis en todas las fichas, pulse el botón para guardarlos únicamente después de haber especificado todos sus requisitos.
- : Use la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la vista general de Análisis programados.

8.5. Resultados del análisis



El cuadro de diálogo ***Información general de resultados del análisis*** proporciona una lista de resultados de todos los análisis ejecutados hasta el momento. La tabla proporciona la siguiente información sobre 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 completado
  - o No se encontraron infecciones, el análisis se interrumpió antes de terminar
  - o Infecciones encontradas y no reparadas, análisis completado
  - o Infecciones encontradas y no reparadas, el análisis se interrumpió antes de terminar
  - o Infecciones encontradas y reparadas o eliminadas, análisis completado
  - o Infecciones encontradas y reparadas o eliminadas, el análisis se interrumpió antes de terminar
- ***Nombre***: la columna proporciona el nombre del respectivo análisis. Se tratará de uno de los dos análisis predefinidos o de un análisis programado propio.
- ***Hora de inicio***: muestra la fecha y hora exactas de inicio del análisis.
- ***Hora de finalización***: muestra la fecha y hora exactas de finalización, pausa o interrupción del análisis.
- ***Objetos probados***: proporciona el número total de objetos analizados.
- ***Infecciones***: muestra el número de infecciones encontradas eliminadas/totales.

- ***Alta / Media / Baja***: las siguientes tres columnas indican el número de infecciones encontradas según su gravedad (alta, media y baja).
- ***Rootkits***: proporciona el número total de rootkits encontrados durante el análisis.

Controles del cuadro de diálogo

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

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

: use la flecha verde en la sección superior izquierda del cuadro de diálogo para volver atrás en la interfaz principal de usuario con la información general del componente.

8.6. Detalles de los resultados del análisis

Para abrir una vista con la información detallada de un resultado de análisis seleccionado, haga clic en el botón ***Ver detalles*** disponible en el cuadro de diálogo Información general de resultados del análisis. Será redirigido a la misma interfaz de diálogo que describe detalladamente la información sobre un resultado de análisis. La información se divide en tres fichas:

- ***Resumen***: en esta ficha se ofrece información básica sobre el análisis, como si se completó correctamente, si se detectaron amenazas y qué sucedió con ellas.
- ***Detalles***: en esta ficha se muestra toda la información sobre el análisis, incluidos los detalles sobre las amenazas detectadas. Exportar la información general a un archivo le permite guardar el resultado del análisis en forma de archivo .csv.
- ***Detecciones:*** en este ficha solo se muestra si durante el análisis se detectaron amenazas, y proporciona información detallada sobre ellas:

  Gravedad de tipo información: información o advertencias. No hay una verdadera amenaza. Normalmente documentos que contienen macros, documentos o archivos protegidos con una contraseña, archivos bloqueados, etc.

