AVG Protection

Manual del Usuario

Revisión del documento 2015.04 (3/24/2015)

Contenidos

1. Introducción

Felicitaciones por haber adquirido el paquete de AVG Protection. Con este paquete podrá disfrutar de todas las funciones de **AVG Internet Security 2015**, ahora ampliadas con **AVG Zen**.

AVG Zen

Esta herramienta de administración invaluable puede cuidarlo a usted y a toda su familia. Todos sus dispositivos estarán reunidos oportunamente en un lugar para mantener fácilmente el control sobre el estado de Protección, Rendimiento y Privacidad de cada uno. Con **AVG Zen** ya no es necesario comprobar cada dispositivo uno por uno. Incluso puede realizar tareas de análisis y mantenimiento y reparar los problemas de seguridad más urgentes de manera remota. **AVG Zen** se integra directamente a su paquete, de manera que funciona automáticamente desde el inicio.

Haga clic aquí para aprender acerca de AVG Zen

AVG Internet Security 2015

: esta aplicación de seguridad galardonada proporciona varios niveles de protección para todo lo que realiza en línea, lo que supone que no tiene que preocuparse por el robo de identidad, los virus o la visita a sitios dañinos. La Tecnología de Nube Protectora de AVG y la Red de Protección de la Comunidad de AVG están incluidas, lo que significa que recopilamos la información sobre amenazas más actual y la compartimos con nuestra comunidad para garantizar que sus miembros reciben la mejor protección. Puede comprar y realizar operaciones bancarias en línea de forma segura, disfrutar su vida en redes sociales o navegar y buscar con la confianza de una protección en tiempo real.

Haga clic aquí para aprender acerca de AVG Internet Security 2015.

1.1. Requisitos de hardware

Requisitos mínimos de hardware para **AVG Internet Security 2015**:

- CPU Intel Pentium a 1.5 GHz o superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, 7 y 8) de memoria RAM
- 1.3 GB de espacio libre en el disco duro *(para la instalación)*

Requisitos recomendados de hardware para **AVG Internet Security 2015**:

- CPU Intel Pentium a 1.8 GHz o superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, 7 y 8) de memoria RAM
- 1.6 GB de espacio libre en el disco duro *(para la instalación)*

1.2. Requisitos del sistema

AVG Internet Security 2015 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 (x86 y x64, todas las ediciones)
- Windows 8 (x32 y x64)

  (y posiblemente Service Packs superiores para determinados sistemas operativos)

El componente Identity no es admitido en Windows XP x64. En este sistema operativo, puede instalar AVG Internet Security 2015, pero sólo sin el componente IDP.

2. AVG Zen

Esta parte del manual de usuario proporciona documentación completa para AVG Zen. Observe que este manual describe únicamente la versión Equipo de este producto.

AVG, un desarrollador de software de protección famoso en todo el mundo, avanza aún más hacia sus clientes y la satisfacción total de sus necesidades de seguridad. El nuevo AVG Zen conecta con eficacia los dispositivos de escritorio a móvil y los datos y las personas detrás de ellos en un paquete sencillo con el objetivo de simplificar nuestras complicadas vidas digitales. Mediante una aplicación, AVG Zen les facilita a los usuarios el poder ver la configuración de seguridad y privacidad de todos sus dispositivos desde un solo lugar.

La idea detrás de AVG Zen es que el individuo con todos estos dispositivos recupere el control de sus datos y su seguridad, ya que creemos que a través del control viene la libertad de elección. De hecho, AVG no está aquí para decirle que está mal compartir o rastrear de por sí; en lugar de ello, queremos brindar a nuestros clientes información que les permitirá controlar qué comparten y si están siendo rastreados, y a tomar sus propias decisiones informadas. Una opción para gozar de libertad para vivir la vida como quieren y educar a sus familias o solicitar un empleo sin miedo a ver invadida su privacidad.

Otra cosa muy positiva acerca de AVG Zen es que ofrece a nuestros clientes una experiencia de usuario constante en todos los dispositivos, de manera tal que hasta los principiantes pueden aprender rápidamente cómo administrar y asegurar sus diversos dispositivos con facilidad. Al menos eso es algo que se vuelve más fácil en un mundo cada vez más complejo. Por último, y sobre todo, AVG Zen está diseñado para traer tranquilidad a personas reales mientras viven sus vidas cotidianas. A medida que internet se vuelve el centro de nuestro mundo conectado, AVG Zen está allí para unir los puntos.

Esta parte de la documentación contiene una descripción de las funciones específicas de AVG Zen. Si necesita información sobre otros productos de AVG, consulte la otra parte de esta documentación, o también guías de usuario específicas. Puede descargar estas guías desde el sitio web de AVG..

2.1. Proceso de instalación de Zen

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

2.1.1. Cuadro de Diálogo de Bienvenida

El proceso de instalación se inicia siempre con esta ventana. Aquí selecciona el **idioma** utilizado en la aplicación AVG Zen.

Si desea modificar la carpeta de destino de su instalación, haga clic en el vínculo ***Personalizar instalación*** y hágalo en el cuadro de diálogo que se acaba de abrir.

Para más información puede leer el Acuerdo de Licencia del Software de ***AVG*** y la Política de Perzonalización y Privacidad de ***AVG***. Simplemente haga clic en el vínculo correcto y aparecerá el texto completo en una nueva ventana.

Si está de acuerdo con estos términos, continúe con la instalación haciendo clic en el botón **Aceptar e instalar**.

Tras una instalación exitosa, se necesita reiniciar el equipo. Puede reiniciar desde el cuadro de diálogo final de la instalación (haciendo clic en el botón **Reiniciar ahora**) o aplazar la acción para más tarde. No obstante, tenga en cuenta que sin el reinicio del equipo es posible que algunos productos AVG no se visualicen correctamente en la interfaz de usuario de Zen y que la aplicación en conjunto no funcione adecuadamente.

2.1.2. Carpeta de Destino

Este cuadro de diálogo es opcional, se activa haciendo clic en el vínculo ***Personalizar instalación*** en el cuadro de diálogo anterior de la instalación.

En él, puede establecer la ***carpeta de destino*** para la instalación. Si no está satisfecho con la ubicación predeterminada donde se debe instalar AVG Zen (es decir, en la carpeta de archivos de programa de la unidad C), puede ingresar una nueva ruta de forma manual en el cuadro de texto o usar el vínculo **Buscar** (junto al cuadro de texto). Mediante el vínculo se visualiza la estructura de la unidad y se puede seleccionar la respectiva carpeta.

Ahora haga clic en el botón **Aceptar e Instalar** para iniciar el proceso mismo de instalación.

Tras una instalación exitosa, se necesita reiniciar el equipo. Puede reiniciar desde el cuadro de diálogo final de la instalación (haciendo clic en el botón **Reiniciar ahora**) o aplazar la acción para más tarde. No obstante, tenga en cuenta que sin el reinicio del equipo es posible que algunos productos AVG no se visualicen correctamente en la interfaz de usuario de Zen y que la aplicación en conjunto no funcione adecuadamente.

2.2. Interfaz de usuario de Zen

Este es el cuadro de diálogo principal de su interfaz de usuario de AVG Zen. En cualquier otro cuadro de diálogo, siempre hay un botón en la esquina superior izquierda. Si hace clic en él, regresa a esta pantalla principal (en algunos cuadros de diálogo consiguientes, este botón lo lleva sólo un paso atrás, es decir, al cuadro de diálogo anterior de la serie).

Este cuadro de diálogo consta de varias secciones diferentes:

- Iconos Categoría
- Cinta de opciones Dispositivos
- Botón Mensajes
- Botón Estado
- Botón Actualizar
- Botón Configuraciones

2.2.1. Iconos Categoría

Los iconos Categoría le permiten instalar productos de software AVG, ver su estado y abrir simplemente su interfaz del usuario. El administrador de la red de Zen también puede utilizarlos para ver y administrar productos AVG instalados en dispositivos remotos. Utilice la cinta de opciones Dispositivos para repasar todos los dispositivos remotos disponibles en su red de Zen.

Dentro de cada icono, hay un círculo y el color depende del estado de los productos dentro de esta categoría (debe esforzarse para que permanezca verde). Para algunas categorías, puede ver simplemente un semicírculo que significa que ya tiene un producto de esta categoría, pero que falta instalar otro producto.

Si bien siempre se ve el mismo grupo de iconos sin importar qué tipo de dispositivo visualiza, el contenido de los iconos puede diferir según el tipo de dispositivo controlado (equipo de escritorio, Android o Mac).

2.2.1.1. Equipos

PROTECCIÓN

AVG Internet Security: este software de seguridad proporciona varios niveles de protección para todo lo que realiza en línea, lo que supone que no tiene que preocuparse por el robo de identidad, los virus o la visita a sitios dañinos. La Tecnología de Nube Protectora de AVG y la Red de Protección de la Comunidad de AVG están incluidas, lo que significa que recopilamos la información sobre amenazas más actual y la compartimos con nuestra comunidad para garantizar que sus miembros reciben la mejor protección. Puede comprar y realizar operaciones bancarias en línea de forma segura, disfrutar su vida en redes sociales o navegar y buscar con la confianza de una protección en tiempo real.

Vista general de estados

- si AVG Internet Security no está instalado, este icono permanece gris y el texto a continuación dice "No protegido", pero puede hacer clic en él para instalar simplemente esta aplicación AVG.
- si existen demasiados problemas a los que prestar atención (como el caso en que todo AVG Internet Security esté desactivado), el círculo dentro de este icono aparece en rojo y el texto a continuación dice "No protegido". Si sólo enfrenta unos pocos problemas menores, el icono aparece en verde, pero el texto a continuación dice "Parcialmente protegido". En ambos casos, verá un número en un círculo naranja (en la esquina superior derecha del icono) que muestra la cantidad de problemas a los que debe prestar atención. Use el botón Mensajes para ver una lista de problemas y posiblemente solucionarlos.
- si no existe ningún problema con AVG Internet Security, el círculo dentro de este icono aparece en verde y el texto a continuación dice "Protegido".

Qué ocurre luego de hacer clic en este icono:

- si AVG Internet Security todavía no está instalado: se abre un nuevo cuadro de diálogo que permite instalar AVG Internet Security. Lea más acerca de la instalación de productos AVG.
- si está viendo sus propios dispositivos con AVG Internet Security instalado: se abre la interfaz del

usuario de AVG Internet Security.
- si está viendo (como administrador) un dispositivo remoto que tiene instalado AVG Internet Security: abre un diálogo que contiene un breve resumen del estado de AVG Internet Security en el dispositivo remoto. Este cuadro de diálogo le permite llevar a cabo varias acciones remotas, como ejecutar un análisis (el botón **Analizar ahora**) o realizar una actualización (el botón **Actualizar**). A otras acciones remotas, como activar componentes de protección anteriormente desactivados, se puede acceder al hacer clic en el botón **Mostrar detalles**, que abre el cuadro de diálogo Mensajes para el dispositivo actualmente seleccionado. Lea más acerca de la visualización y administración de dispositivos remotos.

RENDIMIENTO

AVG PC TuneUp: con esta aplicación puede restaurar toda la capacidad de rendimiento del sistema operativo, los juegos y los programas. AVG PC TuneUp también permite ejecutar tareas de mantenimiento importantes, como la limpieza del disco duro y del registro, tanto de forma automática como manual. AVG PC TuneUp reconoce rápidamente si hay algún problema en su sistema y le ofrece soluciones simples. Además, con AVG PC TuneUp también se puede cambiar la apariencia del sistema Windows de forma completamente personalizada.

Vista general de estados

- Si AVG PC TuneUp no está instalado, este icono permanece gris y el texto a continuación dice "No ajustado", pero puede hacer clic en él para instalar simplemente esta aplicación AVG.
- Si existen demasiados problemas a los que prestar atención (como el caso en que todo AVG PC TuneUp esté desactivado), el círculo dentro de este icono aparece en rojo y el texto a continuación dice "No ajustado". Si sólo enfrenta unos pocos problemas menores, el icono aparece en verde, pero el texto a continuación dice "Parcialmente ajustado". En ambos casos, verá un número en un círculo naranja (en la esquina superior derecha del icono) que muestra la cantidad de problemas a los que debe prestar atención. Use el botón Mensajes para ver una lista de problemas y posiblemente solucionarlos.
- Si no existe ningún problema con AVG PC TuneUp, el círculo dentro de este icono aparece en verde y el texto a continuación dice "Ajustado".

Qué ocurre luego de hacer clic en este icono:

- si AVG PC TuneUp todavía no está instalado : se abre un nuevo cuadro de diálogo que le permite instalar AVG PC TuneUp. Lea más acerca de la instalación de productos AVG.
- si está viendo sus propios dispositivos con AVG PC TuneUp instalado: se abre la interfaz del usuario de AVG PC TuneUp.
- si está viendo (como administrador) un dispositivo remoto que tiene instalado AVG PC TuneUp : abre un diálogo que contiene un breve resumen del estado de AVG PC TuneUp en el dispositivo remoto. Este cuadro de diálogo le permite llevar a cabo varias acciones remotas, como ejecutar mantenimiento (el botón **Ejecutar mantenimiento**) o realizar una actualización (el botón **Actualizar**). A otras acciones remotas se puede acceder al hacer clic en el botón **Mostrar detalles**, que abre el cuadro de diálogo Mensajes para el dispositivo actualmente seleccionado. Lea más acerca de la visualización y administración de dispositivos remotos.

PRIVACIDAD E IDENTIDAD

Esta categoría consta de dos partes diferentes: AVG PrivacyFix (complemento de navegador de seguridad) y Identity Protection (un componente de la aplicación AVG Internet Security). Para obtener un círculo completo (de ser posible, verde), debe tener instaladas las dos aplicaciones.

