



AVG AntiVirus 2013

Manual del usuario

Revisión del documento 2013.11 (13.2.2013.)

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

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

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

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

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



Contenido

1. Introducción	5
2. Requisitos de instalación de AVG	6
2.1 Sistemas operativos compatibles	6
2.2 Requisitos mínimos y recomendados de hardware	6
3. Proceso de instalación de AVG	7
3.1 Bienvenido: Selección de idioma	7
3.2 Bienvenido: Contrato de licencia	8
3.3 Activar la licencia	9
3.4 Seleccionar el tipo de instalación	10
3.5 Opciones personalizadas	12
3.6 Instalar AVG Security Toolbar	12
3.7 Progreso de la instalación	14
3.8 La instalación se ha realizado correctamente	15
4. Después de la instalación	16
4.1 Registro del producto	16
4.2 Acceso a la interfaz del usuario	16
4.3 Análisis de todo el equipo	16
4.4 Análisis Eicar	16
4.5 Configuración predeterminada de AVG	17
5. Interfaz del usuario de AVG	18
5.1 Navegación superior	19
5.2 Información del estado de seguridad	24
5.3 Descripción general de los componentes	25
5.4 Mis aplicaciones	26
5.5 Analizar / Actualizar vínculos rápidos	26
5.6 Icono en la bandeja de sistema	27
5.7 Gadget de AVG	29
5.8 AVG Advisor	30
5.9 AVG Accelerator	31
6. Componentes de AVG	32
6.1 Equipo	32
6.2 Navegación web	33
6.3 Identidad	35



6.4 Correos electrónicos.....	37
6.5 Quick Tune.....	39
7. AVG Security Toolbar.....	41
8. AVG Do Not Track.....	43
8.1 Interfaz de AVG Do Not Track.....	43
8.2 Información sobre los procesos de seguimiento.....	45
8.3 Bloqueo de los procesos de seguimiento.....	46
8.4 Configuración de AVG Do Not Track.....	46
9. Configuración avanzada de AVG.....	48
9.1 Apariencia.....	48
9.2 Sonidos.....	51
9.3 Desactivar temporalmente la protección de AVG.....	52
9.4 Protección del equipo.....	53
9.5 Analizador de correos electrónicos.....	58
9.6 Protección de la navegación web.....	69
9.7 Identity Protection.....	72
9.8 Análisis.....	73
9.9 Programaciones.....	79
9.10 Actualizar.....	87
9.11 Excepciones.....	91
9.12 Bóveda de virus.....	93
9.13 Autoprotección AVG.....	94
9.14 Preferencias de privacidad.....	94
9.15 Ignorar estado de error.....	97
9.16 Advisor: Redes.....	98
10. Análisis de AVG.....	99
10.1 Análisis predefinidos.....	100
10.2 Análisis en el Explorador de Windows.....	108
10.3 Análisis desde línea de comandos.....	109
10.4 Programación de análisis.....	112
10.5 Resultados del análisis.....	120
10.6 Detalles de los resultados del análisis.....	121
11. Bóveda de virus.....	122
12. Historial.....	124



12.1 Resultados del análisis	124
12.2 Detección de la Protección residente.....	125
12.3 Detección de la Protección del correo electrónico.....	128
12.4 Hallazgos de Online Shield.....	129
12.5 Registro de historial de eventos.....	131
13. Actualizaciones de AVG.....	133
13.1 Ejecución de actualizaciones.....	133
13.2 Niveles de actualización.....	133
14. Preguntas frecuentes y soporte técnico.....	135



1. Introducción

Este manual de usuario proporciona documentación completa para el usuario relacionada con **AVG AntiVirus 2013**.

AVG AntiVirus 2013 ofrece protección en tiempo real contra las amenazas más sofisticadas. Puede conversar, descargar e intercambiar archivos con confianza; jugar juegos y mirar videos sin preocupaciones o interrupciones; descargar, compartir archivos y enviar mensajes de forma segura; disfrutar su vida en redes sociales, o navegar y buscar con la confianza de una protección en tiempo real.



2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG AntiVirus 2013 tiene como propósito proteger las estaciones de trabajo con los siguientes sistemas operativos:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 y x64, todas las ediciones)
- Windows 7 (x 86 y x64, todas las ediciones)
- Windows 8 (x32 y x64)

(y posiblemente Service Packs superiores para determinados sistemas operativos)

Nota: El componente [Identity](#) no es admitido en Windows XP x64. En este sistema operativo, puede instalar AVG AntiVirus 2013, pero sólo sin el componente IDP.

2.2. Requisitos mínimos y recomendados de hardware

Requisitos mínimos de hardware para **AVG AntiVirus 2013**:

- CPU Intel Pentium a 1.5 GHz o superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memoria RAM
- 1.3 GB de espacio libre en el disco duro (*para la instalación*)

Requisitos recomendados de hardware para **AVG AntiVirus 2013**:

- CPU Intel Pentium a 1.8 GHz o superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memoria RAM
- 1.6 GB de espacio libre en el disco duro (*para la instalación*)



3. Proceso de instalación de AVG

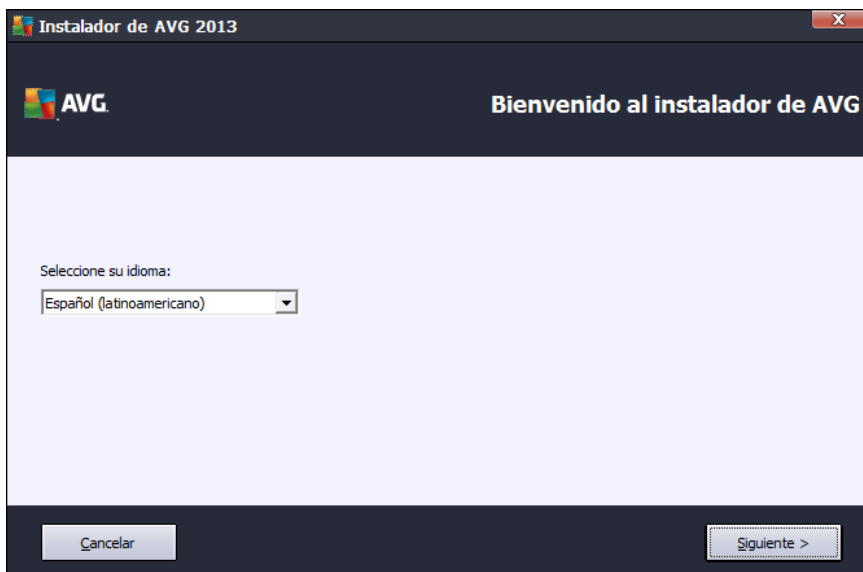
Para instalar **AVG AntiVirus 2013** en su equipo debe obtener el archivo de instalación más reciente. Para asegurarse de instalar la versión actualizada de **AVG AntiVirus 2013**, se recomienda que descargue el archivo de instalación del sitio web de AVG (<http://www.avg.com/>). La sección **Soporte / Descargas** proporciona una descripción general estructurada para cada edición de AVG.

Si tiene dudas sobre los archivos que necesita descargar e instalar, se recomienda que utilice el servicio **Seleccionar producto** en la parte inferior de la página web. Después de responder a tres preguntas sencillas, este servicio definirá los archivos exactos que necesita. Presione el botón **Continuar** para obtener acceso a una lista completa de archivos de descarga que se ajustan a sus necesidades personales.

Una vez que ha descargado y guardado el archivo de instalación en el disco duro, puede iniciar el proceso de instalación. La instalación es una secuencia de cuadros de diálogo sencillos y fáciles de entender. Cada cuadro de diálogo describe brevemente qué se debe hacer en cada paso del proceso de instalación. Ofrecemos una explicación detallada de cada ventana de diálogo a continuación:

3.1. Bienvenido: Selección de idioma

El proceso de instalación se inicia con el cuadro de diálogo **Bienvenido al instalador de AVG**:



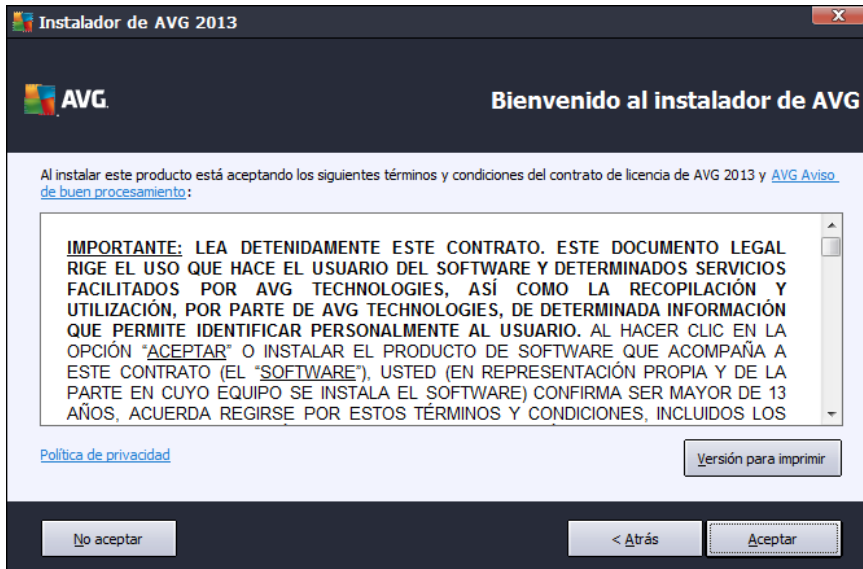
En este cuadro de diálogo puede seleccionar el idioma que se utilizará para el proceso de instalación. Haga clic en el cuadro combinado para desplegar el menú de idiomas. Seleccione el idioma que desee y el proceso de instalación seguirá en el idioma elegido.

Atención: en este momento sólo selecciona el idioma del proceso de instalación. La aplicación AVG AntiVirus 2013 se instalará en el idioma seleccionado, y en inglés, que siempre se instala automáticamente. No obstante, es posible instalar más idiomas y trabajar con AVG AntiVirus 2013 en cualquiera de ellos. Se le solicitará que confirme su selección completa de idiomas alternativos en uno de los siguientes cuadros de diálogo de configuración denominados [Opciones personalizadas](#).



3.2. Bienvenido: Contrato de licencia

El cuadro de diálogo *Bienvenido al instalador de AVG* proporciona el texto completo del contrato de licencia de AVG:



Lea atentamente el texto completo. Para confirmar que lo leyó, lo entendió y acepta el contrato, presione el botón **Aceptar**. Si no está conforme con el contrato de licencia, presione el botón **No aceptar** y el proceso de instalación se terminará de inmediato.

Política de privacidad de AVG

Además del contrato de licencia, este cuadro de diálogo de configuración también le ofrece la opción de obtener más información sobre el **Aviso de buen procesamiento de AVG**, la **Personalización de AVG** y la **Política de privacidad de AVG** (todas las funciones mencionadas se muestran en el cuadro de diálogo en la forma de un hipervínculo activo que lo lleva al sitio web dedicado donde podrá encontrar información detallada). Haga clic en el vínculo correspondiente para ir al sitio web de AVG (<http://www.avg.com/>) donde podrá encontrar el texto completo de estas declaraciones.

Botones de control

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

- **Versión para imprimir**: haga clic en el botón para mostrar el texto completo del contrato de licencia de AVG en una interfaz web, y bien organizado para imprimir.
- **No aceptar**: haga clic para rechazar el contrato de licencia. El proceso de configuración se cancelará inmediatamente. **AVG AntiVirus 2013** no se instalará.
- **Atrás**: haga clic para volver al cuadro de diálogo de configuración anterior.



- **Aceptar:** haga clic para confirmar que ha leído, comprendido y aceptado el contrato de licencia. La instalación continuará y avanzará un paso, al cuadro de diálogo de configuración siguiente.

3.3. Activar la licencia

En el cuadro de diálogo **Activar su licencia**, se le solicitará que ingrese su número de licencia en el campo de texto proporcionado:

Dónde encontrar el número de licencia

El número de venta se puede encontrar en el paquete del CD en la caja de **AVG AntiVirus 2013**. El número de licencia se encuentra en el correo electrónico de confirmación que recibió después de la compra en línea de **AVG AntiVirus 2013**. Debe escribir el número exactamente como se muestra. Si está disponible el formulario digital del número de licencia (*en el correo electrónico*), se recomienda utilizar el método de copiar y pegar para insertarlo.

Cómo utilizar el método de copiar y pegar

Si utiliza el método de **copiar y pegar** para especificar su número de licencia de **AVG AntiVirus 2013** en el programa, se asegurará de que el número se introduce correctamente. Por favor siga estos pasos:

- Abra el correo electrónico que contiene su número de licencia.
- Haga clic con el botón primario del mouse al principio del número de licencia, manténgalo presionado, arrastre el mouse hasta el final del número y, entonces, suelte el botón. El número deberá quedar resaltado.
- Presione la tecla **Ctrl** y, mientras la mantiene presionada, presione la tecla **C**. De este modo se copia el número.



- Haga clic en la posición en la que desee pegar el número copiado.
- Presione la tecla **Ctrl** y, mientras la mantiene presionada, presione la tecla **V**. De este modo se pega el número en la ubicación seleccionada.

Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- **Cancelar**: haga clic para salir del proceso de configuración inmediatamente; **AVG AntiVirus 2013** no se instalará.
- **Atrás**: haga clic para volver al cuadro de diálogo de configuración anterior.
- **Siguiente**: haga clic para seguir con la instalación y avanzar un paso.

3.4. Seleccionar el tipo de instalación

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



Instalación rápida

Para la mayoría de los usuarios, se recomienda especialmente que conserve la instalación **Express** estándar. De esta forma instalará **AVG AntiVirus 2013** en el modo completamente automático con configuración predefinida por el proveedor del programa, incluido el [Gadget de AVG](#), [AVG Security Toolbar](#) y habiendo configurado AVG Secure Search como el proveedor de búsqueda predeterminado. Esta configuración proporciona la máxima seguridad combinada con el uso óptimo de los recursos. En el futuro, si es necesario cambiar la configuración, siempre se puede hacer



directamente en la aplicación **AVG AntiVirus 2013**.

Presione el botón **Siguiente** para continuar con el siguiente cuadro de diálogo del proceso de instalación.

Instalación personalizada

La opción **Instalación personalizada** sólo debe ser utilizada por usuarios con experiencia que tengan un motivo importante para instalar **AVG AntiVirus 2013** con una configuración distinta de la estándar (por ejemplo, para ajustarse a necesidades específicas del sistema). Si elige esta opción, una sección nueva llamada **Carpeta de destino** aparece en el cuadro de diálogo. Ahora especifique la ubicación donde **AVG AntiVirus 2013** debe instalarse. De forma predeterminada, **AVG AntiVirus 2013** se instalará en la carpeta de archivos de programa ubicada en el disco C:, como se estableció en el campo de texto del cuadro de diálogo. Si desea cambiar esta ubicación, utilice el botón **Examinar** para ver la estructura de la unidad y seleccione la carpeta correspondiente. Para volver al destino predeterminado predefinido por el proveedor del software, utilice el botón **Predeterminado**.

Luego, presione el botón **Siguiente** para pasar al cuadro de diálogo [Opciones personalizadas](#).

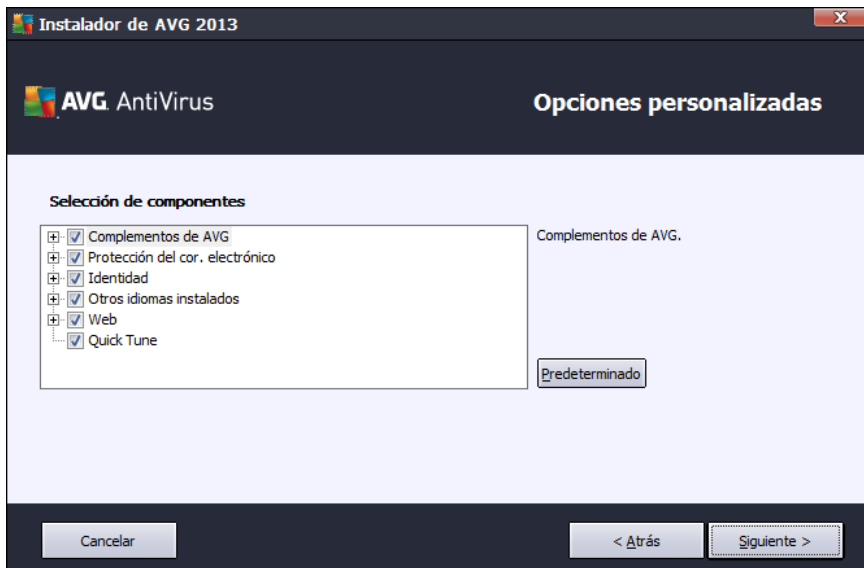
Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- **Cancelar**: haga clic para salir del proceso de configuración inmediatamente; **AVG AntiVirus 2013** no se instalará.
- **Atrás**: haga clic para volver al cuadro de diálogo de configuración anterior.
- **Siguiente**: haga clic para seguir con la instalación y avanzar un paso.

3.5. Opciones personalizadas

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



La sección **Selección de componentes** proporciona una descripción general de todos los componentes de **AVG AntiVirus 2013** que se pueden instalar. Si la configuración predeterminada no se adecua a sus necesidades, puede quitar/agregar componentes específicos. **Sin embargo, sólo puede seleccionar de entre los componentes incluidos en la edición del AVG que compró.** Resalte cualquier elemento de la lista **Selección de componentes** y aparecerá una breve descripción del componente correspondiente en la parte derecha de esta sección. Para obtener información detallada sobre las funciones de cada componente, consulte el capítulo [Descripción general de los componentes](#) de esta documentación. Para volver a la configuración predeterminada predefinida por el proveedor del software, utilice el botón **Predeterminado**.

Botones de control

Al igual que en la mayoría de los cuadros de diálogo de configuración, hay tres botones de control disponibles:

- **Cancelar:** haga clic para salir del proceso de configuración inmediatamente; **AVG AntiVirus 2013** no se instalará.
- **Atrás:** haga clic para volver al cuadro de diálogo de configuración anterior.
- **Siguiete:** haga clic para seguir con la instalación y avanzar un paso.

3.6. Instalar AVG Security Toolbar

En el cuadro de diálogo **Instalar AVG Security Toolbar**, decida si desea instalar el componente **AVG Security Toolbar**. Si no cambia la configuración predeterminada, este componente se instalará automáticamente en su navegador de Internet (*los navegadores compatibles actualmente*



son Microsoft Internet Explorer 6.0 o superior y Mozilla Firefox 3.0 y superior) para proporcionarle una protección exhaustiva en línea mientras navega por Internet. Por el momento, los navegadores de Internet admitidos son Internet Explorer (versión 6.0 y superior) o Mozilla Firefox (versión 3.0 y superior). No se admite ningún otro navegador (en caso de que utilice un navegador de Internet alternativo, como Avant Browser, puede producirse un comportamiento inesperado).



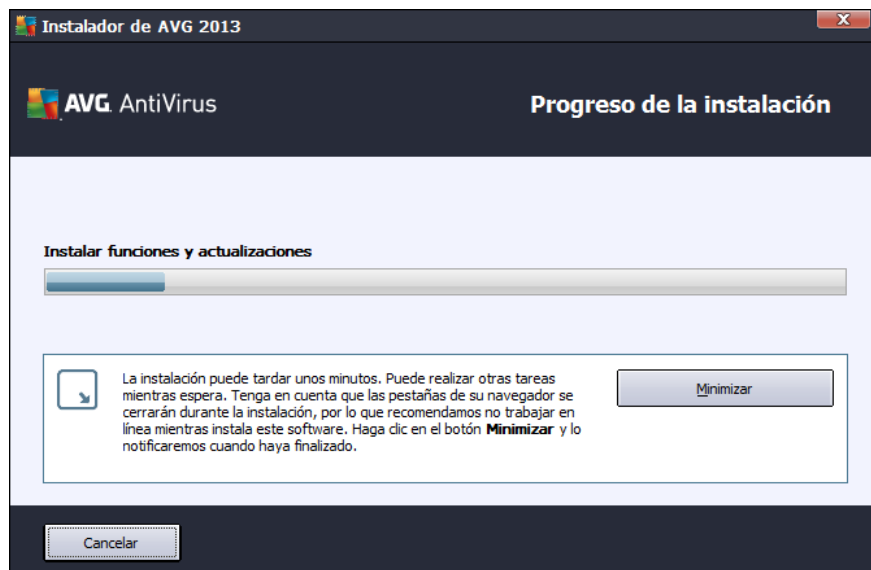
En el cuadro de diálogo verá opciones para decidir sobre la siguiente configuración:

- **Establecer y mantener AVG Secure Search como mi proveedor de búsquedas predeterminado:** mantener marcada para confirmar que desea utilizar el motor de búsqueda AVG Secure Search, que colabora estrechamente con Link Scanner Surf Shield para su máxima seguridad en línea.
- **Instalar AVG Security Toolbar para mejorar mi protección de Internet:** mantener marcada para instalar AVG Security Toolbar, que ofrece la máxima seguridad al navegar por Internet.



3.7. Progreso de la instalación

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



Después de finalizar el proceso de instalación, pasará automáticamente al siguiente cuadro de diálogo.

Botones de control

Hay dos botones de control disponibles en este diálogo:

- **Minimizar:** el proceso de instalación puede demorar varios minutos. Haga clic en el botón para minimizar la ventana de diálogo a un icono visible en la barra del sistema. El cuadro de diálogo aparece una vez finalizada la instalación.
- **Cancelar:** este botón solo debe usarse si desea interrumpir el proceso de instalación actual. Tenga en cuenta que, en un caso así, **AVG AntiVirus 2013** no se instalará.



3.8. La instalación se ha realizado correctamente

El cuadro de diálogo *La instalación se realizó correctamente* confirma que **AVG AntiVirus 2013** se ha instalado y configurado por completo:



Programa de mejora del producto y Política de privacidad

Aquí puede decidir si desea participar en el **Programa de mejora del producto** (para obtener información detallada, consulte el capítulo [Configuración avanzada de AVG / Programa de mejora del producto](#)) que recopila información anónima sobre las amenazas detectadas con el fin de aumentar el nivel general de seguridad de Internet. Todos los datos se tratan como confidenciales y de conformidad con la Política de privacidad de AVG; haga clic en el vínculo **Política de privacidad** para dirigirse al sitio web de AVG (<http://www.avg.com/>) donde podrá encontrar el texto completo de la Política de privacidad de AVG. Si está de acuerdo, deje marcada la opción (la opción está marcada de forma predeterminada).

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



4. Después de la instalación

4.1. Registro del producto

Una vez finalizada la instalación de **AVG AntiVirus 2013**, registre su producto en línea en el sitio web de AVG (<http://www.avg.com/>). Tras el registro, dispondrá de pleno acceso a la cuenta de usuario AVG, el boletín de actualizaciones de AVG y otros servicios que se ofrecen exclusivamente para los usuarios registrados. La forma más fácil de registrarse es directamente desde la interfaz del usuario de **AVG AntiVirus 2013**. Seleccione el elemento [/ Opciones / Inscribirse ahora](#) en la navegación superior. Se lo dirigirá a la página **Registro** en el sitio web de AVG (<http://www.avg.com/>). Siga las instrucciones proporcionadas en la página.

4.2. Acceso a la interfaz del usuario

Se puede obtener acceso al [cuadro de diálogo principal de AVG](#) de varios modos:

- haga doble clic en el [icono de la bandeja del sistema AVG](#)
- haga doble clic en el icono AVG del escritorio
- desde el menú **Inicio / Todos los programas / AVG / AVG 2013**

4.3. Análisis de todo el equipo

Existe el riesgo potencial de que un virus informático se transmitiera a su equipo antes de la instalación de **AVG AntiVirus 2013**. Por esta razón debe ejecutar un [Análisis de todo el equipo](#) para estar seguro de que no hay infecciones en su equipo. El primer análisis puede tardar un tiempo (*alrededor de una hora*) pero es recomendable ejecutarlo para asegurar de que su equipo no se alteró por una amenaza. Para obtener instrucciones sobre la ejecución de un [Análisis de todo el equipo](#) consulte el capítulo [Análisis de AVG](#).

4.4. Análisis Eicar

Para confirmar que **AVG AntiVirus 2013** se ha instalado correctamente, puede realizar el análisis EICAR.

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

Intente descargar el archivo *eicar.com* y guárdelo en el disco local. Inmediatamente después de confirmar la descarga del archivo de prueba, **AVG AntiVirus 2013** reaccionará a él mediante una advertencia. Esta notificación demuestra que AVG se ha instalado correctamente en su equipo.



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

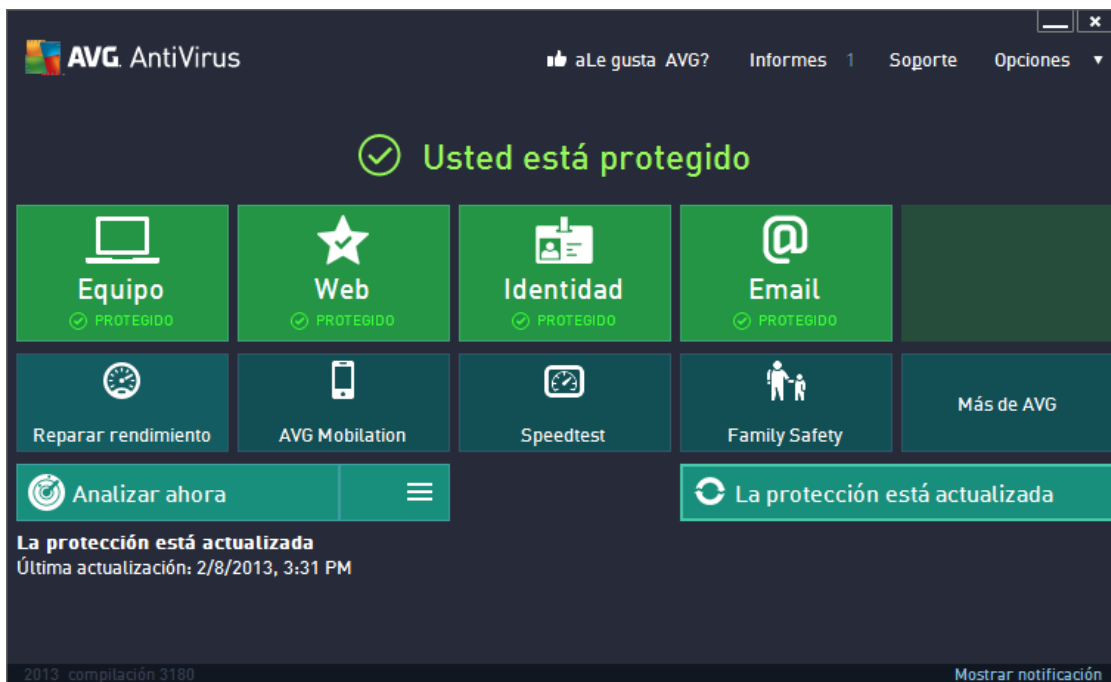
4.5. Configuración predeterminada de AVG

La configuración predeterminada (*por ejemplo, la configuración de la aplicación inmediatamente después de la instalación*) de **AVG AntiVirus 2013** está definida por el proveedor de software para que todos los componentes y funciones proporcionen un rendimiento óptimo. **No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Solo un usuario experimentado puede llevar a cabo cambios en la configuración.** Si desea cambiar la configuración de AVG para que se adapte mejor a sus necesidades, vaya a [Configuración avanzada de AVG](#): seleccione el elemento del menú principal del sistema *Opciones/Configuración avanzada* y modifique la configuración de AVG en el cuadro de diálogo [Configuración avanzada de AVG](#) que aparece.



5. Interfaz del usuario de AVG

AVG AntiVirus 2013 se abre con la ventana principal:



La ventana principal se divide en varias secciones:

- **La navegación de la línea superior** comprende cuatro vínculos activos alineados en la sección superior de la ventana principal (*¿Le gusta AVG?*, *Informes*, *Soporte*, *Opciones*). [Detalles >>](#)
- **Información del estado de seguridad** proporciona información básica sobre el estado actual de su **AVG AntiVirus 2013**. [Detalles >>](#)
- **La descripción general de los componentes instalados** puede encontrarse en una cinta horizontal de bloques en la sección central de la ventana principal. Los componentes se muestran como bloques verde claro etiquetados mediante el icono del componente respectivo, y proporcionan información sobre su estado. [Detalles >>](#)
- **Mis aplicaciones** se describen gráficamente en la cinta central inferior de la ventana principal y le ofrecen una descripción general de las aplicaciones complementarias a **AVG AntiVirus 2013** que ya están instaladas en su equipo o que se recomienda instalar. [Detalles >>](#)
- **Los vínculos rápidos Analizar / Actualizar** están situados en la línea inferior de bloques en la ventana principal. Estos botones permiten un acceso inmediato a las funciones más importantes y de uso más frecuente de AVG. [Detalles >>](#)

Fuera de la ventana principal de **AVG AntiVirus 2013**, hay dos elementos más de control que puede usar para acceder a la aplicación:



- **El icono de la bandeja del sistema**, que se ubica en la esquina derecha inferior del monitor (*en la bandeja del sistema*) e indica el estado actual de **AVG AntiVirus 2013**. [Detalles >>](#)
- **El Gadget de AVG**, que está accesible en la barra lateral de Windows (*admitido en el sistema operativo Windows Vista/7/8 solamente*) y permite el rápido acceso al análisis y la actualización dentro de **AVG AntiVirus 2013**. [Detalles >>](#)

5.1. Navegación superior

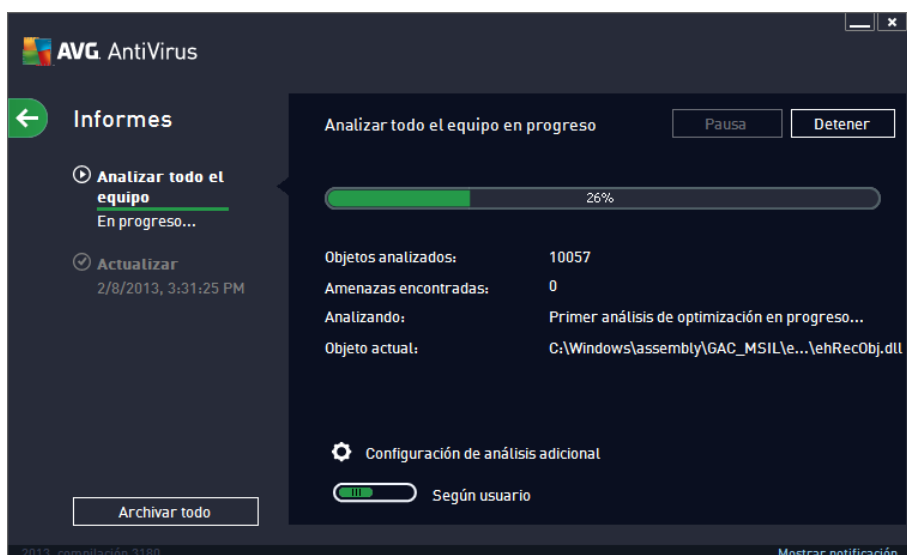
La **navegación superior** comprende varios vínculos activos alineados en la sección superior de la ventana principal. La navegación incluye los siguientes botones:

5.1.1. Me gusta AVG

Haga un solo clic en el vínculo para conectarse a la [comunidad de Facebook de AVG](#) y compartir la más reciente información de AVG, novedades, sugerencias y trucos para su máxima seguridad en Internet.

5.1.2. Informes

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



5.1.3. Soporte

Abre un nuevo cuadro de diálogo estructurado en cuatro pestañas donde podrá encontrar información relevante sobre **AVG AntiVirus 2013**:

- **Licencia y soporte**: la pestaña proporciona información sobre el nombre del producto, el número de licencia y la fecha de vencimiento. En la sección inferior del cuadro de diálogo



también encontrará una descripción general organizada claramente de todos los contactos disponibles para soporte al cliente. Los siguientes vínculos y botones activos están disponibles en la pestaña:

- o **(Re)Activar:** haga clic para abrir el nuevo cuadro de diálogo de **activación del software AVG**. Escriba su número de licencia en el campo correspondiente para reemplazar su número de venta (*que utiliza durante la instalación de AVG AntiVirus 2013*), o bien cambiar su número de licencia actual por otro (*por ej., al actualizar a un producto de AVG superior*).
- o **Copiar al portapapeles:** utilice este vínculo para copiar el número de licencia y pegarlo donde sea necesario. De esta forma puede tener la seguridad de que el número de licencia se ingrese correctamente.
- o **Renovar ahora:** le recomendamos que compre su renovación de licencia de **AVG AntiVirus 2013** algún tiempo antes de que expire la licencia actual, al menos un mes antes. Se le notificará tiempo antes de que llegue la fecha de vencimiento. Haga clic en este vínculo para dirigirse al sitio web de AVG (<http://www.avg.com/>) donde encontrará información detallada sobre el estado de su licencia, la fecha de vencimiento y la oferta de renovación/actualización.