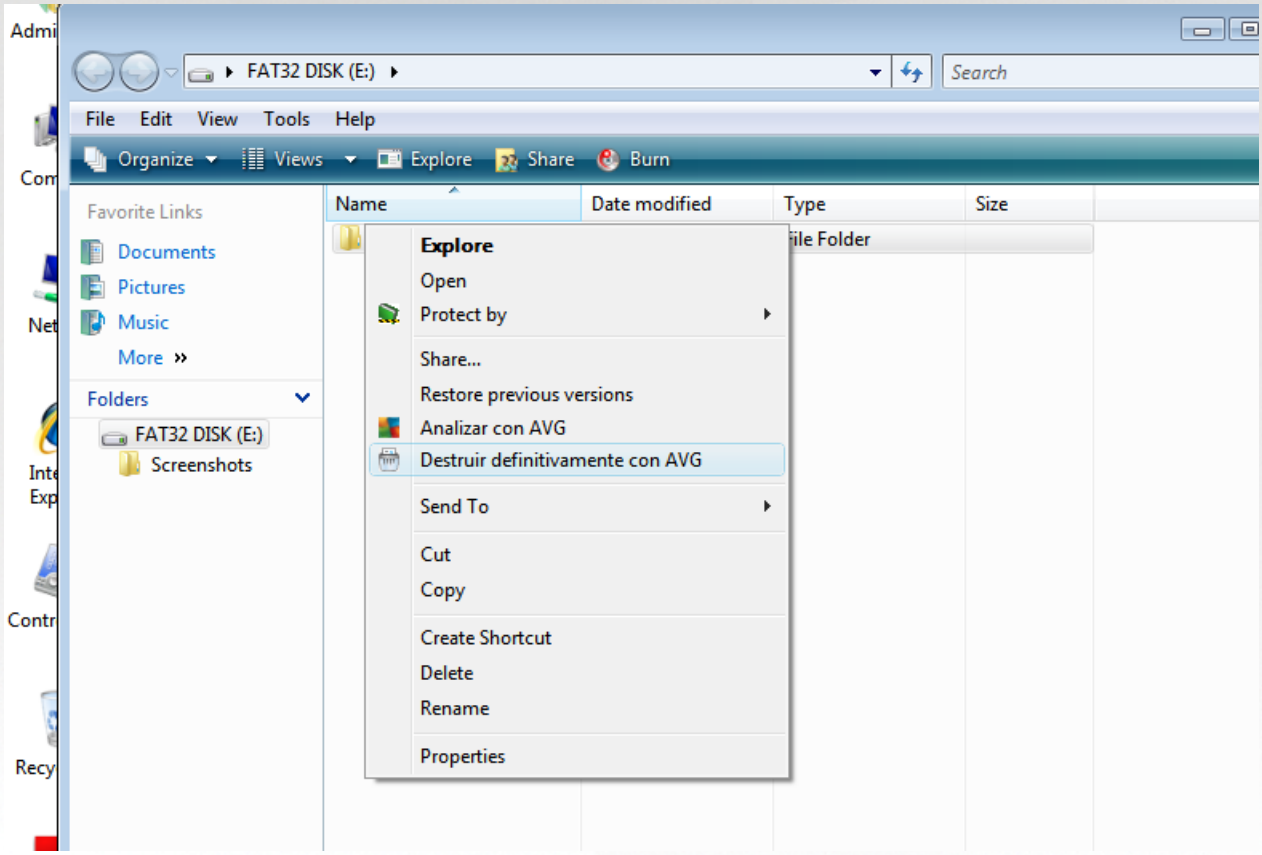
  Gravedad media: normalmente programas potencialmente no deseados *(como adware)* o cookies de seguimiento.

  Gravedad alta: amenazas graves como virus, troyanos, ataques de vulnerabilidad, etc. Asimismo, objetos detectados con el método de detección heurístico, es decir, amenazas aún no incluidas en la base de datos de virus.

9. AVG File Shredder

AVG File Shredder se ha diseñado para eliminar archivos con total seguridad, es decir, de forma que no puedan recuperarse, ni siquiera con herramientas de software avanzadas diseñadas para este fin.

Para destruir un archivo o una carpeta, haga clic con el botón derecho en él en el administrador de archivos *(Explorador de Windows, Total Commander, etc.)* y seleccione ***Destruir definitivamente con AVG*** en el menú contextual. Los archivos de la papelera también se pueden destruir. Si un archivo concreto de una ubicación específica *(p. ej. el CD-ROM)* no se puede destruir de manera fiable, se le notificará o la opción del menú contextual no estará disponible.



Tenga siempre en cuenta: Una vez que haya destruido un archivo, no podrá volver a recuperarlo.

10. Almacén de virus

El ***Almacén de virus*** es un entorno seguro para la gestión de objetos sospechosos o infectados detectados en los análisis de AVG. Cuando se detecta un objeto infectado durante el análisis y AVG no puede repararlo automáticamente, se le solicita que decida lo que se hará con el objeto sospechoso. La acción recomendada es mover el archivo infectado al ***Almacén de virus*** para su posterior tratamiento. La finalidad principal del ***Almacén de virus*** es guardar cualquier archivo eliminado durante un tiempo determinado para que pueda asegurarse de que ya no lo necesita en su ubicación original. Si observa que la ausencia del archivo causa problemas, puede enviar el archivo en cuestión para que sea analizado o restaurarlo a la ubicación original.