AVG PrivacyFix: este complemento de navegador de seguridad lo ayuda a comprender y a controlar la recopilación de datos. Verifica la exposición de su privacidad en Facebook, Google y LinkedIn y, con un clic,

lo dirige a la configuración donde puede solucionarlo. Se evita que más de 1200 rastreadores sigan sus movimientos en línea. Además, puede ver qué sitios web se reservan el derecho a vender sus datos personales y puede solicitar fácilmente que eliminen la información que manejan sobre usted. Por último, recibe alertas sobre los riesgos de privacidad al visitar sitios y sabe cuándo cambian las políticas.

AVG Internet Security: componente Identity Protection: este componente (una parte de la aplicación AVG Internet Security) le ofrece a su equipo protección en tiempo real contra amenazas nuevas e incluso desconocidas. Supervisa todos los procesos (incluso los ocultos) y cientos de patrones de comportamiento 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.

Vista general de estados

- si no tiene instalada ninguna de las aplicaciones anteriores, este icono permanece gris y el texto a continuación dice "Sin configuración", pero puede hacer clic en él para instalar simplemente estas aplicaciones AVG.
- si tiene instalada sólo una de estas aplicaciones, habrá únicamente un semicírculo dentro de este icono. El color depende del estado de la aplicación instalada: puede ser verde ("Activo" / "Protegido") o rojo ("Desactivado" / "No protegido").
- Si ambas aplicaciones están instaladas, estando una activa y la desactivada, el círculo dentro de este icono será rojo y tendrá un texto indicando "Parcialmente protegido".
- Si las dos aplicaciones están instaladas y activas, verá un círculo verde completo dentro de este icono con un texto indicando "Protegido". ¡Felicitaciones, su privacidad e identidad son totalmente seguras!

Después de hacer clic en este icono, se abre un nuevo cuadro de diálogo que consta de otros dos iconos: para AVG Identity Protection y para AVG PrivacyFix. Estos iconos son igual de interactivos que los iconos primarios en la interfaz del usuario principal de su aplicación AVG Zen y también se puede hacer clic en ellos.

- si todavía no tiene instalada una o ninguna de estas aplicaciones, puede hacer clic en el botón **Adquiéralo en forma GRATUITA** para remediarlo. Lea más acerca de la instalación de productos AVG.
- si al menos una de estas aplicaciones está instalada, puede hacer clic en su icono para abrir su interfaz del usuario.
- si está viendo (como administrador) un dispositivo remoto con estas aplicaciones instaladas: abre un diálogo que contiene un breve resumen del estado de estas dos aplicaciones en el dispositivo remoto. No obstante, este diálogo es puramente informativo y no se puede modificar nada. Lea más acerca de la visualización y administración de dispositivos remotos.

SOPORTE

(el círculo dentro de este icono es verde cuando se encuentra disponible soporte mientras que el texto a continuación dice "Cubierto")

Al hacer clic en este icono, se abre un nuevo cuadro de diálogo que contiene vínculos a los recursos de soporte más comunes. Para leer acerca de las opciones de soporte que ofrece AVG, haga clic aquí.

Quizás desee revisar los siguientes temas relacionados:

- ¿Cómo instalar productos AVG?
- ¿Cómo ver o administrar productos AVG?

2.2.1.2. Dispositivos Android

Este manual trata únicamente sobre aspectos de AVG Zen relacionados con equipos de escritorio; sin embargo, como administrador es probable que también tenga algunos dispositivos Android™ en su red. En este caso, no se sorprenda si ve un contenido diferente en los iconos Categoría de estos dispositivos.

Aplicaciones AVG para dispositivos móviles disponibles actualmente:

- ***AVG AntiVirus*** (gratis o pago): esta aplicación lo protege de virus, malware, spyware y mensajes de texto nocivos, y lo ayuda a mantener sus datos personales a salvo. Con esta aplicación recibirá una protección contra malware y virus simple y efectiva, un analizador de aplicación en tiempo real, un localizador de teléfono, un task killer, un bloqueador de aplicaciones y una limpieza del dispositivo local para protegerlo contra las amenazas a su privacidad e identidad en línea. La protección que proporciona el analizador de seguridad en tiempo real lo mantiene protegido de las aplicaciones y los juegos que descarga.
- ***AVG Cleaner*** (gratis): esta aplicación le permite rápidamente borrar y limpiar su navegador de llamadas y de mensajes de textos, así como también identificar y eliminar el caché no deseado de los datos de las aplicaciones que se encuentren en la memoria interna del dispositivo y de la tarjeta SD. Optimiza de forma significativa el espacio de almacenamiento para ayudar a que su dispositivo Android™ tenga un mejor rendimiento y funcione sin problemas.
- ***AVG PrivacyFix*** (gratis): esta aplicación le brinda una forma simple de administrar su configuración de privacidad en línea a través de su dispositivo móvil. Le otorga acceso a un panel principal que le muestra fácil y rápidamente qué datos comparte y con quién en Facebook, Google y LinkedIn. Si desea cambiar algo, un simple clic lo lleva directamente adonde puede cambiar la configuración. La nueva protección de rastreo por WiFi le posibilita preconfigurar redes WiFi que conoce y autorizar y detener su dispositivo frente al rastreo de otras redes.

Las categorías individuales son las siguientes:

PROTECCIÓN

Al hacer clic en este icono se le muestra información acerca de **AVG AntiVirus**, acerca del análisis y sus resultados, y también acerca de actualizaciones de definiciones de virus. Como administrador de red, también puede ejecutar un análisis (el botón **Analizar ahora**) o realizar una actualización (el botón **Actualizar**) de un dispositivo Android remoto.

RENDIMIENTO

Al hacer clic en este icono se le muestran datos relativos al rendimiento, esto es, qué funciones de rendimiento de **AVG AntiVirus** están activas (***Task Killer***, ***Estado de la Batería***, ***Plan de Datos*** (sólo versión paga) y ***Uso de Almacenamiento***), y si la aplicación **AVG Cleaner** está instalada y ejecutándose (junto con algunas estadísticas).

PRIVACIDAD

Al hacer clic en este icono se le muestran datos relativos a la privacidad, esto es, qué funciones de privacidad de **AVG AntiVirus** están activas (***Bloqueo de Aplicaciones***, ***Copia de Respaldo de Aplicaciones*** y ***Bloqueador de Llamadas y Mensajes***), y si la aplicación **AVG PrivacyFix** está instalada y ejecutándose.

ANTIRROBO

Al hacer clic en este icono se le muestra información acerca de la función ***Antirrobo*** de **AVG AntiVirus**, que

le permite ubicar su dispositivo móvil robado mediante Google Maps. Si existe una versión paga (**Pro**) de **AVG AntiVirus** instalada en un dispositivo conectado, adicionalmente verá el estado de la función ***Cámara Trampa*** (que permite tomar una foto secreta de cualquiera que intente desbloquear el móvil) y de la función ***Device Lock*** (que permite al usuario bloquear el dispositivo móvil en el momento en que la tarjeta SIM es reemplazada).

Quizás desee revisar los siguientes temas relacionados:

- ¿Cómo conectar su móvil Android a una red de Zen existente?
- ¿Cómo ver o administrar productos AVG?

2.2.1.3. Dispositivos Mac

Este manual trata únicamente sobre aspectos de AVG Zen relacionados con equipos de escritorio; sin embargo, como administrador es probable que también tenga algunos dispositivos Mac en su red. En este caso, no se sorprenda si ve un contenido diferente en los iconos Categoría de estos dispositivos.

Aplicaciones AVG Mac disponibles actualmente (sólo en inglés):

- ***AVG AntiVirus*** (gratis): esta aplicación poderosa le permite analizar carpetas o archivos específicos en busca de virus y otras amenazas, o incluso realizar un análisis exhaustivo de toda su Mac con un único clic. También está disponible una protección en tiempo real, que funciona silenciosamente en segundo plano. Cada archivo que abra, copie o guarde se analiza automáticamente sin tornar lenta su Mac.
- ***AVG Cleaner*** (gratis): esta aplicación le permite eliminar el desorden innecesario, como archivos de caché y no deseados, historial de archivos descargados, contenidos de la papelera, etc. para liberar espacio. También puede encontrar archivos duplicados en el disco duro y eliminar rápidamente copias innecesarias.

Las categorías individuales son las siguientes:

PROTECCIÓN

Al hacer clic en este icono se le muestra información acerca de **AVG AntiVirus**, acerca del análisis y sus resultados, y también acerca de actualizaciones de definiciones de virus. También puede ver si la protección en tiempo real está activa o no. Como administrador de red, también puede actualizar AVG AntiVirus en un dispositivo remoto (el botón **Actualizar**) o activar la protección en tiempo real previamente desactivada (a través del cuadro de diálogo Mensajes al que se puede acceder haciendo clic en el botón **Mostrar detalles**). Lea más acerca de la visualización y administración de dispositivos remotos.

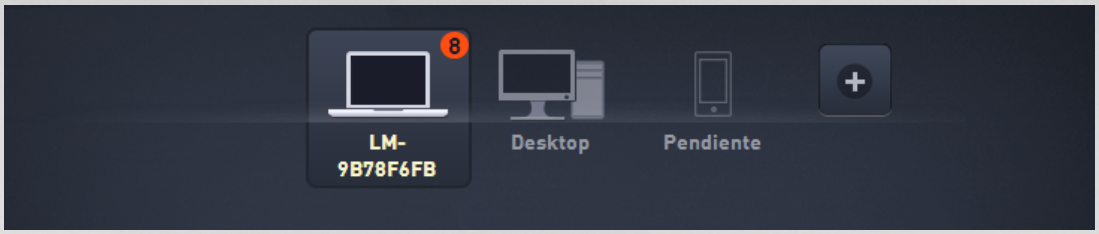
RENDIMIENTO

Al hacer clic en este icono verá datos relativos al rendimiento, esto es, datos sobre los dos componentes de **AVG Cleaner**: ***Disk Cleaner*** y ***Duplicate Finder***. Puede ver cuándo tuvo lugar la última prueba con estas funciones de rendimiento y cuáles fueron los resultados.

Quizás desee revisar los siguientes temas relacionados:

- ¿Cómo conectar su Mac a una red de Zen existente?
- ¿Cómo ver o administrar productos AVG?

2.2.2. Cinta de opciones de Dispositivos



Esta parte de la interfaz de usuario de AVG Zen muestra todos los dispositivos disponibles en su red de Zen. Si es un usuario individual o si sólo está conectado a la red de Zen de alguien, solamente verá un dispositivo, su dispositivo actual. Sin embargo, como administrador de red puede tener tantos dispositivos en vista que quizás deba utilizar los botones de flechas para verlos a todos.

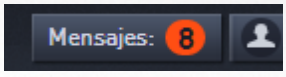
Seleccione el dispositivo que desea ver haciendo clic en su icono. Verá que la sección Categorías cambia correctamente y muestra el estado de los productos AVG en el dispositivo seleccionado. También puede observar un número en un círculo naranja que aparece en la esquina superior derecha de algunos iconos. Esto significa que hay problemas con productos AVG en este dispositivo a los que quizás desee prestarles atención. Haga clic en el botón Mensajes para hacerlo y para obtener más información.

Como administrador de la red de Zen es posible que desee añadir nuevos dispositivos a su red. Para ello, haga clic en el botón  que se encuentra del lado derecho de la cinta de opciones.

Quizás desee revisar los siguientes temas relacionados:

- ¿Cómo añadir dispositivos a su red?
- ¿Cómo quitar dispositivos de su red?

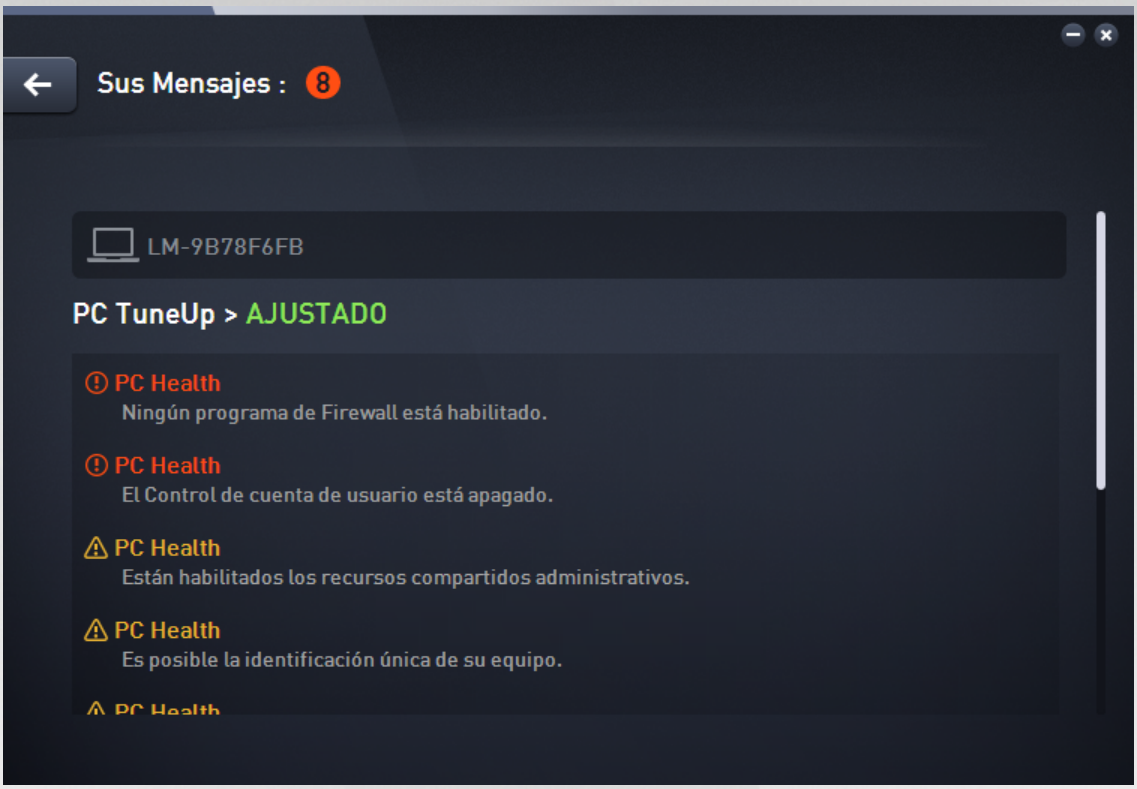
2.2.3. Botón Mensajes



Este botón se encuentra arriba de la cinta de opciones Dispositivos y a la izquierda del botón Estado. Sin embargo, aparece únicamente si hay algún problema con productos AVG en su dispositivo actual. El número en un círculo naranja muestra la cantidad de problemas a los que debe prestarle atención (este círculo naranja puede incluso contener un signo de exclamación como advertencia de que alguna aplicación AVG se encuentra totalmente desactivada).