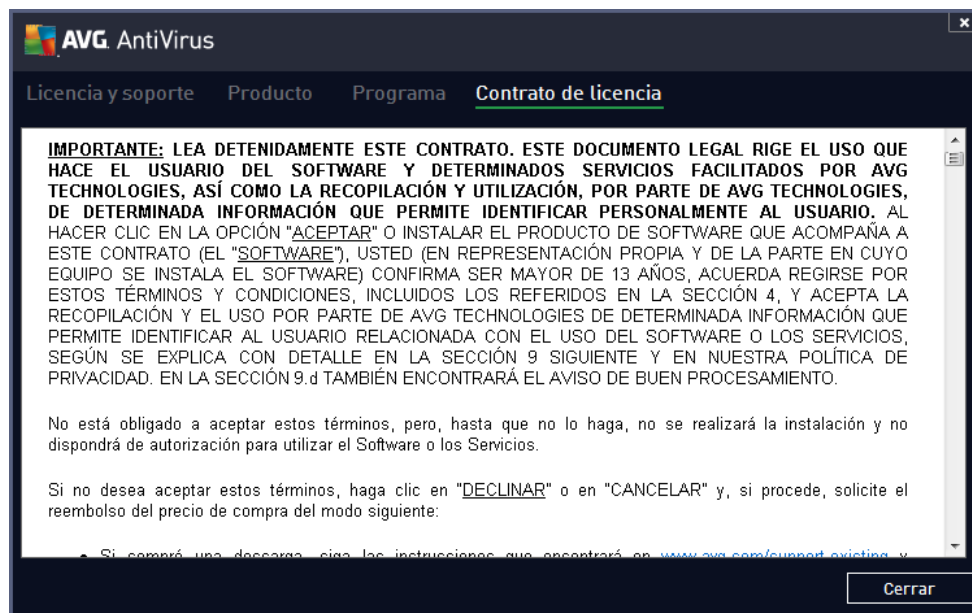
- **Producto:** la pestaña proporciona una descripción general de los datos técnicos más importantes de **AVG AntiVirus 2013** en referencia a la información del producto, los componentes instalados, la protección de correo electrónico instalada y la información del sistema:



- **Programa:** en esta pestaña podrá encontrar información sobre la versión del archivo del programa y sobre el código de terceros utilizado en el producto:



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



5.1.4. Opciones

El mantenimiento de **AVG AntiVirus 2013** está accesible a través del elemento **Opciones**. Haga clic en la flecha para abrir el menú desplegable:

- **[Analizar el Equipo](#)**: realiza un análisis del equipo completo.
- **[Analizar la carpeta seleccionada...](#)**: cambia a la interfaz de análisis de AVG y permite definir qué archivos y carpetas se analizarán dentro de la estructura de árbol de su equipo.
- **[Analizar archivo...](#)**: le permite ejecutar una evaluación a pedido sobre un único archivo específico. Haga clic en esta opción para abrir una nueva ventana con la estructura de árbol de su disco. Seleccione el archivo deseado y confirme la ejecución del análisis.
- **[Actualizar](#)**: ejecuta automáticamente el proceso de actualización de **AVG AntiVirus 2013**.
- **[Actualizar desde directorio...](#)**: ejecuta el proceso de actualización desde los archivos de actualización ubicados en una carpeta específica en el disco local. Sin embargo, esta opción sólo se recomienda en casos de emergencia, como en situaciones en que no existe una conexión a Internet disponible (por ejemplo, su equipo se encuentra infectado y está desconectado de Internet, su equipo está conectado a una red sin acceso a Internet, etc.). En la nueva ventana abierta, seleccione la carpeta donde guardó el archivo de actualización anteriormente y ejecute el proceso de actualización.
- **[Bóveda de virus](#)**: abre la interfaz del espacio de cuarentena (Bóveda de virus) en el cual AVG elimina todas las infecciones detectadas que no pueden repararse automáticamente por alguna razón. Los archivos infectados se aíslan dentro de esta cuarentena, garantizando la seguridad de su equipo, y al mismo tiempo se guardan los archivos infectados para repararlos en el futuro si existe la posibilidad.
- **[Historial](#)**: ofrece otras opciones de submenú específicas:
 - **[Resultados del análisis](#)**: abre un cuadro de diálogo que proporciona una descripción



general de los resultados del análisis.

- [Detección de Protección residente](#): abre un cuadro de diálogo con una descripción general de las amenazas detectadas por la Protección residente.
- *Detección de Identity Protection*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por Identity Protection.
- [Detección mediante la Protección del correo electrónico](#): abre un cuadro de diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente Protección del correo electrónico.
- [Hallazgos de Online Shield](#): abre un cuadro de diálogo con una descripción general de las amenazas detectadas por Online Shield.
- [Registro de historial de eventos](#): abre la interfaz del registro del historial de todas las acciones de **AVG AntiVirus 2013** registradas.
- [Configuración avanzada...](#): abre el cuadro de diálogo Configuración avanzada de AVG en el cual es posible editar la configuración de **AVG AntiVirus 2013**. Generalmente, se recomienda mantener la configuración predeterminada de la aplicación como se encuentra definida por el distribuidor del software.
- **Contenidos de la Ayuda**: abre los archivos de ayuda de AVG.
- **Obtener soporte**: abre el sitio web de AVG (<http://www.avg.com/>) en la página del centro de soporte al cliente.
- **Su web AVG**: abre el sitio web de AVG (<http://www.avg.com/>).
- **Acerca de virus y amenazas**: abre la Enciclopedia de virus en línea donde puede buscar información detallada acerca del virus identificado.
- **(Re)Activar**: abre el cuadro de diálogo **Activar AVG** y muestra datos que ha proporcionado durante el proceso de instalación. Dentro de este cuadro de diálogo puede introducir el número de licencia para reemplazar el número de venta (*el cual ha instalado con AVG*), o para reemplazar el número de licencia antiguo (*por ejemplo, cuando se actualiza a un nuevo producto AVG*).
- **Inscribirse ahora / Mi cuenta**: le permite conectarse a la página de registro del sitio web de AVG (<http://www.avg.com/>). Introduzca su información de registro; sólo los clientes que registren su producto AVG podrán recibir soporte técnico gratuito. Si utiliza la versión de prueba de **AVG AntiVirus 2013**, los dos últimos elementos aparecen como **Comprar ahora** y **Activar**, con lo que puede comprar la versión completa del programa inmediatamente. Para **AVG AntiVirus 2013** instalado con un número de venta, los elementos aparecen como **Registrar** y **Activar**.
- **Acerca de AVG**: abre un nuevo cuadro de diálogo con cuatro pestañas que proporcionan datos sobre su licencia adquirida y soporte accesible, información del producto y del programa, además del texto completo del acuerdo de licencia.



5.2. Información del estado de seguridad

La sección **Información del estado de seguridad** está situada en la parte superior de la ventana principal de **AVG AntiVirus 2013**. En esta sección siempre encontrará información sobre el estado de seguridad actual de su **AVG AntiVirus 2013**. Consulte la descripción general de los iconos que posiblemente se muestran en esta sección, y su significado:



: el icono verde indica que **AVG AntiVirus 2013 está completamente operativo**. Su equipo está totalmente protegido, actualizado y todos los componentes instalados funcionan correctamente.



: el icono amarillo indica que **uno o más componentes están configurados de manera incorrecta** y debería prestar atención a su configuración o a sus propiedades. No hay problemas críticos en **AVG AntiVirus 2013** y probablemente ha optado por desactivar algunos componentes por alguna razón. Aún está protegido. Sin embargo, preste atención a la configuración de los componentes con problemas. El componente configurado incorrectamente se mostrará con una cinta naranja de advertencia en la [interfaz de usuario principal](#).

El icono amarillo aparece también si, por algún motivo, ha decidido ignorar el estado de error del componente. La opción **Ignorar estado de error** está disponible en la sección [Configuración avanzada / Ignorar estado de error](#). Allí tendrá la opción de expresar que es consciente del estado de error del componente pero que, por alguna razón, desea conservar su **AVG AntiVirus 2013** de esta manera y no desea que se le advierta al respecto. Puede ser necesario utilizar esta opción en una situación específica, pero es muy recomendable desactivar la opción **Ignorar el estado de error** a la mayor brevedad posible.

De forma alternativa, el icono amarillo también se mostrará si su **AVG AntiVirus 2013** requiere reiniciar el equipo (**es necesario reiniciar**). Preste atención a esta advertencia y reinicie su equipo.



: el icono naranja indica que **AVG AntiVirus 2013 se encuentra en estado crítico**. Uno o varios componentes no funcionan correctamente y **AVG AntiVirus 2013** no puede proteger su equipo. Preste atención de inmediato para corregir el problema notificado! Si no puede corregir el error sin ayuda, póngase en contacto con el equipo de [soporte técnico de AVG](#).

En caso de que AVG AntiVirus 2013 no esté configurado para un rendimiento óptimo, aparece un nuevo botón llamado Haga clic para reparar (de forma alternativa, Haga clic para reparar todo si el problema concierne a más de un componente) junto a la información de estado de seguridad. Presione el botón para iniciar un proceso automático de confirmación y configuración del programa. Se trata de una forma fácil de configurar AVG AntiVirus 2013 para un rendimiento óptimo y alcanzar el máximo nivel de seguridad.

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

Nota: la información del estado de **AVG AntiVirus 2013** también se puede obtener en cualquier momento del [icono de la bandeja del sistema](#).



5.3. Descripción general de los componentes

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

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

Lista de componentes instalados

En **AVG AntiVirus 2013**, la sección **Descripción general de los componentes** contiene información sobre los siguientes componentes:

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

Acciones accesibles

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



5.4. Mis aplicaciones

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

- **Protección para dispositivos móviles** es una aplicación que protege su teléfono celular de virus y malware. También le ofrece la posibilidad de seguir su teléfono inteligente de forma remota si en algún momento se separa de él.
- **LiveKive** es específico para las copias de resguardo en línea en servidores seguros. LiveKive realiza automáticamente una copia de resguardo de todos sus archivos, fotos y música en un lugar seguro, para que pueda compartirlos con su familia y amigos y tener acceso a ellos desde cualquier dispositivo con acceso a Internet, incluidos los dispositivos iPhone y Android.
- **Family Safety** le ayuda a proteger a sus hijos de sitios web, contenido multimedia y búsquedas en línea inadecuados, y le brinda reportes sobre su actividad en línea. AVG Family Safety utiliza una tecnología de análisis de secuencias de teclas para supervisar las actividades de sus hijos, tanto en salas de chat como en redes sociales. Si detecta palabras, frases o contenido utilizados para ofrecer un trato vejatorio a los niños en línea, se le notificará inmediatamente por SMS o correo electrónico. Esta aplicación le permite establecer el nivel adecuado de protección para cada uno de sus hijos y supervisarlos de manera individual mediante inicios de sesión únicos.
- **La aplicación PC Tuneup** es una herramienta avanzada para el análisis detallado y la corrección del sistema, respecto a cómo podría mejorarse la velocidad y el rendimiento general del equipo.
- **MultiMi** reúne todas sus cuentas de correo electrónico y redes sociales en un solo lugar para facilitar el contacto con su familia y amigos, navegar por Internet, compartir fotos, videos y archivos. MultiMi incluye el servicio LinkScanner, que lo protege contra la creciente cantidad de amenazas en Internet mediante el análisis de las páginas web que hay detrás de todos los vínculos de cualquier página que visite y asegurándose de que son seguras.
- **AVG Toolbar** está disponible directamente en su navegador web y le ofrece máxima seguridad al navegar por Internet.

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

5.5. Analizar / Actualizar vínculos rápidos

Los **Vínculos rápidos** están ubicados en la línea inferior de botones de la [interfaz de usuario](#) de **AVG AntiVirus 2013**. Estos vínculos le permiten un acceso inmediato a las funciones más importantes y de uso más común de la aplicación, es decir, análisis y actualizaciones. Los vínculos rápidos están disponibles en todos los cuadros de diálogo de la interfaz del usuario:

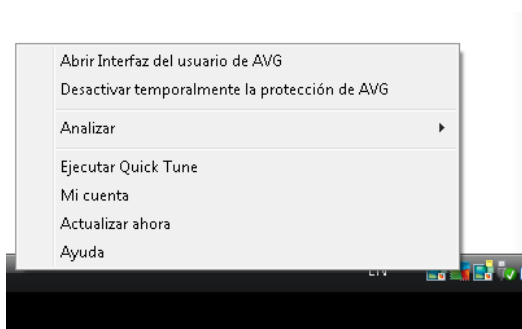
- **Analizar ahora:** el botón está gráficamente dividido en dos secciones. Siga el vínculo

Analizar ahora para iniciar [Analizar todo el equipo](#) de inmediato, y supervise su progreso y resultados en la ventana [Informes](#) que se abre automáticamente. El botón **Opciones** abre el cuadro de diálogo **Opciones de análisis** donde puede [análisis programados](#) y editar parámetros de [Analizar todo el equipo](#) / [Analizar carpetas o archivos](#). (Para obtener información detallada, consulte el capítulo [Análisis de AVG](#))




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

5.6. Icono en la bandeja de 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 su **AVG AntiVirus 2013**. Está visible en todo momento en la bandeja del sistema, tanto si la [interfaz del usuario](#) de **AVG AntiVirus 2013** está abierta como si no:



Visualización del icono de la bandeja del sistema de AVG

-  Si aparece de color completo sin elementos agregados, el icono indica que todos los componentes de **AVG AntiVirus 2013** están activos y funcionando totalmente. Sin embargo, el icono puede mostrarse también de esta forma en situaciones en las que uno de los componentes no está funcionando totalmente pero el usuario ha decidido que se [ignore el estado del componente](#). (Con la confirmación de la opción *Ignorar el estado del componente*, expresa que es consciente del [estado de error del componente](#) pero que, por algún motivo, desea mantenerlo así y no desea que se le advierta de la situación).
-  El icono con un signo de exclamación indica que un componente (o incluso varios componentes) se encuentran en [estado de error](#). Preste siempre atención a tales advertencias e intente corregir el problema de configuración de un componente que no está configurado correctamente. Para realizar los cambios en la configuración del componente, haga doble clic en el icono de la bandeja del sistema para abrir la [interfaz del usuario de la aplicación](#). Para obtener información detallada acerca de qué componentes se encuentran en [estado de error](#), consulte la sección [Información del estado de seguridad](#).
-  El icono de la bandeja del sistema se puede mostrar también a colores con un haz de luz que parpadea o gira. Esta versión gráfica señala un proceso de actualización actualmente ejecutado.



-  La visualización alternativa de un icono a colores con una flecha significa que se está ejecutando uno de los análisis de **AVG AntiVirus 2013**.

Información del icono de la bandeja del sistema de AVG

El **icono de la bandeja del sistema de AVG** también informa sobre actividades actuales dentro de **AVG AntiVirus 2013** y sobre posibles cambios de estado en el programa (*por ej., inicio automático de un análisis o actualización programado, cambio de estado de un componente, ocurrencia de estado de error, ...*) a través de una ventana emergente que se abre desde el icono de la bandeja del sistema.

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

El **icono de la bandeja del sistema de AVG** se puede utilizar también como vínculo de acceso rápido a la [interfaz del usuario](#) de **AVG AntiVirus 2013**, con sólo hacer doble clic en él. Al hacer clic con el botón secundario en el icono se abre un pequeño menú contextual con las opciones siguientes:

- **Abrir Interfaz del usuario de AVG:** haga clic aquí para abrir la [interfaz del usuario](#) de **AVG AntiVirus 2013**.
- **Desactivar temporalmente la protección de AVG:** la opción le permite desactivar la protección completa que usted realizó **AVG AntiVirus 2013** anteriormente. Recuerde que no debe usar esta opción si no es absolutamente necesario. En la mayoría de los casos, no es necesario desactivar antes **AVG AntiVirus 2013** de instalar nuevo software o controladores, ni siquiera si el instalador o el asistente de software le sugiere que cierre los programas y aplicaciones que se estén ejecutando para asegurarse de que no se producen interrupciones no deseadas durante el proceso de instalación. Si tiene que desactivar temporalmente **AVG AntiVirus 2013**, debe volver a activarlo en cuanto termine. Si está conectado a Internet o a una red durante el tiempo que el software antivirus está desactivado, su equipo será vulnerable ante los ataques..
- **Análisis:** haga clic aquí para abrir el menú contextual de [análisis predefinidos](#) ([Análisis de todo el equipo](#) y [Análisis de archivos/carpetas](#)) y seleccione el análisis que corresponda; se iniciará inmediatamente.
- **Análisis en ejecución...:** este elemento se muestra sólo si se está ejecutando un análisis en ese momento en el equipo. Para este análisis puede establecer la prioridad, o detener o pausar el análisis que se está ejecutando. Están disponibles también las siguientes acciones: *Establecer prioridad para todos los análisis, Pausar todos los análisis* o *Detener todos los análisis*.
- **Ejecutar PC Analyzer:** haga clic aquí para iniciar el componente PC Analyzer
- **Mi cuenta:** abre la página principal de MyAccount, donde puede administrar sus productos de suscripción, comprar protección adicional, descargar archivos de instalación, comprobar pedidos y facturas anteriores, y administrar su información personal.
- **Actualizar ahora:** inicia inmediatamente una [actualización](#).



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

5.7. Gadget de AVG

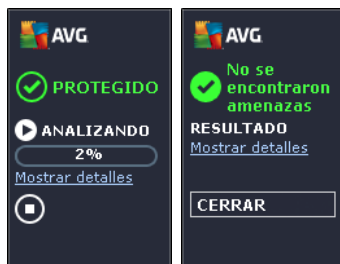
El **gadget de AVG** se muestra en el escritorio de Windows (*barra lateral de Windows*). Esta aplicación sólo es compatible con los sistemas operativos Windows Vista y Windows 7/8. **El gadget de AVG** ofrece un acceso inmediato a las funciones más importantes de **AVG AntiVirus 2013**, es decir, [análisis](#) y [actualización](#):



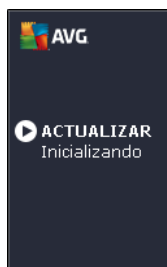
Controles del gadget de AVG



Si es necesario, el gadget de AVG le permite iniciar un análisis o una actualización de inmediato; también proporciona un vínculo rápido que lo conecta a las principales redes sociales y ofrece búsqueda rápida:

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



- **Actualizar ahora:** haga clic en el vínculo **Actualizar ahora** para iniciar la actualización de **AVG AntiVirus 2013** directamente desde el gadget:

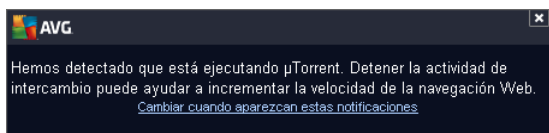


- **Vínculo a Twitter** : abre una nueva interfaz del **gadget de AVG** en la que se proporciona un resumen de los últimos suministros de AVG publicados en Twitter. Siga el vínculo **Ver todos los suministros de Twitter de AVG** para abrir el navegador de Internet en una ventana nueva; irá directamente al sitio web de Twitter, en concreto a la página dedicada a las noticias relacionadas con AVG:
- **Vínculo a Facebook** : abre el explorador de Internet con el sitio web de Facebook, específicamente en la página de la **comunidad de AVG**.
- **Cuadro de búsqueda**: escriba una palabra clave y obtenga inmediatamente los resultados de la búsqueda en una nueva ventana que se abre con su navegador web predeterminado.

5.8. AVG Advisor

AVG Advisor ha sido diseñado para detectar problemas que podrían ralentizar su equipo o ponerlo en riesgo y para recomendar una acción que solucione la situación. Si experimenta una ralentización repentina del equipo (*navegación en Internet, rendimiento en general*), a menudo no es evidente cuál es la razón y, en consecuencia, cómo resolver el problema. Es aquí donde se incorpora **AVG Advisor**. Mostrará una notificación en la bandeja del sistema que le informa cuál puede ser el problema, y le sugiere cómo solucionarlo. **AVG Advisor** continúa supervisando todos los procesos en ejecución dentro de su PC para detectar posibles problemas y además, ofrece consejos sobre cómo evitarlos.

AVG Advisor está visible en forma de un cuadro de diálogo emergente que se desliza sobre la bandeja del sistema:



Específicamente, **AVG Advisor** monitorea lo siguiente:

- **El estado de cualquier navegador web actualmente abierto.** Los navegadores web pueden sobrecargar la memoria, específicamente si múltiples ventanas o pestañas han estado abiertas por un determinado tiempo, y consumen demasiados recursos del sistema, ralentizando de esta forma el equipo. En esta situación, a menudo resulta de utilidad reiniciar el navegador web.
- **Ejecución de conexiones de punto a punto.** Después de usar el protocolo P2P para compartir archivos, en ocasiones la conexión puede permanecer activa, usando una cantidad determinada de su ancho de banda. Como resultado, puede experimentar una



ralentización de la navegación en la red.

- **Red desconocida con un nombre familiar.** Esto por lo general solo se aplica a los usuarios que se conectan a varias redes, comúnmente con equipos portátiles: Si una red nueva y desconocida tiene el mismo nombre que una red conocida utilizada con frecuencia (por ej., Casa o MiWifi), se puede crear confusión y puede conectarse sin intención a una red completamente desconocida y potencialmente insegura. **AVG Advisor** puede evitar esto advirtiéndole que el nombre conocido se refiere en realidad a una red nueva. Por supuesto, si decide que la red desconocida es segura, puede guardarla en la una lista de **AVG Advisor** de redes conocidas de modo que no se informe nuevamente.

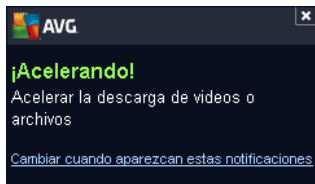
En cada una de estas situaciones, **AVG Advisor** le advierte de los posibles problemas que se pueden ocasionar y proporciona el nombre y el icono del proceso o de la aplicación en conflicto. Además, **AVG Advisor** sugiere los pasos que se deben tomar para evitar los posibles problemas.

Exploradores web soportados

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

5.9. AVG Accelerator

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



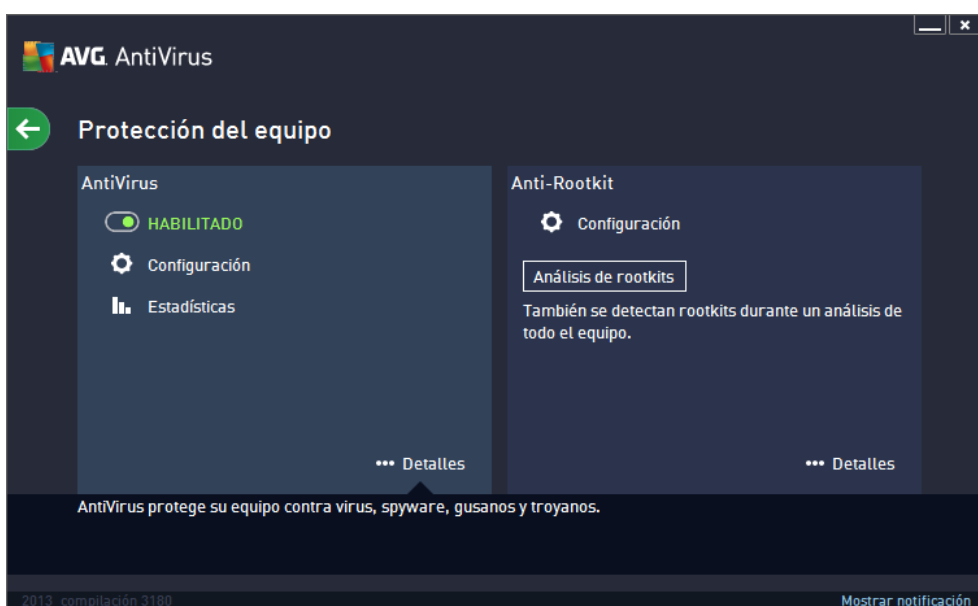


6. Componentes de AVG

6.1. Equipo

El componente **Equipo** cubre dos servicios de seguridad principales: **AntiVirus** y **Anti-Rootkit**.


- **AntiVirus** comprende un motor de análisis que protege todos los archivos, las áreas del sistema del equipo y los medios removibles (*disco flash, etc.*) y analiza en busca de virus conocidos. Se bloquearán los virus detectados para que no puedan realizar ninguna acción y después se limpiarán o pondrán en la [Bóveda de virus](#). Ni siquiera advertirá el proceso, dado que esta protección residente se ejecuta "en segundo plano". AntiVirus también usa el análisis heurístico, donde los archivos se analizan en busca de características comunes de virus. Esto significa que AntiVirus puede detectar un virus nuevo y desconocido si este contiene algunas características típicas de los virus ya existentes. **AVG AntiVirus 2013** también puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas dentro del sistema (*distintas clases de spyware, adware, etc.*). Además, AntiVirus analiza el registro de su sistema para comprobar si posee entradas sospechosas y archivos temporales de Internet, y le permite tratar todos esos elementos potencialmente dañinos de la misma manera en la que trata cualquier otra infección.
- **Anti-Rootkit** es una herramienta especializada que detecta y elimina con eficacia los rootkits peligrosos, es decir, los programas y las tecnologías que pueden camuflar la presencia de software malicioso en el equipo. Un rootkit está diseñado para tomar el control fundamental de un sistema informático, sin la autorización de los propietarios ni los administradores legítimos del sistema. Anti-Rootkit puede detectar rootkits según un conjunto de reglas predefinido. Si Anti-Rootkit encuentra un rootkit, no significa necesariamente que el rootkit está infectado. En ocasiones, los rootkits se utilizan como controladores o forman parte de aplicaciones correctas.








Controles del cuadro de diálogo


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

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

 **Configuración:** haga clic en el botón para ir a la interfaz de [configuración avanzada](#). De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, [AntiVirus](#) o [Anti-Rootkit](#). En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus 2013**, pero solamente se recomienda que lo hagan usuarios experimentados.

 **Estadísticas:** haga clic en el botón para ir a la página dedicada en el sitio web de AVG (<http://www.avg.com/>). En esta página puede encontrar una descripción general con datos estadísticos detallados de todas las actividades de **AVG AntiVirus 2013** realizadas en su equipo en un periodo de tiempo especificado y en total.

 **Detalles:** haga clic en el botón y se mostrará una breve descripción del servicio resaltado en la parte inferior del cuadro de diálogo.

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

En la sección Anti-Rootkit, también encontrará un botón **Análisis de rootkits** específico que puede usar para iniciar el análisis de rootkits independiente directamente (*no obstante, el análisis de rootkits es una parte implícita de [Analizar todo el equipo](#)*).

6.2. Navegación web

El componente **Protección de exploración web** comprende dos servicios: **LinkScanner Surf-Shield** y **Online Shield**:

- **LinkScanner Surf-Shield** le protege contra el creciente número de amenazas fugaces que aparecen en la Web. Estas amenazas pueden esconderse en cualquier tipo de sitio web, desde gubernamentales y de marcas grandes y reconocidas hasta de negocios pequeños, y rara vez permanecen allí por más de 24 horas. LinkScanner protege analizando las


páginas que están detrás de los vínculos de cualquier página web que esté viendo, y se asegura de que sean seguras en el único momento en que verdaderamente importa: cuando está por hacer clic en ellos. **LinkScanner Surf-Shield no está diseñado para proteger plataformas de servidor.**

- **Online Shield** es un tipo de protección residente en tiempo real; analiza el contenido de las páginas web visitadas (y los archivos que puedan contener) incluso antes de que se visualicen en el navegador o de que se descarguen en el equipo. Online Shield detecta si la página que se va a visitar contiene algún javascript peligroso e impide que se visualice la página. Asimismo, reconoce el malware que contiene una página y detiene su descarga de inmediato para que nunca entre en el equipo. Esta poderosa protección bloqueará el contenido malicioso de cualquier página que intente abrir, y evitará que se descargue en su equipo. Con esta característica activada, al hacer clic en un vínculo o escribir la URL de un sitio peligroso, se evitará que se abra la página web, protegiéndolo de infecciones inadvertidas. Es importante recordar que las páginas web vulnerables pueden infectar su equipo simplemente mediante una visita al sitio afectado. **Online Shield no está diseñado para proteger plataformas de servidor.**




Controles de diálogo


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


 **Activado / Desactivado:** el botón puede recordarle a un semáforo, tanto en su apariencia como en su funcionalidad. Haga un solo clic para alternar entre dos posiciones. El color verde significa **Activado**, que implica que el servicio de seguridad LinkScanner Surf-Shield / Online Shield está activo y completamente funcional. El color rojo representa el estado **Desactivado**; es decir, el servicio está desactivado. Si no tiene un buen motivo para desactivar el servicio, se recomienda estrictamente que conserve la configuración




predeterminada para todos los ajustes de seguridad. La configuración predeterminada garantiza el óptimo rendimiento de la aplicación, y su máxima seguridad. Si, por algún motivo, desea desactivar el servicio, se le advertirá acerca del posible riesgo de manera inmediata mediante el signo rojo **Advertencia** y la información de que no posee protección completa en ese momento. **Tenga en cuenta que debe activar el servicio otra vez tan pronto sea posible.**

 **Configuración:** haga clic en el botón para redirigirse a la interfaz de [configuración avanzada](#). De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, [LinkScanner Surf-Shield](#) u [Online Shield](#). En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus 2013**, pero solamente se recomienda que lo hagan usuarios experimentados.

 **Estadísticas:** haga clic en el botón para ir a la página dedicada en el sitio web de AVG (<http://www.avg.com/>). En esta página puede encontrar una descripción general con datos estadísticos detallados de todas las actividades de **AVG AntiVirus 2013** realizadas en su equipo en un periodo de tiempo especificado y en total.

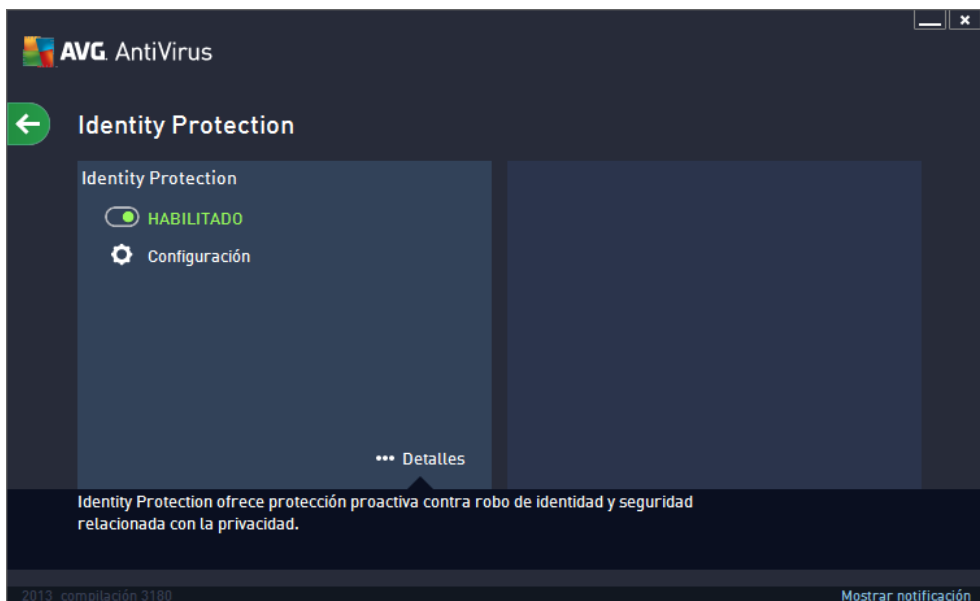
 **Detalles:** haga clic en el botón y se mostrará una breve descripción del servicio resaltado en la parte inferior del cuadro de diálogo.

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

6.3. Identidad


El componente **Identity Protection** proporciona ejecución del servicio **Identity Shield**, que brinda protección constante a sus activos digitales contra amenazas nuevas y desconocidas en Internet:


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





Controles del cuadro de diálogo

En el cuadro de diálogo, encontrará los controles a continuación:

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

 **Configuración:** haga clic en el botón para redirigirse a la interfaz de [configuración avanzada](#). De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, [Identity Protection](#). En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus 2013**, pero solamente se recomienda que lo hagan usuarios experimentados.

 **Detalles:** haga clic en el botón y se mostrará una breve descripción del servicio resaltado en la parte inferior del cuadro de diálogo.

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

Lamentablemente, en **AVG AntiVirus 2013**, el servicio Identity Alert no está incluido. Si desea usar este tipo de protección, siga el botón **Actualizar para activar** para dirigirse a la página web dedicada donde puede comprar la licencia de Identity Alert.



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

6.4. Correos electrónicos


El componente **Protección del correo electrónico** cubre los siguientes dos servicios de seguridad: **Analizador de correos electrónicos** y **Anti-Spam**:

- **Analizador de correos electrónicos:** una de las fuentes más comunes de virus y troyanos es el correo electrónico. El phishing (suplantación de identidad) y el spam hacen del correo electrónico una fuente aún mayor de riesgos. Las cuentas de correo electrónico gratuitas son más propensas a recibir esos correos maliciosos (*ya que es muy raro que empleen tecnología anti-spam*), y los usuarios domésticos confían demasiado en tales correos. También los usuarios domésticos, navegan en sitios desconocidos y llenan formularios en línea con datos personales (*como su dirección de correo electrónico*), aumentando la exposición a ataques a través del correo electrónico. Las empresas normalmente utilizan cuentas de correo electrónico corporativas y emplean filtros anti-spam, etc., para reducir el riesgo. El componente Protección del correo electrónico es responsable de analizar cada mensaje enviado o recibido; siempre que se detecta un virus en un correo electrónico, se coloca en la [Bóveda de virus](#) de inmediato. El componente también puede filtrar determinados tipos de archivos adjuntos de correo electrónico, así como agregar un texto de certificación a los mensajes no infectados. **El Analizador de correos electrónicos no está diseñado para plataformas de servidor.**
- **Anti-Spam** comprueba todos los mensajes de correo electrónico entrantes y marca los no deseados como spam (*spam hace referencia al correo electrónico no solicitado, en su mayoría publicidades de un producto o servicio, que se envía de forma masiva a una gran cantidad de direcciones de correo electrónico al mismo tiempo, lo que llena los buzones de los destinatarios. No son spam los correos comerciales legítimos a los cuales los consumidores han dado su consentimiento*). Anti-Spam puede modificar el asunto del correo electrónico (*identificado como spam*) agregando una cadena de texto especial. Luego puede filtrar fácilmente sus mensajes en el cliente de correo electrónico. El componente Anti-Spam usa varios métodos de análisis para procesar cada mensaje y ofrece la mayor protección posible contra mensajes de correo electrónico no deseados. Anti-Spam utiliza una base de datos que se actualiza regularmente para la detección del spam. También es posible usar servidores RBL (*bases de datos públicas con direcciones de correo electrónico de "spammers conocidos"*), así como agregar manualmente direcciones de correo electrónico a la Lista blanca (*nunca marcar como spam*) y a la Lista negra (*marcar siempre como spam*).




Controles del cuadro de diálogo


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


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


En la sección Analizador de correos electrónicos, puede ver dos botones de "semáforo". De esta forma puede especificar individualmente si desea que el Analizador de correos electrónicos compruebe los mensajes entrantes o salientes, o ambos. De forma predeterminada, el análisis está activado para los mensajes entrantes y desactivado para los salientes, cuando el riesgo de infección es relativamente bajo.

 **Configuración:** haga clic en el botón para redirigirse a la interfaz de [configuración avanzada](#). De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, [Analizador de correos electrónicos](#) o Anti-Spam. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG AntiVirus 2013**, pero solamente se recomienda que lo hagan

usuarios experimentados.