La interfaz del ***Almacén de virus*** se abre en una ventana independiente y ofrece información general de los objetos infectados puestos en cuarentena:

- ***Fecha de adición***: fecha y hora en la que se detectó y se movió al Almacén de virus el archivo sospechoso.
- ***Amenaza***: en caso de que decida instalar el componente de Identidad con su **AVG AntiVirus**, se le proporcionará una identificación gráfica de la severidad de la búsqueda en esta sección: desde "sin problemas" *(con tres puntos verdes)* hasta "muy peligroso" *(con tres puntos rojos)*. También podrá encontrar información sobre el tipo de infección y su localización original. El enlace *Más información* lleva a una página con información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Origen***: especifica qué componente de **AVG AntiVirus** ha detectado la amenaza correspondiente.
- ***Notificaciones***: esporádicamente se pueden generar algunas notas en esta columna que proporcionan comentarios detallados sobre la correspondiente amenaza detectada.

Botones de control

En la interfaz del ***Almacén de virus*** están disponibles los siguientes botones de control:

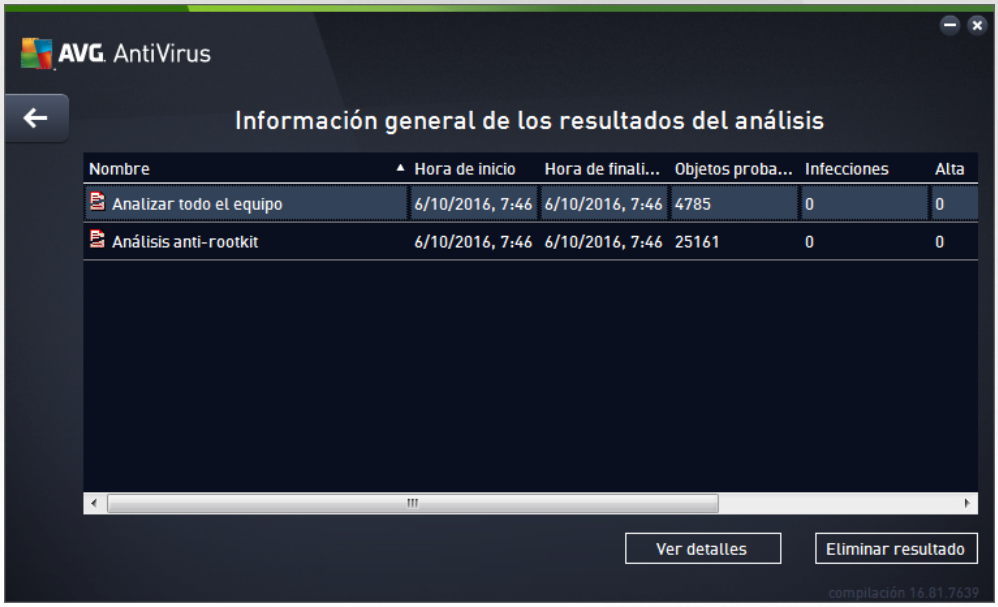
- ***Restaurar***: vuelve a colocar el archivo infectado en su ubicación original en el disco.
- ***Restaurar como***: mueve el archivo infectado a una carpeta seleccionada.
- ***Enviar a analizar***: el botón sólo se activa cuando selecciona un objeto en la lista de detecciones superior. En tal caso, tiene la opción de enviar la detección seleccionada al laboratorio de virus de AVG para que realice un análisis en mayor detalle. Tenga en cuenta que esta característica solo sirve para enviar falsos positivos, es decir, archivos que ha detectado como infectados o sospechosos, pero que en realidad cree que son inofensivos.
- ***Detalles***: para obtener información detallada sobre una amenaza específica del ***Almacén de virus*** destaque 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***: quita el archivo infectado del ***Almacén de virus*** de manera completa e irreversible.
- ***Vaciar Almacén***: quita todo el contenido del ***Almacén de virus*** completamente. Al quitar los archivos del ***Almacén de virus***, desaparecen del disco de manera irreversible (*no se mueven a la Papelera de reciclaje*).