Como administrador de la red,también puede acceder al cuadro de diálogo ***Mensajes*** para dispositivos remotos al hacer clic en el botón **Mostrar detalles** (en la vistaicono de Categoría). Recuerde que este botón sólo está disponible si existen problemas urgentes que requieren de su atención. Haga clic aquí para leer sobre esta y otras acciones de administración remotas.

Luego de hacer clic en este botón, aparece un nuevo cuadro de diálogo:



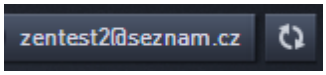
Este cuadro de diálogo muestra la lista de problemas ordenados por categoría de producto. Los problemas aparecen de diferentes colores (rojo, amarillo o verde), lo que permite distinguir problemas urgentes de problemas menos urgentes.

Si es un administrador con más de un dispositivo en su red, este cuadro de diálogo es ligeramente diferente. Hay una vista general de dispositivos en el lado izquierdo, lo que le permite ver únicamente mensajes relacionados con este dispositivo en particular. Sin embargo, si desea visualizar mensajes para todos los dispositivos en una lista ordenada, puede elegir la opción ***TODOS LOS DISPOSITIVOS*** (es la que se encuentra más arriba en la vista general).

Algunos problemas pueden manejarse directamente desde este cuadro de diálogo. Aparecen con un botón de acción especial (generalmente denominado **Reparar ahora**) junto a ellos. Como administrador de red, puede reparar dichos problemas de manera remota, directamente desde su AVG Zen. Como usuario individual o conectado, sólo puede administrar los productos AVG de su propio dispositivo, pero aun así, es mucho más cómodo ver todos los problemas juntos, sin tener que abrir la interfaz de las aplicaciones individuales.

Por ejemplo, al ver el texto ***"EL FIREWALL NECESITA REINICIAR EL EQUIPO: para activar el firewall, reinicie su equipo"***, puede hacer clic en el botón **Reiniciar ahora**. Inmediatamente después, su equipo se reiniciará para activar el componente Firewall.

2.2.4. Botón Estado



Este botón muestra su modo de usuario actual. Como administrador de la red de Zen, normalmente verá su correo electrónico de MyAccount que utilizó para conectarse a la red.

Tras hacer clic en este botón, se muestra una lista de acciones adicionales. Las acciones disponibles dependen del modo de usuario que utiliza actualmente:

Como usuario individual:

- **Conectar**: le permite conectarse a un red de Zen existente (o crear una nueva).
- **Visitar AVG MyAccount**: inicia su navegador y abre el sitio web https://myaccount.avg.com/, permitiéndole iniciar sesión en su AVG MyAccount.

Como usuario conectado:

- **Iniciar sesión como Administrador**: haga clic para obtener derechos de administrador, lo que le permitirá ver y administrar esta Zen red (inicio de sesión requerido).
- **Salir de Esta Red**: haga clic para salir de esta red de Zen (confirmación requerida).
- **Más Información**: muestra un diálogo informativo acerca de la Zen red a la que está conectado actualmente y su administrador.
- **Visitar AVG MyAccount**: inicia su navegador y abre el sitio web https://myaccount.avg.com/, permitiéndole iniciar sesión en su AVG MyAccount.

Como administrador:

- **Cerrar sesión como Administrador**: haga clic para perder sus derechos de administrador y convertirse en un usuario conectado dentro de la misma Zen red.
- **Visitar AVG MyAccount**: inicia su navegador y abre el sitio web https://myaccount.avg.com/, permitiéndole iniciar sesión en su AVG MyAccount.

¿Qué es AVG MyAccount?

AVG MyAccount es un servicio gratuito de AVG basado en la web (nube) que le permite:

- visualizar sus productos registrados y la información de licencia
- renovar su suscripción y descargar los productos con facilidad
- comprobar pedidos y facturas anteriores
- administrar sus datos personales y su contraseña
- utilizar AVG Zen

Se puede acceder a AVG MyAccount directamente en el sitio web https://myaccount.avg.com/.

2.2.4.1. Tres modos de usuario

Básicamente, existen tres modos de usuario en AVG Zen. El texto que aparece en el **botón Estado** depende de cuál está usando actualmente:

- **Usuario individual** (el botón Estado muestra ***Conectar***) : acaba de instalar AVG Zen. No es ni administrador de AVG MyAccount ni está conectado a ninguna red, por lo tanto, únicamente puede ver y administrar productos AVG instalados en este dispositivo.

- **Usuario conectado** (el botón Estado muestra ***Conectado***) : acaba de usar un código de emparejamiento, y así aceptó una invitación a la red de alguien. El administrador de esta red puede ahora ver y administrar todos los productos AVG en su dispositivo. Respecto a usted, todavía puede ver y administrar productos AVG instalados en este dispositivo (como si fuese un usuario individual).

Si ya no desea permanecer en una red, puede dejarla fácilmente.

- **Administrador** (el botón Estado muestra el nombre actual de ***AVG MyAccount***) : inició sesión con su MyAccount (quizás creó una nueva previamente). Esto significa que tiene acceso a todas las AVG Zen funciones. Puede añadir dispositivos a su red, ver de forma remota productos AVG instalados en ellos y, de ser necesario, eliminarlos de su red. Incluso puede realizar varias acciones remotas en los dispositivos conectados.

Quizás desee revisar los siguientes temas relacionados:

- ¿Cómo aceptar invitaciones?
- ¿Cómo conectarse a una red de Zen existente?
- ¿Cómo crear una nueva red de Zen?
- ¿Cómo salir de una red?
- ¿Cómo ver o administrar productos AVG?

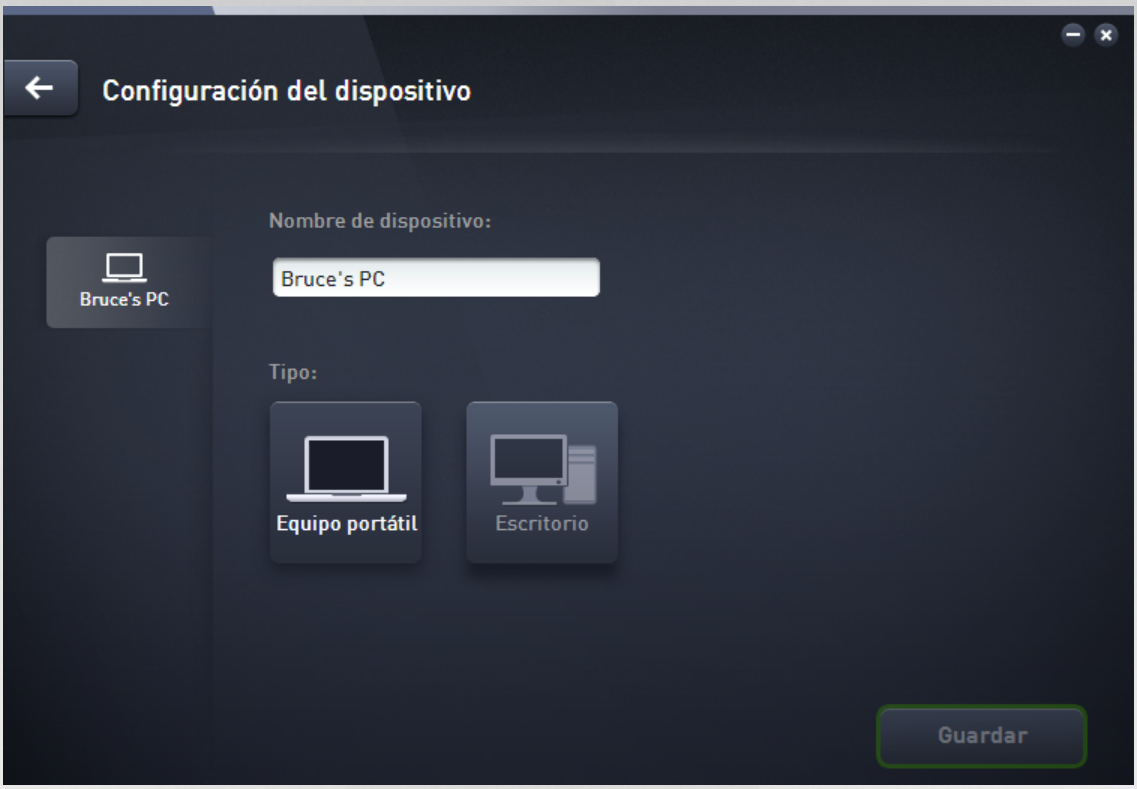
2.2.5. Botón Actualizar

Hacer clic en este diminuto botón (que se encuentra a la derecha del botón Estado) actualiza inmediatamente todos los datos para todos los dispositivos y categorías. Esto puede ser útil por ejemplo en caso de que un dispositivo agregado recientemente no haya aparecido aún en la cinta de opciones Dispositivos, aunque usted sepa que ya está conectado y desea ver sus detalles.

2.2.6. Botón Configuraciones

Hacer clic en este diminuto botón (que se encuentra a la derecha del botón Actualizar) abre un pequeño cuadro de diálogo emergente.

Puede hacer clic en la opción ***Configuración de dispositivos*** para abrir el cuadro de diálogo Configuración de dispositivo, lo que le permite modificar el nombre y tipo de su dispositivo (así también como de otros dispositivos en su red de Zen, si existiesen y si es el administrador de esta red). Este cuadro de diálogo le permite quitar dispositivos de su red.



Además, puede hacer clic en la opción ***Acerca de AVG Internet Security 2015*** para ver información sobre su producto de software o incluso para leer el Contrato de Licencia.

Quizás desee revisar los siguientes temas relacionados:

- ¿Cómo modificar el nombre o tipo de dispositivo?
- ¿Cómo quitar dispositivos de su red?

2.3. Guías paso a paso

Este capítulo contiene algunas guías paso a paso que describen las operaciones más comunes en el entorno de Zen.

2.3.1. ¿Cómo aceptar invitaciones?

Si utiliza productos AVG en más de un dispositivo, o no tiene suficiente experiencia y desea que alguien controle sus productos AVG y lo ayude a reparar cualquier problema, quizás desee añadir su equipo o móvil Android™ a alguna red de Zen existente. Sin embargo, primero debe recibir una invitación de su administrador de red, por lo tanto, debe solicitarle que le envíe una invitación por correo electrónico. Luego de recibirla, ábrala y encuentre dentro un **código de invitación**.

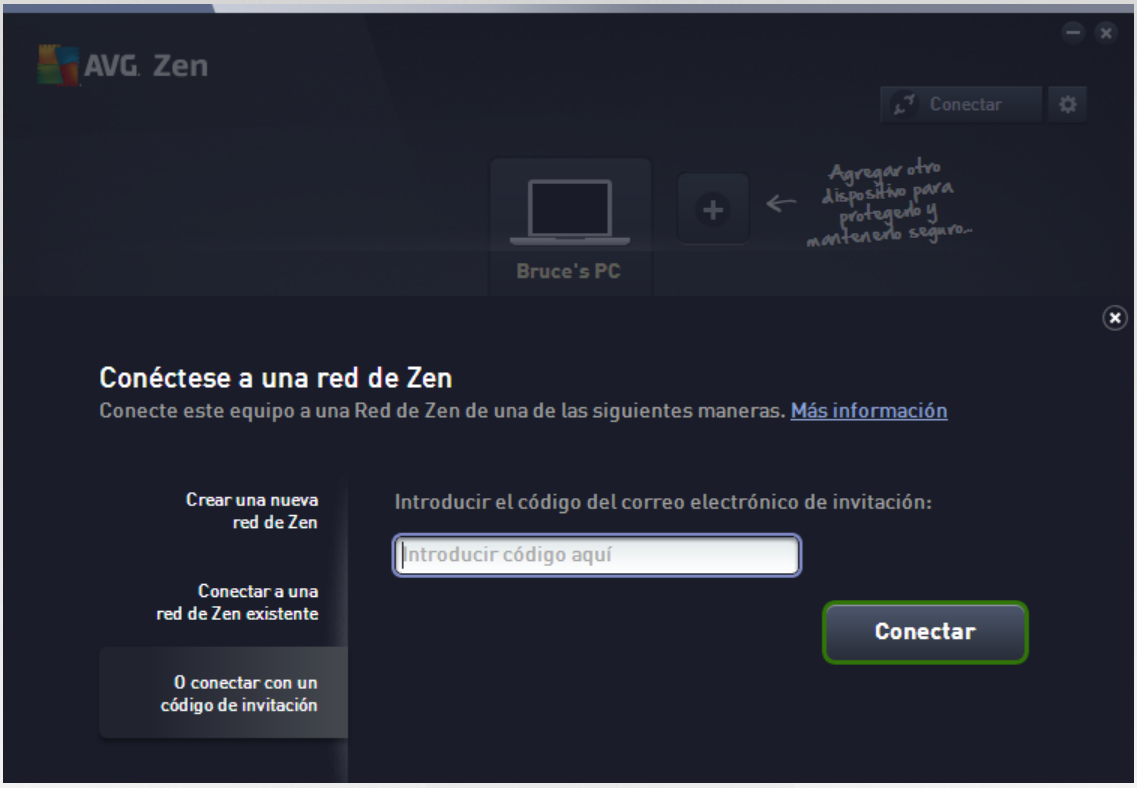
Lo que haga a continuación depende de si desea agregar un equipo de escritorio o dispositivo móvil Android™:

Dispositivos de escritorio:

1. Instale AVG Zen (si todavía no lo hizo).

2. Haga clic en el botón Estado (con el texto que dice ***Conectar***) y confirme haciendo clic en el botón ***Continuar*** en el pequeño cuadro de diálogo emergente.