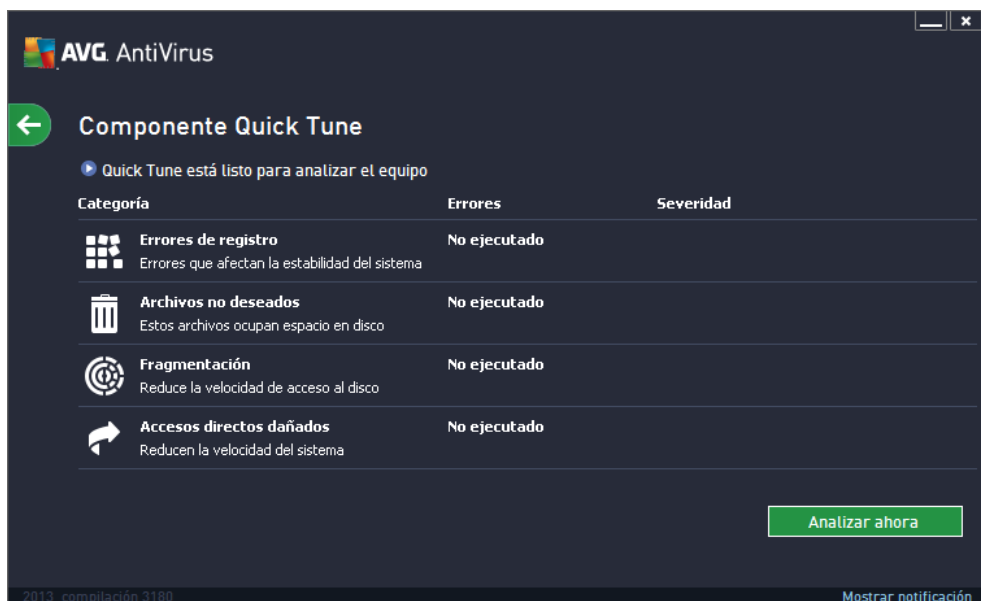
 **Estadísticas:** haga clic en el botón para ir a la página dedicada en el sitio web de AVG (<http://www.avg.com/>). En esta página puede encontrar una descripción general con datos estadísticos detallados de todas las actividades de **AVG AntiVirus 2013** realizadas en su equipo en un periodo de tiempo especificado y en total.

 **Detalles:** haga clic en el botón y se mostrará una breve descripción del servicio resaltado en la parte inferior del cuadro de diálogo.

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

6.5. Quick Tune

El componente **Quick Tune** es una herramienta avanzada para el análisis detallado y la corrección del sistema sobre cómo podrían mejorarse la velocidad y el rendimiento general del equipo:



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

- **Errores en el registro** mostrará el número de errores en el Registro de Windows que podrían estar reduciendo la velocidad de su equipo o haciendo que aparezcan mensajes de error.
- **Archivos no deseados** proporciona el número de archivos que consumen espacio en el disco duro y que probablemente se eliminen. Normalmente se tratará de varios tipos de archivos temporales, así como de archivos de la Papelera de reciclaje.
- **Fragmentación** calculará el porcentaje del disco duro que está fragmentado, es decir, que se ha utilizado durante mucho tiempo de forma que la mayoría de los archivos ahora están separados en distintas partes del disco físico.



- **Accesos directos dañados** encontrará los accesos directos que ya no funcionan, que conducen a ubicaciones inexistentes, etc.

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



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

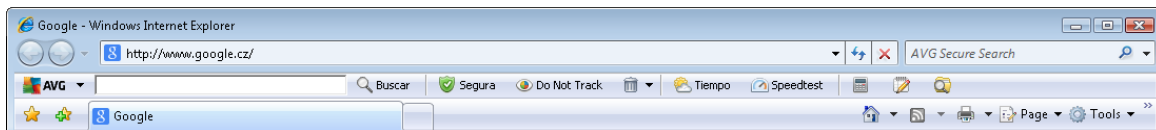
Botones de control

- **Analizar ahora** (se muestra antes de que se inicie el análisis): presione este botón para ejecutar el análisis del equipo inmediatamente
- **Reparar ahora** (se muestra cuando el análisis ha terminado): presione el botón para reparar todos los errores encontrados. Una vez finalizado el proceso de corrección, recibirá una descripción general de los resultados.
- **Cancelar**: presione este botón para detener el análisis en ejecución o para volver al [cuadro de diálogo principal de AVG](#) predeterminado (descripción general de los componentes) cuando el análisis se haya completado



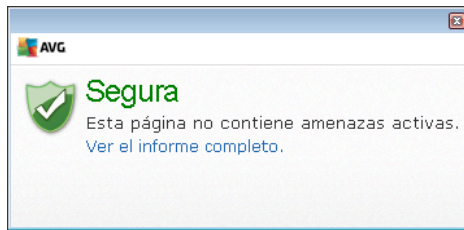
7. AVG Security Toolbar

AVG Security Toolbar es una herramienta que colabora estrechamente con el servicio LinkScanner Surf-Shield y que le ofrece la máxima seguridad mientras navega por Internet. En **AVG AntiVirus 2013**, la instalación de **AVG Security Toolbar** es opcional; durante el [proceso de instalación](#) se le invita a decidir si se debe instalar el componente. **AVG Security Toolbar** está disponible directamente en su navegador de Internet. Por el momento, los navegadores de Internet admitidos son Internet Explorer (*versión 6.0 y superior*) y/o Mozilla Firefox (*versión 3.0 y superior*). No se admite ningún otro navegador (*en caso de que utilice un navegador de Internet alternativo, como Avant Browser, puede producirse un comportamiento inesperado*).



AVG Security Toolbar consta de los siguientes elementos:

- **Logotipo de AVG** con el menú desplegable:
 - **Nivel de amenaza actual:** abre la página web del laboratorio de virus con una visualización gráfica del nivel de amenaza actual en Internet.
 - **AVG Threat Labs:** abre el sitio web de **AVG Threat Labs** específico (*en <http://www.avgthreatlabs.com>*) donde puede encontrar información sobre la seguridad y el nivel de amenaza actual en línea de varios sitios web.
 - **Ayuda de Toolbar:** abre la ayuda en línea donde se describe todo el funcionamiento de **AVG Security Toolbar**.
 - **Enviar comentarios acerca del producto:** abre una página web con un formulario que puede rellenar para darnos su opinión acerca de **AVG Security Toolbar**.
 - **Desinstalar AVG Security Toolbar:** abre una página web que proporciona una descripción detallada de cómo desactivar **AVG Security Toolbar** en cada uno de los exploradores web soportados.
 - **Acerca de...:** abre una nueva ventana con información acerca de la versión de **AVG Security Toolbar** actualmente instalada.
- **Campo de búsqueda:** realice búsquedas en Internet mediante **AVG Security Toolbar** con la certeza de estar completamente seguro y protegido, dado que todos los resultados de búsqueda mostrados son cien por ciento seguros. Escriba la palabra clave o una frase en el campo de búsqueda y presione el botón **Buscar** (o *Intro*).
- **Seguridad de sitio:** este botón abre un nuevo diálogo con información sobre el nivel de la amenaza actual (*Actualmente seguro*) de la página que está visitando. Este breve resumen se puede ampliar y muestra detalles completos de todas las actividades de seguridad relacionadas con la página directamente en la ventana del navegador (*Ver informe completo*):



- **Do Not Track**: el servicio DNT lo ayuda a identificar los sitios web que están recopilando datos sobre sus actividades en línea, y le da la posibilidad de permitir o no esta práctica. [Detalles >>](#)
- **Eliminar**: el botón de la papelera de reciclaje ofrece un menú desplegable desde donde puede seleccionar si desea eliminar información de navegación, descargas, formularios en línea, o si desea eliminar todo su historial de búsquedas de una vez.
- **Tiempo**: este botón abre un nuevo cuadro de diálogo con información acerca del tiempo actual en su ubicación, junto con la previsión del tiempo para los próximos dos días. Esta información se actualiza periódicamente, cada 3-6 horas. En este cuadro de diálogo, puede cambiar la ubicación deseada manualmente y decidir si desea ver la información de temperatura en grados Celsius o Fahrenheit.



- **Facebook**: este botón le permite conectarse a la red social [Facebook](#) directamente desde **AVG Security Toolbar**.
- **Speedtest**: este botón lo redirige a una aplicación en línea que puede ayudarlo a verificar la calidad de su conexión a Internet (*ping*) y su velocidad de carga y descarga.
- Botones de acceso directo para el acceso rápido a estas aplicaciones: **Calculadora**, **Bloc de notas**, **Explorador de Windows**.



8. AVG Do Not Track


AVG Do Not Track le ayuda a identificar los sitios web que recopilan datos acerca de sus actividades en línea. **AVG Do Not Track**, que es parte de [AVG Security Toolbar](#), muestra los sitios web o los anunciantes que recopilan datos acerca de sus actividades y le da la posibilidad de permitir o no esta práctica.

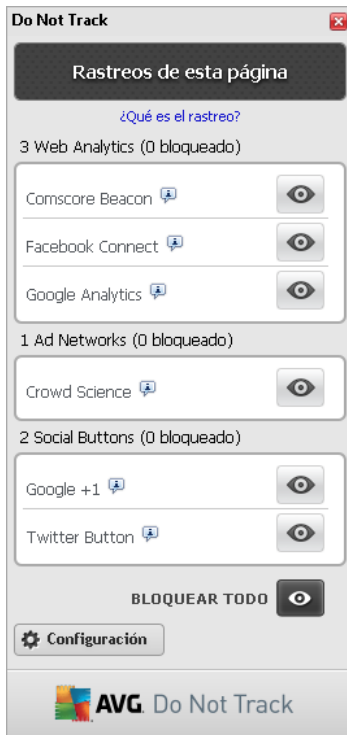
- **AVG Do Not Track** le proporciona información adicional sobre la política de privacidad de cada servicio respectivo, además de un enlace directo para excluirse del servicio, si se encuentra disponible.
- Además, **AVG Do Not Track** admite el [protocolo W3C DNT](#) para notificar automáticamente a los sitios que no desea que realicen seguimiento de sus actividades. Esta notificación está habilitada de manera predeterminada, pero se puede modificar en cualquier momento.
- El servicio de **AVG Do Not Track** se facilita bajo estos [términos y condiciones](#).
- **AVG Do Not Track** está habilitado de manera predeterminada, pero puede deshabilitarse fácilmente en cualquier momento. Puede encontrar instrucciones en el artículo de las Preguntas frecuentes que trata [cómo deshabilitar la función AVG Do Not Track](#).
- Para obtener más información sobre **AVG Do Not Track**, visite nuestro [sitio web](#).

Actualmente, la función **AVG Do Not Track** es compatible únicamente con Mozilla Firefox, Chrome e Internet Explorer.

8.1. Interfaz de AVG Do Not Track

Mientras está en línea, **AVG Do Not Track** lo advierte rápidamente cuando se detecta cualquier tipo de actividad de recopilación de datos. En tal caso, el icono **AVG Do Not Track** ubicado en [AVG Security Toolbar](#) cambia su apariencia; se muestra un pequeño número junto al icono que

proporciona información sobre diversos servicios de recopilación de datos detectados:  Haga clic en el icono para ver el cuadro de diálogo a continuación:



Todos los servicios de recopilación de datos detectados se enumeran en el resumen **Rastreadores en esta página**. Son tres los tipos de actividades de recopilación de datos que reconoce **AVG Do Not Track**:

- **Web Analytics** (*permitidos en forma predeterminada*): servicios empleados para mejorar el rendimiento y la experiencia del sitio web respectivo. En esta categoría encontrará servicios como Google Analytics, Omniture o Yahoo Analytics. Recomendamos que no bloquee los servicios de análisis de web, ya que es posible que el sitio web no funcione en la forma prevista.
- **Ad Networks** (*algunos están bloqueados de manera predeterminada*): servicios que recopilan o comparten datos sobre su actividad en línea en varios sitios, ya sea directa o indirectamente, para ofrecerle publicidad personalizada en lugar de publicidad basada en contenido. Esto se determina en función de la política de privacidad de cada Ad Network según se encuentre disponible en sus sitios web. Algunos Ad Networks están bloqueados de manera predeterminada.
- **Social Buttons** (*permitidos en forma predeterminada*): elementos diseñados para mejorar la experiencia en las redes sociales. Estos elementos los incluyen las redes sociales en el sitio que se visita. Pueden recopilar datos sobre su actividad en línea si ha iniciado sesión. Algunos ejemplos de Social Buttons son: complementos sociales de Facebook, el botón de Twitter, Google +1.

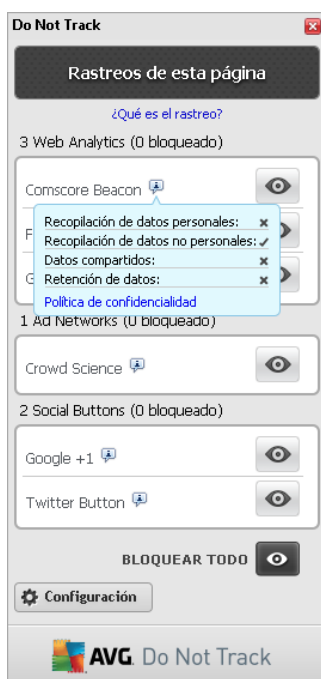
Nota: según los servicios que se ejecutan en segundo plano en el sitio web, es posible que alguna de las tres secciones descritas arriba no aparezcan en el cuadro de diálogo de AVG Do Not Track.

Controles del cuadro de diálogo

- **¿Qué es el rastreo?:** haga clic en este vínculo en la sección superior del cuadro de diálogo para llegar a la página web que proporciona una explicación detallada sobre los principios del rastreo y una descripción de los tipos de rastreo específicos.
- **Bloquear todo:** haga clic en el botón ubicado en la sección inferior del cuadro de diálogo para indicar expresamente que no desea ninguna actividad de recopilación de datos (*para obtener detalles, consulte el capítulo [Bloqueo de los procesos de seguimiento](#)*).
- **Configuración de Do Not Track:** haga clic en este botón en la sección inferior del cuadro de diálogo para llegar a la página web en la que puede ajustar la configuración específica de varios parámetros de **AVG Do Not Track** (*consulte el capítulo [Configuración de AVG Do Not Track](#) para obtener información detallada*).

8.2. Información sobre los procesos de seguimiento



La lista de servicios de recopilación de datos detectados informa sólo el nombre del servicio específico. Para realizar una decisión experta acerca del bloqueo o el acceso del servicio correspondiente, es posible que necesite más información. Mueva su mouse sobre el elemento de la lista en cuestión. Aparecerá un icono de información con detalles sobre el servicio. Sabrá si el servicio recopila datos personales u otros datos disponibles, si esos datos se comparten con terceros y si los datos se almacenan para un posible uso posterior:



En la sección inferior del icono de información podrá ver el hipervínculo **Política de privacidad**, que lo redirige al sitio web dedicado a la política de privacidad del servicio detectado respectivo.

8.3. Bloqueo de los procesos de seguimiento

Con las listas de todos los Ad Networks, Social Buttons o Web Analytics, ahora tiene la opción de controlar qué servicios se deben bloquear. Tiene dos opciones:

- **Bloquear todos.** al seleccionar este botón en la sección inferior del diálogo, indica expresamente que no desea ninguna actividad de recopilación de datos. *(Sin embargo, tenga en cuenta que esta acción quizás afecte la funcionalidad en la página web respectiva en la que el servicio funciona.)*
-  Si no desea bloquear de una vez todos los servicios detectados, puede especificar si desea bloquear o permitir cada servicio individualmente. Puede permitir que algunos de los sistemas detectados se ejecuten (*por ej., Web Analytics*): estos sistemas usan los datos recopilados para optimizar sus sitios web y de esta forma ayudan a mejorar el entorno común de Internet para todos los usuarios. Sin embargo, puede, al mismo tiempo, bloquear todas las actividades de recopilación de datos de los procesos clasificados como Ad Networks. Simplemente haga clic en el icono  junto al servicio respectivo para bloquear la recopilación de datos (*el nombre del proceso aparecerá tachado*) o para volver a permitir la recopilación de datos.

8.4. Configuración de AVG Do Not Track

El cuadro de diálogo **Opciones de Do Not Track** ofrece las siguientes opciones de configuración:



- **Do Not Track está activado:** de forma predeterminada, el servicio DNT está activo (*posición ACTIVADO*). Para desactivar el servicio, cámbielo a la posición DESACTIVADO.
- En la sección central del cuadro de diálogo puede ver un cuadro con una lista de servicios conocidos de recopilación de datos que pueden clasificarse como Ad Networks. De forma



predeterminada, **Do Not Track** bloquea ciertos Ad Networks automáticamente y es decisión suya bloquear o permitir el resto. Para ello, haga clic en el botón **Bloquear todo** debajo de la lista. O bien, puede utilizar el botón **Predeterminados** para cancelar todos los cambios de configuración realizados y regresar a la configuración original.

- **Notificar a los sitios web...:** en esta sección puede activar o desactivar la opción **Notificar a los sitios web que no deseo ser rastreado** (activada de forma predeterminada). Mantenga esta opción marcada para confirmar que desea que **Do Not Track** informe a los proveedores de un servicio de recopilación de datos detectado que usted no desea que lo rastreen.

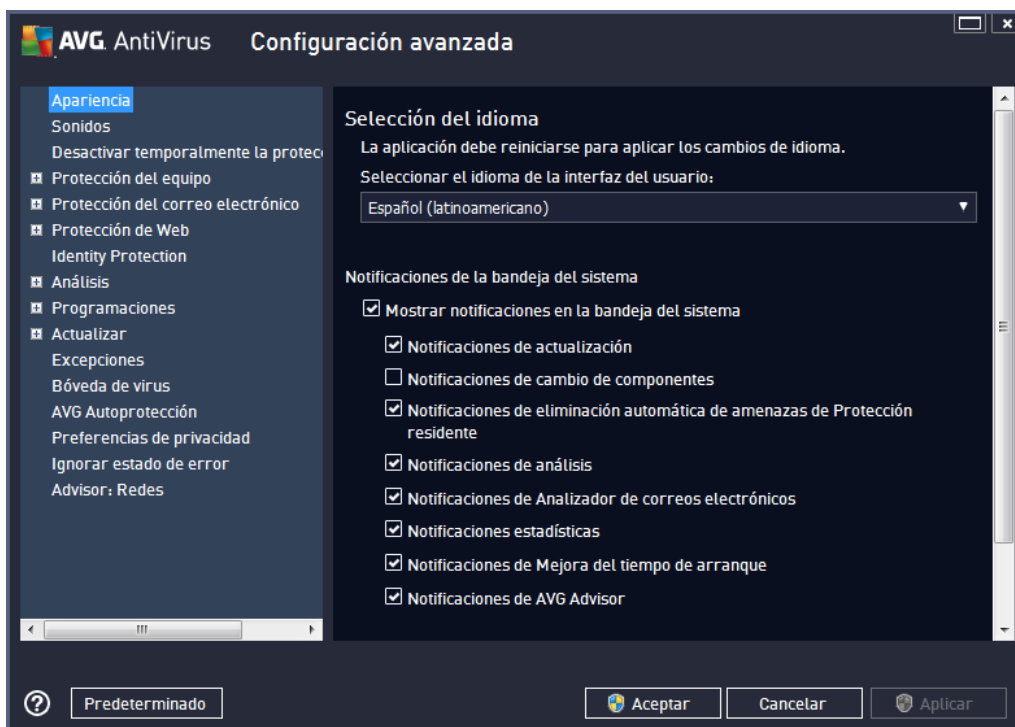


9. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG AntiVirus 2013** se abre en una ventana nueva denominada **Configuración avanzada de AVG**. La ventana está dividida en dos secciones: la parte izquierda ofrece una navegación organizada en forma de árbol hacia las opciones de configuración del programa. Seleccione el componente del que desea cambiar la configuración (o *su parte específica*) para abrir el diálogo de edición en la sección del lado derecho de la ventana.

9.1. Apariencia

El primer elemento del árbol de navegación, **Apariencia**, hace referencia a la configuración general de la [interfaz del usuario AVG AntiVirus 2013](#), y proporciona unas pocas opciones básicas del comportamiento de la aplicación:



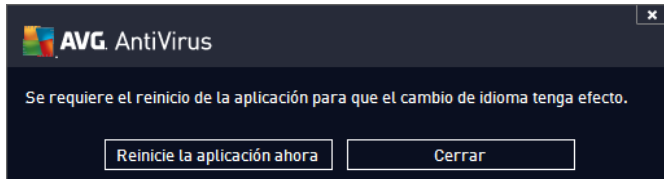
Selección del idioma

En la sección **Selección del idioma** puede seleccionar el idioma deseado en el menú desplegable. Este será el idioma que se utilice en toda la [interfaz del usuario AVG AntiVirus 2013](#). El menú desplegable sólo ofrece los idiomas que haya seleccionado con anterioridad para instalarse durante el proceso de instalación además del inglés (*que se instala automáticamente, de forma predeterminada*). Para terminar de cambiar el idioma de su **AVG AntiVirus 2013** debe reiniciar la aplicación. Por favor siga estos pasos:

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



- Presione el botón **Aceptar** para confirmar.
- Se abre un nuevo cuadro de diálogo que le informa de que para cambiar el idioma de la aplicación debe reiniciar su **AVG AntiVirus 2013**
- Presione el botón **Reinicie la aplicación ahora** para aceptar el reinicio del programa y espere un momento a que el cambio de idioma surta efecto:

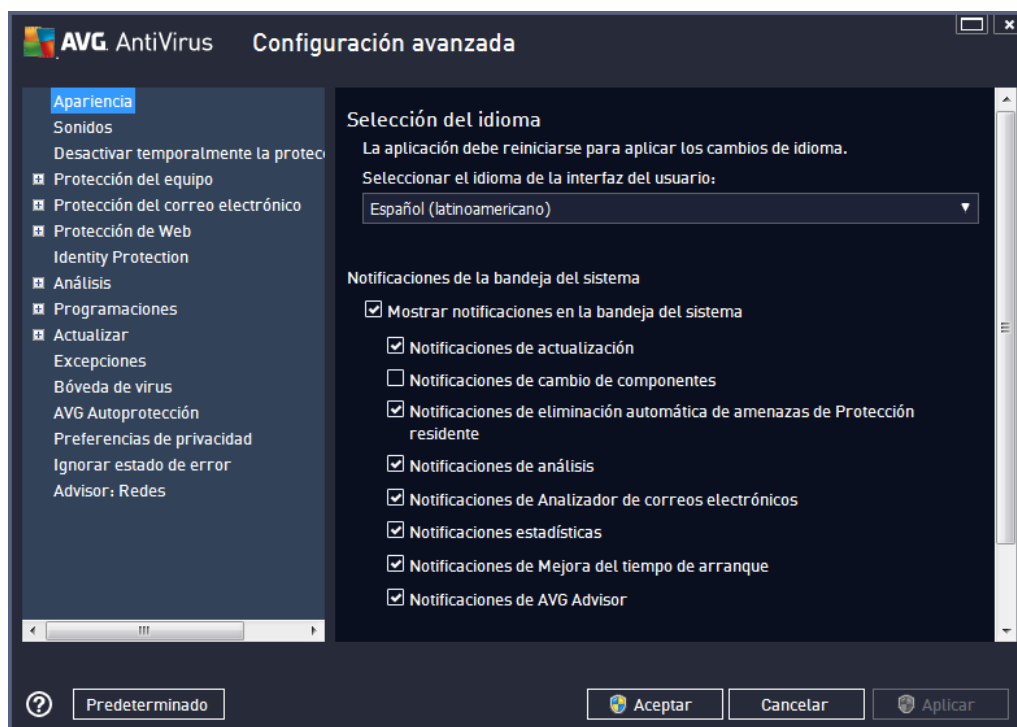


Notificaciones de la bandeja del sistema

En esta sección, puede suprimir la visualización de las notificaciones de la bandeja del sistema sobre el estado de la aplicación **AVG AntiVirus 2013**. De forma predeterminada, se permite la visualización de las notificaciones del sistema. Se recomienda encarecidamente mantener esta configuración. Las notificaciones del sistema informan, entre otras cosas, de la ejecución del proceso de actualización o de análisis, o del cambio de estado de un componente de **AVG AntiVirus 2013**. Es importante que ponga atención a estas notificaciones.

Sin embargo, si por alguna razón decide que no desea que se muestren este tipo de notificaciones, o que sólo desea ver algunas de ellas (*relacionadas con un componente específico de AVG AntiVirus 2013*), puede definir y especificar sus preferencias seleccionando/quitando la marca de selección de las siguientes opciones:

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



- **Notificaciones de actualización** (activada de forma predeterminada): decida si debe visualizarse información sobre la ejecución, el progreso y la finalización del proceso de actualización de **AVG AntiVirus 2013**.
- **Notificaciones de cambio de componentes** (desactivada de forma predeterminada) : decida si debe visualizarse información relativa a la actividad o inactividad de los componentes o los posibles problemas. A la hora de notificar un estado de error de un componente, esta opción equivale a la función informativa del [icono de la bandeja del sistema](#), que notifica un problema en cualquier componente de **AVG AntiVirus 2013**.
- **Notificaciones de eliminación automática de amenazas de Protección residente** (activada de forma predeterminada): decida si debe visualizarse o suprimirse la información relativa a los procesos de guardado, copia y apertura de archivos (esta configuración solo se muestra si la opción *Autoreparar de Protección residente* está activada).
- **Notificaciones de análisis** (activada de forma predeterminada): decida si debe visualizarse información sobre la ejecución automática del análisis programado, su progreso y resultados.
- **Las notificaciones de Analizador de correos electrónicos** (activada de forma predeterminada): decida si debe visualizarse información sobre el análisis de todos los mensajes de correo electrónico entrantes y salientes.
- **Notificaciones estadísticas** (activada de forma predeterminada): mantenga la opción seleccionada para permitir la notificación regular de revisión de estadísticas en la bandeja del sistema.



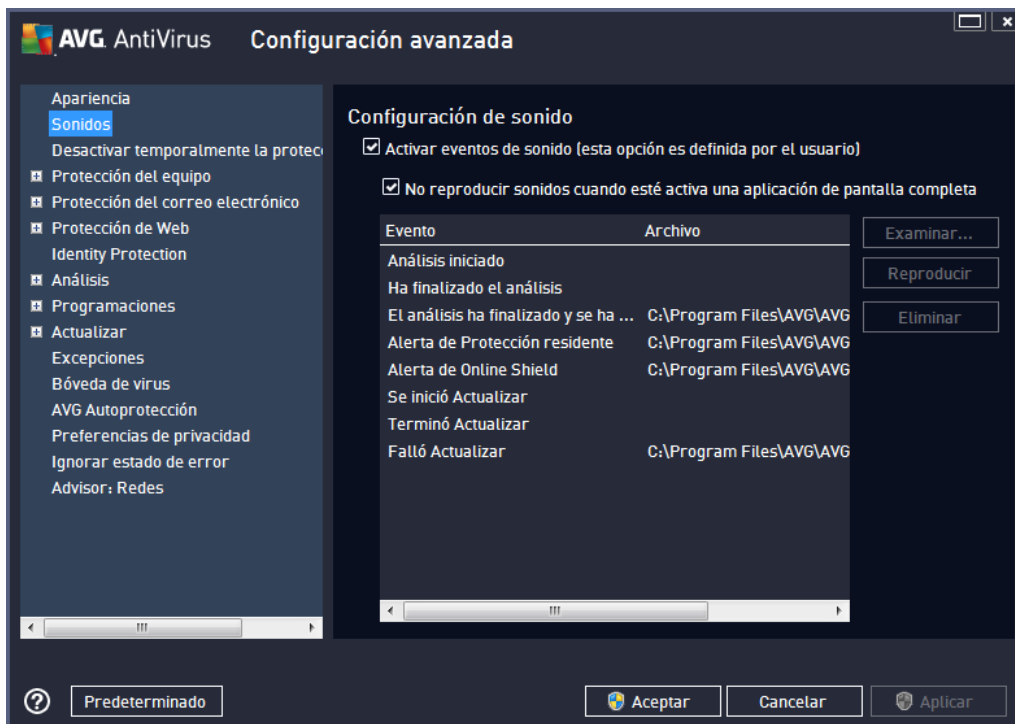
- **Notificaciones de Mejora del tiempo de arranque** (desactivada de forma predeterminada): decida si desea que se le informe sobre la aceleración del tiempo de arranque de su equipo.
- **Notificaciones de AVG Advisor** (activada de forma predeterminada): decida si debe mostrar la información de las actividades de [AVG Advisor](#) en el panel deslizable en la bandeja del sistema.

Modo de juego

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

9.2. Sonidos

En el cuadro de diálogo **Sonidos**, puede especificar si desea que se le informe acerca de acciones específicas de **AVG AntiVirus 2013** mediante una notificación sonora:



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



(consulte también el capítulo [Configuración avanzada/Apariencia](#) en este documento).

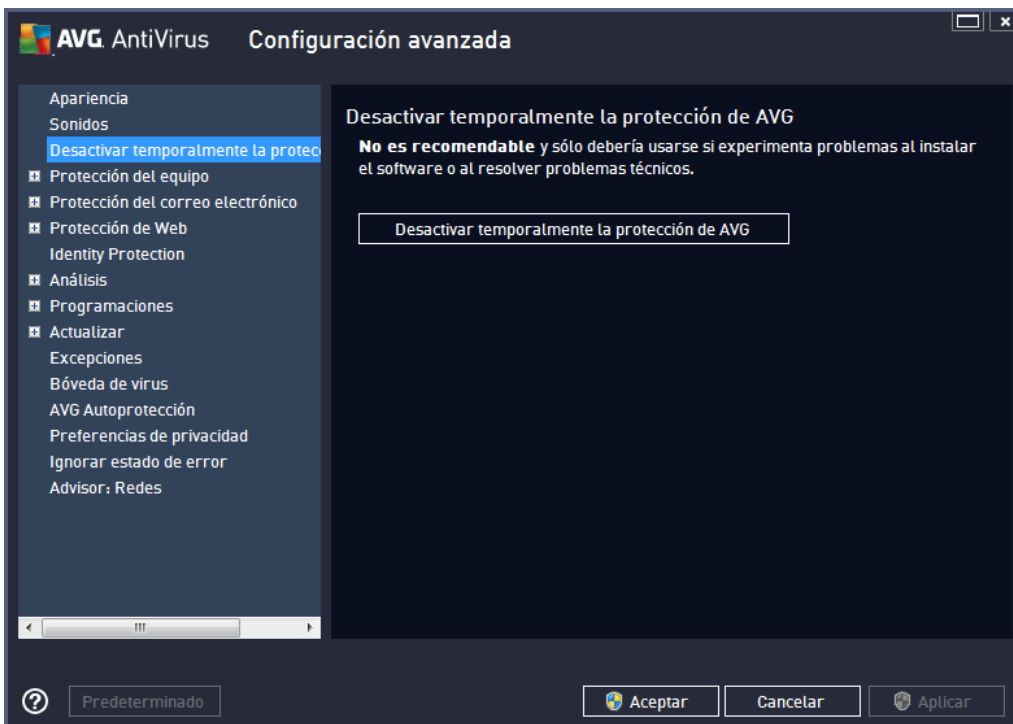
Botones de control

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

9.3. Desactivar temporalmente la protección de AVG

En el cuadro de diálogo **Desactivar temporalmente la protección de AVG** tiene la opción de desactivar toda la protección que proporciona **AVG AntiVirus 2013** a la vez.

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



En la mayoría de los casos, **no es necesario** desactivar **AVG AntiVirus 2013** antes de instalar nuevo software o controladores, ni siquiera si el instalador o el asistente de software le sugiere que cierre los programas y aplicaciones que se estén ejecutando para asegurarse de que no se producen interrupciones no deseadas durante el proceso de instalación. Si realmente experimenta problemas durante la instalación, intente primero desactivar la protección residente (**Activar Protección residente**). Si tiene que desactivar temporalmente **AVG AntiVirus 2013**, debe volver a activarlo en cuanto termine. Si está conectado a Internet o a una red durante el tiempo que el software antivirus está desactivado, su equipo será vulnerable ante los ataques..



Cómo desactivar la protección de AVG

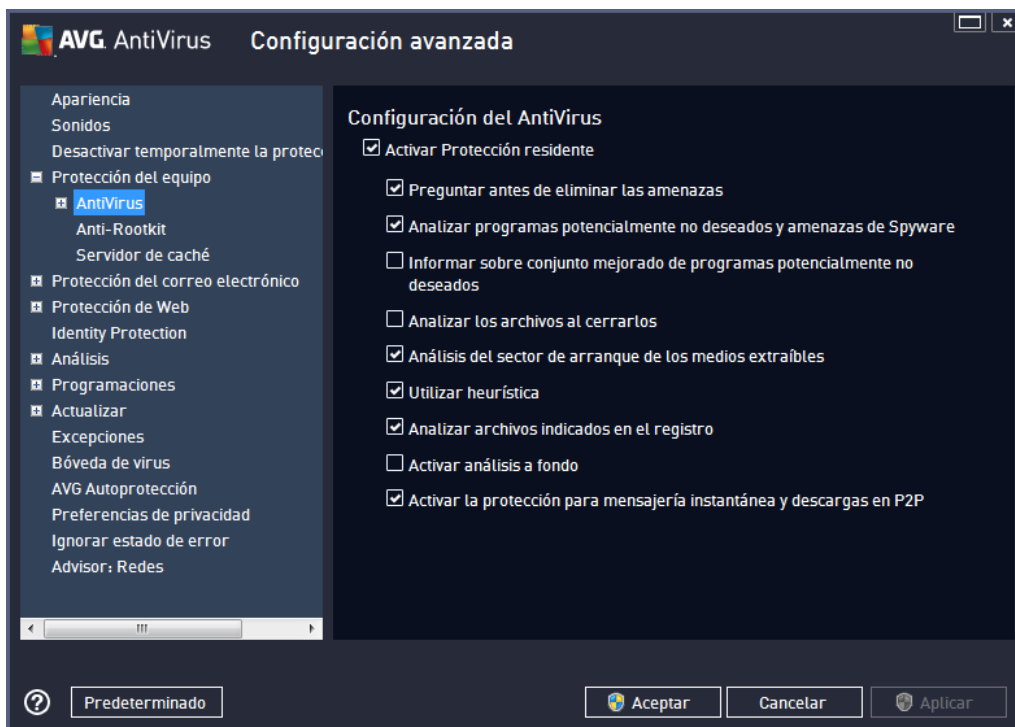
Marque la casilla de verificación **Desactivar temporalmente la protección de AVG** y presione el botón **Aplicar** para confirmar su elección. En el cuadro de diálogo **Desactivar temporalmente la protección de AVG** recién abierto, especifique por cuánto tiempo desea desactivar su **AVG AntiVirus 2013**. De forma predeterminada, la protección permanece desactivada durante 10 minutos, que deberían ser suficientes para cualquier tarea común, como la instalación de nuevo software, etc. Puede definir un periodo de tiempo más prolongado; sin embargo, esta opción no es recomendada de no ser absolutamente necesaria. Posteriormente, todos los componentes desactivados se activarán automáticamente otra vez. Como máximo, puede desactivar la protección de AVG hasta reiniciar nuevamente el equipo.