11. Historial

La sección ***Historial*** incluye información sobre todos los eventos ya transcurridos *(como actualizaciones, análisis, detecciones, etc.)* e informes sobre estos eventos. Esta sección está disponible desde la interfaz de usuario principal a través del elemento ***Opciones / Historial***. Además, el historial de todos los eventos se divide en las siguientes partes:

- Resultados del análisis
- Resultados de Resident Shield
- Resultados de protección del correo electrónico
- Resultados de Online Shield
- Historial de eventos

11.1. Resultados del análisis



El cuadro de diálogo ***Información general de resultados del análisis*** está disponible a través del elemento de menú ***Opciones / Historial / Resultados del análisis*** en la línea superior de navegación de la ventana principal de **AVG AntiVirus**. Este cuadro de diálogo muestra una lista de todos los análisis realizados anteriormente e información sobre sus resultados:

- ***Nombre***: designación del análisis; puede ser el nombre de uno de los análisis predefinidos o un nombre que el usuario le haya dado a su análisis programado personalizado. Cada uno de los nombres incluye un icono que indica el resultado del análisis:

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

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

 - el icono rojo advierte que se detectó una infección durante el análisis y que no fue posible eliminarla

Los iconos pueden ser de un solo color o estar divididos en dos partes: un icono de un solo color indica que el análisis se completó correctamente; un icono de dos colores indica que el análisis se canceló o se interrumpió.

Nota: *Nota: para ver información detallada sobre cada análisis, abra el cuadro de diálogo Resultados del análisis, al que puede acceder mediante el botón Ver detalles (ubicado en la parte inferior de este cuadro de diálogo).*

- ***Hora de inicio***: fecha y hora en que se inició el análisis
- ***Hora de finalización***: fecha y hora en que finalizó el análisis
- ***Objetos probados***: número de objetos que se comprobaron durante el análisis
- ***Infecciones***: número de infecciones de virus detectadas / eliminadas
- ***Alta / Media***: estas columnas indican el número de infecciones encontradas/eliminadas de gravedad alta y media, respectivamente
- ***Información***: información relacionada con el transcurso y resultado del análisis *(por lo general, con su finalización o interrupción)*
- ***Rootkits***: número de rootkits detectados

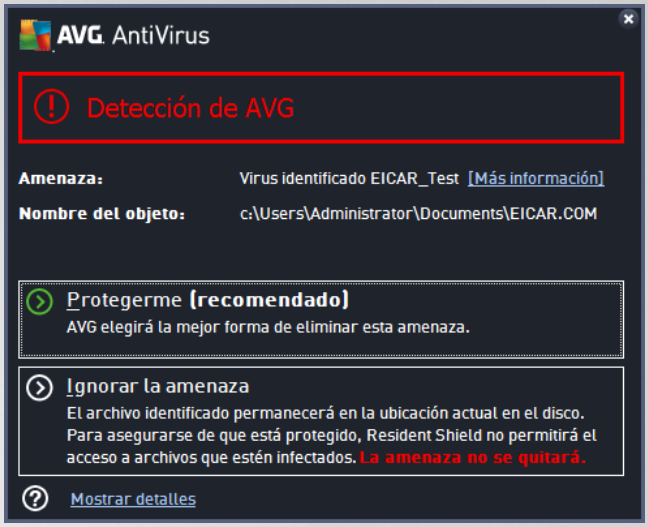
Botones de control

Los botones de control del cuadro de diálogo ***Información general de los resultados del análisis*** son los siguientes:

- ***Ver detalles***: pulse este botón para pasar al cuadro de diálogo Resultados del análisis, donde podrá ver datos detallados sobre el análisis seleccionado
- ***Eliminar resultado***: pulse este botón para eliminar el elemento seleccionado de la información general de los resultados del análisis
- : para volver al cuadro de diálogo principal predeterminado de AVG *(información general de los componentes),* utilice la flecha de la esquina superior izquierda de este cuadro de diálogo

11.2. Resultados de Resident Shield

El servicio ***Resident Shield*** es una parte del componente ***Equipo*** y analiza archivos copiados, abiertos o guardados. Cuando se detecte un virus o cualquier otro tipo de amenaza, se le notificará inmediatamente mediante el siguiente cuadro de diálogo:



En este cuadro de advertencia encontrará información sobre el objeto detectado y asignado como infectado (*Amenaza*) y algunos hechos descriptivos sobre la infección reconocida (*Descripción*). El enlace de *Más información* le lleva a una página que ofrece información detallada sobre las amenazas detectadas dentro de la enciclopedia de virus en línea, si éstas son conocidas. En el cuadro de diálogo, también podrá ver información general de las soluciones disponibles para tratar la amenaza detectada. Una de las alternativas será etiquetarla tal y como se recomienda: ***Protégeme (recomendado). Si es posible, debería decantarse siempre por esta opción.***