3. Seleccione el panel ***Conectar con un código de invitación*** que se encuentra del lado izquierdo del subdiálogo que se acaba de abrir.



4. Use el método copiar y pegar para copiar el código de invitación del correo electrónico en el cuadro de texto apropiado en Zen subdiálogo (o vuelva a ingresarlo de forma manual).

El método de copiar y pegar es un procedimiento común que le permite agregar cualquier cosa que se pueda copiar (texto, imágenes, etc.) al portapapeles de Windows y posteriormente pegarla en otro lugar. Funciona de la siguiente manera:

i. Resalte alguna parte de un texto, en este caso su código de invitación en un correo electrónico. Para ello, mantenga presionado el botón derecho del mouse o la tecla Shift.
ii. Presione ***Ctrl+C*** en su teclado (tenga en cuenta que en este punto no habrá evidencia visible de que el texto se ha copiado con éxito).
iii. Desplácese a la ubicación que desee, en este caso el cuadro de diálogo **Unirse a Red de Zen**, y haga clic en el cuadro de texto en el que desea pegar el texto.
iv. Presione ***Ctrl+V***.
v. Aparece el texto pegado, en este caso su código de invitación. Listo.

5. Haga clic en el botón **Conectar**. Luego de un momento, será parte de la Zen red que eligió. Para usted personalmente, en realidad nada cambia (sólo el texto en su botón Estado cambiará a ***Conectado***). Sin embargo, a partir de este momento el administrador de red controlará su dispositivo, lo que le permite identificar posibles problemas y ayudarlo a solucionarlos. Aún así, si desea dejar esta red, puede hacerlo fácilmente en cualquier momento.

Dispositivos móviles Android:

A diferencia de los dispositivos de escritorio, la conexión de red en los dispositivos móviles Android se realiza directamente dentro de la misma aplicación:

1. En primer lugar, debe tener una de las aplicaciones móviles AVG instaladas y conectadas a alguna Zen red (haga clic aquí para aprender más sobre su conexión móvil Android™ a una Zen red existente). De hecho, aceptar una invitación a un dispositivo móvil implica que sale de la red Zen actual y cambia a una nueva.

2. Abra su aplicación y presione el ***icono de menú*** (de hecho, el logotipo de la aplicación) ubicado en el ángulo superior izquierdo de la pantalla principal.

3. Una vez que se muestra el menú, presione la opción **Administrar dispositivos**.

4. Presione la opción **Unirse a otra Zen red** ubicada al fondo de la pantalla, y luego indique el código de invitación que le fue enviado previamente por este administrador de red; finalmente, presione **Unirse**.

5. ¡Felicitaciones! Ahora es parte de Zen la red. No obstante, si alguna vez cambia de opinión, puede abandonarla en cualquier momento.

Dispositivos Mac:

A diferencia de los dispositivos de escritorio, la conexión de red en los dispositivos Mac se realiza directamente dentro de la misma aplicación:

1. En primer lugar, debe tener una de las aplicaciones AVG para Mac instalada e incluso quizá conectada a alguna Zen red (haga clic aquí para aprender más sobre su conexión Mac a una Zen red existente). Si está conectado, haga clic en el botón en la esquina superior derecha de la pantalla de la aplicación (que actualmente dice "Conectado") y elija **Salir de esta red** en el menú desplegable.

2. El botón en la esquina superior derecha de la pantalla de la aplicación ahora dice "No conectado". Haga clic allí y elija la opción **Conectar** en el menú desplegable.

3. En el cuadro de diálogo que se abre, haga clic en la opción **Usar un código de invitación** ubicada bien a la derecha.

4. Aparece un cuadro de texto que le permite introducir el código de invitación enviado previamente por el administrador de la red. Tras introducir el código, haga clic en el botón **Conectar**.

5. ¡Felicitaciones! Ahora es parte de Zen la red. No obstante, si alguna vez cambia de opinión, puede abandonarla en cualquier momento.

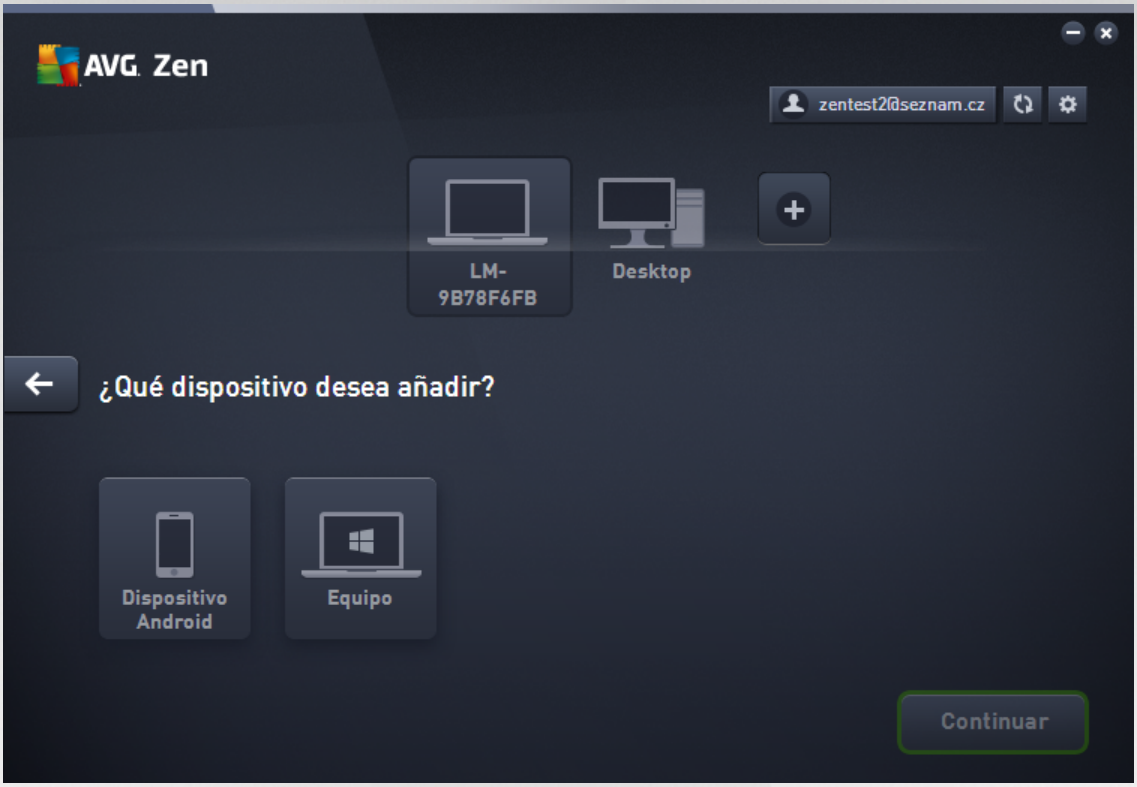
2.3.2. ¿Cómo añadir dispositivos a su red?

1. Para añadir un nuevo dispositivo a su Zen red, primero debe enviar una invitación. Para ello, haga clic en el  botón en el lado derecho de la cinta de opciones Dispositivos.

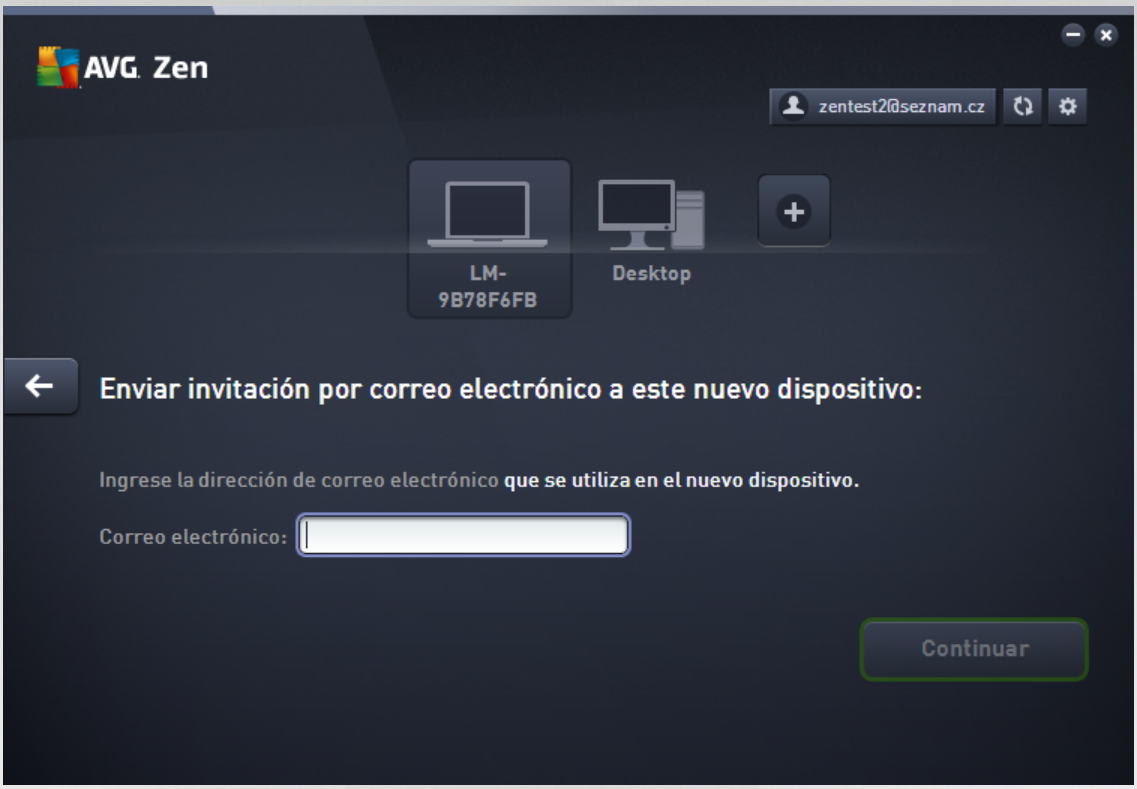
Observe que únicamente los administradores pueden enviar invitaciones y dispositivos a sus redes. Por lo tanto, si no está conectado actualmente a ninguna red de Zen, hágalo o cree una usted mismo.

2. Se abre un nuevo cuadro de diálogo. Elija el tipo de dispositivo que desea añadir (es decir, equipo o móvil

Android™) resaltando el icono adecuado y haga clic en el botón **Continuar**.



3. Aparece otro cuadro de diálogo. Introduzca el correo electrónico que se usa en el nuevo dispositivo y haga clic en el botón **Continuar**.



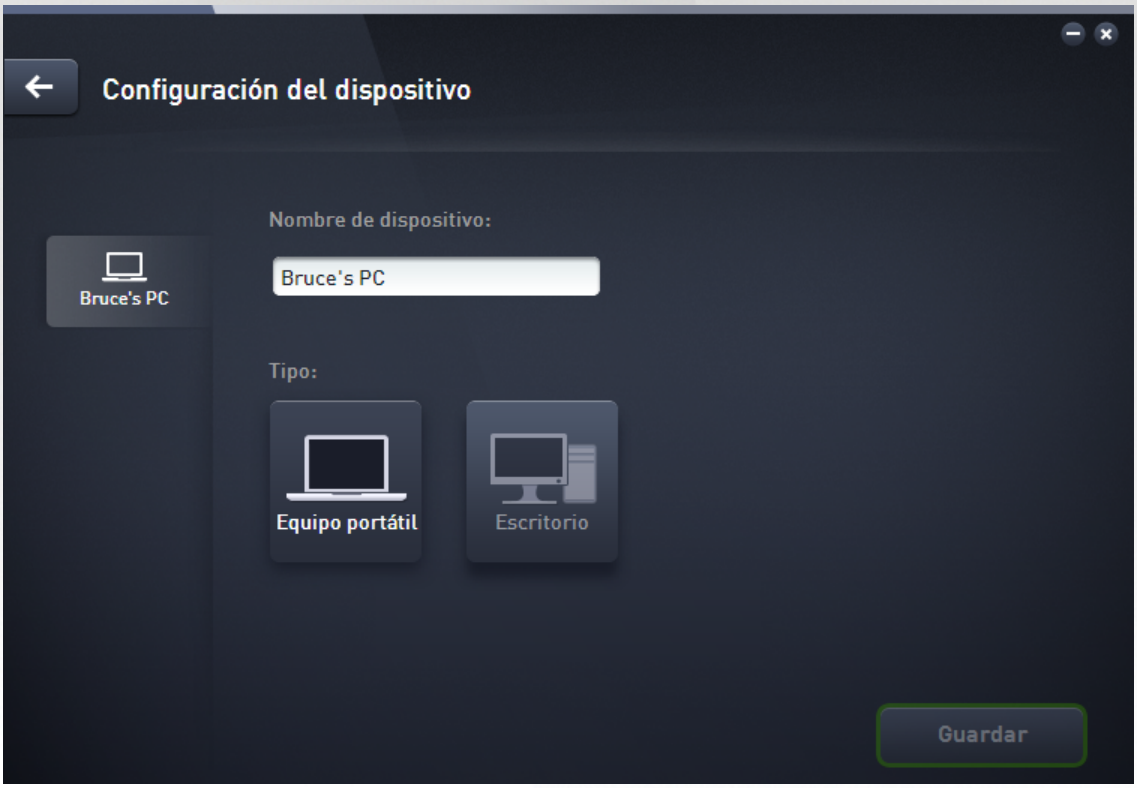
4. Se envía la invitación por correo electrónico. El dispositivo aparece ahora en la cinta de opciones Dispositivos como pendiente. Esto implica que su invitación está esperando aceptación.