9.4. Protección del equipo

9.4.1. AntiVirus

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



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

- **Preguntar antes de eliminar las amenazas** (activada de forma predeterminada): seleccione esta opción para que la Protección residente no realice ninguna acción de manera automática; si la selecciona, muestra un cuadro de diálogo que describe la amenaza detectada y le permite decidir qué debe hacer. Si deja la casilla sin seleccionar, **AVG AntiVirus 2013** reparará la infección automáticamente y, si no es posible, el objeto se moverá a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (activada de forma predeterminada): seleccione esta opción para activar el análisis de spyware y de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar sobre conjunto mejorado de programas potencialmente no deseados** (desactivada de manera predeterminada): seleccione esta opción para detectar paquetes extendidos de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Analizar los archivos al cerrarlos** (desactivada de forma predeterminada): el análisis al cerrar garantiza que AVG analiza los objetos activos (por ejemplo, aplicaciones,

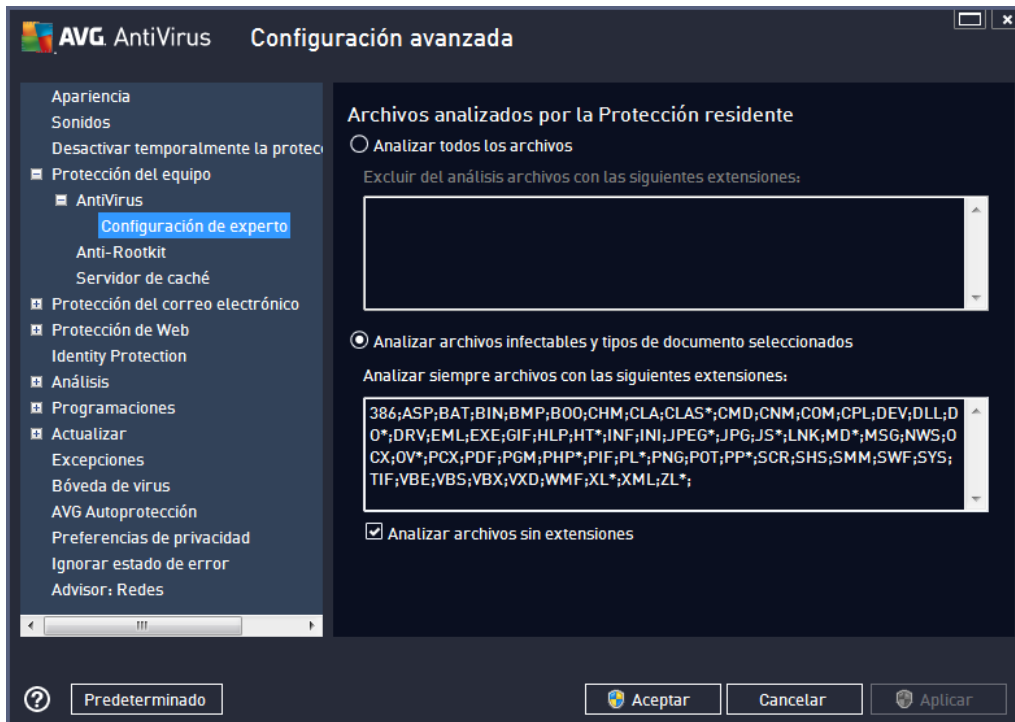


documentos, etc.) cuando se abren y también cuando se cierran; esta función le ayuda a proteger el equipo frente a algunos tipos de virus sofisticados.

- **Análisis del sector de arranque de los medios extraíbles** (activada de manera predeterminada)
- **Utilizar heurística** (activada de forma predeterminada): el análisis heurístico se utilizará para la detección (emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual).
- **Analizar archivos indicados en el registro** (activado de manera predeterminada): este parámetro define que AVG analizará todos los archivos ejecutables añadidos al registro de inicio para evitar que una infección conocida se ejecute durante el siguiente inicio del equipo.
- **Activar análisis a fondo** (desactivada de forma predeterminada): en determinadas situaciones (en un estado de extrema emergencia) puede marcar esta opción para activar los algoritmos más minuciosos, que comprobarán a fondo todos los objetos remotamente amenazantes. Pero recuerde que este método consume mucho tiempo.
- **Activar la protección para mensajería instantánea y descargas en P2P** (activada de forma predeterminada): seleccione esta opción si desea verificar que la comunicación de mensajería instantánea (por ej., AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...) y los datos descargados dentro de redes punto a punto (redes que permiten la conexión directa entre clientes, sin un servidor, lo que resulta potencialmente peligroso; comúnmente utilizadas para compartir archivos de música) no tengan virus.



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

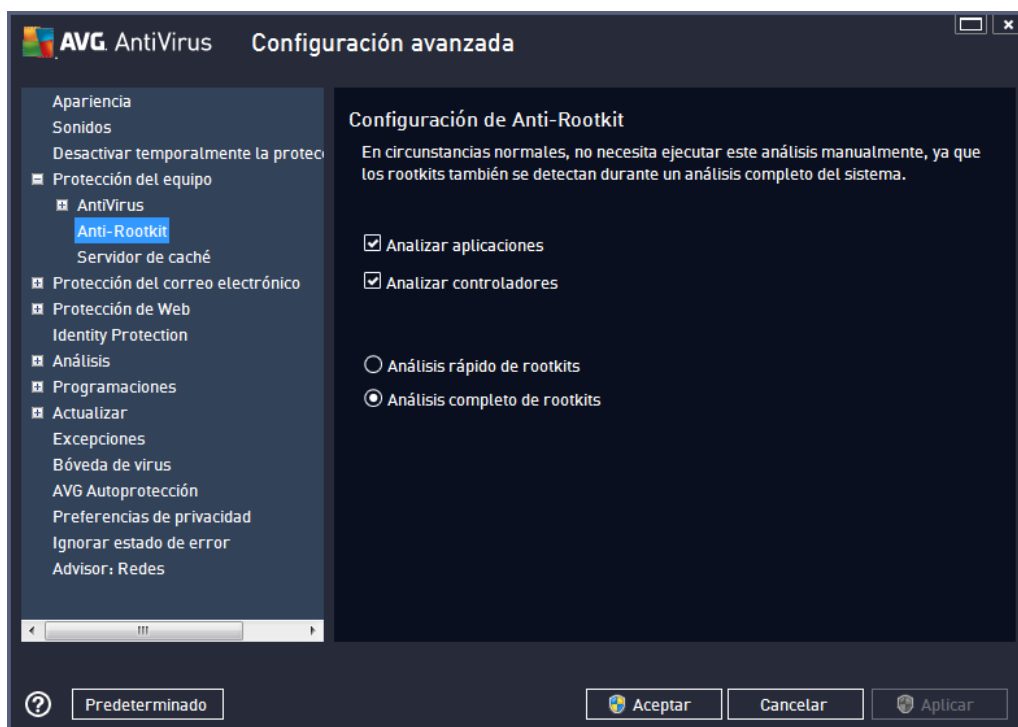


Marque la casilla de verificación respectiva para decidir si desea **Analizar todos los archivos** o solamente **Analizar archivos infectables y tipos de documento seleccionados**. Para agilizar el análisis y proporcionar al mismo tiempo el nivel máximo de protección, recomendamos que conserve la configuración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

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

9.4.2. Anti-Rootkit

En el cuadro de diálogo de la **configuración de Anti-Rootkit**, puede editar la configuración y los parámetros específicos del servicio **Anti-Rootkit** del análisis anti-rootkit. El análisis anti-rootkit es un proceso predeterminado incluido en el [Análisis de todo el equipo](#):

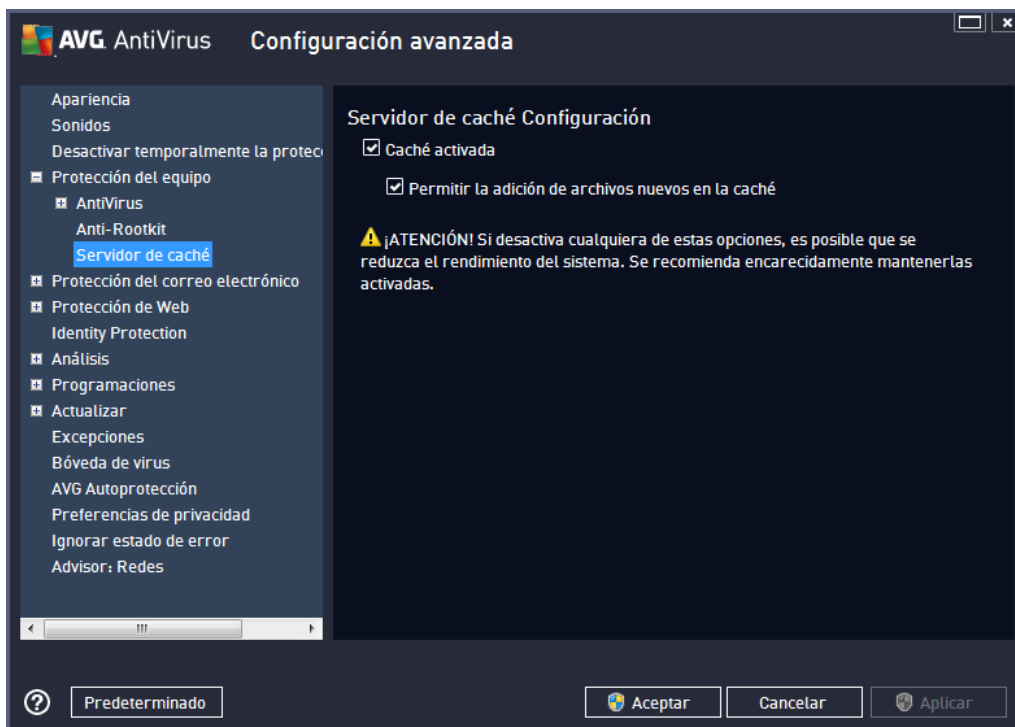


Analizar aplicaciones y **Analizar controladores** le permiten especificar en detalle qué debe incluirse en el análisis anti-rootkit. Esta configuración está diseñada para usuarios avanzados; le recomendamos mantener todas las opciones activadas. También puede seleccionar el modo de análisis de rootkits:

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

9.4.3. Servidor de caché

El cuadro de diálogo **Configuración del servidor de caché** hace referencia al proceso del servidor de caché diseñado para aumentar la velocidad de todos los tipos de análisis de **AVG AntiVirus 2013**:



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

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

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

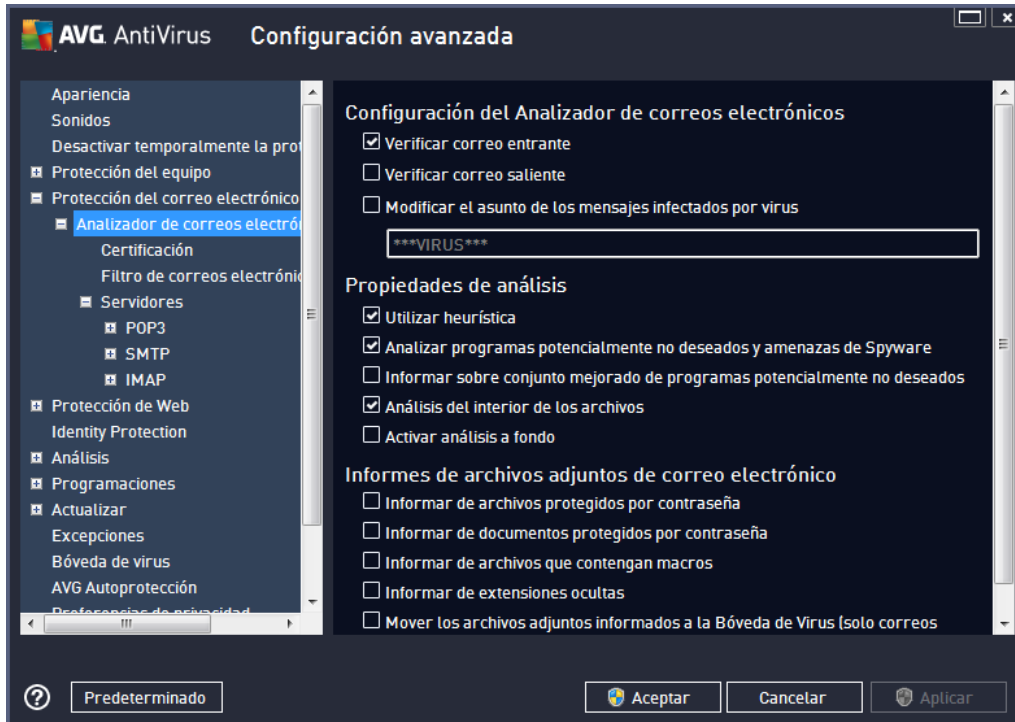
A menos que tenga un buen motivo para desactivar el servidor de caché, se recomienda especialmente que conserve la configuración predeterminada y deje las opciones activadas. De lo contrario, puede experimentar una disminución significativa en la velocidad y el rendimiento de su sistema.

9.5. Analizador de correos electrónicos

En esta sección se puede editar la configuración detallada del [Analizador de correos electrónicos](#) y Anti-Spam:

9.5.1. Analizador de correos electrónicos

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



Análisis de correo electrónico

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

- **Verificar correo entrante** (*activada de forma predeterminada*): marque esta opción para activar o desactivar la opción de análisis de todos los mensajes de correo electrónico enviados a su cliente de correo
- **Verificar correo saliente** (*desactivada de forma predeterminada*): marque esta opción para activar o desactivar la opción de analizar todos los correos electrónicos enviados desde su cuenta
- **Modificar el asunto de los mensajes infectados por virus** (*desactivada de forma predeterminada*): si desea que se le avise si el mensaje de correo electrónico analizado se detectó como infectado, marque este elemento y escriba el texto que desea en el campo de texto. Entonces este texto se agregará al campo "Asunto" de cada mensaje de correo electrónico detectado con el fin de facilitar la identificación y el filtrado. El valor predeterminado es *****VIRUS*****, y recomendamos conservarlo.

Propiedades de análisis

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



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

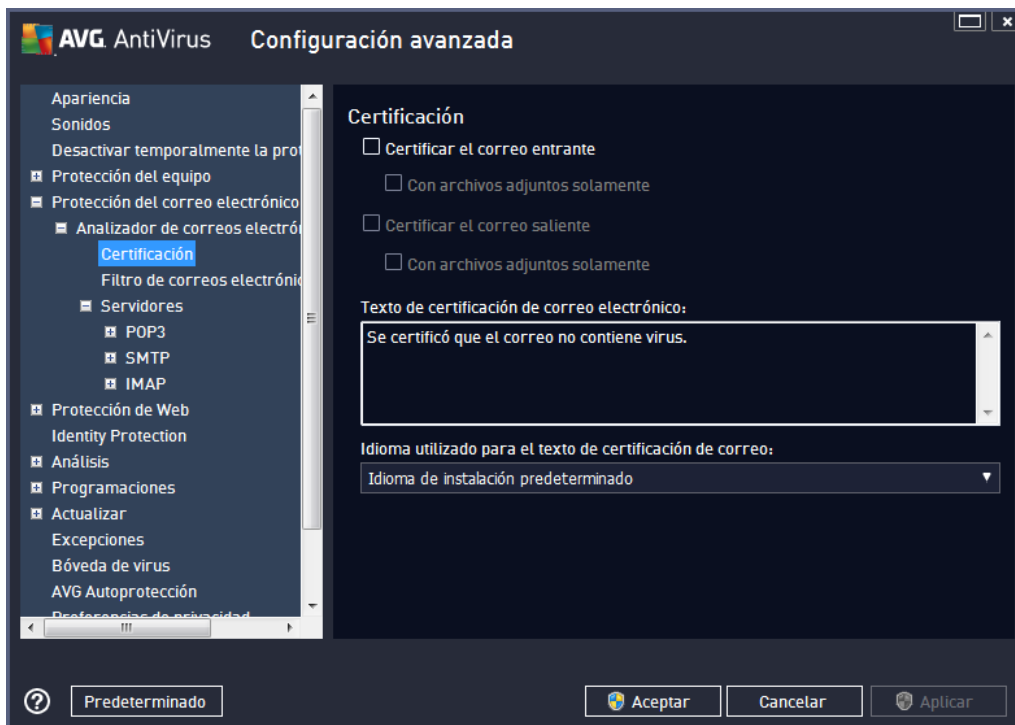
Informes de archivos adjuntos de correo electrónico

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

- **Informar de los archivos protegidos por contraseña:** los archivos (*ZIP, RAR, etc.*) que están protegidos por contraseña no pueden analizarse en busca de virus; seleccione la casilla para informar éstos como potencialmente peligrosos.
- **Informar acerca de los documentos protegidos por contraseña:** no es posible analizar los documentos protegidos por contraseña en busca de virus; seleccione la casilla para informar de ellos como potencialmente peligrosos.
- **Informar acerca de los archivos que contienen macros:** una macro es una secuencia predefinida de pasos encaminados a hacer que ciertas tareas sean más fáciles para el usuario (*las macros de MS Word son ampliamente conocidas*). Como tal, una macro puede contener instrucciones potencialmente peligrosas, y podría ser útil seleccionar la casilla para garantizar que los archivos con macros se reporten como sospechosos.

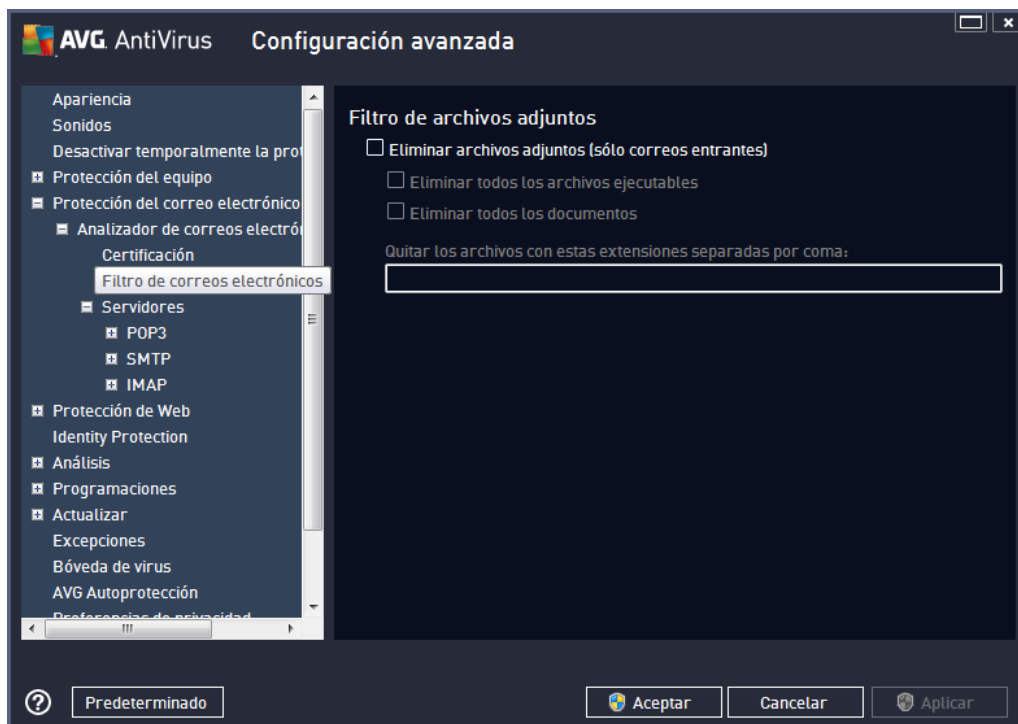
- **Informar acerca de las extensiones ocultas:** las extensiones ocultas pueden hacer, por ejemplo, que un archivo ejecutable sospechoso "algo.txt.exe" parezca un archivo de texto simple inofensivo "algo.txt"; seleccione la casilla para informar de estos archivos como potencialmente peligrosos.
- **Mueva los informes de archivos adjuntos a Bóveda de virus:** especifique si desea que se le notifique mediante correo electrónico acerca de los archivos protegidos con contraseña, los documentos protegidos por contraseña, los archivos que contienen macros y los archivos con extensión oculta detectados como un dato adjunto del mensaje del correo electrónico analizado. Si durante el análisis se identifica un mensaje en estas condiciones, defina si el objeto infeccioso detectado se debe mover a la [Bóveda de virus](#).

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



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

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



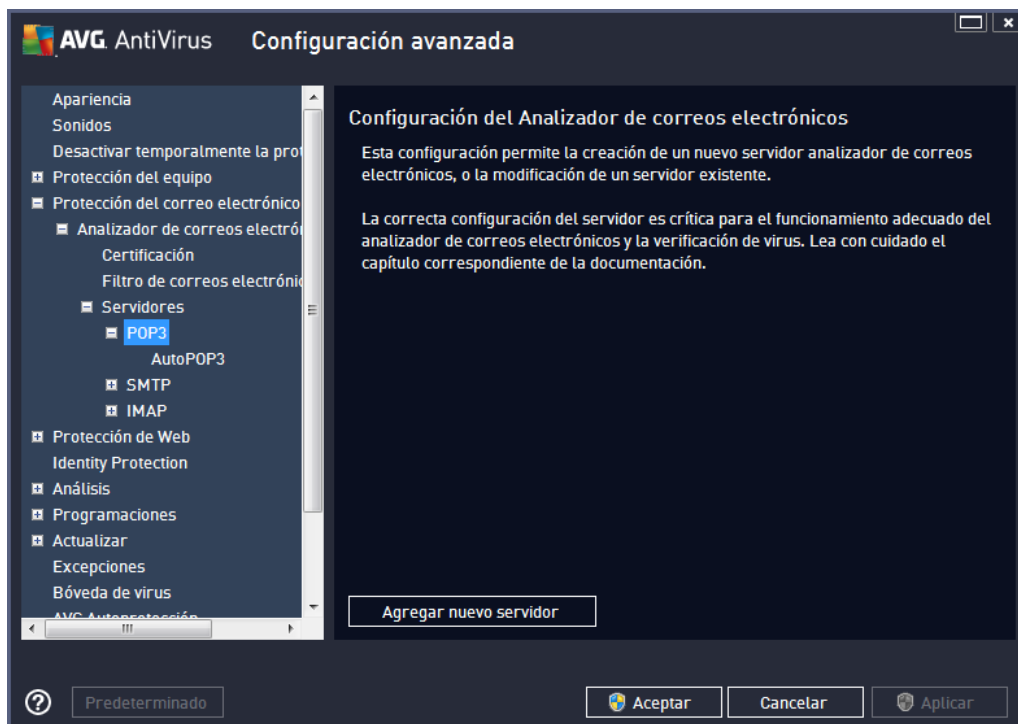
El cuadro de diálogo **Filtro de archivos adjuntos** le permite establecer los parámetros para el análisis de los archivos adjuntos de los mensajes de correo electrónico. De manera predeterminada, la opción **Eliminar archivos adjuntos** está desactivada. Si decide activarla, todos los archivos adjuntos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

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

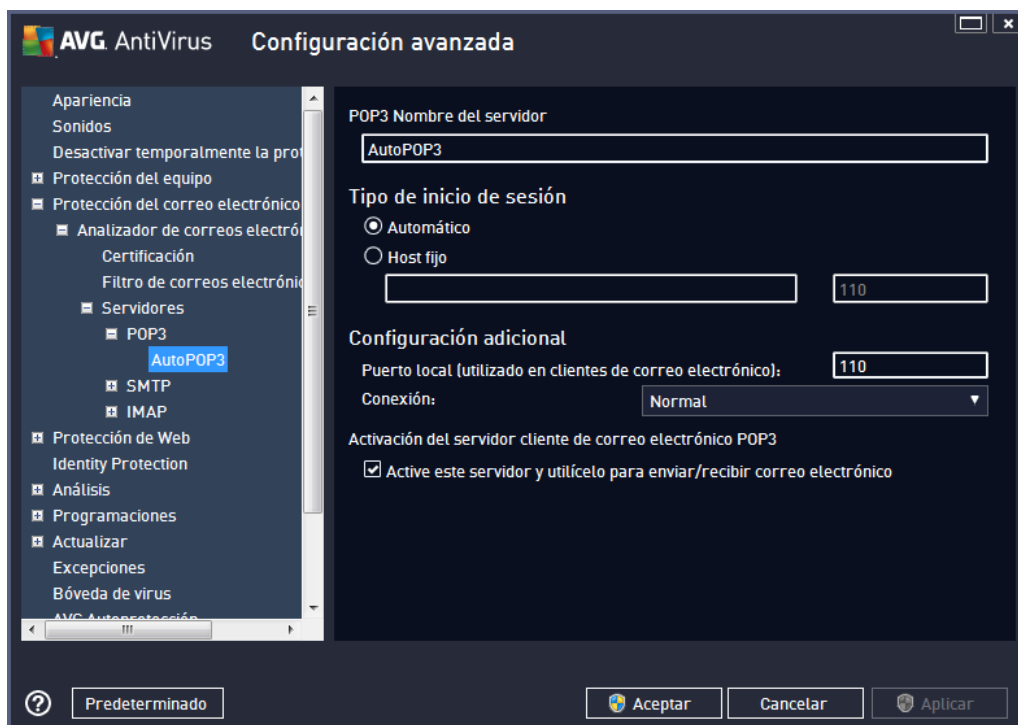
En la sección **Servidores** podrá editar parámetros para los servidores del [Analizador de correos electrónicos](#):

- [Servidor POP3](#)
- [Servidor SMTP](#)
- [Servidor IMAP](#)

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



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

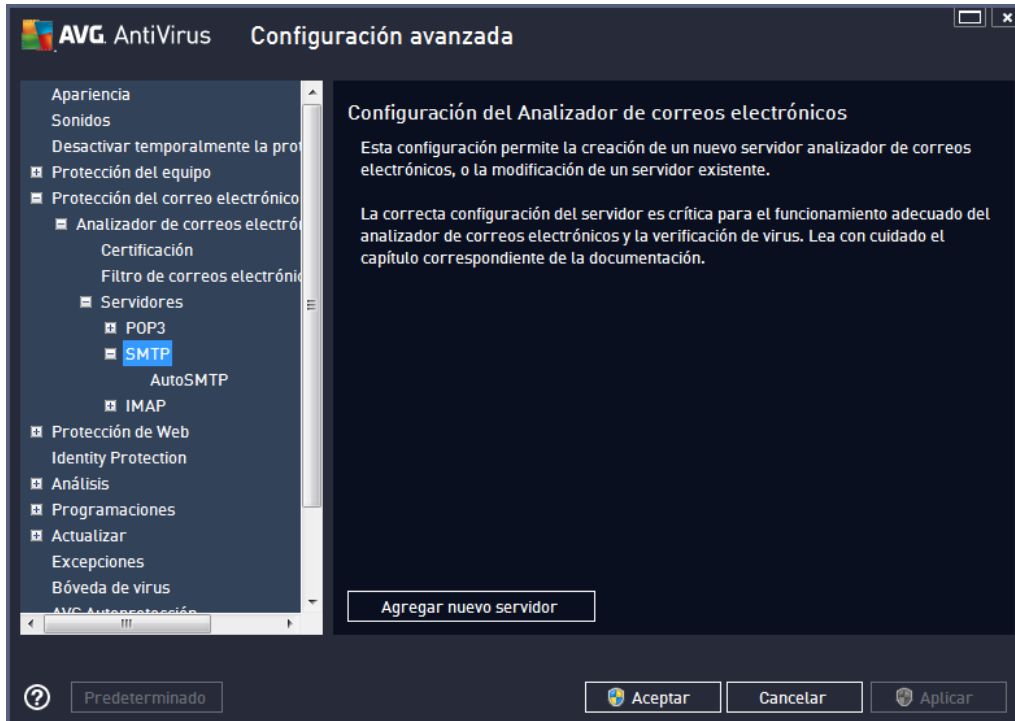


- **Nombre del servidor POP3:** en este campo podrá especificar el nombre de los servidores

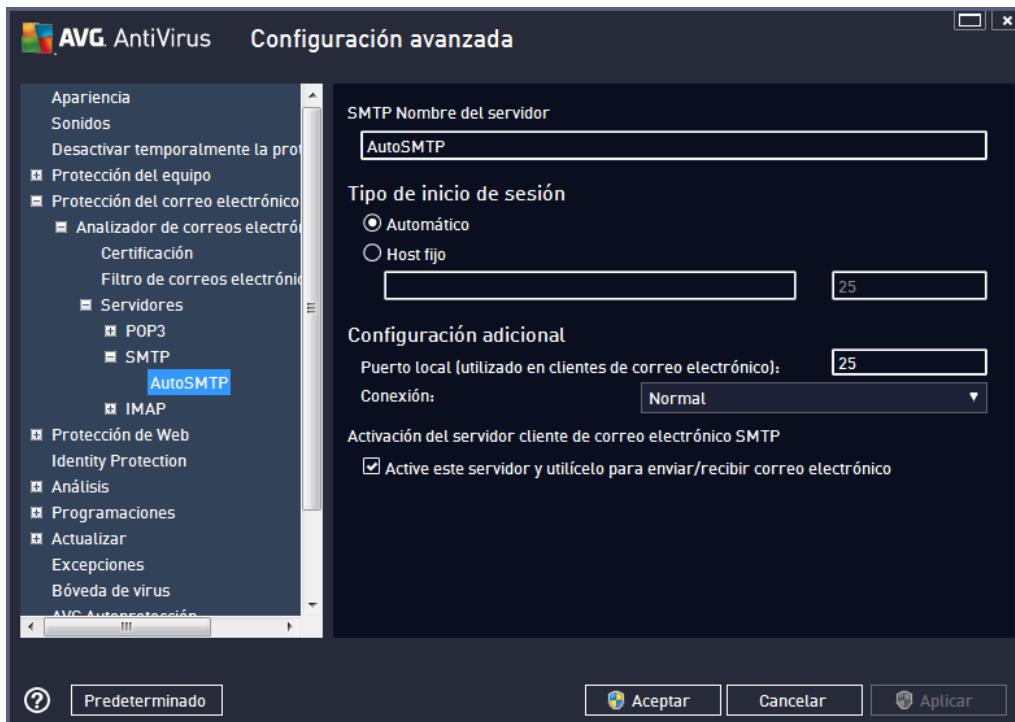


nuevos (para agregar un servidor POP3, haga clic con el botón secundario del mouse en el elemento POP3 del menú de navegación de la izquierda). Para los servidores "AutoPOP3" creados automáticamente, este campo está desactivado.

- **Tipo de inicio de sesión:** define el método para determinar el servidor de correo empleado para el correo entrante:
 - **Automático:** el inicio de sesión se realizará de manera automática, de acuerdo con la configuración del cliente de correo electrónico.
 - **Host fijo:** en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. El nombre de inicio de sesión permanece sin cambiar. Como nombre, puede utilizar un nombre de dominio (por ejemplo, *pop.acme.com*), así como una dirección IP (por ejemplo, *123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (por ejemplo, *pop.acme.com:8200*). El puerto estándar para comunicaciones POP3 es 110.
- **Configuración adicional:** especifica los parámetros con mayor detalle:
 - **Puerto local:** especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Luego debe especificar en su aplicación de correo este puerto como el puerto para comunicaciones POP3.
 - **Conexión:** en el menú desplegable, puede especificar la clase de conexión que desea utilizar (*normal/SSL/SSL predeterminado*). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.
- **Activación del servidor de cliente POP3 de correo electrónico:** seleccione o quite la marca de selección de este elemento para activar o desactivar el servidor POP3 especificado



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

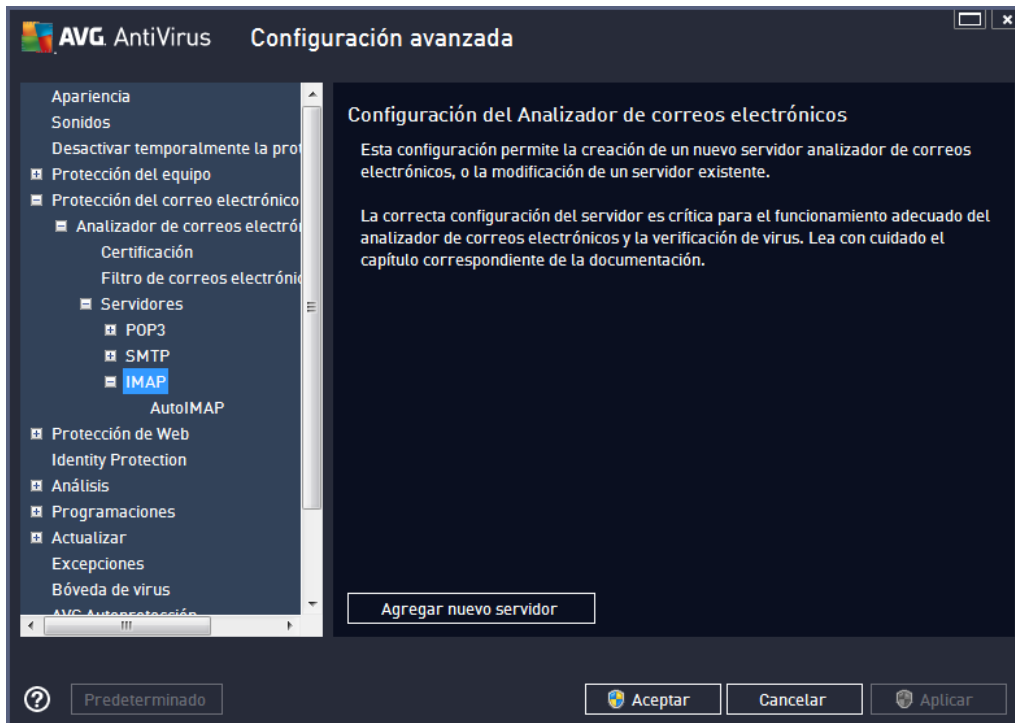


- **Nombre del servidor SMTP:** en este campo podrá especificar el nombre de los servidores

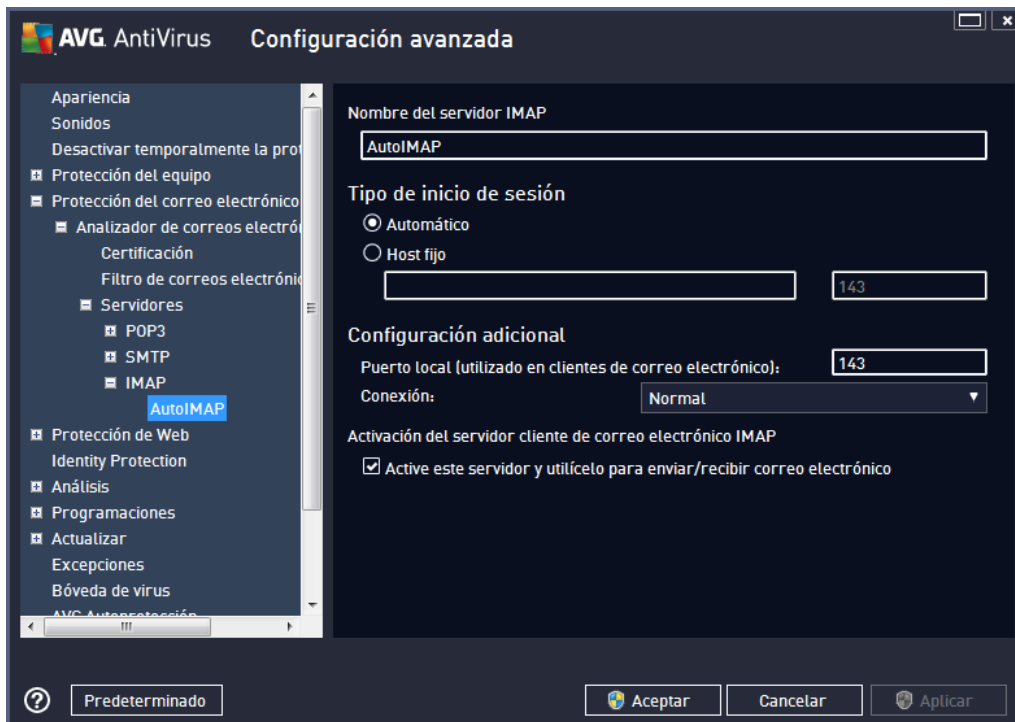


recién agregados (*para agregar un servidor SMTP, haga clic con el botón secundario del mouse en el elemento SMTP del menú de navegación de la izquierda*). Para los servidores "AutoSMTP" creados automáticamente, este campo está desactivado.