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

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

Dentro del cuadro de diálogo ***Detección de Resident Shield*** hay una lista de todas las detecciones de Resident Shield de las que se puede obtener una descripción general. El cuadro de diálogo está disponible a través del menú ***Opciones / Historial / Detección de Resident Shield*** en la línea superior de navegación de la ventana principal de **AVG AntiVirus**. El cuadro de diálogo ofrece información general de los objetos que detectó Resident Shield, que se evaluaron como peligrosos y que se repararon o movieron al Almacén de virus.

Para cada objeto detectado, se proporciona la siguiente información:

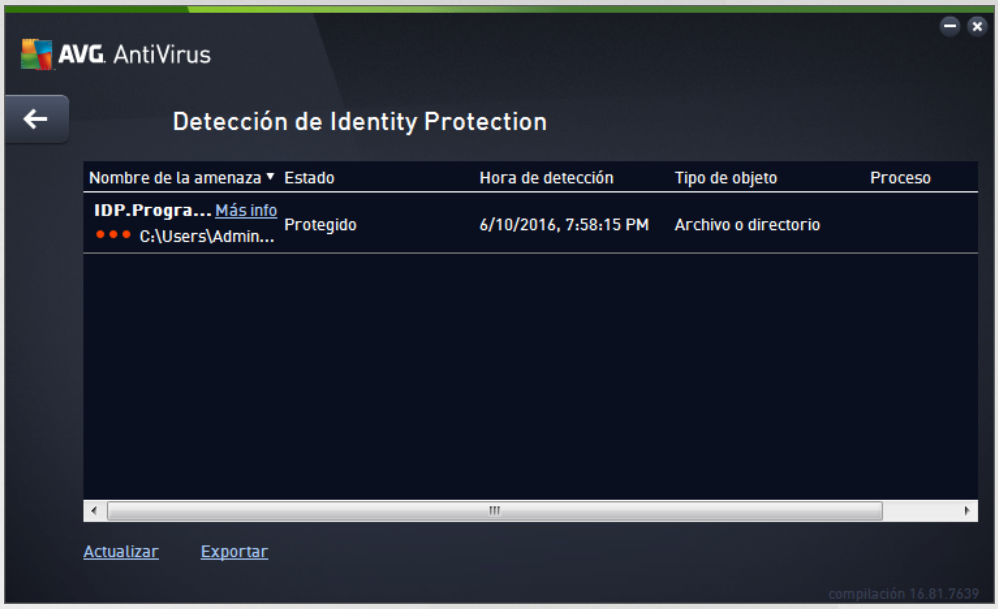
- ***Nombre de la amenaza***: descripción (*posiblemente incluso el nombre*) del objeto detectado y su ubicación. El enlace *Más información* lleva a una página con información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Estado***: acción realizada con el objeto detectado
- ***Hora de detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: la acción que se realizó para activar el objeto potencialmente peligroso y así hacer que fuese detectado

Botones de control

- ***Actualizar***: actualiza la lista de resultados detectados por ***Online Shield***
- ***Exportar***: exporta la lista completa de los objetos detectados a un archivo
- ***Quitar seleccionados***: en la lista puede resaltar registros seleccionados y utilizar este botón para eliminar únicamente los elementos elegidos
- ***Quitar todas las amenazas***: utilice el botón para borrar todos los registros de la lista en este cuadro de diálogo
- : para volver al cuadro de diálogo principal predeterminado de AVG *(información general de los componentes),* utilice la flecha de la esquina superior izquierda de este cuadro de diálogo

11.3. Resultados de Identity Protection

El cuadro de diálogo ***Resultados de Identity Protection*** está disponible a través del menú ***Opciones / Historial / Resultados de Identity Protection*** en la línea superior de navegación de la ventana principal de **AVG AntiVirus**.