Mientras su invitación permanece en estado pendiente, puede elegir **Reenviar el vínculo de invitación**, o **Cancelar la invitación** totalmente.

5. Inmediatamente después de aceptada su invitación, puede modificar el nombre y el tipo del dispositivo que se acaba de añadir (aunque, también se puede hacer más adelante). Ahora, el dispositivo forma parte de su Zen red y puede visualizar de forma remota productos AVG instalados en él. ¡Felicitaciones, se ha convertido en un verdadero Zen administrador!

2.3.3. ¿Cómo modificar el nombre o tipo de dispositivo?

1. Haga clic en el botón Configuraciones, luego seleccione ***Configuración de dispositivos*** en el cuadro de diálogo emergente.



2. Las configuraciones que se aplican a su dispositivo actualmente seleccionado. Se muestra una lista de dispositivos actualmente disponibles en su red (es decir, aquellos que han aceptado invitaciones) en una columna de iconos del lado izquierdo del cuadro de diálogo Configuración de Dispositivos. Simplemente haga clic en los iconos individuales para cambiar de uno a otro.

3. El cuadro de diálogo ***Nombre del Dispositivo*** muestra el nombre de su dispositivo actualmente seleccionado. Puede borrarlo y reemplazarlo con cualquier nombre que desee.

4. A continuación, puede establecer el ***Tipo*** de su dispositivo actualmente seleccionado (Teléfono, Tablet, Equipo portátil o Escritorio). Simplemente haga clic en un icono adecuado.

5. Haga clic en el botón **Guardar** para confirmar los cambios.

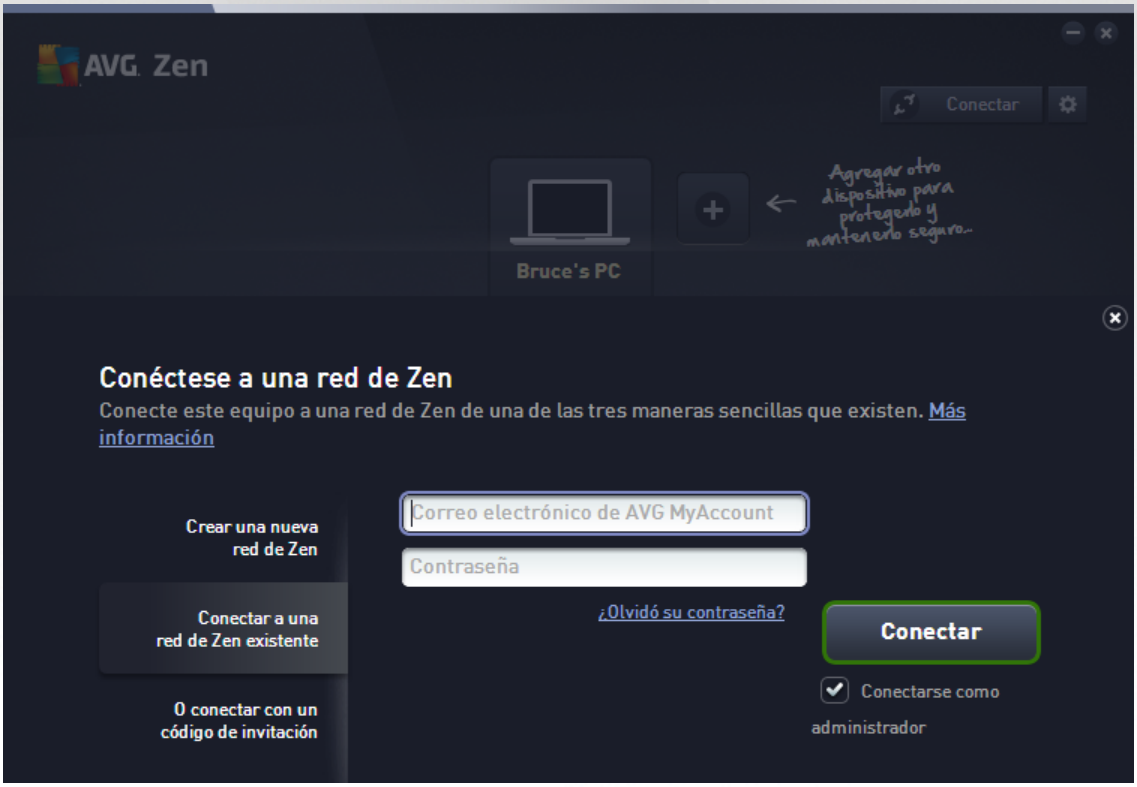
2.3.4. ¿Cómo conectarse a una red de Zen existente?

Dispositivos de escritorio:

1. Si no está conectado actualmente a ninguna AVG MyAccount, haga clic en el botón Estado (con el texto que dice ***Conectar***) y confirme haciendo clic en el botón **Continuar** en el pequeño cuadro de diálogo emergente.

Si ya está conectado a alguna AVG MyAccount, primero debe cerrar sesión para poder conectarse a una diferente. Haga clic en el botón Estado (con su nombre actual de AVG MyAccount en él) y confirme haciendo clic en el botón **Cerrar Sesión** en el pequeño cuadro de diálogo emergente.

2. Seleccione el panel ***Conectar a una red Zen existente*** que se encuentra del lado izquierdo del subdiálogo que se acaba de abrir.



3. Introduzca su nombre de usuario y contraseña de AVG MyAccount. Si todavía no tiene su propia AVG MyAccount, simplemente cree una nueva. Si desea iniciar sesión como administrador para poder ver productos AVG en dispositivos remotos en esta Zen red, conserve la marca de verificación en el cuadro ***Conectarse como administrador***. De no ser así, actuará únicamente como usuario conectado.

Si olvidó su contraseña, haga clic en el vínculo ***¿Olvidó su contraseña?*** (bajo el cuadro de texto de contraseña). Esto lo redireccionará a la página web, lo que le permite recuperar su contraseña olvidada.

4. Haga clic en el botón **Conectar**. El proceso de conexión debería realizarse en unos pocos segundos. Luego de una conexión correcta, debe ver su nombre de MyAccount en el botón Estado.

Dispositivos móviles Android:

A diferencia de los dispositivos de escritorio, la conexión de red en los dispositivos móviles Android se realiza directamente dentro de la misma aplicación:

1. Si desea conectar su dispositivo móvil Android a la Zen red, debe descargar una de las aplicaciones móviles AVG (esto es, AVG AntiVirus, AVG Cleaner o AVG PrivacyFix). Esto puede realizarse fácilmente en Google Play, desde donde todas estas aplicaciones pueden descargarse e instalarse gratuitamente. Para que la conexión funcione adecuadamente, asegúrese de que utiliza la última versión disponible.

2. Después de que la aplicación AVG se haya instalado, ábrala y presione el ***icono de menú*** (de hecho, el logotipo de la aplicación) ubicado en el ángulo superior izquierdo de la pantalla principal.

3. Una vez que se muestra el menú, presione la opción **Administrar dispositivos**.

4. Aquí, presione la pestaña **Inicio de sesión** e indique las credenciales adecuadas de AVG MyAccount (esto es, su ***nombre de usuario*** y ***contraseña***).

5. ¡Felicitaciones! Ahora es parte de Zen la red. Después de hacer clic en el icono de menú, debería ver ahora el texto ***Está conectado como:*** junto con su nombre actual de AVG MyAccount en la parte superior del menú. No obstante, si alguna vez cambia de opinión, puede abandonarla en cualquier momento.

Dispositivos Mac:

A diferencia de los dispositivos de escritorio, la conexión de red en los dispositivos Mac se realiza directamente dentro de la misma aplicación:

1. Si desea conectar su dispositivo Mac a la Zen red, debe descargar una de las aplicaciones AVG para Mac (esto es, AVG AntiVirus o AVG Cleaner). Esto puede realizarse fácilmente en el Centro de descargas de AVG o en Mac App Store, desde donde todas estas aplicaciones pueden descargarse e instalarse gratuitamente. Para que la conexión funcione adecuadamente, asegúrese de que utiliza la última versión disponible.

2. Tras haber instalado la aplicación AVG, ábrala. Verá un botón rectangular en la esquina superior derecha de la pantalla de la aplicación (indicando ahora "No conectado"). Haga clic allí y elija la opción **Conectar** en el menú desplegable.

3. En el cuadro de diálogo recién abierto, haga clic en la opción del medio **Iniciar sesión en AVG MyAccount** (ya debería estar seleccionada por defecto).

4. Introduzca las credenciales de AVG MyAccount correspondientes, esto es, su ***nombre de usuario*** (correo electrónico de MyAccount) y ***contraseña***.

5. ¡Felicitaciones! Ahora es parte de Zen la red. El botón en la esquina superior derecha ahora dice "Conectado"; si hace clic allí, podrá ver a qué red está conectado actualmente. No obstante, si alguna vez cambia de opinión, puede abandonarla en cualquier momento.

2.3.5. ¿Cómo crear una nueva red de Zen?

Para crear (y administrar) una nueva red de Zen, primero tiene que crear su AVG MyAccount personal. Básicamente, existen dos maneras de hacerlo: utilizando su navegador web o directamente desde la misma aplicación AVG Zen.

Desde el navegador:

1. Use su navegador para abrir el sitio web https://myaccount.avg.com/.

2. Haga clic en el botón **Crear AVG MyAccount**.

3. Indique su correo electrónico de inicio de sesión, establezca su contraseña, vuelva a escribirla y haga clic en el botón **Crear cuenta**.

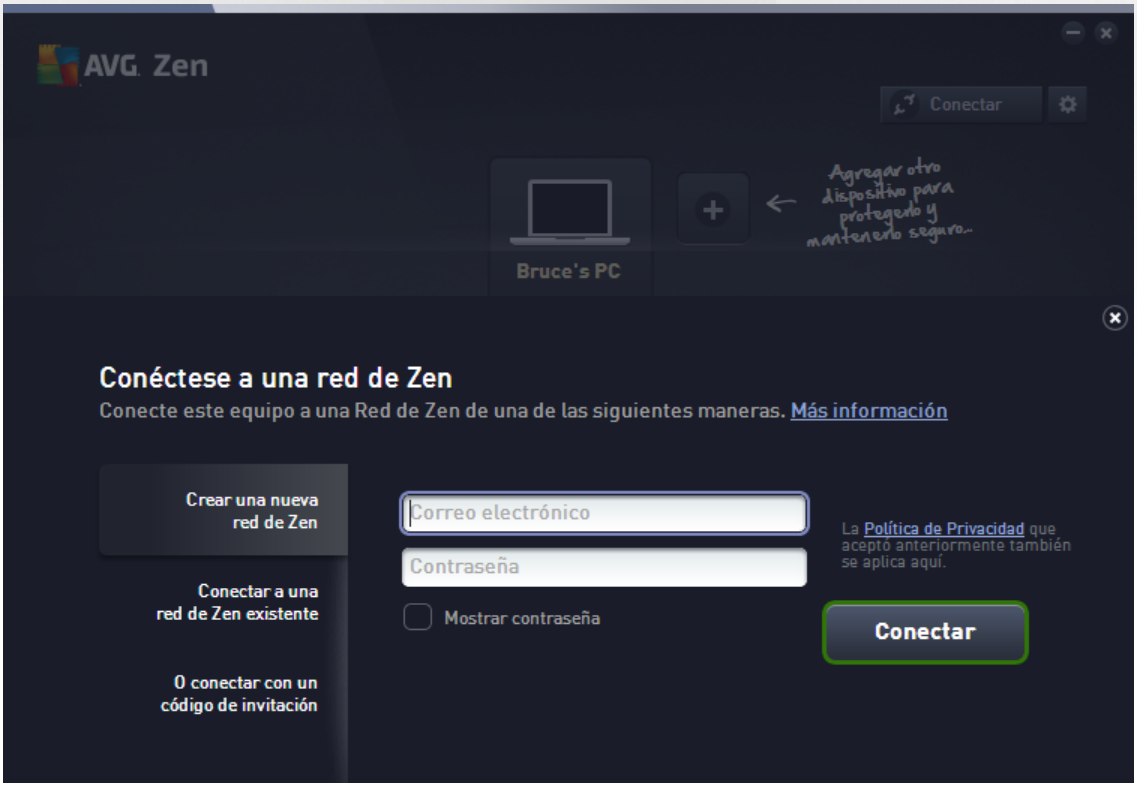
4. Se le enviará un vínculo para activar su AVG MyAccount (a la dirección de correo electrónico que utilizó en el paso 3). Debe hacer clic en este vínculo para finalizar la creación de su MyAccount. Si no ve este correo electrónico en su bandeja de entrada, quizá lo haya recibido en la carpeta de correo no deseado.

Desde AVG Zen:

1. Si no está conectado actualmente a ninguna AVG MyAccount, haga clic en el botón Estado (con el texto que dice ***Conectar***) y confirme haciendo clic en el botón **Continuar** en el pequeño cuadro de diálogo emergente.

Si ya está conectado a alguna AVG MyAccount, primero debe cerrar sesión para poder conectarse a una diferente. Haga clic en el botón Estado (con su nombre actual de AVG MyAccount en él) y confirme haciendo clic en el botón **Cerrar sesión** en el pequeño cuadro de diálogo emergente.

2. Asegúrese de que el panel ***Crear una nueva Zen red*** en el lado izquierdo del subdiálogo que se acaba de abrir esté seleccionado.