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



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



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

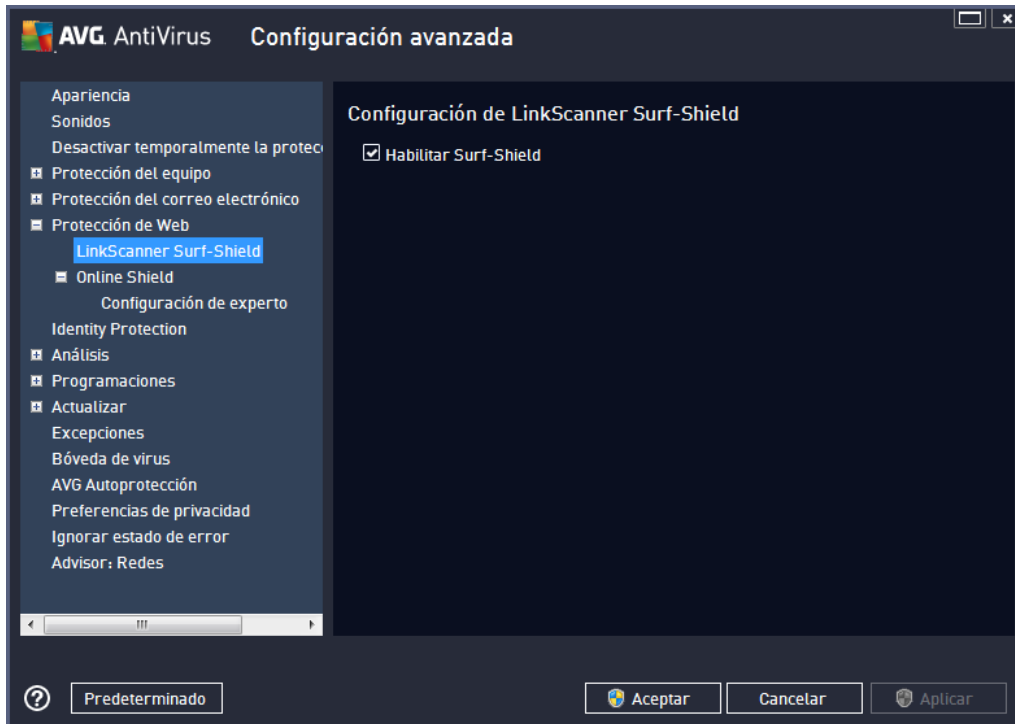


recién agregados (*para agregar un servidor IMAP, haga clic con el botón secundario del mouse en el elemento IMAP del menú de navegación de la izquierda*). Para los servidores "AutoIMAP" creados automáticamente, este campo está desactivado.

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

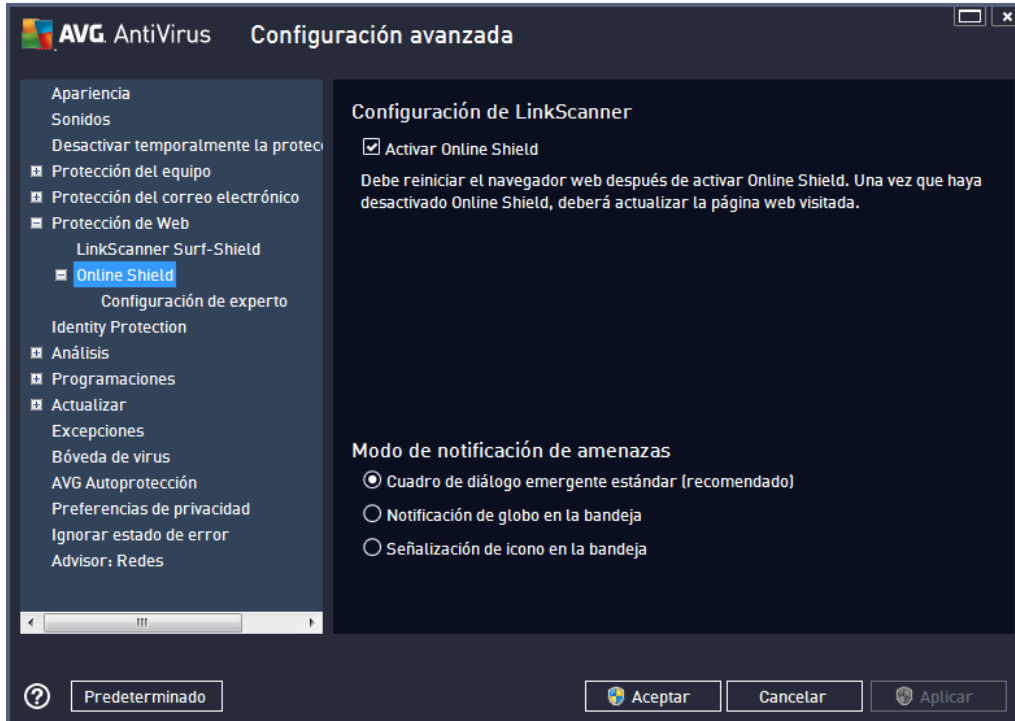
9.6. Protección de la navegación web

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



- **Activar Surf-Shield** (*activado de forma predeterminada*): protección (*en tiempo real*) activa contra sitios de explotación a medida que se accede a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario accede a ellos a través de un navegador web (*o cualquier otra aplicación que utilice HTTP*).
- **Agregue 'Asegurado con LinkScanner'...** (*desactivado de forma predeterminada*): confirme esta opción para asegurarse de que todos los mensajes enviados desde las redes sociales Facebook/MySpace que contengan hipervínculos activos estarán certificados como comprobados por LinkScanner.

9.6.1. Online Shield

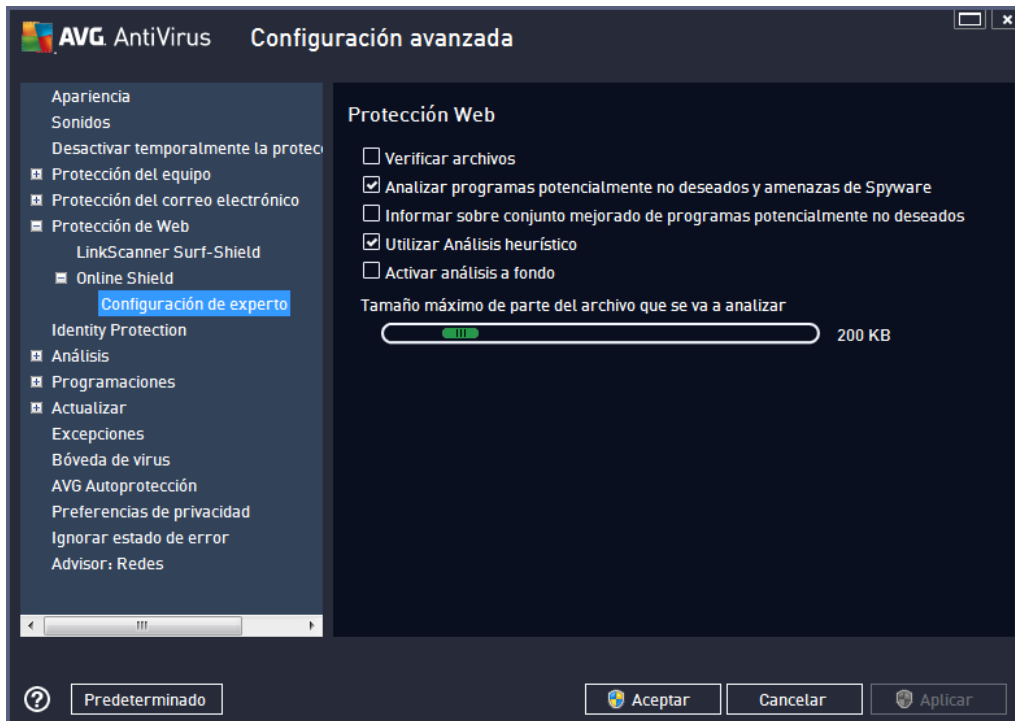


El cuadro de diálogo **Online Shield** ofrece las siguientes opciones:

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

Modo de notificación de amenazas

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



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

- **Habilitar Protección web:** esta opción confirma que **Online Shield** debe realizar un análisis o el contenido de la página www. Siempre y cuando esta opción esté activada (*de forma predeterminada*), también puede activar/desactivar estos elementos:
 - **Verificar archivos:** (*desactivada de manera predeterminada*): analiza el contenido de los archivos que pudieran existir en la página web que se visualizará.
 - **Analizar programas potencialmente no deseados y amenazas de Spyware** (*activada de forma predeterminada*): seleccione esta opción para activar el análisis de spyware y de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
 - **Informar sobre conjunto mejorado de programas potencialmente no deseados:** (*desactivada de manera predeterminada*): seleccione esta opción para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
 - **Utilizar análisis heurístico:** (*activada de manera predeterminada*): analiza el contenido de la página que se visualizará utilizando el método de análisis heurístico (



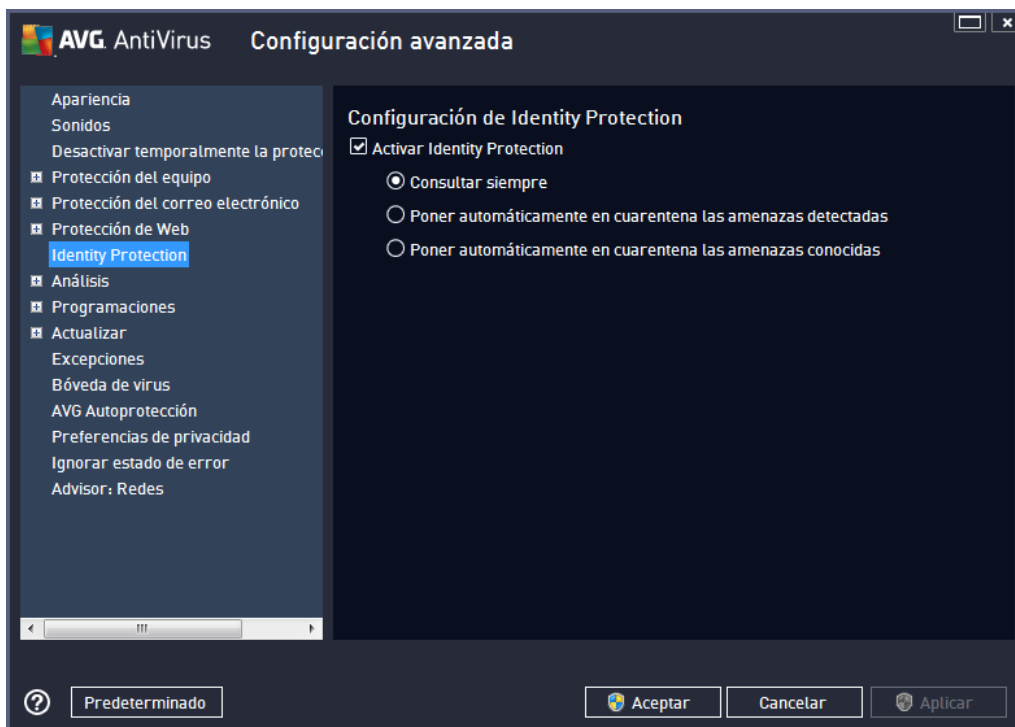
emulación dinámica de las instrucciones del objeto analizado en un entorno virtual).

- **Activar análisis a fondo** (*desactivado de manera predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Tamaño máximo de parte del archivo que se va a analizar**: si los archivos incluidos están presentes en la página visualizada, también puede analizar su contenido incluso antes de que se descarguen en el equipo. Sin embargo, el análisis de archivos grandes toma bastante tiempo y es posible que la descarga de la página web se ralentice de modo notable. Puede emplear la barra deslizante para especificar el tamaño máximo de archivo que se analizará con **Online Shield**. Incluso si el archivo descargado es más grande de lo especificado y, por lo tanto, no se analizará con Online Shield, todavía estará protegido: si el archivo está infectado, la **Protección residente** lo detectará de inmediato.
- **Excluir host/IP/dominio**: puede escribir el nombre exacto de un servidor (*host, dirección IP, dirección IP con máscara o URL*) o un dominio que no debe analizarse con **Online Shield** en el campo de texto. Por lo tanto, excluya solamente hosts de los que esté absolutamente seguro de que nunca le proveerán de contenido peligroso.

9.7. Identity Protection

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

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



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

Es altamente recomendable no hacer esto a menos que sea absolutamente necesario.

Cuando Identity Protection está activa, se puede especificar qué hacer cuando se detecta una amenaza:

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

9.8. Análisis

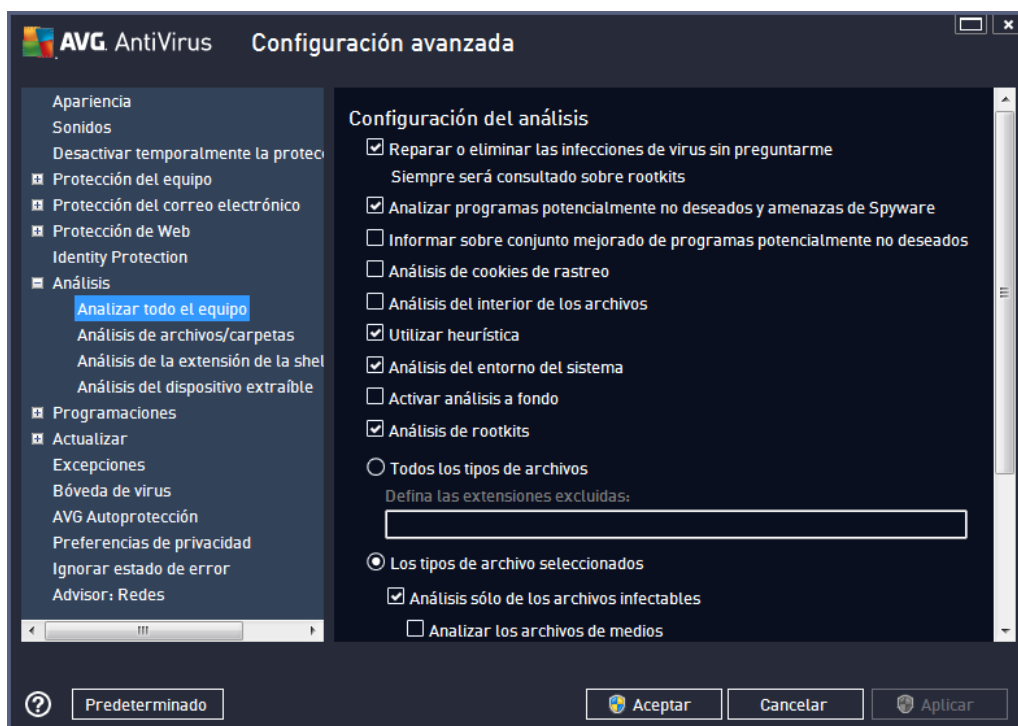
La configuración avanzada del análisis se divide en cuatro categorías con referencia a los tipos específicos de análisis definidos por el proveedor del software:

- **[Analizar todo el equipo](#)**: análisis predefinido estándar de todo el equipo

- **[Análisis de la extensión de la shell](#)**: análisis específico de un objeto seleccionado directamente del entorno del Explorador de Windows
- **[Análisis de archivos/carpetas](#)**: análisis estándar predefinido de áreas seleccionadas del equipo
- **[Análisis del dispositivo extraíble](#)**: análisis específico de dispositivos extraíbles conectados a su equipo

9.8.1. Análisis de todo el equipo

La opción **Análisis de todo el equipo** le permite editar los parámetros de uno de los análisis predefinidos por el proveedor de software, el [Análisis de todo el equipo](#):



Configuración del análisis

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

- **Reparar o eliminar las infecciones de virus sin preguntarme** (activado de manera predeterminada): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (activada de forma predeterminada): seleccione esta opción para activar el análisis de spyware y de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen



intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

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

También debe decidir si desea analizar

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



Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

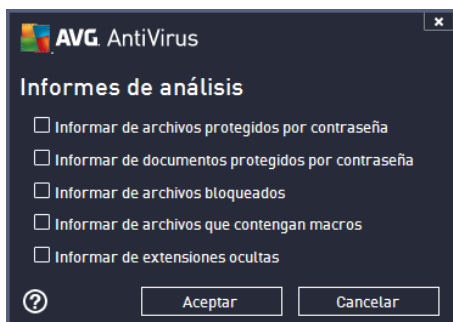
- De manera opcional, puede decidir si desea **Analizar archivos sin extensiones**: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

Ajustar el tiempo que tarda el análisis en completarse

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

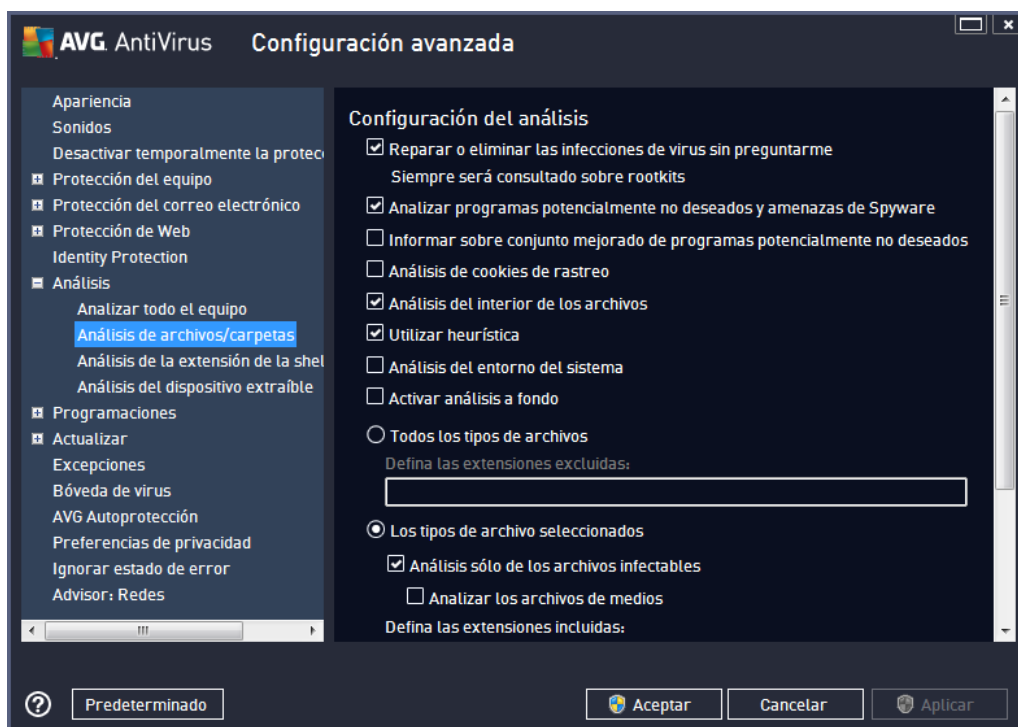
Configurar informes de análisis adicionales ...

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



9.8.2. Análisis de archivos/carpetas

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

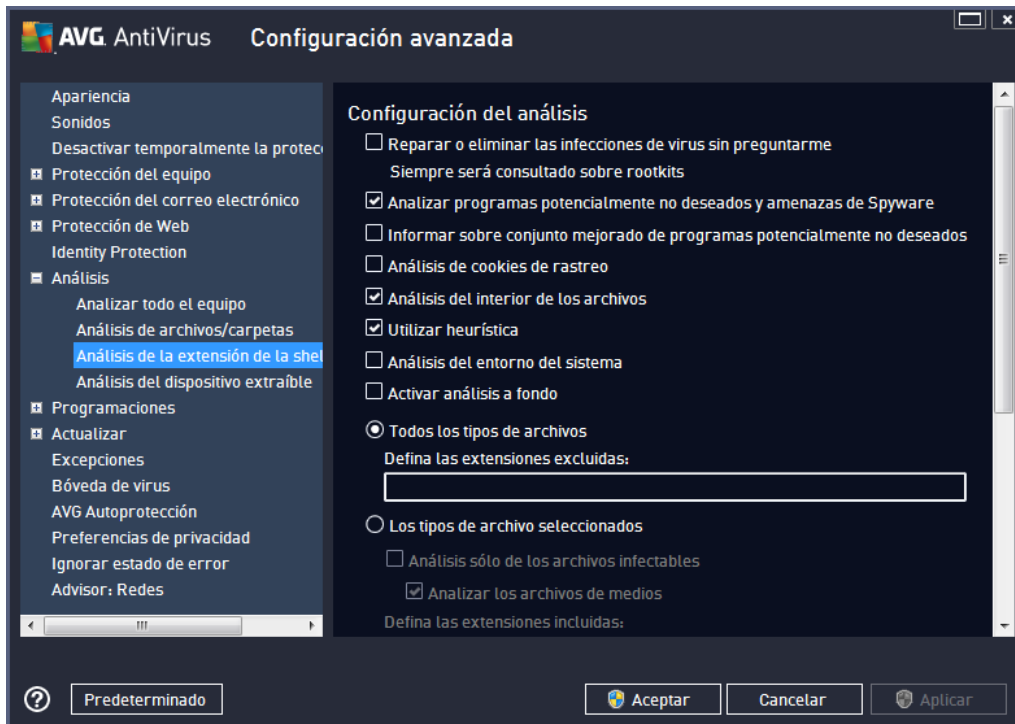


Todos los parámetros definidos en este diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con [Análisis de archivos o carpetas](#).

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

9.8.3. Análisis de la extensión de la shell

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



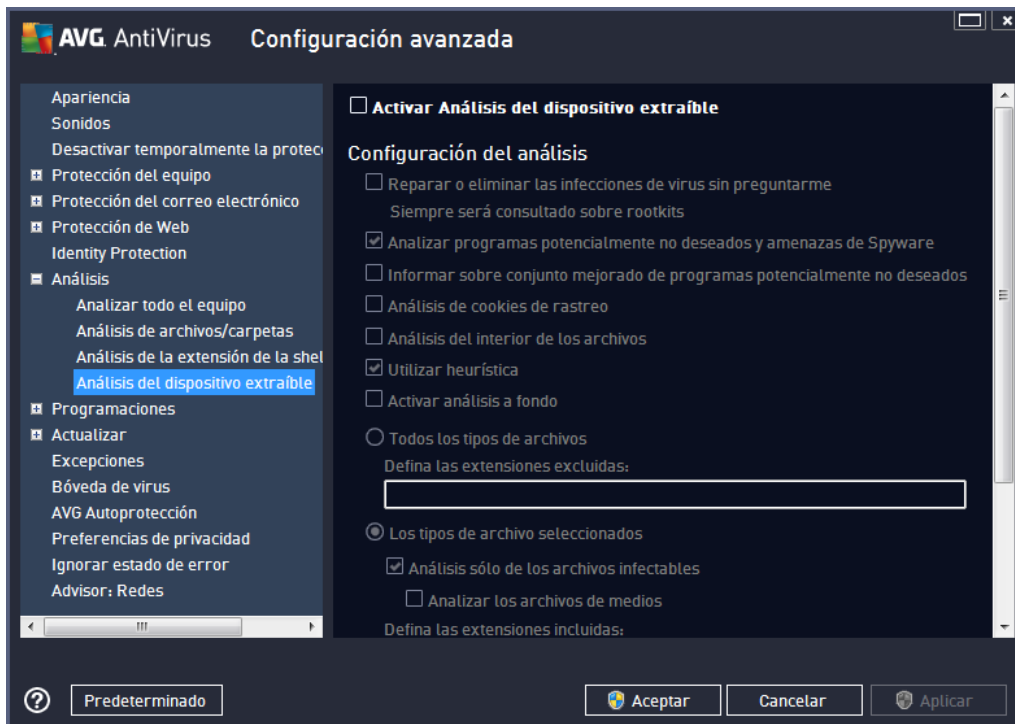
La lista de parámetros muestra parámetros idénticos a los que están disponibles para [Analizar todo el equipo](#). Sin embargo, la configuración predeterminada es diferente (*por ejemplo, el análisis de todo el equipo no comprueba de manera predeterminada los archivos, pero sí analiza el entorno del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

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

En comparación con el cuadro de diálogo [Analizar todo el equipo](#), el cuadro de diálogo **Análisis de la extensión de la shell** también incluye la sección **Otros ajustes relacionados con la interfaz de usuario de AVG**, donde puede especificar si desea tener acceso al progreso del análisis y sus resultados desde la interfaz de usuario de AVG. Asimismo, puede definir que el resultado del análisis sólo se muestre en caso de que se detecte una infección durante el análisis.

9.8.4. Análisis del dispositivo extraíble

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



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

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

9.9. Programaciones

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

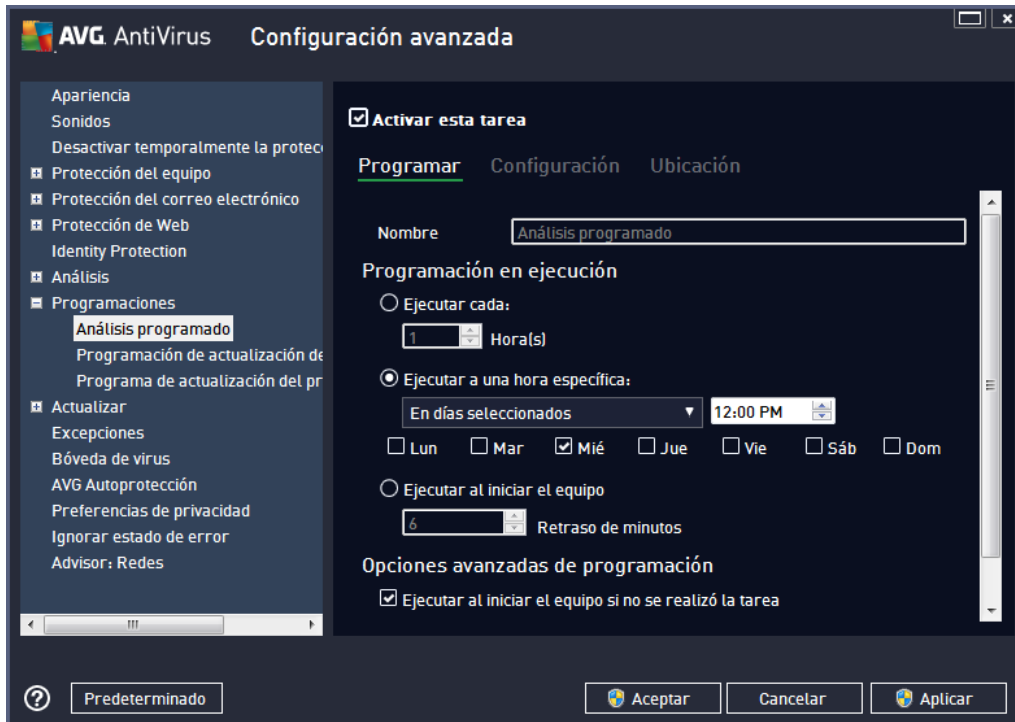
- [Análisis programado](#)
- [Programación de actualización de las definiciones](#)
- [Programación de actualización del programa](#)

9.9.1. Análisis programado

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



activar cuando sea necesario:



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

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

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

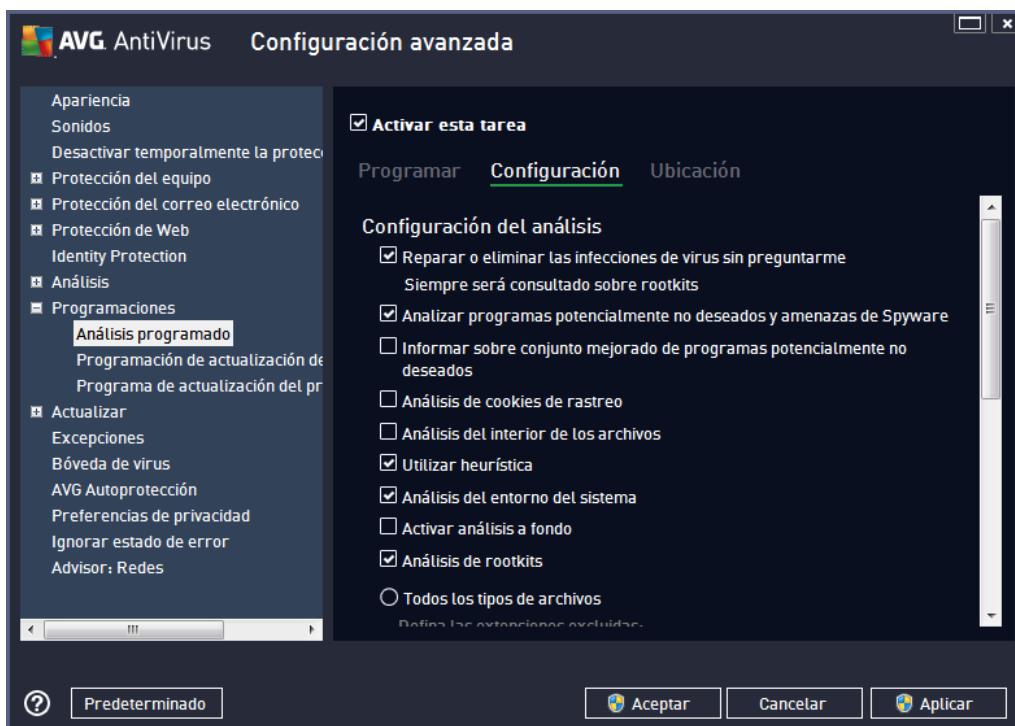
Programación en ejecución

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

Opciones avanzadas de programación

Esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado. Una vez que se inicia el análisis programado en la hora que se especificó, se le informará de este hecho mediante una ventana emergente que se abre sobre el [icono en la bandeja de sistema AVG](#).