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

- ***Nombre de la amenaza***: descripción *(posiblemente incluso el nombre)* del objeto detectado y su ubicación. El enlace *Más información* lleva a una página con información detallada sobre la amenaza detectada dentro de la enciclopedia de virus en línea.
- ***Estado***: acción realizada con el objeto detectado
- ***Hora de detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: la acción que se realizó para activar el objeto potencialmente peligroso y así hacer que fuese detectado

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

Botones de control

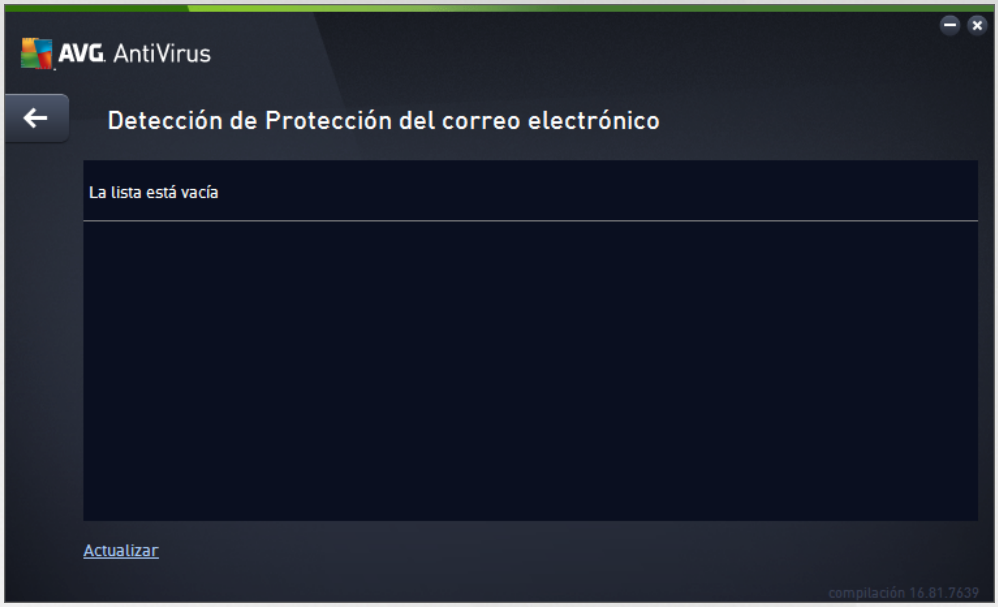
Los botones de control disponibles en la interfaz de ***Resultados de Identity Protection*** son los siguientes:

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

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

11.4. Resultados de Protección del correo electrónico

El cuadro de diálogo ***Resultados de Protección del correo electrónico*** está disponible a través del menú ***Opciones / Historial / Resultados de Protección del correo electrónico*** en la línea superior de navegación de la ventana principal de **AVG AntiVirus**.



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

- ***Nombre de detección***: descripción *(posiblemente incluso el nombre)* del objeto detectado y su origen.
- ***Resultado***: acción realizada con el objeto detectado
- ***Hora de detección***: fecha y hora en que se detectó el objeto sospechoso
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: la acción que se realizó para activar el objeto potencialmente peligroso y así hacer que fuese detectado

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

Botones de control

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

siguientes:

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

11.5. Resultados de Online Shield

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

En este cuadro de diálogo de advertencia encontrará información sobre el objeto detectado e identificado como infectado (*Amenaza*) y algunos hechos descriptivos sobre la infección reconocida (*Nombre del objeto*). El vínculo *Más información* le redirigirá a la enciclopedia de virus en línea, donde puede encontrar información detallada sobre la infección detectada, en caso de que se conozca. El cuadro de diálogo incluye los siguientes elementos de control:

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

La página web sospechosa no se abrirá y la detección de amenaza se registrará en la lista de ***Resultados de Online Shield***. El cuadro de diálogo está disponible a través del menú del elemento ***Opciones / Historial / Resultados de Online Shield*** en la línea superior de navegación de la ventana principal de **AVG AntiVirus** .