3. Indique su correo electrónico de inicio de sesión y establezca su contraseña (marque el cuadro ***Mostrar contraseña*** debajo si desea ver los caracteres ocultos), luego haga clic en el botón **Conectar**.

4. Luego de unos segundos, estará conectado a la red recién creada con derechos de administrador. Esto implica que puede añadir dispositivos a su red, ver de forma remota productos AVG instalados en ellos y, de ser necesario, eliminarlos de su red.

2.3.6. ¿Cómo instalar productos AVG?

1. Los productos AVG se pueden instalar fácilmente a través de Zen. Para ello, haga clic en un icono Categoría que elija (el icono será gris, lo que indica que todavía no tiene producto en esta categoría, o quizás será la mitad verde, lo que significa que ya tiene un producto en esta categoría, pero que falta instalar otro producto).

2. Si desea iniciar la instalación del producto de inmediato, sólo debe hacer clic en el botón **Adquiéralo de forma GRATUITA**. El producto se instalará automáticamente con la configuración predeterminada.

   Si desea controlar el proceso de instalación, haga clic en el botón con flecha pequeña (a la derecha del botón **Adquiéralo de forma GRATUITA**) y haga clic en **Instalación personalizada**. De esta forma, visualizará la instalación como una serie de cuadros de diálogo, lo que le permite modificar la carpeta de destino, los componentes instalados, etc.

Los procesos de instalación de varios productos AVG se describen en detalle en la otra parte de esta documentación, o también en guías de usuario específicas. Tales guías pueden descargarse fácilmente desde el sitio web de AVG..

3. A medida que avanza la instalación, debe ver que aparece el círculo verde dentro del icono Categoría

seleccionado. Luego de la correcta instalación, se completa el círculo verde dentro del icono (en algunas categorías puede ser simplemente un semicírculo, lo que indica que hay otros productos dentro de esta categoría que se pueden instalar). Observe que el círculo (o semicírculo) puede cambiar de color (amarillo o rojo) inmediatamente después de la instalación. Esto significa que hay algunos problemas dentro del producto que requieren su atención.

4. Recibirá un mensaje de confirmación (que aparecerá justo debajo de los iconos Categoría) que indica que la instalación ha finalizado correctamente.

2.3.7. ¿Cómo dejar una red?

Dispositivos de escritorio:

1. Si forma parte de alguna Zen red y desea dejarla, es muy fácil hacerlo. En primer lugar, haga clic en el botón Estado (con el texto que dice ***Conectado***) y haga clic en el botón **Dejar Esta Red** en el pequeño cuadro de diálogo emergente para continuar.

2. Ahora tiene que confirmar que realmente desea dejar la Zen red. Para ello, haga clic en el botón **Dejar**.

3. Luego de unos segundos, estará desconectado permanentemente. Su administrador de red anterior ya no podrá administrar productos AVG en su equipo. El texto en su botón Estado cambiará a ***Conectar*** (es decir, a su estado inicial).

Dispositivos móviles Android:

A diferencia de los dispositivos de escritorio, la conexión de red en los dispositivos móviles Android se realiza directamente dentro de la misma aplicación:

1. Abra su aplicación AVG y presione el ***icono de menú*** (de hecho, el logotipo de la aplicación) ubicado en el ángulo superior izquierdo de la pantalla principal.

2. En la parte superior del menú, debería ver el texto ***Está conectado como:*** junto con su actual nombre de AVG MyAccount. Al lado hay un pequeño icono en forma de puerta con una flecha señalando hacia la derecha. Haga clic en él.

3. Confirme que realmente desea salir de la Zen red haciendo clic en el botón **Aceptar**.

4. Luego de unos segundos, estará desconectado permanentemente. Su administrador de red anterior ya no podrá administrar productos AVG en su móvil Android™. No obstante, puede conectarse fácilmente a esta (o a cualquier otra) Zen red de nuevo, ya sea directamente o aceptando una invitación.

Dispositivos Mac:

A diferencia de los dispositivos de escritorio, la conexión de red en los dispositivos Mac se realiza directamente dentro de la misma aplicación:

1. Abra la aplicación AVG y haga clic en un botón rectangular en la esquina superior derecha de la pantalla de la aplicación (que ahora indica "Conectado").

2. En la parte superior del menú desplegable, debería ver el texto ***Está conectado a la siguiente red de Zen:*** junto con su actual nombre de AVG MyAccount.

3. Justo debajo de Zen la información de la red hay una opción para **Salir de esta red**. Haga clic en ella.

4. Luego de unos segundos, estará desconectado permanentemente. Su administrador de red anterior ya no podrá administrar productos AVG en su dispositivo Mac. No obstante, puede conectarse fácilmente a esta (o a cualquier otra) Zen red de nuevo, ya sea directamente o aceptando una invitación.

2.3.8. ¿Cómo quitar dispositivos de su red?

1. Si desea que algún dispositivo ya no forme parte de su Zen red, puede eliminarlo fácilmente. Haga clic en el botón Configuraciones, luego seleccione ***Configuración de dispositivos*** en el cuadro de diálogo emergente.

2. En el lado izquierdo del cuadro de diálogo Configuración de dispositivos, hay una lista de dispositivos disponibles actualmente en su red que aparecen en una columna de iconos. Cambie al dispositivo que desea eliminar haciendo clic en el icono con su nombre.

3. Verá el vínculo ***Eliminar de red*** junto al borde inferior del cuadro de diálogo. Haga clic en él.

Observe que no existe este vínculo en configuraciones para el dispositivo que está actualmente en uso. Este dispositivo se considera el núcleo de su red y, por lo tanto, no se puede eliminar.

4. Ahora tiene que confirmar que realmente desea eliminar este dispositivo de la Zen red. Para ello, haga clic en el botón **Eliminar**.

5. El dispositivo quedará eliminado de forma permanente luego de unos segundos. Ya no podrá administrar productos AVG en él. El dispositivo eliminado también desaparecerá de la cinta de opciones Dispositivos en su Interfaz del Usuario.

2.3.9. ¿Cómo ver o administrar productos AVG?

Si desea visualizar y administrar su propio dispositivo

De hecho, sólo debe hacer clic en un icono Categoría adecuado. Esto abre la interfaz del usuario del producto AVG, lo que le permite explorar y configurar todo lo que desee. Por ejemplo, si hace clic en el icono ***PROTECCIÓN***, se abre la interfaz del usuario de AVG Internet Security, etc. Si una categoría consta de más de un producto, deberá hacer clic en su icono y luego seleccionar un subicono adecuado (como AVG PrivacyFix en la categoría ***PRIVACIDAD E IDENTIDAD***).

Los productos AVG que pueden verse y administrarse mediante Zen se describen en detalle en la otra parte de esta documentación, o también en guías de usuario específicas. No dude en descargar estos manuales desde el sitio web de AVG..

Si existen algunos problemas urgentes que requieren su atención, también puede hacer clic en el botón Mensajes. El cuadro de diálogo que acaba de abrir contiene una lista de problemas y dificultades. Algunos pueden incluso manejarse directamente desde este cuadro de diálogo. Estos problemas aparecen con un botón de acción especial junto a ellos.

Si desea visualizar y administrar un dispositivo remoto (administradores únicamente)

Esto es bastante fácil. Elija el dispositivo que desea ver desde la cinta de opciones Dispositivos y haga clic en un icono Categoría adecuado. A continuación, se abre un nuevo cuadro de diálogo que contiene un breve resumen de los estados de los productos AVG en esta categoría.

Como administrador, puede utilizar varios botones para realizar varias acciones remotas en productos AVG de su red de Zen. Las acciones disponibles dependen del tipo de dispositivo (equipo de escritorio, Android o Mac) y el icono de Categoría que esté viendo actualmente. Recuerde que es posible que no se pueda acceder a algunas acciones (como analizar o actualizar) si ya fueron realizadas recientemente. En la siguiente lista se encuentran todas las acciones remotas disponibles para los productos AVG:

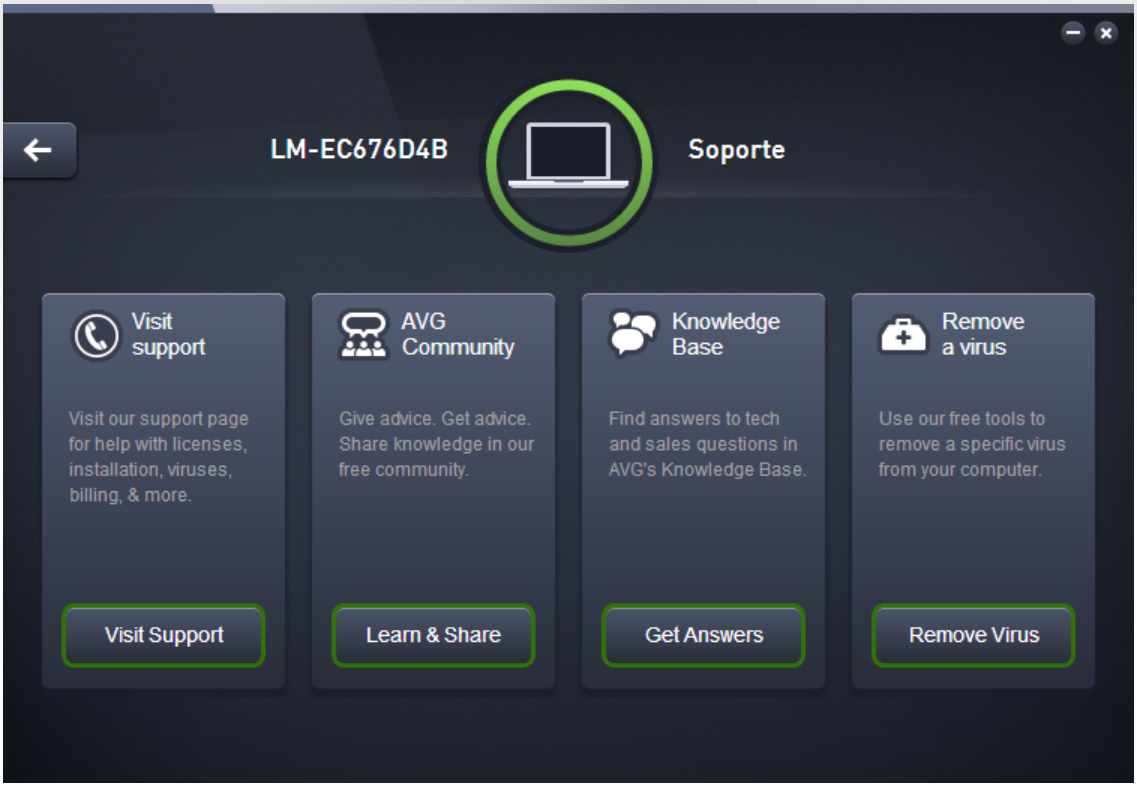
TIPO DE DISPOSITIVO	ICONO DE CATEGORÍA	ACCIONES REMOTAS DISPONIBLES
Equipo	***PROTECCIÓN (AVG Internet Security)***	• Botón **Analizar ahora**: al hacer clic sobre él se inicia de inmediato el análisis, que comprueba que no haya virus ni otro software dañino en el dispositivo remoto. Luego de la finalización del análisis, se le informarán los resultados de inmediato. Haga clic aquí para obtener más información sobre los análisis de AVG Internet Security. • Botón **Actualizar**: al hacer clic sobre él se inicia el proceso de actualización de AVG Internet Security en el dispositivo remoto. Todas las aplicaciones antivirus deben estar siempre actualizadas para garantizar el nivel máximo de protección. Haga clic aquí para obtener más información sobre la importancia de las actualizaciones de AVG Internet Security.

TIPO DE DISPOSITIVO	ICONO DE CATEGORÍA	ACCIONES REMOTAS DISPONIBLES
		• Botón **Mostrar detalles**: este botón sólo está disponible si existen problemas urgentes que requieren de su atención. Al hacer clic sobre él se abrirá el cuadro de diálogo Mensajes para el dispositivo actualmente seleccionado. Este cuadro de diálogo muestra la lista de problemas ordenados por categoría de producto. Algunos pueden resolverse de inmediato al hacer clic en el botón **Reparar ahora**. En AVG Internet Security, puede, por ejemplo, activar componentes de protección previamente desactivados.
Equipo	***RENDIMIENTO (AVG PC TuneUp)***	• Botón **Ejecutar mantenimiento**: al hacer clic sobre él comienza el mantenimiento del sistema, un conjunto de varias tareas destinadas a limpiar el sistema en el dispositivo remoto, aumentar su velocidad y optimizar su rendimiento. • Botón **Actualizar**: al hacer clic sobre él se inicia el proceso de actualización de AVG PC TuneUp en el dispositivo remoto. Es muy importante mantener AVG PC TuneUp actualizado, ya que sus funciones individuales se expanden o adaptan continuamente para que se ajuste a la última tecnología y se reparen los errores. • Botón **Mostrar detalles**: este botón sólo está disponible si existe algún problema urgente que requiere su atención. Al hacer clic sobre él se abrirá el cuadro de diálogo Mensajes para el dispositivo actualmente seleccionado. Este cuadro de diálogo muestra la lista de problemas ordenados por categoría de producto. Algunos pueden resolverse de inmediato al hacer clic en el botón **Reparar ahora**.
Android	***PROTECCIÓN (AVG AntiVirus)***	• Botón **Analizar ahora**: al hacer clic sobre él se inicia de inmediato el análisis, que comprueba que no haya virus ni otro contenido dañino en el dispositivo Android remoto. Luego de la finalización del análisis, se le informarán los resultados de inmediato. • Botón **Actualizar**: al hacer clic sobre él se inicia el proceso de actualización de AVG AntiVirus en el dispositivo Android remoto. Todas las aplicaciones antivirus deben estar siempre actualizadas para garantizar el nivel máximo de protección. • Botón **Mostrar detalles**: este botón sólo está disponible si existe algún problema urgente que requiere su atención. Al hacer clic sobre él se abrirá el cuadro de diálogo Mensajes para el dispositivo actualmente seleccionado. Este cuadro de diálogo muestra la lista de problemas ordenados por categoría de producto. No obstante, para AVG AntiVirus para Android, este diálogo es puramente informativo y no se puede modificar nada.