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



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

- **Reparar o eliminar las infecciones de virus sin preguntarme** (activada de forma predeterminada): si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (activado de forma predeterminada): marcar para activar el análisis de spyware, además de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un



riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- **Informar sobre conjunto mejorado de programas potencialmente no deseados** (*desactivado de forma predeterminada*): marcar para detectar paquetes extendidos de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Análisis de cookies de rastreo** (*desactivado de forma predeterminada*): este parámetro especifica que se deben detectar cookies durante el análisis; (las cookies *HTTP* se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico)
- **Análisis del interior de los archivos** (*desactivado de forma predeterminada*): este parámetro especifica que el análisis debe comprobar todos los archivos, incluso si se almacenan dentro de un archivo, por ej., ZIP, RAR, ...
- **Utilizar método heurístico** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.
- **Analizar el entorno del sistema** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- **Activar análisis a fondo** (*desactivado de forma predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Analizar en busca de rootkits** (*activado de forma predeterminada*): Anti-Rootkit busca en su equipo posibles rootkits, es decir, programas y tecnologías que cubran la actividad de malware en su equipo. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

También debe decidir si desea analizar

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



Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

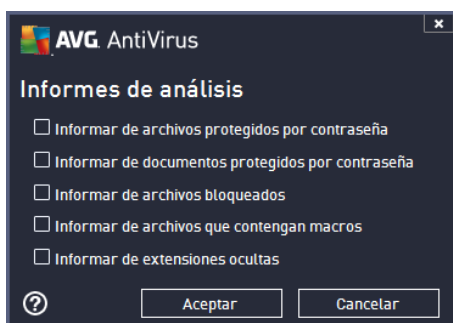
- De manera opcional, puede decidir si desea **Analizar archivos sin extensiones**: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

Ajustar el tiempo que tarda el análisis en completarse

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

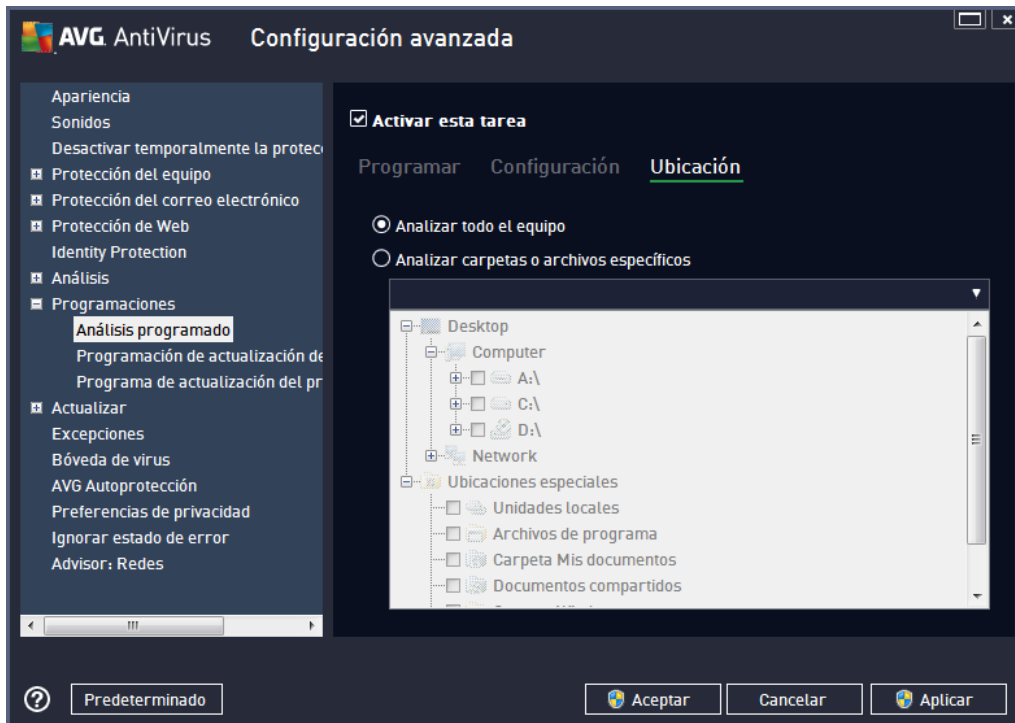
Configurar informes de análisis adicionales

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



Opciones de apagado del equipo

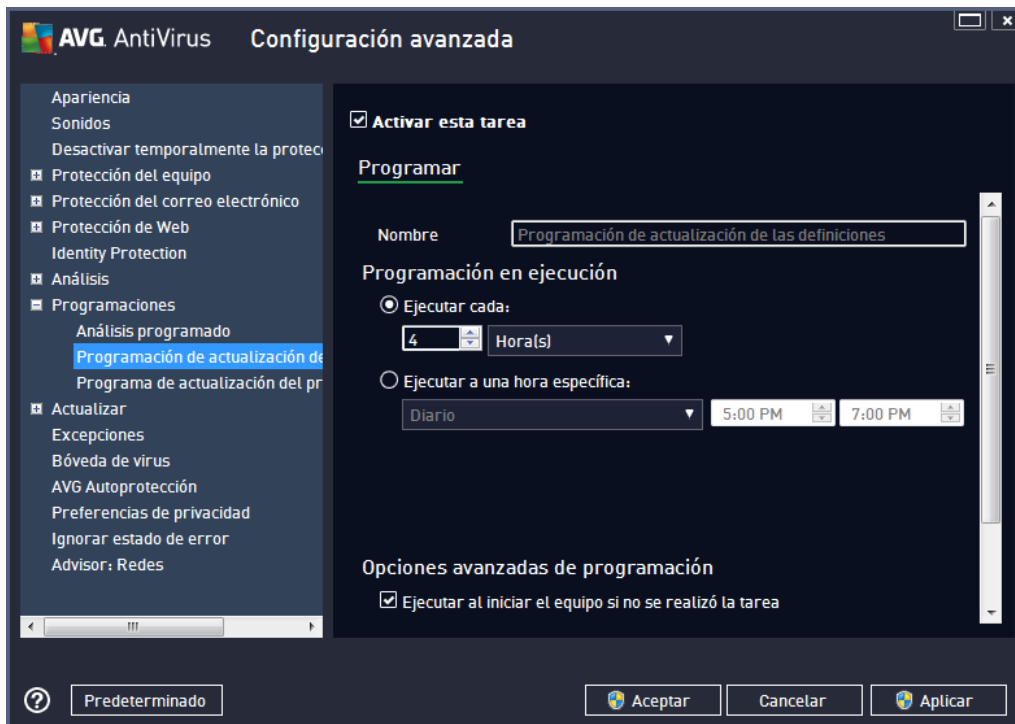
En la sección **Opciones de apagado del equipo**: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (**Apagado del equipo después de la finalización del análisis**), se activa una nueva opción, que permite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



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

9.9.2. Programación de actualización de las definiciones

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



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

Programación en ejecución

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

Opciones avanzadas de programación

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

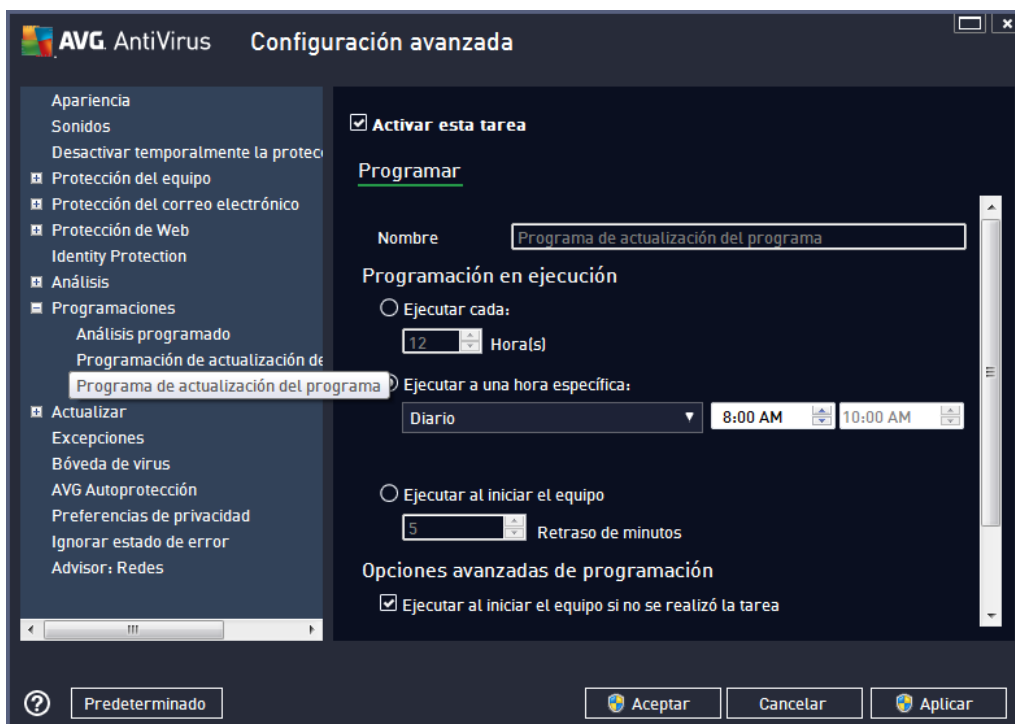
Otra configuración de actualización

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

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

9.9.3. Programación de actualización del programa

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



El campo de texto **Nombre** (desactivado para todos los programas predeterminados) indica el nombre asignado a este programa por proveedor de programa.

Programación en ejecución

Aquí, especifique los intervalos de tiempo para la ejecución de la actualización del programa recién programada. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto periodo de tiempo (**Ejecutar cada ...**), definiendo una fecha y hora exactas (**Ejecutar a una hora específica ...**) o posiblemente definiendo un evento con el que se debe asociar la ejecución de la actualización (**Acción basada en el inicio del equipo**).

Opciones avanzadas de programación

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



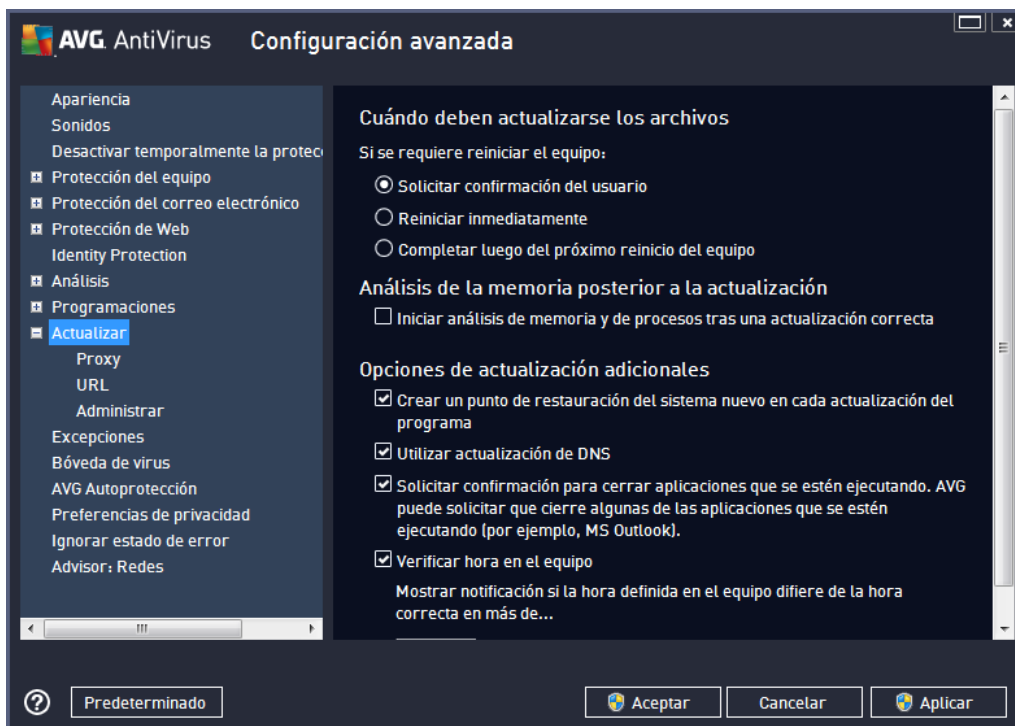
Otra configuración de actualización

Marque la opción **Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet** para asegurarse de que, si se interrumpe la conexión a Internet y el proceso de actualización de Anti-Spam falla, se iniciará otra vez inmediatamente después de restaurar la conexión a Internet. Una vez que se inicia la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el [icono de la bandeja del sistema AVG](#) (siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo [Configuración avanzada/Apariencia](#)).

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

9.10. Actualizar

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



Cuándo deben actualizarse los archivos

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



- **Solicitar confirmación del usuario** (*activada de forma predeterminada*): se le pedirá que apruebe un reinicio del equipo, necesario para finalizar el proceso de [actualización](#).
- **Reiniciar inmediatamente**: el equipo se reiniciará inmediatamente de forma automática después de que el proceso de [actualización](#) haya finalizado, y no será necesaria la aprobación del usuario.
- **Completar luego del próximo reinicio del equipo**: la finalización del proceso de [actualización](#) se pospondrá hasta el próximo reinicio del equipo. Tenga en cuenta que esta opción sólo se recomienda si puede estar seguro de que el equipo se reinicia regularmente, al menos diariamente.

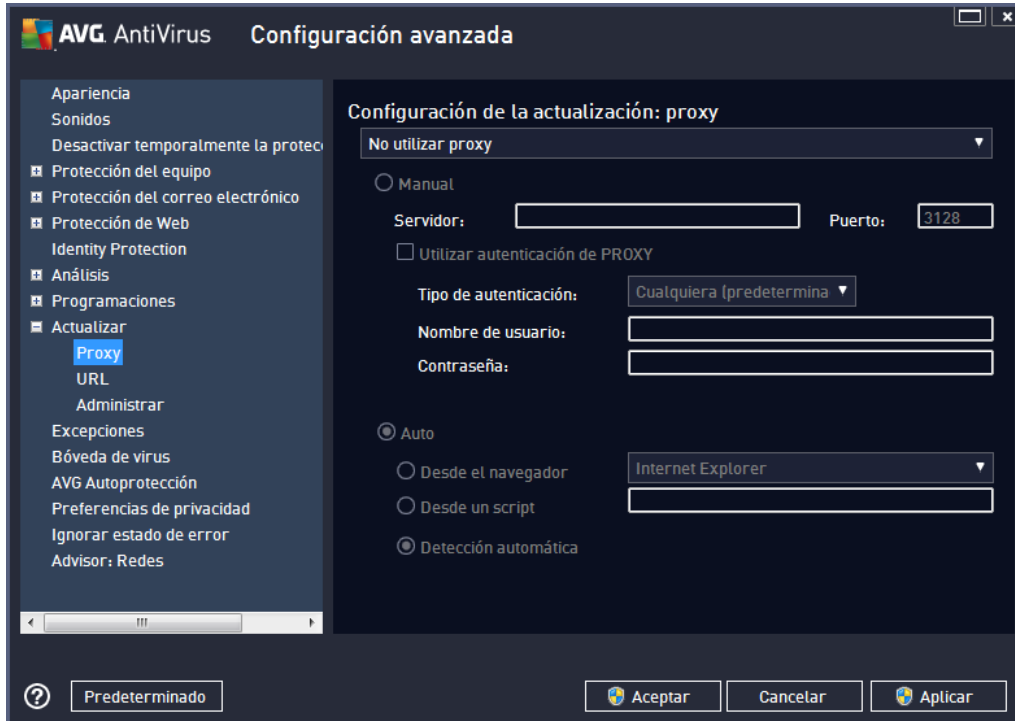
Análisis de la memoria posterior a la actualización

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

Opciones de actualización adicionales

- **Crear un nuevo punto de restauración del equipo durante cada actualización del programa**: antes de iniciar cada actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Se puede obtener acceso a esta opción mediante Inicio/Todos los programas/Accesorios/Herramientas del sistema/Restaurar sistema, pero se recomienda que sólo los usuarios experimentados realicen cambios. Mantenga esta casilla seleccionada si desea hacer uso de esta funcionalidad.
- **Utilizar actualización de DNS** (*activado de manera predeterminada*): si este elemento está marcado, una vez que se inicia la actualización, su **AVG AntiVirus 2013** busca la información sobre la última versión de la base de datos de virus y la última versión del programa en el servidor DNS. A continuación, sólo se descargan y aplican los archivos más pequeños e indispensables para la actualización. De esta manera, se minimiza la cantidad de datos que se deben descargar y el proceso de actualización se ejecuta con mayor rapidez.
- **Solicitar confirmación para cerrar aplicaciones que se estén ejecutando** (*activado de forma predeterminada*): con este elemento tendrá la seguridad de que ninguna aplicación actualmente en ejecución se cerrará sin su permiso, si se requiere para que el proceso de actualización finalice.
- **Verificar hora del equipo**: marque esta opción para declarar que desea recibir una notificación en caso de que la hora del equipo difiera por más horas de las especificadas de la hora correcta.

9.10.1. Proxy



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

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

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

Configuración manual

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

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



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

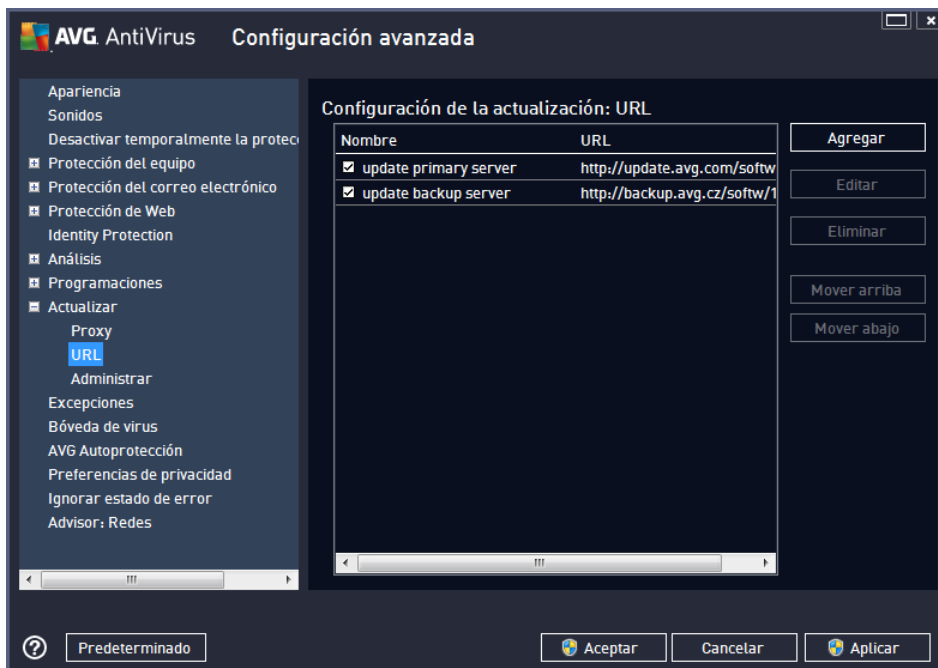
Configuración automática

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

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

9.10.2. URL

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



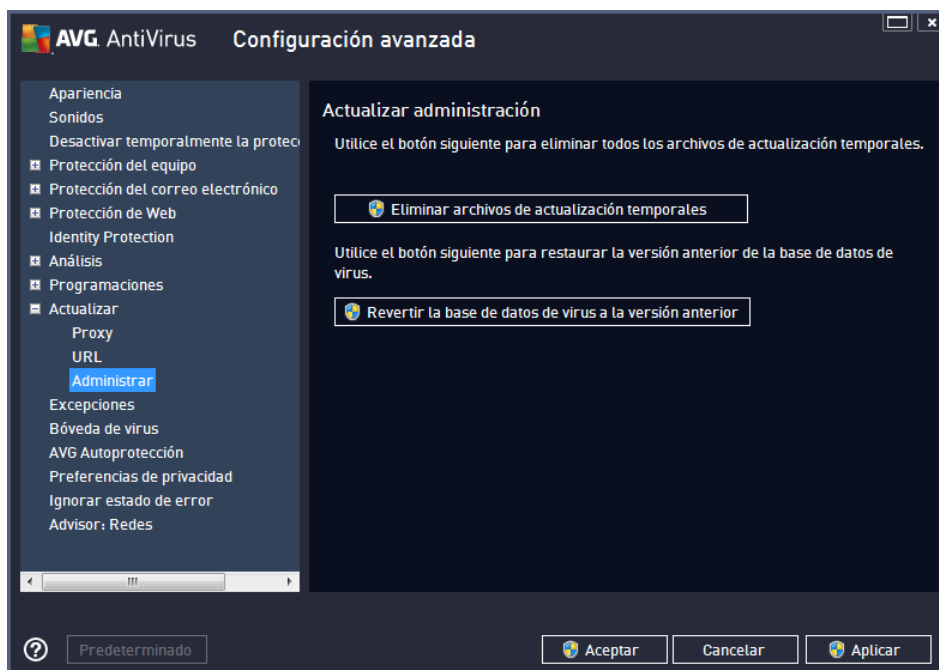
Botones de control

La lista y los elementos se pueden modificar por medio de los siguientes botones de control:

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

9.10.3. Administrar

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

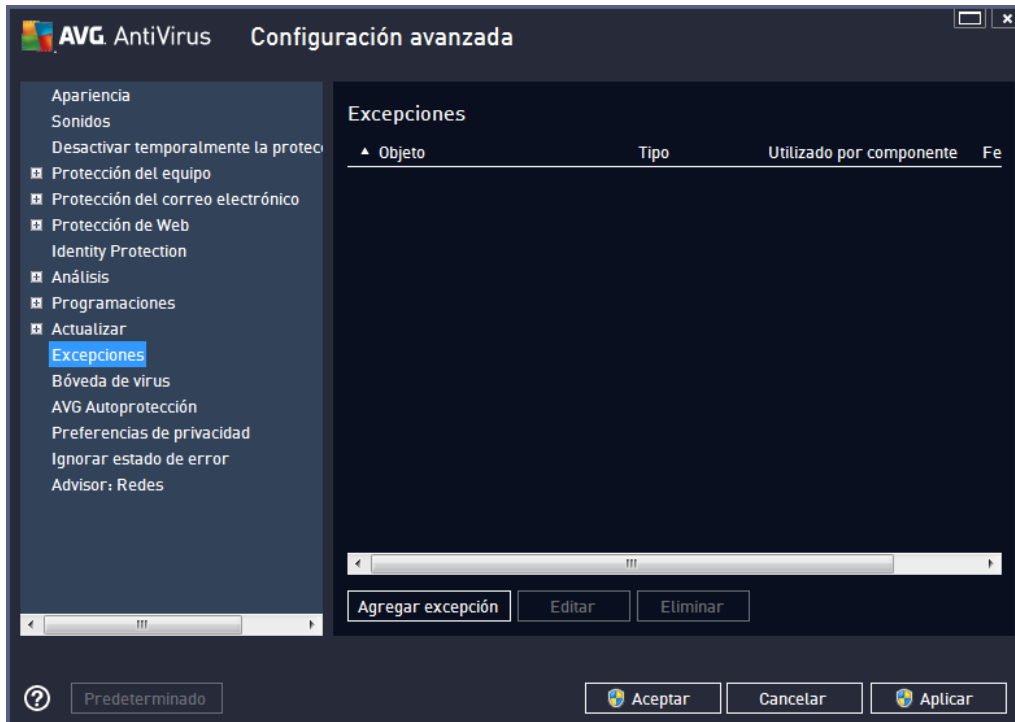


- **Eliminar archivos de actualización temporales:** presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada estos archivos se guardan durante 30 días*)
- **Revertir la base de datos de virus a la versión anterior:** presione este botón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

9.11. Excepciones

En el cuadro de diálogo **Excepciones** puede definir excepciones, es decir, elementos que ignorará **AVG AntiVirus 2013**. Generalmente, deberá definir una excepción si AVG continúa detectando un programa o archivo como amenaza, o bloqueando un sitio web seguro como peligroso. Agregue ese archivo o sitio web a esta lista de excepciones, y AVG no le informará sobre él ni lo bloqueará más.

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

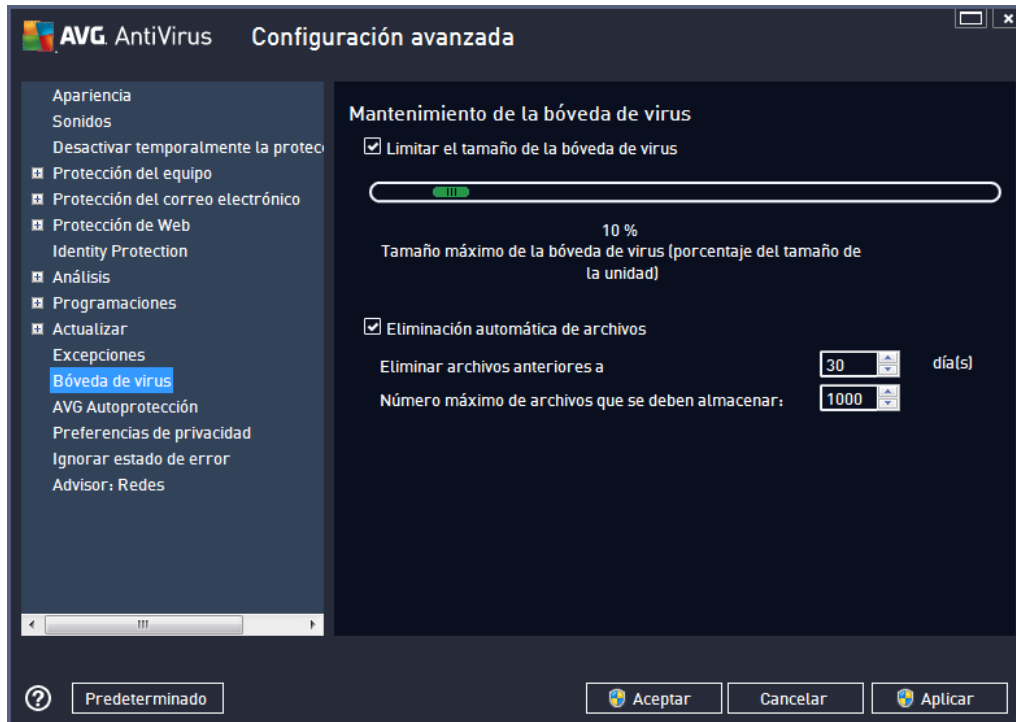


La tabla en el cuadro de diálogo muestra una lista de excepciones, si ya se definió alguna. Cada elemento tiene una casilla de verificación a su lado. Si la casilla de verificación está marcada, la excepción está en vigor; en caso contrario, la excepción está definida, pero no se utiliza. Al hacer clic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

Botones de control

- **Agregar excepción:** haga clic para abrir un nuevo cuadro de diálogo donde puede especificar el elemento que debe excluirse del análisis de AVG. En primer lugar, se lo invitará a definir el tipo de objeto, es decir, si se trata de un archivo, una carpeta o URL. A continuación, deberá examinar su disco para proporcionar la ruta de acceso al objeto respectivo o escribir la URL. Finalmente, puede seleccionar las funciones de AVG que deben ignorar el objeto seleccionado (*Protección residente, Identity Protection, Análisis, Anti-Rootkit*).
- **Editar:** este botón solamente está activo si ya se han definido algunas excepciones, y se enumeran en la tabla. Luego, puede usar el botón para abrir el cuadro de diálogo de edición sobre una excepción seleccionada y configurar los parámetros de la excepción.
- **Eliminar:** utilice este botón para cancelar una excepción previamente definida. Puede eliminarlas una por una, o resaltar un bloque de excepciones en la lista y cancelar las excepciones definidas. Después de cancelar la excepción, el archivo, carpeta o URL respectivo será comprobado por AVG otra vez. Tenga en cuenta que sólo se quitará la excepción, no el archivo ni la carpeta.

9.12. Bóveda de virus

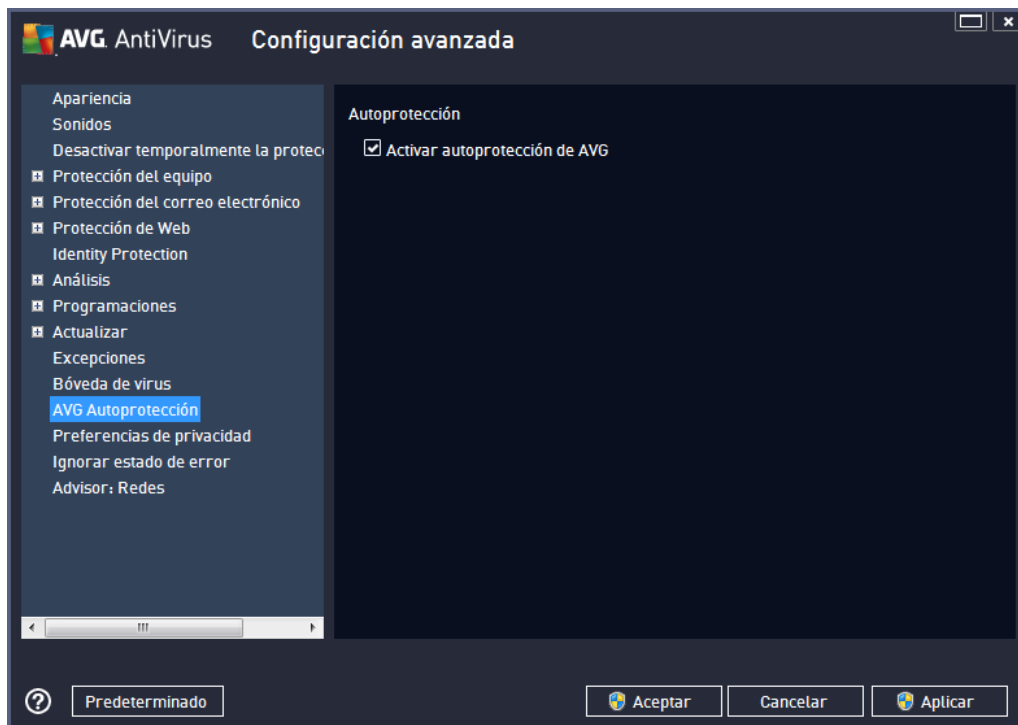


El cuadro de diálogo **Mantenimiento de la Bóveda de virus** permite definir varios parámetros relacionados con la administración de objetos almacenados en la [Bóveda de virus](#):

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



9.13. Autoprotección AVG

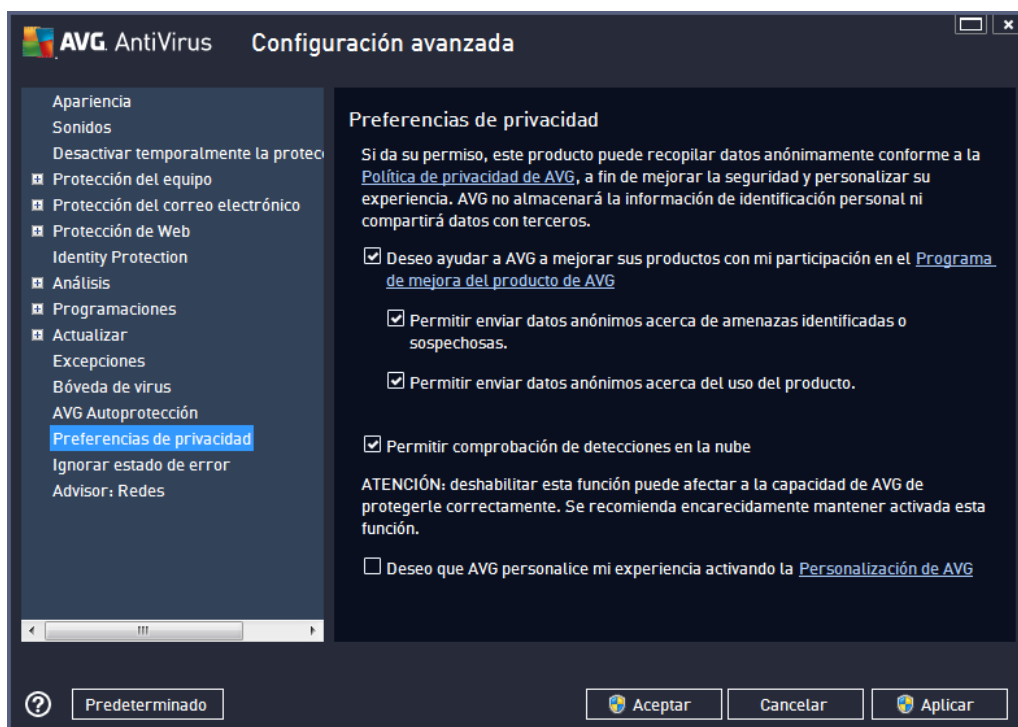


El elemento **Autoprotección de AVG** permite que **AVG AntiVirus 2013** proteja sus propios procesos, archivos, claves de registro y controladores para que no se modifiquen ni desactiven. La razón principal para esta clase de protección es que algunas amenazas sofisticadas intentan desactivar la protección antivirus, y luego causan daño a su equipo libremente.

Recomendamos que esta función se mantenga activada.

9.14. Preferencias de privacidad

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



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

- **Deseo ayudar a AVG a mejorar sus productos a través de mi participación en el Programa de mejora del producto de AVG (activado de forma predeterminada)** - Si desea ayudarnos a mejorar **AVG AntiVirus 2013**, deje marcada la casilla de verificación. De este modo, se podrán notificar todas las amenazas encontradas a AVG, por lo que podremos recopilar información actualizada sobre malware de todos los participantes repartidos por el mundo y, a cambio, mejorar la protección de todos. Los informes se realizan automáticamente, por lo tanto no le causan ninguna molestia, y no se incluye en ellos ningún dato de identificación personal.
 - **Permita enviar datos acerca de correo electrónico mal identificado, previa autorización del usuario (activada de forma predeterminada)**: envíe información sobre mensajes de correo electrónico identificados incorrectamente como spam, o sobre mensajes de spam no detectados por el servicio Anti-Spam. Al enviar este tipo de información, se le solicitará su confirmación.
 - **Permitir enviar datos anónimos acerca de amenazas identificadas o sospechosas (activada de forma predeterminada)**: envíe información sobre cualquier código o patrón de conducta sospechoso o definitivamente peligroso (ya sea un virus, spyware o una página web maliciosa a la que está intentando obtener acceso) detectado en su equipo.
 - **Permitir enviar datos anónimos acerca del uso del producto (activado de forma predeterminada)**: envíe datos estadísticos básicos sobre el uso de la aplicación, como el número de detecciones, análisis ejecutados, actualizaciones exitosas o no exitosas, etc.
- **Permitir la comprobación de las detecciones en la nube (activado de forma**



predeterminada): se comprobará si las amenazas detectadas están realmente infectadas, con el fin de descartar falsos positivos.

- **Deseo que AVG personalice mi experiencia personalice mi experiencia activando la Personalización de AVG:** esta función analiza de forma anónima el comportamiento de los programas y aplicaciones instalados en su equipo. En función de esto, AVG puede ofrecerle servicios enfocados a sus necesidades, para garantizarle la máxima seguridad.

Amenazas más comunes

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

- **Un virus** es un código malicioso que se copia y propaga por sí solo, frecuentemente sin ser notado hasta que el daño está hecho. Algunos virus son una amenaza seria, eliminando o cambiando deliberadamente los archivos, mientras que otros pueden hacer algo aparentemente inofensivo, como tocar una pieza de música. Sin embargo, todos los virus son peligrosos debido a su capacidad básica para multiplicarse: incluso un virus simple puede apoderarse de toda la memoria del equipo en un instante y causar una falla.
- **Un gusano** es una subcategoría de virus que, a diferencia de un virus normal, no necesita un objeto "portador" al que adjuntarse, sino que se envía a sí mismo a otros equipos de manera independiente, normalmente a través del correo electrónico y, como resultado, con frecuencia sobrecarga los servidores de correo electrónico y los sistemas de red.
- **El spyware** se define normalmente como una categoría de malware (*malware = cualquier software malicioso, incluyendo programas que contienen virus*), normalmente caballos de Troya, encaminado a robar información personal, contraseñas, números de tarjeta de crédito, o a infiltrarse en un equipo y permitir al atacante controlarlo de manera remota; todo, por supuesto, sin el conocimiento o el consentimiento del propietario del equipo.
- Los **Programas potencialmente no deseados** son un tipo de spyware que puede ser peligroso para su equipo, pero no tiene por qué serlo necesariamente. Un ejemplo específico de un PUP es el adware, un software diseñado para distribuir publicidad, normalmente mostrando ventanas emergentes con anuncios publicitarios; resulta molesto, pero no es realmente nocivo.
- **Las cookies de rastreo** también se pueden considerar una clase de spyware, ya que estos pequeños archivos, almacenados en el navegador y enviados automáticamente al sitio web "primario" cuando lo visita nuevamente, pueden contener datos como su historial de navegación y otra información similar.
- **Vulnerabilidad** es un código malicioso que se aprovecha de una falla o vulnerabilidad en un sistema operativo, navegador de Internet u otro programa esencial.
- **El phishing** es un intento por conseguir datos personales confidenciales fingiendo ser una organización confiable y bien conocida. Normalmente, se ponen en contacto con las víctimas potenciales mediante un correo electrónico masivo pidiéndoles, por ejemplo, que actualicen los detalles de su cuenta bancaria. Para hacerlo, se les invita a que sigan el vínculo que se les proporciona, el cual los lleva a un sitio web del banco falso.
- **Hoax (engaño)** es un correo electrónico masivo que contiene información peligrosa,



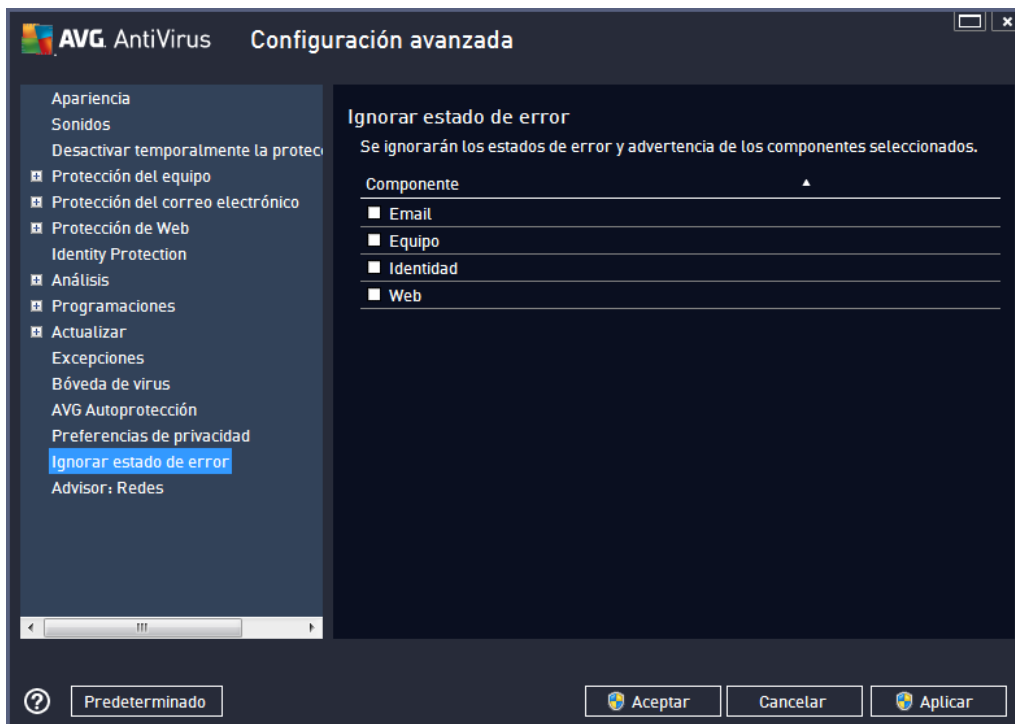
alarmante o solo molesta e inútil. Muchas de las amenazas anteriores utilizan mensajes de correo electrónico masivo para propagarse.