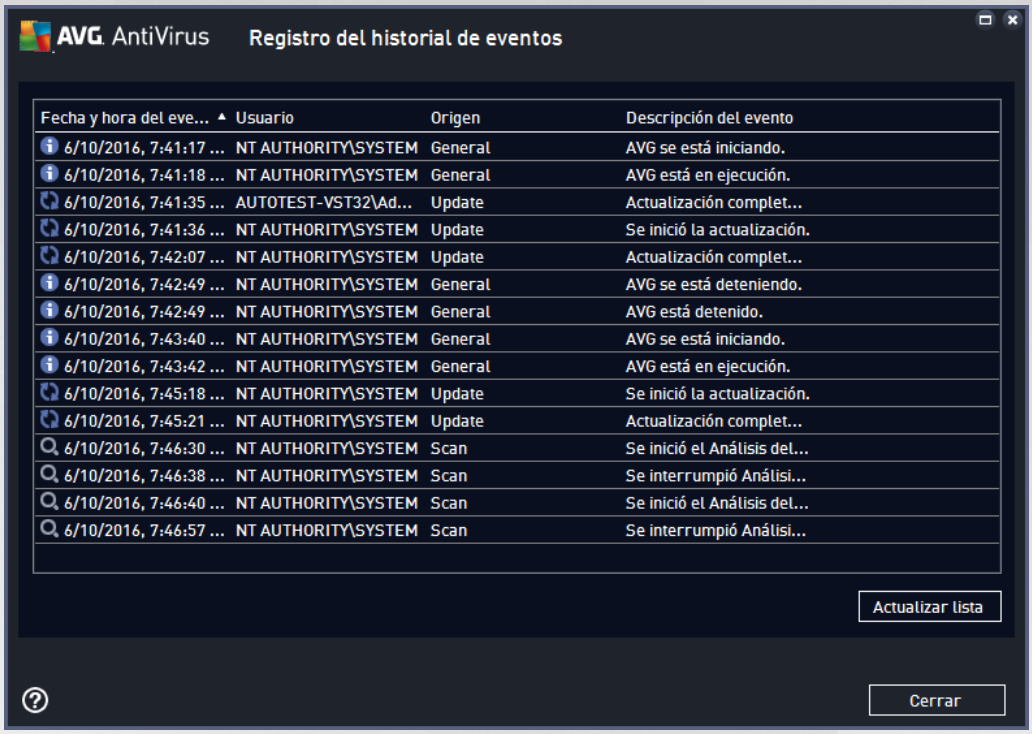
Para cada objeto detectado, se proporciona la siguiente información:

- ***Nombre de la amenaza***: descripción (*nombre posible*) del objeto detectado y su fuente (*página web*); el enlace de *Más información* le lleva a una página que ofrece información detallada sobre las amenazas detectadas dentro de la enciclopedia de virus en línea.
- ***Estado***: acción realizada con el objeto detectado
- ***Hora de detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de objeto***: tipo del objeto detectado

Botones de control

- ***Actualizar***: actualiza la lista de resultados detectados por ***Online Shield***
- ***Exportar***: exporta la lista completa de los objetos detectados a un archivo
- ←: para volver al cuadro de diálogo principal predeterminado de AVG *(información general de los componentes),* utilice la flecha de la esquina superior izquierda de este cuadro de diálogo

11.6. Historial de eventos



El cuadro de diálogo ***Historial de eventos*** está disponible a través del menú ***Opciones / Historial / Historial de eventos*** en la línea superior de navegación de la **AVG AntiVirus** ventana principal. En este cuadro de diálogo puede encontrar un resumen de los eventos más importantes que ocurrieron durante el funcionamiento de **AVG AntiVirus**. El cuadro de diálogo proporciona registros de los diferentes tipos de eventos: información acerca de las actualizaciones de la aplicación de AVG; información sobre el inicio, finalización o detención del análisis (*incluyendo pruebas ejecutadas automáticamente*); información sobre los eventos conectados con la detección de virus (*tanto por Resident Shield como por el análisis*), incluida la ubicación del incidente, y otros eventos importantes.

De cada evento se ofrece la siguiente información:

- ***Fecha y hora del evento*** proporciona la fecha y hora exactas en que ocurrió el evento.
- ***Usuario*** indica el nombre del usuario conectado en el momento en que ocurrió el evento.
- ***Origen*** proporciona información sobre el componente de origen u otra parte del sistema de AVG que provocó el evento.
- ***Descripción del evento*** proporciona un breve resumen de lo que ha sucedido en realidad.