TIPO DE DISPOSITIVO	ICONO DE CATEGORÍA	ACCIONES REMOTAS DISPONIBLES
Mac	***PROTECCIÓN (AVG AntiVirus)***	• Botón **Actualizar**: al hacer clic sobre él se inicia el proceso de actualización de AVG AntiVirus en el dispositivo Mac remoto. Todas las aplicaciones antivirus deben estar siempre actualizadas para garantizar el nivel máximo de protección. • Botón **Mostrar detalles**: este botón sólo está disponible si existe algún problema urgente que requiere su atención. Al hacer clic sobre él se abrirá el cuadro de diálogo Mensajes para el dispositivo actualmente seleccionado. Este cuadro de diálogo muestra la lista de problemas ordenados por categoría de producto. Para AVG AntiVirus para Mac, puede utilizar el botón **Reparar ahora** para activar la protección en tiempo real previamente desactivada.

2.4. Preguntas Frecuentes y Soporte

El soporte para usuarios de AVG Zen es fácilmente accesible en cualquier momento mediante el icono de categoría ***SOPORTE***.



El nuevo cuadro de diálogo que se abre contiene vínculos a los recursos de soporte más comunes.

NOMBRE DE CATEGORÍA	TEXTO DE BOTÓN	DESCRIPCIÓN
Asistencia técnica	***Asistencia Técnica***	Esta página le da acceso a soporte profesional a usuarios de AVG. Puede hacer preguntas respecto a licencias, instalación, virus y funciones de productos específicos.
Comunidad AVG	***Aprenda y Comparta***	Comunidad AVG es una excelente manera de obtener consejos de otros usuarios de AVG (y también de ofrecer consejos usted mismo). No dude en compartir su conocimiento en esta comunidad de clientes de AVG.
Base de Conocimientos	***Obtener Respuestas***	Algunas preguntas sobre productos AVG son más frecuentes que otras. En esta página, encontrará respuestas a las preguntas más comunes. No dude en probar; quizás, la solución a su problema lo está esperando justo aquí.
Eliminar un virus	***Eliminar virus***	AVG ofrece una cantidad de herramientas de software gratuitas para eliminar un virus específico de su equipo. Puede descargarlas desde esta página.

3. AVG Internet Security

Este manual de usuario proporciona documentación completa para el usuario relacionada con **AVG Internet Security 2015**.

No obstante, también puede optar por utilizar otras fuentes de información:

- ***Archivo de ayuda***: Está disponible una sección de *Resolución de Problemas* incluida directamente en el archivo de ayuda **AVG Internet Security 2015** *(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 las FAQ. Se puede obtener acceso a esta sección por medio de la opción de menú ***Centro de Soporte / Preguntas Frecuentes y Tutoriales***. Una vez más, todas las preguntas están divididas de forma bien organizada en las categorías de ventas, técnicas y sobre virus.

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

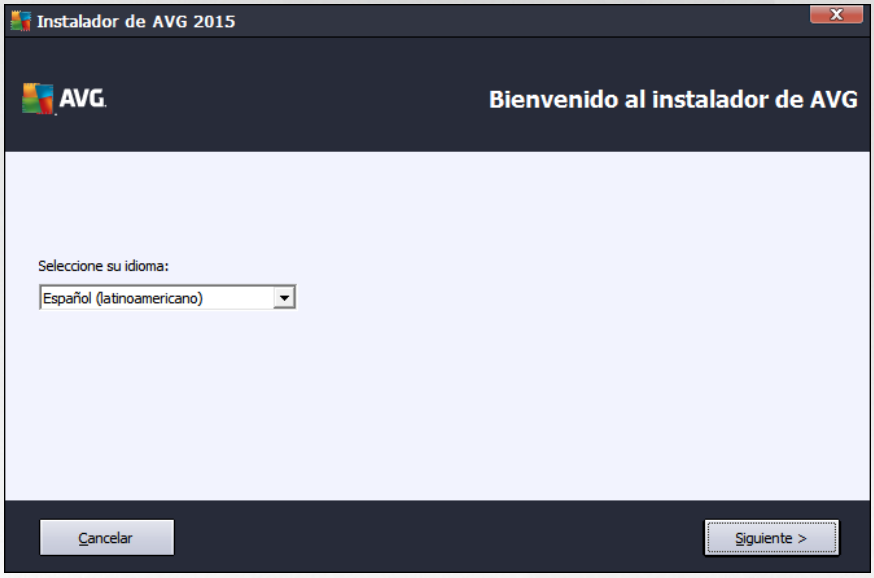
- ***Foro de discusión***: también puede utilizar el foro de discusión de usuarios de AVG en http://forums.avg.com.

3.1. Proceso de instalación de AVG

Para instalar **AVG Internet Security 2015** en su equipo debe obtener el archivo de instalación más reciente. Para asegurarse de instalar la versión actualizada de **AVG Internet Security 2015**, se recomienda que descargue el archivo de instalación del sitio web de AVG (http://www.avg.com/). La sección ***Soporte*** proporciona una descripción general estructurada de los archivos de instalación para cada edición de AVG. Una vez que ha descargado y guardado el archivo de instalación en el disco duro, puede iniciar el proceso de instalación. La instalación es una secuencia de cuadros de diálogo sencillos y fáciles de entender. Cada cuadro de diálogo describe brevemente qué se debe hacer en cada paso del proceso de instalación. Ofrecemos una explicación detallada de cada ventana de diálogo a continuación:

3.1.1. Bienvenido: Selección de idioma

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

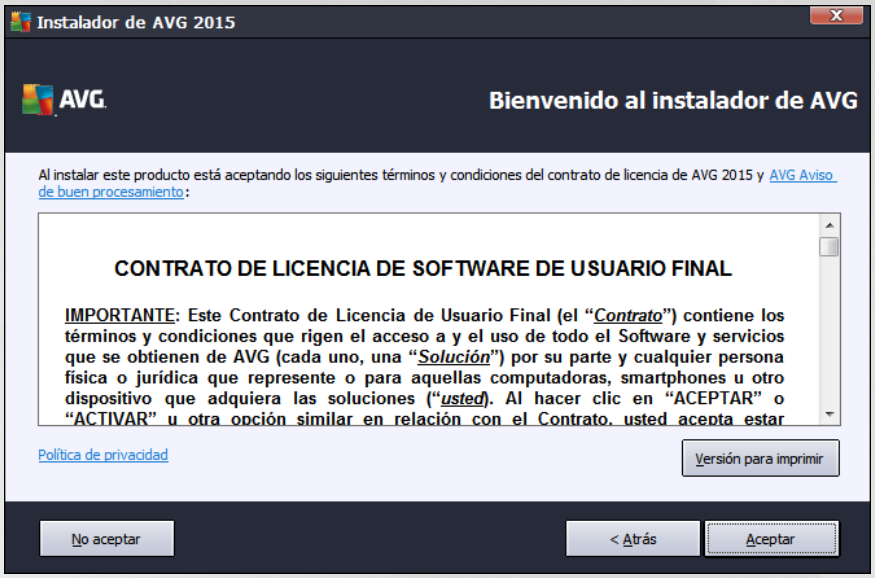


En este cuadro de diálogo puede seleccionar el idioma que se utilizará para el proceso de instalación. Haga clic en el cuadro combinado para desplegar el menú de idiomas. Seleccione el idioma que desee y el proceso de instalación seguirá en el idioma elegido.

Atención: en este momento sólo selecciona el idioma del proceso de instalación. La aplicación AVG Internet Security 2015 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 Internet Security 2015 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.

3.1.2. 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 acepto*** y el proceso de instalación se terminará de inmediato.

Aviso de Correcto Procesamiento y 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 Correcto Procesamiento de AVG*** y la ***Política de Privacidad de AVG***. Las funciones mencionadas se visualizan en el cuadro de diálogo en forma de un hipervínculo activo que lo lleva al sitio web correspondiente, en el que 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.

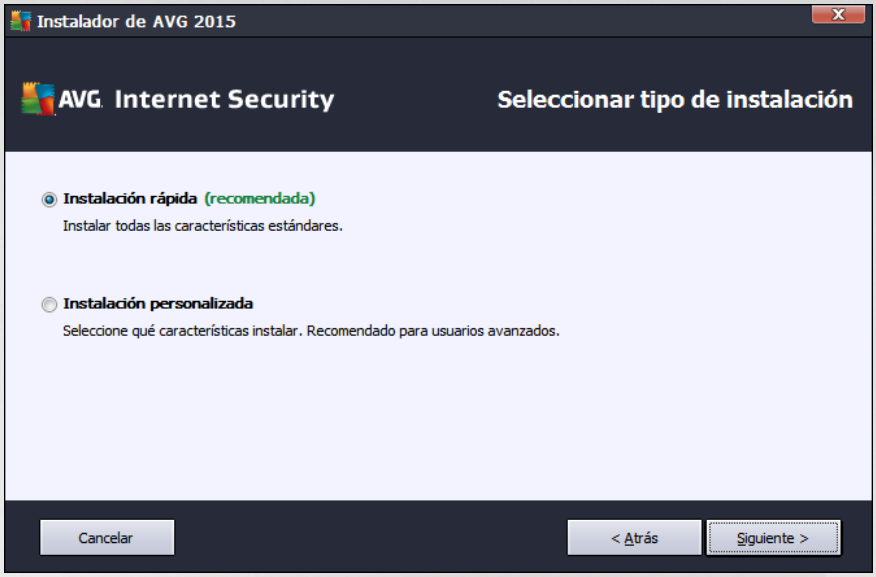
Botones de control

En el primer cuadro de diálogo de configuración, los siguientes botones de control están 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 Internet Security 2015** 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.

3.1.3. Seleccionar el tipo de instalación

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



Instalación rápida

Para la mayoría de los usuarios, se recomienda especialmente que conserve la instalación ***Express*** estándar. De esta forma instalará **AVG Internet Security 2015** en el modo completamente automático con configuración predefinida por el proveedor del programa. Esta configuración proporciona la máxima seguridad combinada con el uso óptimo de los recursos. En el futuro, si es necesario cambiar la configuración, siempre se puede hacer directamente en la aplicación **AVG Internet Security 2015**.

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 Internet Security 2015** con una configuración distinta de la estándar (por ejemplo, para ajustarse a necesidades específicas del sistema). Si elige esta alternativa, una opción nueva llamada ***Carpeta de destino*** se activará en el cuadro de diálogo. Ahora especifique la ubicación donde **AVG Internet Security 2015** debe instalarse. De forma predeterminada, **AVG Internet Security 2015** 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 Internet Security**

2015 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.

3.1.4. 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 Internet Security 2015** 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***.

En este paso, también puede decidir instalar otras variantes de idioma del producto *(por defecto, la aplicación se instala con el idioma que seleccionó como idioma de comunicación de la instalación y en inglés)*.

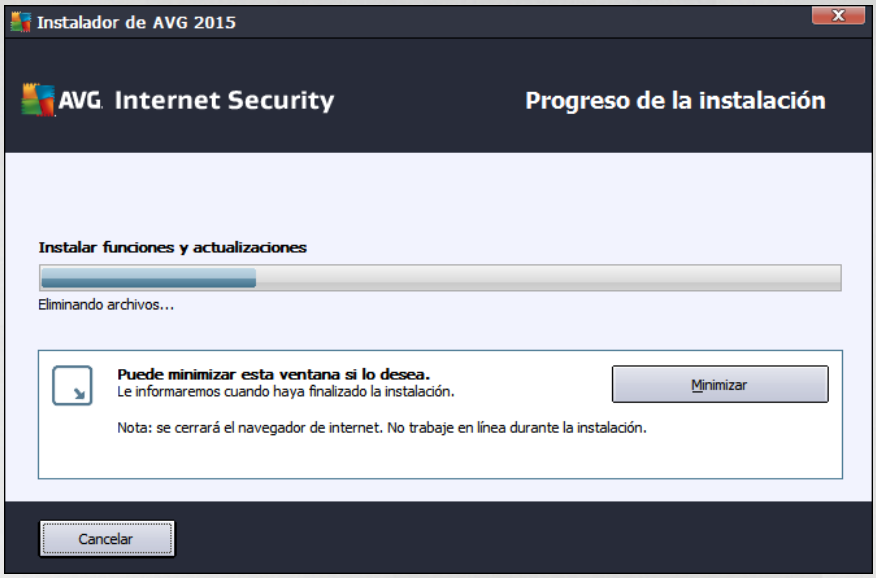
Botones de control

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 Internet Security 2015** 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.

3.1.5. 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.

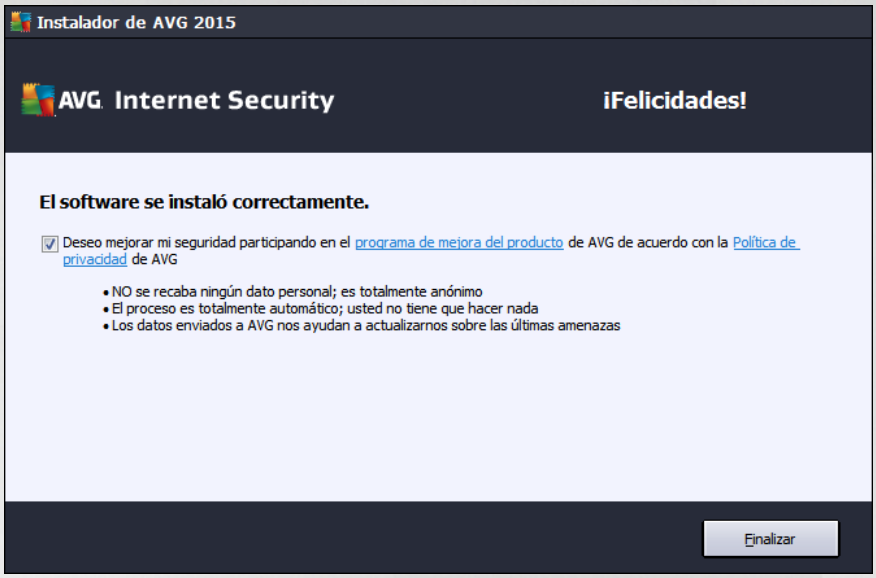
Botones de control

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 sólo debe usarse si desea interrumpir el proceso de instalación actual. Tenga en cuenta que, en un caso así, **AVG Internet Security 2015** no se instalará.