- **Los sitios web maliciosos** son aquellos que deliberadamente instalan el software malicioso en su equipo, y los sitios objeto de piratería que hacen lo mismo, sólo que estos son sitios web legítimos que han sido alterados para infectar a los visitantes.

Para protegerle de todos estos tipos diferentes de amenazas, AVG AntiVirus 2013 incluye componentes especializados. Para obtener una breve descripción de ellos, consulte el capítulo [Descripción general de los componentes](#).

9.15. Ignorar estado de error

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



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

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

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



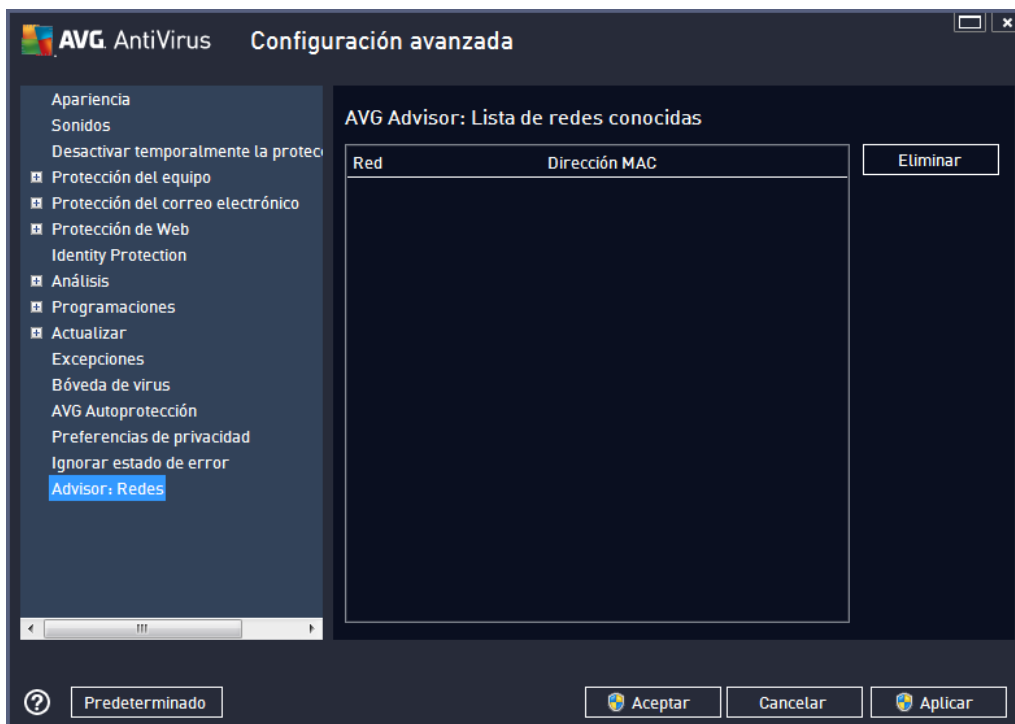
este caso el icono en la bandeja de sistema informa automáticamente del estado de error del componente. Sin embargo, en este caso específico no podemos hablar de un error real debido a que usted mismo lo introdujo deliberadamente, y está consciente del riesgo potencial. A su vez, una vez que el icono se muestra en color gris, no puede informar realmente de ningún error adicional posible que pueda aparecer.

Para esta situación, dentro del cuadro de diálogo **Ignorar estado de error** puede seleccionar componentes que pueden estar en un estado de error (o desactivado) y de los cuales no desee recibir información. Presione el botón **Aceptar** para confirmar.

9.16. Advisor: Redes

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

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

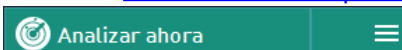


Nota: la función de redes conocidas dentro de AVG Advisor no se admite en Windows XP de 64 bits.

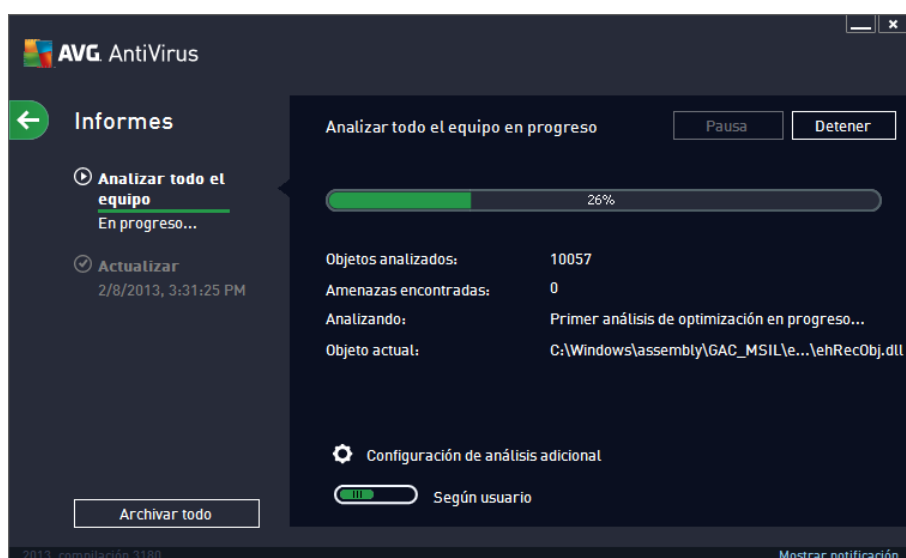
10. Análisis de AVG

De forma predeterminada, **AVG AntiVirus 2013** no ejecuta análisis, dado que después del análisis inicial (*al que se lo invitará a iniciar*), debe protegerse perfectamente mediante los componentes residentes de **AVG AntiVirus 2013**, que siempre están en guardia y no permiten que código malicioso ingrese en su equipo. Por supuesto, puede [programar un análisis](#) para que se ejecute a intervalos regulares, o ejecutar manualmente un análisis según sus necesidades en cualquier momento.

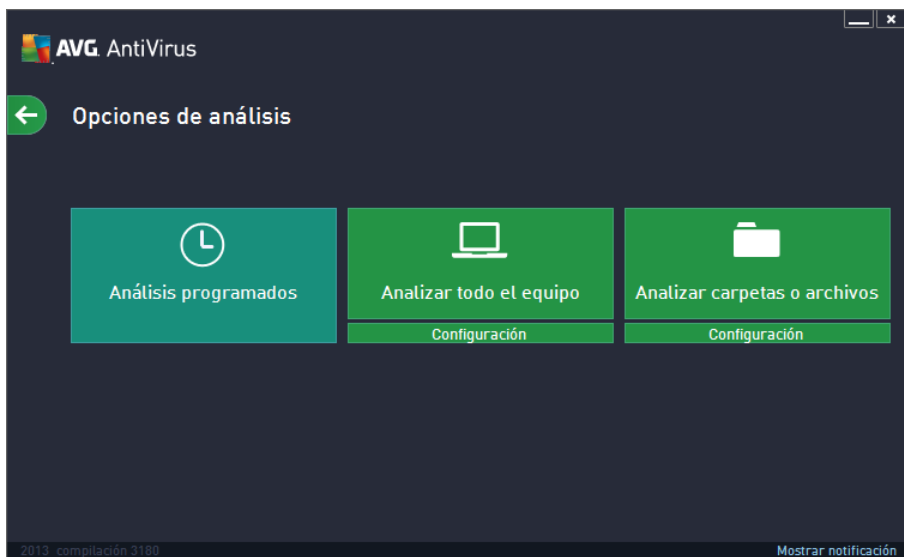
Puede acceder a la interfaz de análisis de AVG desde la [interfaz de usuario principal](#) a través del botón dividido gráficamente en dos secciones:



- **Analizar ahora:** presione el botón para iniciar [Analizar todo el equipo](#) de inmediato y supervisar su progreso y resultados en la ventana [Informes](#) que se abre automáticamente:



- **Opciones:** seleccione este botón (*se muestra gráficamente como tres líneas horizontales en un campo verde*) para abrir el cuadro de diálogo **Opciones de análisis**, donde puede [análisis programados](#) y editar parámetros de [Analizar todo el equipo](#) / [Analizar carpetas o archivos](#):



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

- **Análisis programados:** haga clic en esta opción para abrir un nuevo cuadro de diálogo [con una descripción general de todas las programaciones de análisis](#). Antes de definir sus propios análisis, solamente podrá ver en la tabla un análisis programado predefinido por el proveedor del software. El análisis está desactivado de manera predeterminada. Para encenderlo, haga clic con el botón derecho y seleccione la opción *Activar tarea* en el menú contextual. Una vez que se active el análisis programado, puede [editar su configuración](#) a través del botón *Editar análisis programado*. También puede hacer clic en el botón *Agregar análisis programado* para crear una nueva programación de análisis propia.
- **Analizar todo el equipo / Configuración:** el botón está dividido en dos secciones. Haga clic en la opción *Analizar todo el equipo* para iniciar de inmediato el análisis de todo el equipo (*para ver detalles sobre el análisis de todo el equipo, consulte el capítulo respectivo llamado [Análisis predefinidos / Analizar todo el equipo](#)*). Si hace clic en la sección *Configuración* situada debajo, irá al cuadro de diálogo de [configuración del análisis de todo el equipo](#).
- **Analizar carpetas o archivos / Configuración:** nuevamente, el botón está dividido en dos secciones. Haga clic en la opción *Analizar carpetas o archivos* para iniciar de inmediato el análisis de áreas seleccionadas del equipo (*para ver detalles sobre el análisis de los archivos o carpetas seleccionados, consulte el capítulo llamado [Análisis predefinidos / Analizar carpetas o archivos](#)*). Si hace clic en la sección *Configuración* situada debajo, irá al cuadro de diálogo de [configuración del análisis de archivos o carpetas](#).

10.1. Análisis predefinidos

Una de las funciones principales de **AVG AntiVirus 2013** es el análisis a pedido. Los análisis a pedido están diseñados para analizar varias partes de su equipo cuando existen sospechas de una posible infección de virus. De todas formas, se recomienda llevar a cabo dichos análisis con regularidad aun si no cree que se vayan a detectar virus en su equipo.



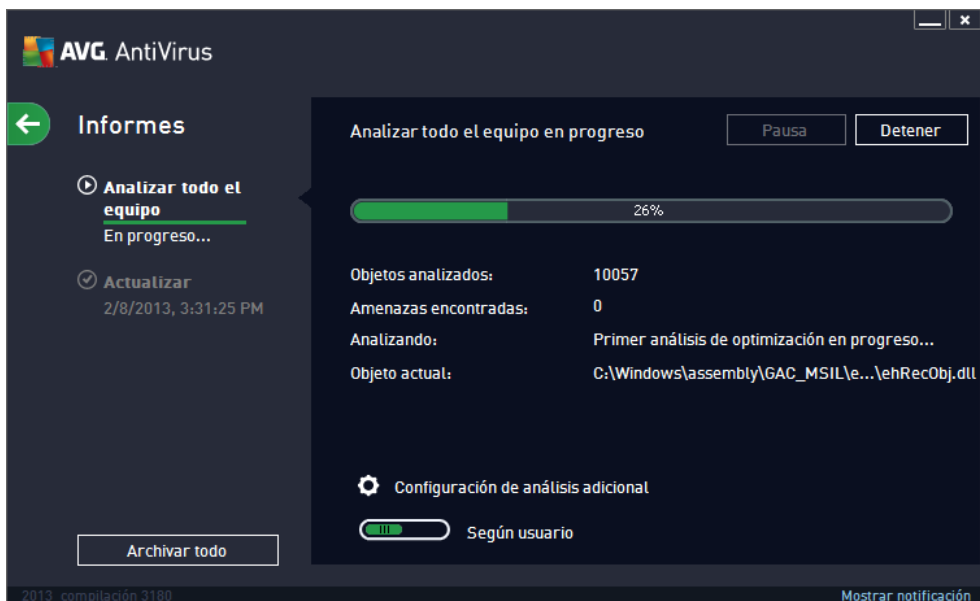
En **AVG AntiVirus 2013** encontrará los siguientes tipos de análisis predefinidos por el proveedor del software:

10.1.1. Analizar todo el equipo

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

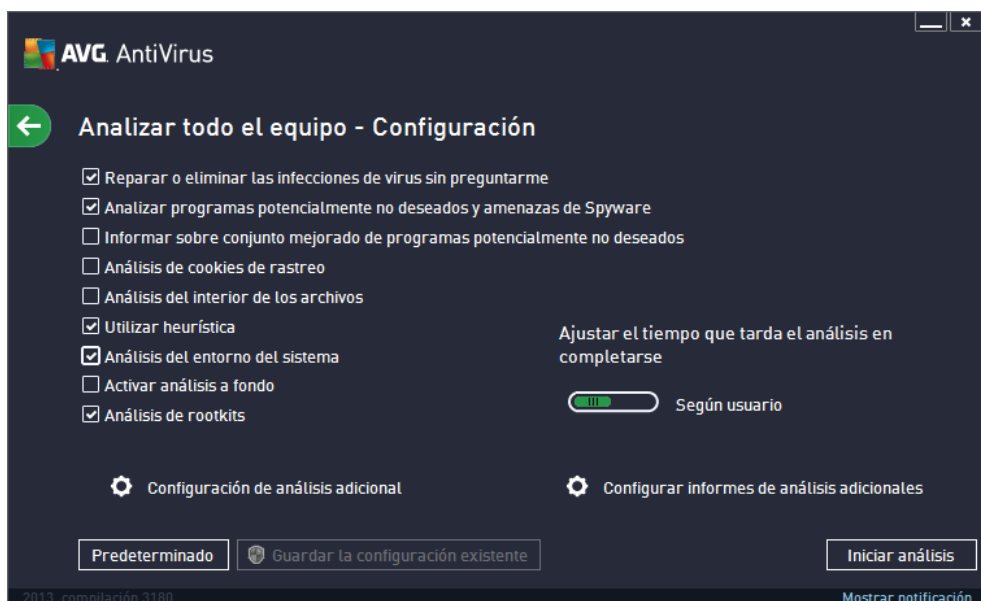
Ejecución del análisis

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



Edición de la configuración de análisis

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

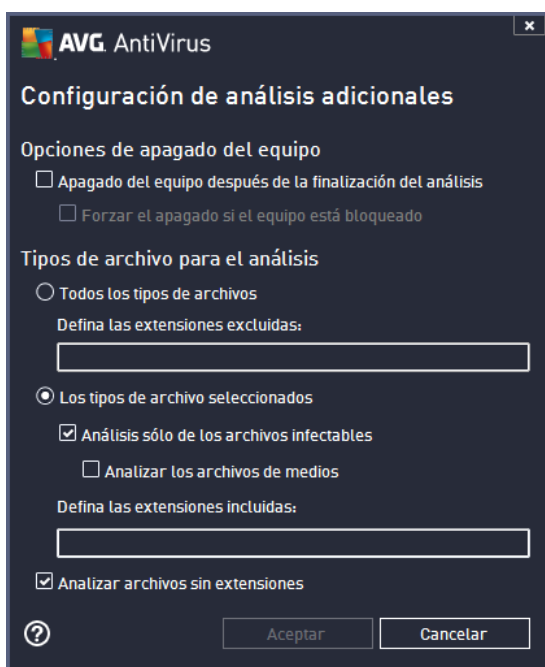


En los parámetros de análisis, puede activar o desactivar parámetros según sea necesario.

- **Reparar o eliminar las infecciones de virus sin preguntarme** (activado de manera predeterminada): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si hay una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (activada de forma predeterminada): seleccione esta opción para activar el análisis de spyware y de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar el conjunto mejorado de programas potencialmente no deseados** (desactivada de manera predeterminada): seleccione esta opción para detectar un paquete extendido de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Analizar cookies de rastreo** (desactivado de manera predeterminada): este parámetro estipula que se deben detectar las cookies; (las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de su carrito de compras electrónico).
- **Analizar el interior de los archivos** (activado de manera predeterminada): este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos almacenados dentro de otros archivos, por ejemplo, ZIP, RAR, etc.
- **Utilizar método heurístico** (activado de manera predeterminada): el análisis heurístico (la

emulación dinámica de las instrucciones del objeto analizado en un entorno virtual) será uno de los métodos empleados para la detección de virus durante el análisis.

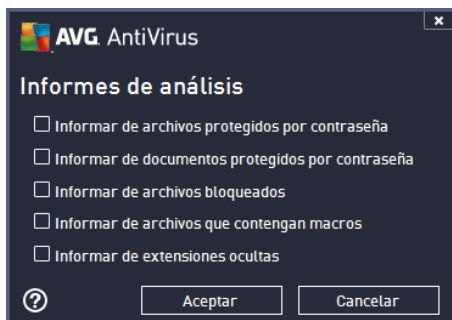
- **Análisis del entorno del sistema** (activado de manera predeterminada): el análisis también comprobará las áreas del sistema del equipo.
- **Activar análisis a fondo** (desactivado de manera predeterminada): en determinadas situaciones (con sospechas de que el equipo está infectado) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Configuración de análisis adicional:** el vínculo abre un nuevo cuadro de diálogo Configuración de análisis adicional, donde puede especificar los siguientes parámetros:



- **Opciones de apagado del equipo:** decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (**Apagado del equipo después de la finalización del análisis**), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (**Forzar el apagado si el equipo está bloqueado**).
- **Tipos de archivo para el análisis.** además debe decidir si desea que se analicen:
 - **Todos los tipos de archivos** con la opción de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;
 - **Tipos de archivos seleccionados.** puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de*

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

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



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

10.1.2. Analizar carpetas o archivos

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

Ejecución del análisis

El **análisis de archivos o carpetas** se puede ejecutar directamente desde el cuadro de diálogo [Opciones de análisis](#) haciendo clic en el botón **Analizar carpetas o archivos**. Se abre un nuevo



cuadro de diálogo denominado **Seleccione archivos o carpetas específicos para el análisis**. En la estructura de árbol del equipo, seleccione aquellas carpetas que desea analizar. La ruta a cada carpeta seleccionada se genera automáticamente y aparece en el cuadro de texto de la parte superior de este cuadro de diálogo. También existe la opción de analizar una carpeta determinada y, a la vez, excluir de este análisis sus subcarpetas; para ello, escriba un signo menos "-" delante de la ruta generada automáticamente (*consulte la captura de pantalla*). Para excluir toda la carpeta del análisis utilice el signo de admiración "!". Finalmente, para iniciar el análisis, presione el botón **Iniciar análisis**; el proceso de análisis es básicamente idéntico al [Análisis de todo el equipo](#).



Edición de la configuración de análisis

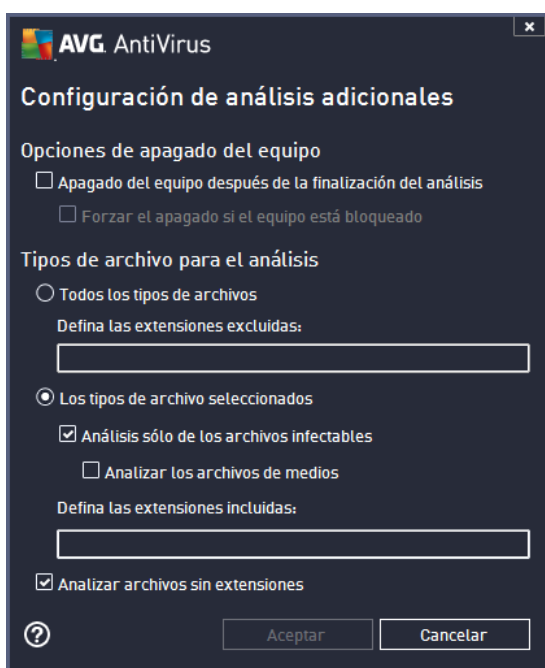
Puede editar la configuración de **Analizar carpetas o archivos** en el cuadro de diálogo **Analizar carpetas o archivos - Configuración** (el cuadro de diálogo está disponible a través del vínculo [Configuración para Analizar carpetas o archivos dentro del cuadro de diálogo Opciones de análisis](#)).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



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

- **Reparar / eliminar una infección de virus sin preguntarme** (activada de forma predeterminada): Si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible una reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la [Bóveda de virus](#).
- **Analizar programas potencialmente no deseados y amenazas de Spyware** (activado de forma predeterminada): Marcar para activar el análisis de spyware, además de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar sobre conjunto mejorado de programas potencialmente no deseados** (desactivado de forma predeterminada): Marcar para detectar paquetes extendidos de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Análisis de cookies de rastreo** (desactivado de forma predeterminada): Este parámetro especifica que se deben detectar cookies; (las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico)
- **Análisis del interior de los archivos** (activado de forma predeterminada): Este parámetro define que el análisis debe comprobar todos los archivos almacenados dentro de archivos, por ej., ZIP, RAR, ...
- **Utilizar heurística** (activado de forma predeterminada): Análisis heurístico (la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual) será uno de los métodos empleados para la detección de virus durante el análisis.

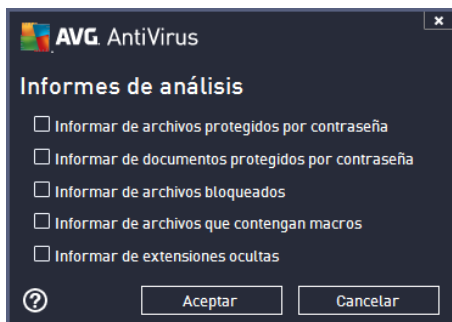
- **Análisis del entorno del sistema** (desactivado de forma predeterminada): El análisis también comprobará áreas del sistema de su equipo.
- **Activar análisis a fondo** (desactivado de forma predeterminada): En determinadas situaciones (con sospechas de que el equipo está infectado) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Configuración de análisis adicional:** el vínculo abre un nuevo cuadro de diálogo **Configuración de análisis adicional**, donde puede especificar los siguientes parámetros:



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

extensiones de los archivos que siempre deben analizarse.

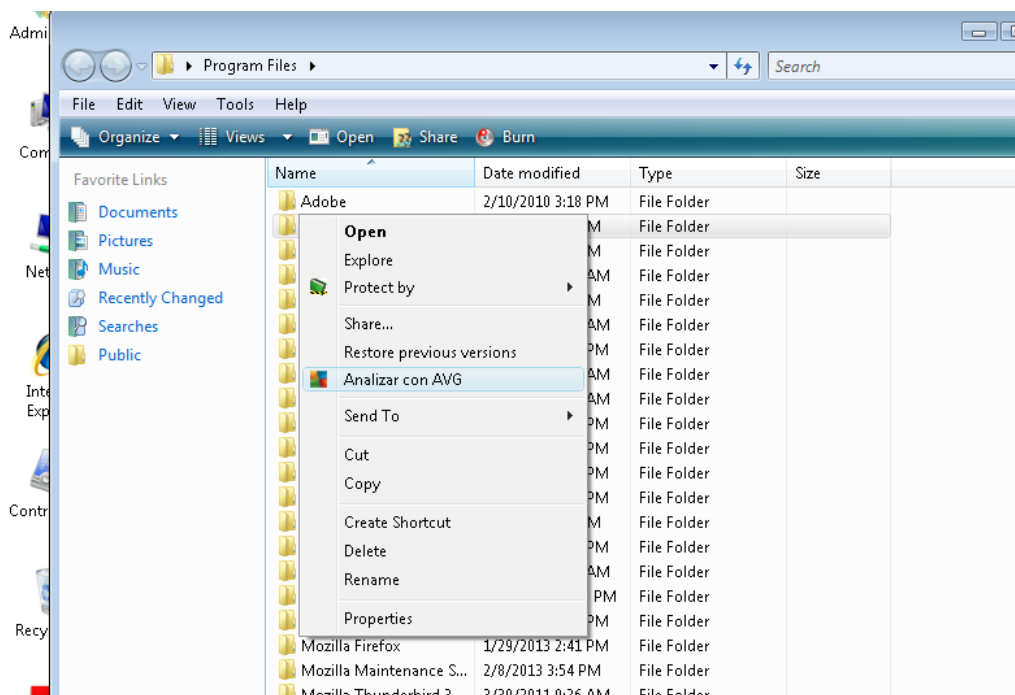
- De manera opcional, puede decidir si desea **Analizar archivos sin extensiones**: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.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



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

10.2. Análisis en el Explorador de Windows

Además de los análisis predefinidos ejecutados para todo el equipo o sus áreas seleccionadas, **AVG AntiVirus 2013** también ofrece la opción de análisis rápido de un objeto específico directamente en el entorno del Explorador de Windows. Si desea abrir un archivo desconocido y no está seguro de su contenido, puede analizarlo a pedido. Siga estos pasos:



- Dentro del Explorador de Windows, resalte el archivo (o carpeta) que desea comprobar
- Haga clic con el botón secundario del mouse sobre el objeto para abrir el menú contextual.
- Seleccione la opción **Analizar con AVG** para que el archivo se analice con **AVG AntiVirus 2013**

10.3. Análisis desde línea de comandos

En **AVG AntiVirus 2013** existe la opción de realizar el análisis desde la línea de comandos. Puede utilizar esta opción, por ejemplo, en servidores, o bien al crear un script por lotes que se ejecutará automáticamente una vez reiniciado el equipo. Desde la línea de comandos, puede ejecutar el análisis con la mayoría de los parámetros ofrecidos en la interfaz gráfica de usuario de AVG.

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

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

Sintaxis del comando

La sintaxis del comando es la siguiente:

- **avgscanx /parámetro ...** p. ej., **avgscanx /comp** para analizar todo el equipo
- **avgscanx /parámetro /parámetro ..** al utilizar varios parámetros, estos deben alinearse en una fila y separarse mediante un espacio y un signo de barra



- si un parámetro requiere que se proporcione un valor específico (p. ej., el parámetro */scan* requiere información sobre qué áreas seleccionadas del equipo se deben analizar, por lo que debe proporcionar una ruta de acceso exacta hasta la sección seleccionada), los valores se separan mediante punto y coma, por ejemplo: *avgscanx /scan=C:\;D:*

Parámetros del análisis

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

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

Análisis desde CMD iniciado desde la interfaz gráfica

Cuando ejecuta su equipo en el modo seguro de Windows, existe también una opción de iniciar el análisis desde la línea de comandos en la interfaz gráfica del usuario. El análisis en sí mismo se iniciará desde la línea de comandos, el cuadro de diálogo **Compositor de línea de comandos** sólo le permite especificar la mayoría de los parámetros de análisis en la comodidad de la interfaz gráfica.

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

10.3.1. Parámetros del análisis desde CMD

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

- */SCAN* [Analizar carpetas o archivos específicos](#) */SCAN=ruta de acceso;ruta de acceso (es decir, /SCAN=C:\;D:\)*
- */COMP* [Análisis de todo el equipo](#)
- */HEUR* Utilizar análisis heurístico
- */EXCLUDE* Excluir ruta de acceso o archivos del análisis
- */@* Archivo de comandos */nombre de archivo/*
- */EXT* Analizar estas extensiones */por ejemplo EXT=EXE,DLL/*
- */NOEXT* No analizar estas extensiones */por ejemplo NOEXT=JPG/*
- */ARC* Analizar archivos



- /CLEAN Borrarr automáticamente
- /TRASH Mover los archivos infectados a la [Bóveda de virus](#)
- /QT Análisis rápido
- /LOG Generar un archivo de los resultados del análisis
- /MACROW Notificar macros
- /PWDW Notificar archivos protegidos por contraseña
- /ARCBOMBSW Reportar bombas de archivo (*archivos comprimidos reiteradas veces*)
- /IGNLOCKED Omitir archivos bloqueados
- /REPORT Informar a archivo /nombre de archivo/
- /REPAPPEND Anexar al archivo de reporte
- /REPOK Notificar archivos no infectados como correctos
- /NOBREAK No permitir la anulación mediante CTRL+BREAK
- /BOOT Activar la comprobación de MBR/BOOT
- /PROC Analizar los procesos activos
- /PUP Informar Programas potencialmente no deseados
- /PUPEXT Informar de conjunto mejorado de Programas potencialmente no deseados
- /REG Analizar el registro
- /COO Analizar cookies
- /? Mostrar ayuda sobre este tema
- /HELP Visualizar ayuda sobre este tema
- /PRIORITY Establecer prioridad de análisis /Baja, Automática, Alta/ (*consulte [Configuración avanzada / Análisis](#)*)
- /SHUTDOWN Apagado del equipo después de la finalización del análisis
- /FORCESHUTDOWN Forzar el apagado del equipo tras la finalización del análisis
- /ADS Analizar flujo de datos alternos (*sólo NTFS*)
- /HIDDEN Informar archivos con extensión oculta
- /INFECTABLEONLY Analizar los archivos con extensiones infectables

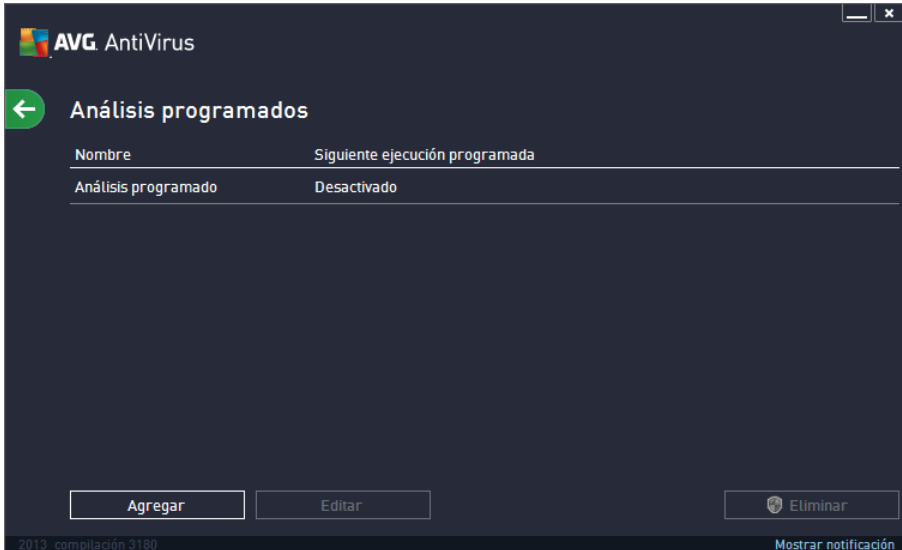


- /THOROUGHSCAN Activar análisis a fondo
- /CLOUDCHECK Verificar falsos positivos
- /ARCBOMBSW Informar de archivos recomprimidos

10.4. Programación de análisis

Con **AVG AntiVirus 2013** puede ejecutar el análisis a pedido (*por ejemplo cuando sospecha que se ha arrastrado una infección a su equipo*) o según un plan programado. Se recomienda especialmente que ejecute los análisis en función de una programación: de esta forma puede asegurarse de que su equipo esté protegido contra posibilidades de infección, y no tendrá que preocuparse sobre si iniciar el análisis y en qué momento. Se debe ejecutar [Analizar todo el equipo](#) periódicamente, al menos una vez a la semana. Sin embargo, si es posible, ejecute el análisis de todo su equipo diariamente, como está establecido en la configuración predeterminada de programación del análisis. Si el equipo siempre está encendido, se pueden programar los análisis fuera del horario de trabajo. Si el equipo algunas veces está apagado, se puede programar que los análisis ocurran [durante un arranque del equipo, cuando no se haya ejecutado la tarea](#).