Botones de control

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

12. Actualizaciones de AVG

Ningún software de seguridad puede garantizar una verdadera protección contra los diversos tipos de amenazas a menos que se actualice regularmente. Los creadores de virus están siempre a la búsqueda de nuevos fallos que puedan aprovechar tanto del software como de los sistemas operativos. Cada día aparecen nuevos virus, nuevo software malicioso y nuevos ataques de piratas informáticos. Por esta razón, los fabricantes de software están continuamente publicando actualizaciones y parches de seguridad para solucionar las brechas que se descubren. Teniendo en cuenta las nuevas amenazas que emergen y la velocidad a la que se difunden, es absolutamente esencial que actualice **AVG AntiVirus** regularmente. La mejor solución es mantener la configuración predeterminada del programa, en la que está establecida la actualización automática. Tenga en cuenta que si la base de datos de virus de **AVG AntiVirus** no está actualizada, el programa no podrá detectar las últimas amenazas.

Es crucial actualizar regularmente la instalación de AVG. Las actualizaciones de las definiciones de virus esenciales deben ser diarias si es posible. Las actualizaciones del programa menos urgentes pueden hacerse semanalmente.

Para proporcionar la máxima seguridad disponible, **AVG AntiVirus** está definido de manera predeterminada para buscar actualizaciones de bases de datos de virus nuevas cada cuatro horas. Puesto que las actualizaciones de AVG no se publican en función de un calendario fijo, sino como respuesta al volumen y a la gravedad de las nuevas amenazas, esta comprobación es fundamental para asegurarse de que la base de datos de virus de AVG se encuentra actualizada en todo momento.

Si desea comprobar si hay nuevos archivos de actualización inmediatamente, utilice el vínculo rápido Actualizar ahora en la interfaz de usuario principal. Este vínculo está disponible en todo momento desde cualquier cuadro de diálogo de la interfaz de usuario. Una vez iniciada la actualización, AVG verificará primero si hay nuevos archivos de actualización disponibles. Si es así, **AVG AntiVirus** comienza a descargarlos e inicia el proceso de actualización en sí. Se le informará sobre los resultados de la actualización en el cuadro de diálogo deslizante situado sobre el icono de bandeja del sistema de AVG.

En caso de que desee reducir el número de inicios de la actualización, puede configurar sus propios parámetros para este proceso. En cualquier caso, ***se recomienda encarecidamente que se inicie la actualización al menos una vez al día.*** La configuración puede editarse desde la sección Configuración avanzada/Programaciones, específicamente en los cuadros de diálogo siguientes:

- Programación de actualización de definiciones

13. Preguntas más frecuentes y soporte técnico

Si tiene algún problema administrativo o técnico con su aplicación **AVG AntiVirus**, existen varias formas de obtener ayuda. Elija entre las siguientes opciones:

- ***Obtener soporte***: en la propia aplicación AVG puede acceder a una página de atención al cliente del 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 diversas opciones de asistencia disponibles. Para continuar, siga las instrucciones de la página web.

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

- ***Resolución de problemas en el archivo de ayuda***: se encuentra disponible una nueva sección de ***resolución de problemas*** disponible directamente en el archivo de ayuda incluido con **AVG AntiVirus** *(para abrir este archivo, presione la tecla F1 en cualquier cuadro de diálogo de la aplicación)*. Esta sección proporciona una lista de las situaciones que ocurren más frecuentemente cuando un usuario desea buscar ayuda profesional para un problema técnico. Seleccione la situación que mejor describa el problema y haga clic en ella para abrir instrucciones detalladas que llevan a su solución.

- ***Centro de soporte del sitio de AVG***: también puede buscar la solución a su problema en el sitio web de AVG (*http://www.avg.com/*). En la ***Sección*** de ayuda puede encontrar información de grupos temáticos centrados en las ventas y los aspectos técnicos, una sección estructurada de preguntas más frecuentes y todos los contactos dispoibles.

- ***AVG ThreatLabs***: hay un sitio web específico relacionado con AVG (*http://www.avg.com/about-viruses*) dedicado a temas de virus, que proporciona información general estructurada sobre las amenazas en línea. También puede encontrar instrucciones sobre cómo quitar virus y spyware, además de consejos para mantenerse protegido.

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