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



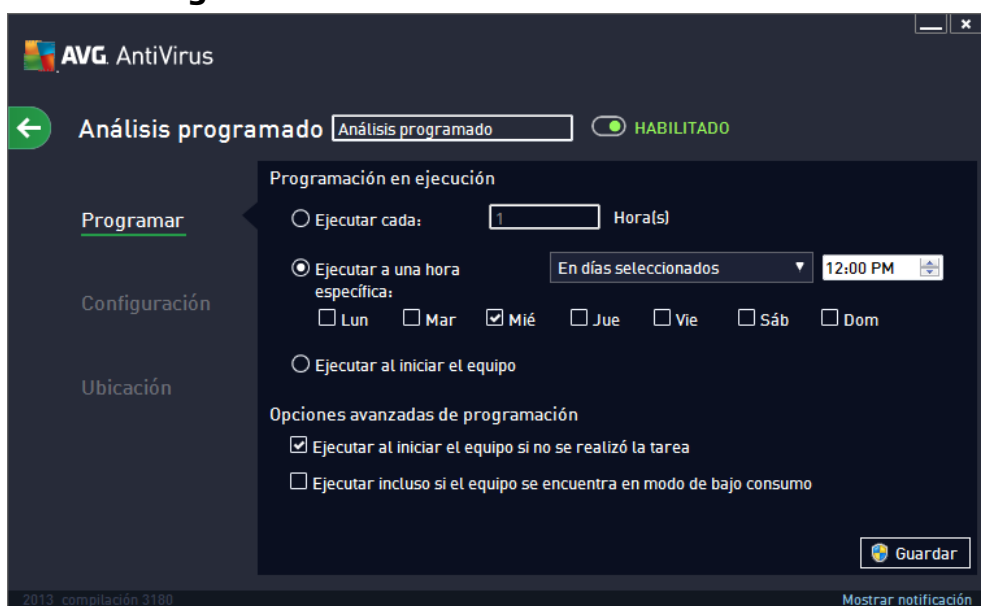
Antes de definir sus propios análisis, solamente podrá ver en la tabla un análisis programado predefinido por el proveedor del software. El análisis está desactivado de manera predeterminada. Para encenderlo, haga clic con el botón derecho y seleccione la opción **Activar tarea** en el menú contextual. Una vez que se active el análisis programado, puede [editar su configuración](#) a través del botón **Editar análisis programado**. También puede hacer clic en el botón **Agregar análisis programado** para crear una nueva programación de análisis propia. Los parámetros del análisis programado se pueden editar (*o se puede configurar una nueva programación*) en tres pestañas:

- [Programar](#)

- [Configuración](#)
- [Ubicación](#)

En cada pestaña puede cambiar el botón del "semáforo"  para desactivar la prueba programada temporalmente y activarla nuevamente según surja la necesidad:

10.4.1. Programar




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

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

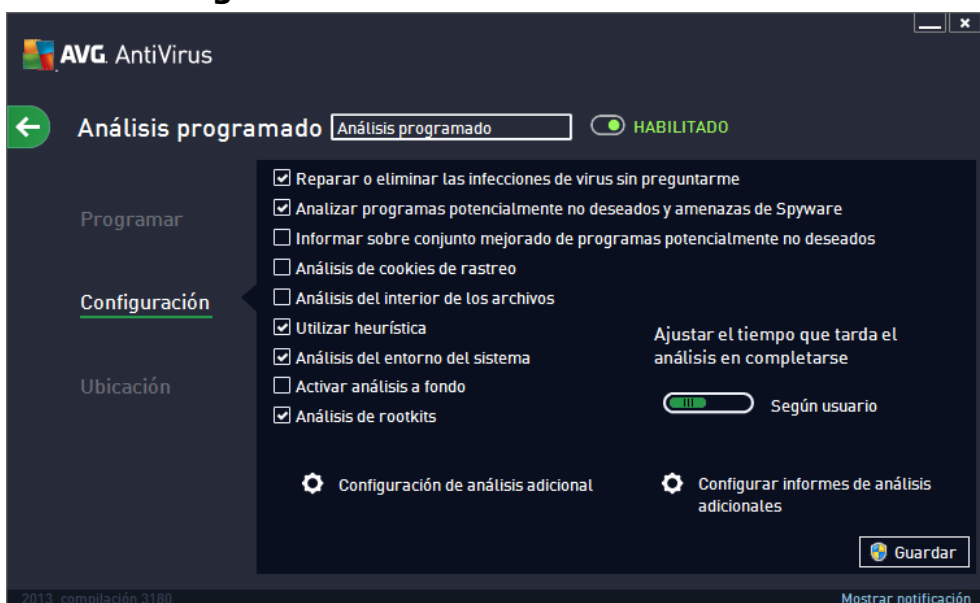
- **Ejecución de programación:** Aquí, puede especificar los intervalos de tiempo para la ejecución del análisis programado recientemente. El tiempo puede definirse con la ejecución repetida tras un periodo de tiempo determinado (*Ejecutar cada ...*) o estableciendo una fecha y hora exactas (*Ejecutar a un intervalo específico de tiempo ...*), o posiblemente mediante la definición de un evento con el que esté asociada la ejecución del análisis (*Ejecutar al iniciar el equipo*).
- **Opciones de programación avanzada:** esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado. Una vez que se inicia el análisis programado en la hora que se especificó, se le informará de este hecho mediante una ventana emergente que se abre sobre el [icono en la bandeja de sistema AVG](#). A continuación aparece un nuevo [icono de la bandeja del sistema AVG](#) (a todo color y brillante) informando de que se está ejecutando un análisis programado. Haga clic con el botón secundario en el icono de ejecución del análisis AVG para abrir un menú contextual donde puede decidir pausar o detener la

ejecución del análisis, y también cambiar la prioridad del análisis que se está ejecutando en ese momento.

Controles en el diálogo

- **Guardar:** guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y cambia a la descripción general de los [análisis programados](#). Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después de haber especificado todos los requisitos.
- : utilice la flecha verde en la sección superior izquierda del diálogo para volver a la descripción general de los [análisis programados](#).

10.4.2. Configuración



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

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

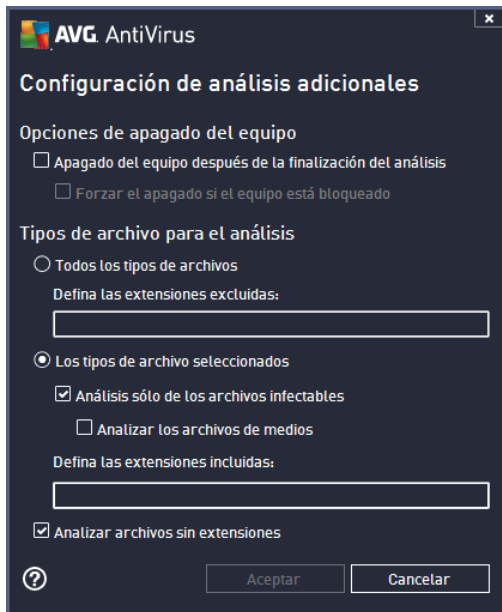
- **Reparar o eliminar las infecciones de virus sin preguntarme** (activada de forma predeterminada): si se identifica un virus durante el análisis, se puede reparar automáticamente si está disponible la reparación. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la [Bóveda de virus](#).



- **Analizar programas potencialmente no deseados y amenazas de Spyware** (*activado de forma predeterminada*): marcar para activar el análisis de spyware, además de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- **Informar sobre conjunto mejorado de programas potencialmente no deseados** (*desactivado de forma predeterminada*): marcar para detectar paquetes extendidos de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
- **Análisis de cookies de rastreo** (*desactivado de forma predeterminada*): este parámetro especifica que se deben detectar cookies durante el análisis; (las cookies *HTTP* se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico)
- **Análisis del interior de los archivos** (*desactivado de forma predeterminada*): este parámetro especifica que el análisis debe comprobar todos los archivos, incluso si se almacenan dentro de un archivo, por ej., ZIP, RAR, ...
- **Utilizar método heurístico** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.
- **Analizar el entorno del sistema** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.
- **Activar análisis a fondo** (*desactivado de forma predeterminada*): en determinadas situaciones (*con sospechas de que el equipo está infectado*) puede seleccionar esta opción para activar los algoritmos de análisis más exhaustivos que analizarán incluso las áreas del equipo que apenas se infectan, para estar absolutamente seguro. Pero recuerde que este método consume mucho tiempo.
- **Analizar en busca de rootkits** (*activado de forma predeterminada*): Anti-Rootkit busca en su equipo posibles rootkits, es decir, programas y tecnologías que cubran la actividad de malware en su equipo. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En algunos casos, secciones o controladores específicos de aplicaciones normales se pueden detectar erróneamente como rootkits.

Configuración de análisis adicional

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



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

Ajustar el tiempo que tarda el análisis en completarse

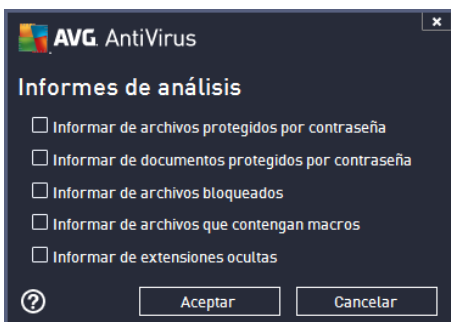
Dentro de esta sección puede especificar de manera adicional la velocidad de análisis deseada dependiendo del empleo de recursos del sistema. De manera predeterminada, el valor de esta opción está establecido en el nivel *según usuario* de empleo automático de recursos. Si desea que




el análisis se realice a más velocidad, tardará menos tiempo, pero el uso de recursos del sistema aumentará de modo notable durante el análisis y el resto de actividades del equipo se ralentizará (*esta opción se puede emplear cuando el equipo está encendido pero no hay nadie trabajando en él*). Por otro lado, puede reducir el uso de recursos del sistema prolongando la duración del análisis.

Configurar informes de análisis adicionales

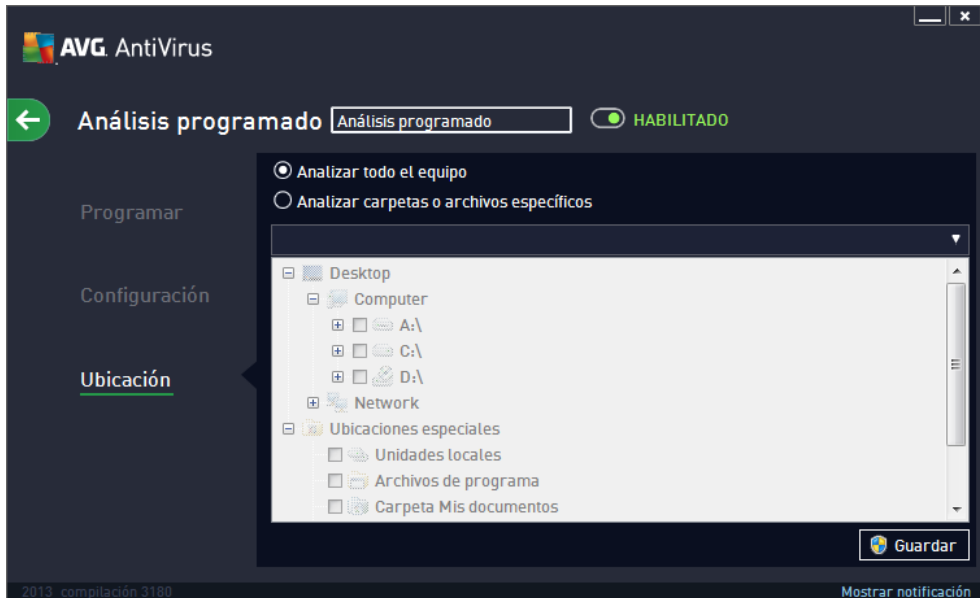
Haga clic en el vínculo **Configurar informes de análisis adicionales...** para abrir una ventana de diálogo denominada **Informes de análisis** donde puede marcar varios elementos para definir de qué hallazgos se debería informar:



Controles del cuadro de diálogo

- **Guardar:** guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y cambia a la descripción general de los [análisis programados](#). Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después de haber especificado todos los requisitos.
- : utilice la flecha verde en la sección superior izquierda del cuadro de diálogo para volver a la descripción general de los [análisis programados](#).

10.4.3. Ubicación



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


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

- **Unidades locales:** todas las unidades de disco duro de su equipo
- **Archivos de programa**
 - C:\Program Files\
 - en la versión de 64 bits C:\Program Files (x86)
- **Carpeta Mis documentos**
 - para Windows XP: C:\Documents and Settings\Default User\My Documents\
 - para Windows Vista/7: C:\Users\user\Documents\
- **Documentos compartidos**

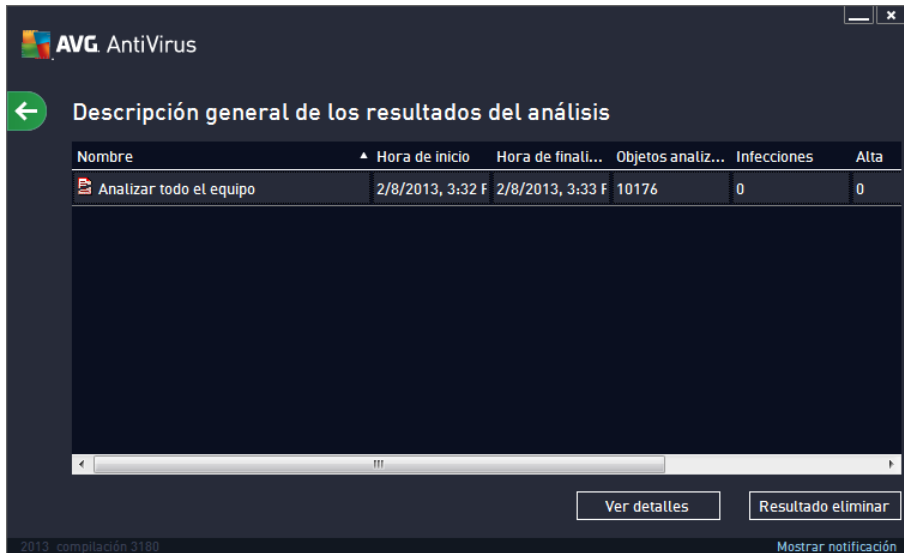


- *para Windows XP:* C:\Documents and Settings\All Users\Documents\
- *para Windows Vista/7:* C:\Users\Public\Documents\
- **Carpeta de Windows:** C:\Windows\
- **Otros**
 - *Unidad del sistema:* el disco duro en el cual está instalado el sistema operativo (normalmente C:)
 - *Carpeta del sistema:* C:\Windows\System32\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







Controles en el diálogo

- **Guardar:** guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y cambia a la descripción general de los [análisis programados](#). Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después de haber especificado todos los requisitos.
- : utilice la flecha verde en la sección superior izquierda del diálogo para volver a la descripción general de los [análisis programados](#).

10.5. Resultados del análisis



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

- **Icono:** la primera columna muestra un icono de información que describe el estado del análisis:
 -  No se han encontrado infecciones; análisis finalizado.
 -  No se han encontrado infecciones; análisis interrumpido antes de finalizar.
 -  Se han encontrado infecciones pero no se han reparado; análisis finalizado.
 -  Se han encontrado infecciones pero no se han reparado; análisis interrumpido antes de finalizar.
 -  Se han encontrado infecciones y se han reparado o eliminado; análisis finalizado.
 -  Se han encontrado infecciones y se han reparado o eliminado; análisis interrumpido antes de finalizar.
- **Nombre:** esta columna incluye el nombre del análisis correspondiente. Se trata de uno de dos [análisis predefinidos](#) o su propio [análisis programado](#).
- **Hora de inicio:** proporciona la fecha y hora exactas de inicio del análisis.
- **Hora de finalización:** proporciona la fecha y hora exactas de inicio, detenimiento o interrupción del análisis.
- **Objetos analizados:** proporciona la cantidad total de todos los objetos analizados.

- **Infecciones:** proporciona el número de infecciones eliminadas o totales encontradas.
- **Alta / Media / Baja:** las tres columnas siguientes proporcionan la cantidad de infecciones encontradas de gravedad alta, media y baja, respectivamente.
- **Rootkits:** proporciona la cantidad total de [rootkits](#) encontrados durante el análisis.

Controles del cuadro de diálogo

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

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



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

10.6. Detalles de los resultados del análisis

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

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

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

●● **Severidad media:** generalmente son PUP (*programas potencialmente no deseados, como adware*) o cookies de rastreo

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

11. Bóveda de virus



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

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

- **Fecha de almacenamiento:** proporciona la fecha y hora en que se ha detectado y transferido el archivo sospechoso a la Bóveda de Virus.
- **Severidad:** en caso de decidir instalar el componente [Identidad](#) dentro de su **AVG AntiVirus 2013**, se proporcionará en esta sección una identificación gráfica de la severidad del hallazgo correspondiente en una escala de cuatro niveles, de inobjetable (*tres puntos verdes*) hasta muy peligroso (*tres puntos rojos*), junto con información sobre el tipo de infección (*en base a su nivel de infección, todos los objetos de la lista pueden estar infectados o potencialmente infectados*)
- **Nombre de la detección:** especifica el nombre de la infección detectada de acuerdo con la [Enciclopedia de virus](#) en línea.
- **Fuente:** especifica qué componente de **AVG AntiVirus 2013** ha detectado la amenaza en cuestión.
- **Mensajes:** en una situación inusual, pueden proporcionarse notas en esta columna con



comentarios detallados de la amenaza en cuestión.

Botones de control

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

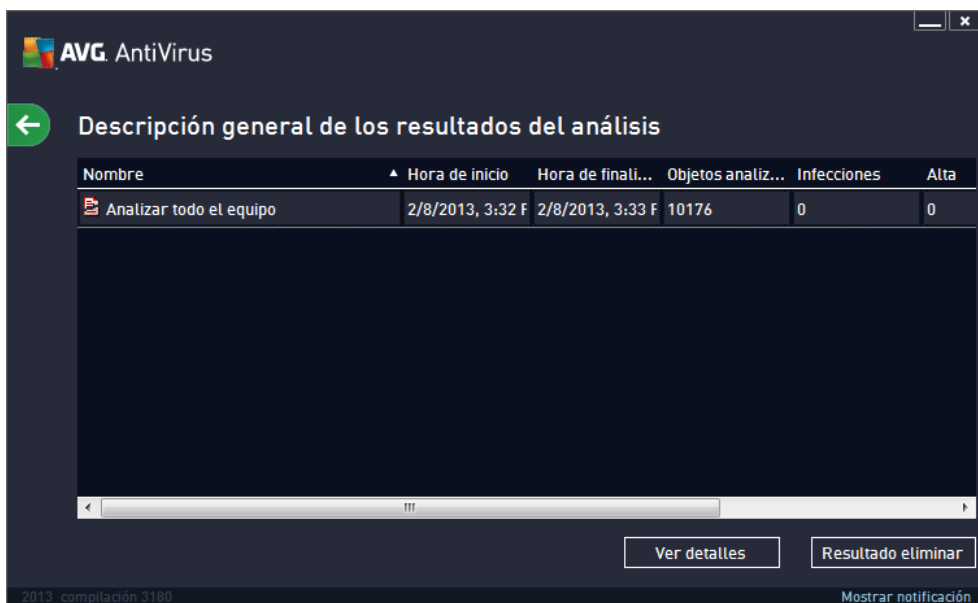
- **Restaurar**: devuelve el archivo infectado a su ubicación original en el disco.
- **Restaurar como**: mueve el archivo infectado a una carpeta seleccionada.
- **Detalles**: para obtener información detallada sobre la cuarentena de amenazas específicas en la **Bóveda de virus**, resalte el elemento seleccionado en la lista y haga clic en el botón **Detalles** para llamar a un nuevo cuadro de diálogo con una descripción de la amenaza detectada.
- **Eliminar**: elimina el archivo infectado de la **Bóveda de virus** de forma total e irreversible.
- **Vaciar la Bóveda de virus**: elimina todo el contenido de la **Bóveda de virus** permanentemente. Al eliminar los archivos de la **Bóveda de virus**, estos archivos se borran del disco de forma irreversible (*no se transfieren a la Papelera de reciclaje*).

12. Historial

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


- [Resultados del análisis](#)
- [Detección de Protección residente](#)
- [Detección mediante la Protección del correo electrónico](#)
- [Hallazgos de Online Shield](#)
- [Registro de historial de eventos](#)

12.1. Resultados del análisis



El cuadro de diálogo **Descripción general de los resultados del análisis** está accesible a través del elemento de menú **Opciones / Historial / Resultados del análisis** en la navegación superior de la ventana principal de **AVG AntiVirus 2013**. El diálogo proporciona una lista de todos los análisis ejecutados anteriormente y la información de sus resultados:


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

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

 - el icono azul indica que durante el análisis se detectó una infección, pero que



el objeto infectado se eliminó automáticamente

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


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

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

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

Botones de control

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

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

12.2. Detección de la Protección residente

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



Dentro de este cuadro de diálogo de advertencia encontrará información sobre el objeto detectado y asignado al estado infectado (*Nombre*), y algunos datos descriptivos sobre la infección reconocida (*Descripción*). El vínculo [Mostrar detalles](#) lo dirigirá a la enciclopedia de virus en línea donde puede encontrar información detallada sobre la infección detectada, si ésta se conoce. En el cuadro de diálogo, también verá una descripción general de las soluciones disponibles sobre cómo tratar la amenaza detectada. Una de las alternativas se etiquetará como recomendada: **Protegerme (recomendado)**. **De ser posible, siempre debe marcar esta opción.**

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

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


Dentro del cuadro de diálogo **Detección de Protección residente** hay una lista de todas las detecciones de Protección residente de las que se puede obtener una descripción general. Este cuadro de diálogo está disponible a través del elemento de menú **Opciones / Historial / Detección de Protección residente** en la navegación superior de la [ventana principal de AVG AntiVirus 2013](#). El cuadro de diálogo ofrece una descripción general de objetos que fueron detectados mediante la protección residente evaluados como peligrosos y reparados o movidos a la [Bóveda de virus](#).



Para cada objeto detectado se proporciona la siguiente información:

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

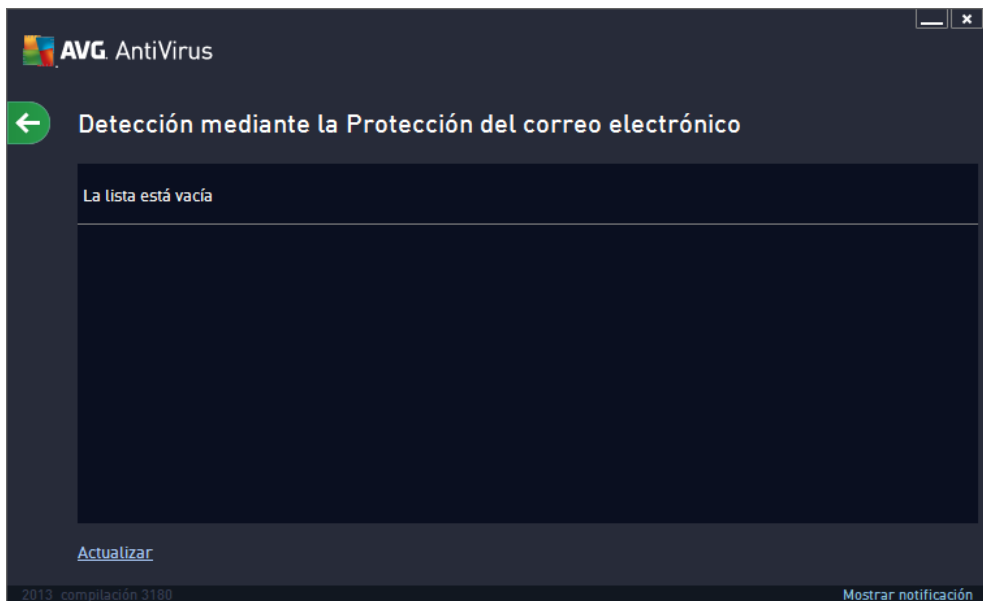
Botones de control

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



12.3. Detección de la Protección del correo electrónico

El cuadro de diálogo **Detección mediante la Protección del correo electrónico** está accesible a través del elemento de menú **Opciones / Historial / Detección mediante la Protección del correo electrónico** en la navegación superior de la ventana principal de **AVG AntiVirus 2013**.



El cuadro de diálogo proporciona una lista de todos los hallazgos detectados por el componente [Correo electrónico](#). Para cada objeto detectado se proporciona la siguiente información:

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


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

Botones de control

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

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



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

12.4. Hallazgos de Online Shield

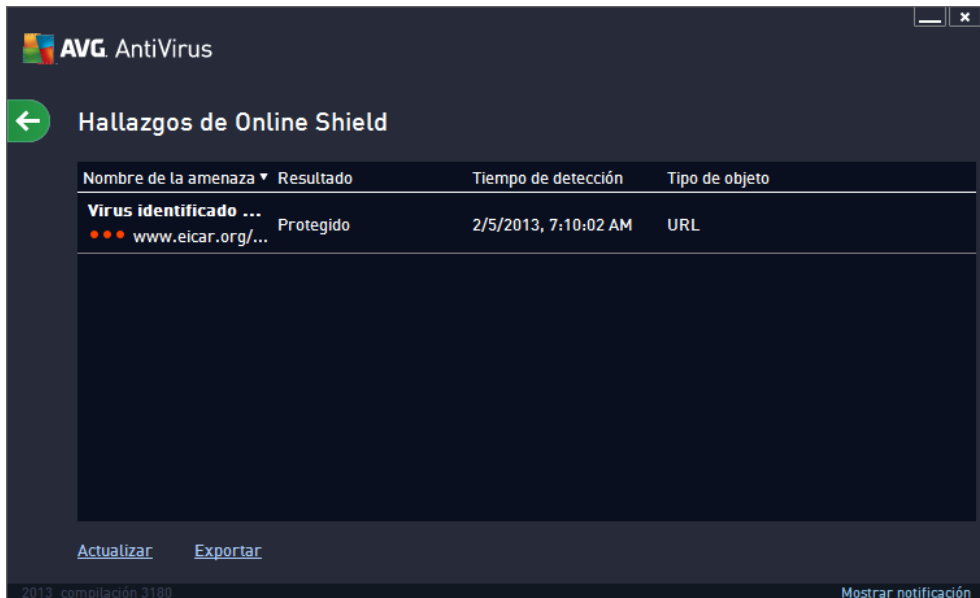
Online Shield analiza el contenido de las páginas web visitadas y los archivos que puedan contener incluso antes de que se visualicen en el navegador web o de que se descarguen en el equipo. Si se detecta una amenaza, se le avisará de forma inmediata mediante el siguiente cuadro de diálogo:



Dentro de este cuadro de diálogo de advertencia encontrará información sobre el objeto detectado y asignado al estado infectado (*Nombre*), y algunos datos descriptivos sobre la infección reconocida (*Descripción*). El vínculo [Mostrar detalles](#) lo dirigirá a la enciclopedia de virus en línea donde puede encontrar información detallada sobre la infección detectada, si son reconocidas. El cuadro de diálogo proporciona los siguientes elementos de control:

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


No se abrirá la página web sospechosa, y la detección de la amenaza se registrará en la lista de los **hallazgos de Online Shield**. Esta descripción general de amenazas detectadas está disponible a través del elemento de menú **Opciones / Historial / Hallazgos de Online Shield** en la navegación superior de la ventana principal **AVG AntiVirus 2013**.



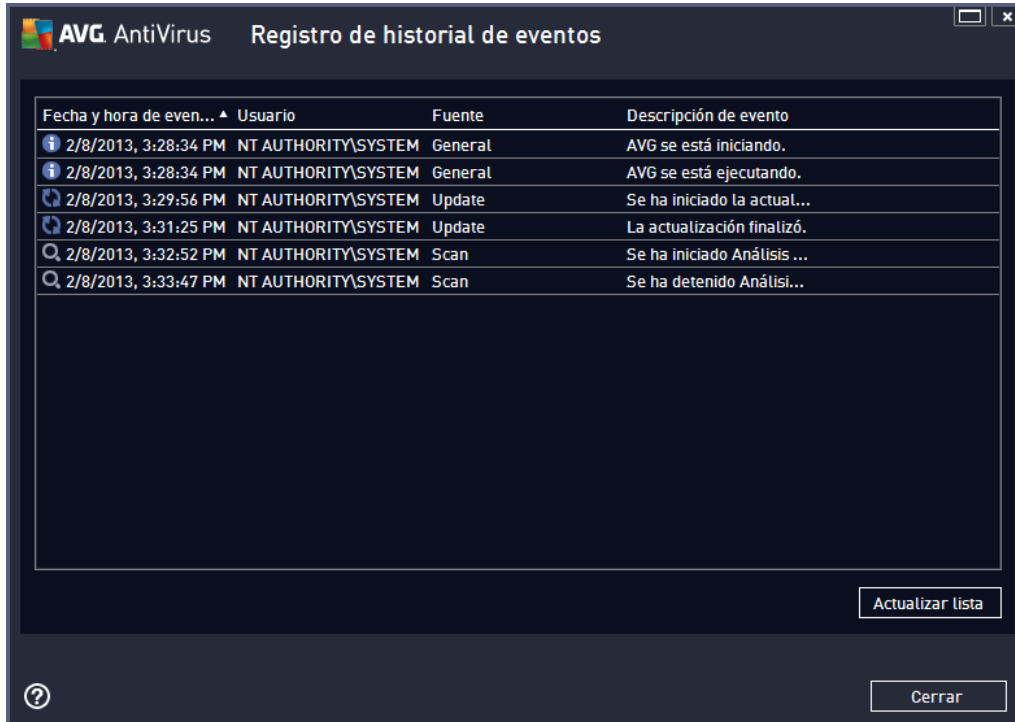
Para cada objeto detectado se proporciona la siguiente información:

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

Botones de control

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

12.5. Registro de historial de eventos



El cuadro de diálogo **Registro de historial de eventos** está accesible a través del elemento de menú **Opciones / Historial / Registro de historial de eventos** en la navegación superior de la ventana principal de **AVG AntiVirus 2013**. En este cuadro de diálogo puede encontrar un resumen de los eventos importantes que se han producido durante el funcionamiento de **AVG AntiVirus 2013**. El cuadro de diálogo proporciona registros de los siguientes tipos de eventos: información sobre actualizaciones de la aplicación AVG; información sobre el inicio, finalización o interrupción del análisis (*incluidas las pruebas realizadas automáticamente*); información sobre eventos relacionados con la detección de virus (*mediante la protección residente o el [análisis](#)*) incluida la ubicación de ocurrencia; y otros eventos importantes.

Para cada evento, se muestra la información siguiente:

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

Botones de control

- **Actualizar lista:** presione este botón para actualizar todas las entradas de la lista de eventos



- **Cerrar:** presione el botón para regresar a la ventana principal de **AVG AntiVirus 2013**



13. Actualizaciones de AVG

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

Teniendo en cuenta la cantidad de nuevas amenazas para su equipo que surgen cada día y la velocidad a la que se propagan, es absolutamente esencial actualizar su **AVG AntiVirus 2013** de manera periódica. La mejor solución consiste en mantener la configuración predeterminada del programa donde está configurada la actualización automática. Tenga en cuenta que si la base de datos de virus de su **AVG AntiVirus 2013** no está actualizada, el programa no podrá detectar las amenazas más recientes.

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

13.1. Ejecución de actualizaciones

Para proporcionar la seguridad máxima disponible, **AVG AntiVirus 2013** está programado de forma predeterminado para buscar nuevas actualizaciones de la base de datos de virus cada pocas horas. Dado que las actualizaciones de AVG no se lanzan de acuerdo a una programación fija, sino que en respuesta a la cantidad y severidad de nuevas amenazas, este control resulta de alta importancia para asegurarse de que su base de datos de virus de AVG se mantenga actualizada en todo momento.

Si desea comprobar si hay nuevos archivos de actualización de inmediato, utilice el vínculo rápido [Actualizar ahora](#) en la interfaz de usuario principal. Este vínculo está disponible en todo momento desde cualquier cuadro de diálogo de la [interfaz de usuario](#). Una vez que se inicia la actualización, AVG verificará primero si hay nuevos archivos de actualización disponibles. Si es así, **AVG AntiVirus 2013** iniciará la descarga y ejecutará el proceso de actualización en sí. Se le informará de los resultados de la actualización en el cuadro de diálogo deslizante situado sobre el icono del sistema AVG.

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

- [Programación de actualización de las definiciones](#)
- [Programación de actualización del programa](#)

13.2. Niveles de actualización

AVG AntiVirus 2013 permite seleccionar dos niveles de actualización:

- **Actualización de definiciones** contiene los cambios necesarios para una protección antivirus, confiable. Por lo general, no incluye cambios del código y sólo actualiza la base



de datos de definiciones. Esta actualización se debe aplicar tan pronto como esté disponible.

- **Actualización del programa** contiene diferentes modificaciones, arreglos y mejoras del programa.

Al [programar una actualización](#), es posible definir parámetros específicos para ambos niveles de actualización:

- [Programación de actualización de las definiciones](#)
- [Programación de actualización del programa](#)

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



14. Preguntas frecuentes y soporte técnico

Si tiene algún problema técnico o referente a la compra de la aplicación **AVG AntiVirus 2013**, existen varios modos de buscar ayuda. Elija una de las opciones siguientes:

- **Obtener soporte:** En la aplicación de AVG usted puede obtener una página dedicada al soporte al cliente en el sitio web de AVG. (<http://www.avg.com/>) Seleccione el elemento del menú principal **Ayuda / Obtener soporte** para acceder al sitio web de AVG con métodos de soporte disponibles. Para continuar, siga las instrucciones de la página web.
- **Soporte (vínculo del menú principal):** el menú de la aplicación AVG (en la parte superior de la interfaz del usuario principal) incluye el vínculo **Soporte**, que abre un cuadro de diálogo nuevo con todos los tipos de información que puede necesitar cuando intente encontrar ayuda. El cuadro de diálogo incluye datos básicos sobre el programa AVG instalado (versión del programa o la base de datos), detalles de la licencia y una lista de vínculos de soporte rápidos:



- **Resolución de problemas en el archivo de ayuda:** Está disponible una sección de **Resolución de problemas** incluida en el archivo de ayuda **AVG AntiVirus 2013** (para abrir el archivo de ayuda, presione la tecla F1 en cualquier diálogo en la aplicación). Esta sección proporciona una lista de las situaciones que se producen con más frecuencia cuando un usuario desea obtener ayuda profesional sobre una cuestión técnica. Seleccione la situación que mejor describa su problema y haga clic en ella para abrir instrucciones detalladas que le permitan solucionarlo.
- **Centro de soporte del sitio web de AVG:** Como alternativa, puede buscar la solución a su problema en el sitio web de AVG (<http://www.avg.com/>). En la sección **Centro de soporte** encontrará una descripción general estructurada de grupos temáticos referentes tanto a cuestiones técnicas como a la compra.
- **Preguntas frecuentes:** en el sitio web de AVG (<http://www.avg.com/>) también encontrará una sección independiente y minuciosamente estructurada de preguntas frecuentes. Se puede obtener acceso a esta sección por medio de la opción de menú **Centro de soporte /**



Preguntas frecuentes. Una vez más, todas las preguntas están divididas de forma bien organizada en las categorías de ventas, técnicas y sobre virus.

- **Acerca de los virus y amenazas.** Una parte específica del sitio web de AVG (<http://www.avg.com/>) está dedicado a los problemas de virus (*se accede a la página web desde el menú principal mediante la opción Ayuda / Acerca de los virus y amenazas*). En el menú, seleccione **Centro de soporte / Acerca de virus y amenazas** para tener acceso a una página que proporciona una descripción general estructurada de información relacionada con amenazas en línea. También encontrará instrucciones sobre cómo eliminar virus y spyware y cómo mantenerse protegido.
- **Foro de discusión:** también puede utilizar el foro de discusión de usuarios de AVG en <http://forums.avg.com>.