3.1.6. ¡Felicidades!

El cuadro de diálogo ***Felicitaciones*** confirma que **AVG Internet Security 2015** 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***.

3.2. Después de la instalación

3.2.1. Registro del producto

Una vez finalizada la instalación de **AVG Internet Security 2015**, 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 Internet Security 2015**. 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.

3.2.2. 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 2015***

3.2.3. Análisis de todo el equipo

Existe el riesgo potencial de que un virus informático se transmitiera a su equipo antes de la instalación de **AVG Internet Security 2015**. 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.

3.2.4. Análisis Eicar

Para confirmar que **AVG Internet Security 2015** 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 Internet Security 2015** 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.

3.2.5. Configuración predeterminada de AVG

La configuración predeterminada (*por ejemplo, la configuración de la aplicación inmediatamente después de la instalación*) de **AVG Internet Security 2015** está definida por el proveedor de software para que todos los componentes y funciones proporcionen un rendimiento óptimo. ***No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración.*** Si desea cambiar la configuración de AVG para que se adapte mejor a sus necesidades, vaya a Configuración avanzada de AVG: seleccione el elemento del menú principal del sistema *Opciones/Configuración avanzada* y modifique la configuración de AVG en el cuadro de diálogo Configuración avanzada de AVG que aparece.

3.3. Interfaz del usuario de AVG

AVG Internet Security 2015 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 Internet Security 2015**. 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 >>
- ***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 Internet Security 2015**, hay un elemento 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 Internet Security 2015**. Detalles >>

3.3.1. Navegación superior

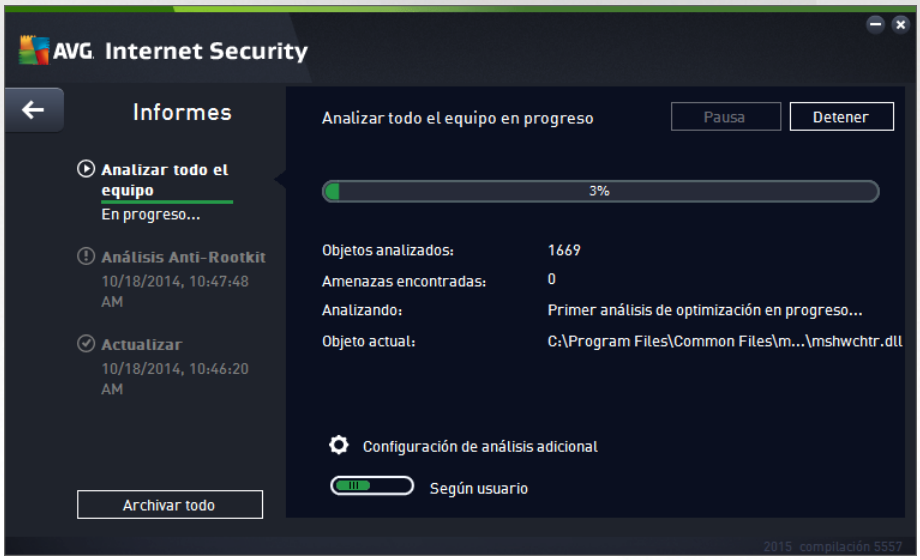
La ***navegación superior*** comprende varios vínculos activos alineados en la sección superior de la ventana principal. La navegación incluye los siguientes botones:

3.3.1.1. Únase a nosotros en Facebook

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.

3.3.1.2. 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:



3.3.1.3. Soporte

Abre un nuevo cuadro de diálogo estructurado en cuatro pestañas donde podrá encontrar información relevante sobre **AVG Internet Security 2015**:

- ***Soporte***: la pestaña proporciona un resumen organizado con claridad de todos los contactos disponibles para el soporte del cliente.
- ***Producto***: la pestaña proporciona una descripción general de los datos técnicos más importantes de **AVG Internet Security 2015** 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.

3.3.1.4. Opciones

El mantenimiento de **AVG Internet Security 2015** 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 Internet Security 2015**.

- ***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 para el espacio de cuarentena, la Bóveda de virus, hacia donde AVG deriva todas las infecciones detectadas. Los archivos infectados se aíslan dentro de esta cuarentena, garantizando la seguridad de 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.

  - *Resultados de la Protección Residente*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por la Protección Residente.

  - *Resultados de Identity Protection*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por el componente Identidad.

  - *Resultados de la Protección del correo electrónico*: abre un cuadro de diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente Protección del correo electrónico.

  - *Resultados de Online Shield*: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por Online Shield.

  - *Registro de historial de eventos*: abre la interfaz del registro del historial de todas las acciones de **AVG Internet Security 2015** registradas.

  - *Registro del Firewall*: abre un cuadro de diálogo con una descripción general detallada de las acciones del Firewall.

- ***Configuración avanzada...***: abre el cuadro de diálogo Configuración avanzada de AVG en el cual es posible editar la configuración de **AVG Internet Security 2015**. Generalmente, se recomienda mantener la configuración predeterminada de la aplicación como se encuentra definida por el distribuidor del software.

- ***Configuración del Firewall...***: abre un cuadro de diálogo independiente para la configuración avanzada del componente Firewall.

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

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

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

- ***Acerca de Virus y Amenazas***: abre la Enciclopedia de virus en línea del sitio web de AVG (*http://*

www.avg.com/) donde puede buscar información detallada acerca del virus identificado.

- ***MyAccount***: permite conectarse a la página de registro del sitio web de ***AVG MyAccount*** (http://www.avg.com/). Cree su cuenta AVG para poder actualizar fácilmente sus licencias y productos AVG registrados, descargar productos nuevos, ver el estado de los pedidos o administrar datos personales y contraseñas. Introduzca su información de registro; sólo los clientes que registren su producto AVG podrán recibir asistencia técnica gratuita.

- ***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 contrato de licencia. *(El mismo cuadro de diálogo puede abrirse mediante el enlace de Soporte de la navegación principal).*

3.3.2. Información del estado de seguridad

La sección ***Información del estado de seguridad*** está situada en la parte superior de la ventana principal de **AVG Internet Security 2015**. En esta sección siempre encontrará información sobre el estado de seguridad actual de su **AVG Internet Security 2015**. Consulte la descripción general de los iconos que posiblemente se muestran en esta sección, y su significado:

: el icono verde indica que ***AVG Internet Security 2015 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 Internet Security 2015** 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 Internet Security 2015** 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 Internet Security 2015** requiere reiniciar el equipo (***es necesario reiniciar***). Preste atención a esta advertencia y reinicie su equipo.

: el icono naranja indica que ***AVG Internet Security 2015 se encuentra en estado crítico***. Uno o varios componentes no funcionan correctamente y **AVG Internet Security 2015** 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 Internet Security 2015 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 Internet Security 2015 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 Internet Security 2015 también se puede obtener en cualquier momento del icono de la bandeja del sistema.*

3.3.3. 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 Internet Security 2015,** 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 librerías dentro de su sistema, y le brinda protección contra adware malicioso, y ***Anti-Rootkit***, que analiza rootkits peligrosos ocultos dentro de aplicaciones, controladores o librerías. Detalles >>
- ***Web***: le brinda protección contra ataques basados en la Web mientras busca y navega por internet. Detalles >>
- ***Identidad***: el componente ejecuta el servicio ***Identity Shield*** que brinda protección constante a 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 >>
- ***Firewall***: controla todas las comunicaciones en cada puerto de la red, protegiéndole contra ataques maliciosos y bloqueando todos los intentos de intrusión. 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.

3.3.4. Analizar / Actualizar vínculos rápidos

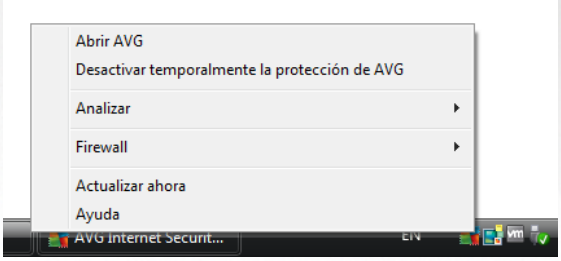
Los ***Vínculos rápidos*** están ubicados en la línea inferior de botones de la interfaz de usuario de **AVG Internet Security 2015**. Estos vínculos le permiten un acceso inmediato a las funciones más importantes y de uso más común de la aplicación, es decir, análisis y actualizaciones. Los vínculos 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)*

3.3.5. 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 Internet Security 2015**. Está visible en todo momento en la bandeja del sistema, tanto si la interfaz del usuario de **AVG Internet Security 2015** 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 Internet Security 2015** 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 señaliza un proceso de actualización actualmente ejecutado.

- La visualización alternativa de un icono a colores con una flecha significa que se está ejecutando uno de los análisis de **AVG Internet Security 2015**.

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 Internet Security 2015** y sobre posibles cambios de estado en el programa (*por ej., inicio automático de un análisis o actualización programado, Cambio de perfil de Firewall, 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 Internet Security 2015**, 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 AVG***: haga clic aquí para abrir la interfaz del usuario de **AVG Internet Security 2015**.

- ***Desactivar temporalmente la protección de AVG***: la opción le permite desactivar la protección completa que usted realizó **AVG Internet Security 2015** 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 Internet Security 2015** 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 Internet Security 2015**, 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.

- ***Firewall***: haga clic para abrir el menú contextual con un acceso rápido a todos los modos de Firewall disponibles. Realice una selección desde la vista general y haga clic para confirmar que desea cambiar el modo de Firewall configurado actualmente.

- ***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 Quick Tune***: haga clic para ejecutar el componente Quick Tune.

- ***Iniciar sesión en AVG MyAccount***: abre la página principal de MyAccount, donde puede administrar sus productos de suscripción, comprar protección adicional, descargar archivos de instalación,

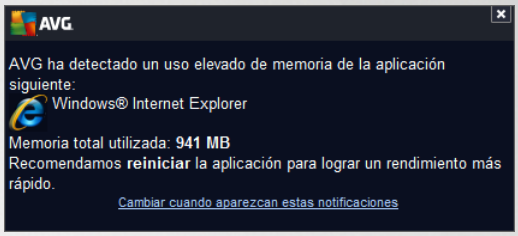
comprobar pedidos y facturas anteriores, y administrar su información personal.

- ***Actualizar ahora***: inicia inmediatamente una actualización.
- ***Ayuda***: abre el archivo de ayuda de la página de inicio.

3.3.6. 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 sólo 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.

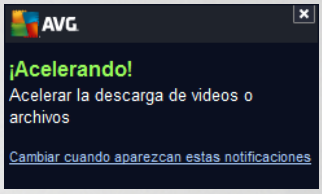
En cada una de estas situaciones, ***AVG Advisor*** le advierte de los posibles problemas que se pueden ocasionar y proporciona el nombre y el icono del proceso o de la aplicación en conflicto. Además, ***AVG Advisor*** sugiere los pasos que se deben tomar para evitar los posibles problemas.

Exploradores web soportados

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

3.3.7. 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.



3.4. Componentes de AVG

3.4.1. Protección del Equipo

El componente ***Equipo*** cubre dos servicios de seguridad principales: ***AntiVirus*** y ***Caja Fuerte de Datos***:

- ***AntiVirus*** comprende un motor de análisis que protege todos los archivos, las áreas del sistema 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 análisis heurístico, donde los archivos se analizan en busca de características comunes de virus. Esto significa que AntiVirus puede detectar un virus nuevo y desconocido si éste contiene algunas características típicas de los virus ya existentes. **AVG Internet Security 2015** 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.

- ***Caja Fuerte de Datos*** le permite crear bóvedas virtuales seguras donde puede almacenar información privada. Los contenidos de la Caja Fuerte de Datos están encriptados y protegidos con una contraseña de su elección para que nadie pueda acceder a ellos sin autorización.

Controles del cuadro de diálogo

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

Habilitado / Deshabilitado: el botón puede recordarle a un semáforo, tanto en su apariencia como en su funcionalidad. Haga un solo clic para alternar entre dos posiciones. El color verde significa ***Habilitado***, que implica que el servicio de seguridad AntiVirus está activo y completamente funcional. El color rojo representa el estado ***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 permite configurar el servicio seleccionado, es decir, AntiVirus. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG Internet Security 2015,** pero solamente se recomienda que lo hagan usuarios experimentados.

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

Cómo crear su caja de seguridad de datos

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

las instrucciones que figuran en la aplicación:

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

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

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

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

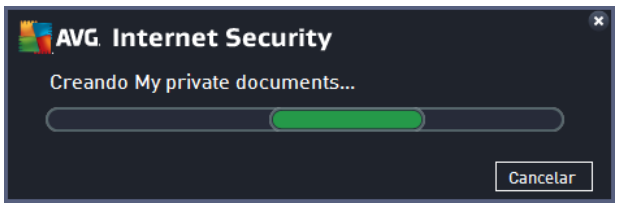
Una vez que haya especificado todos los datos requeridos en los campos de texto, haga clic en el botón ***Siguiente*** para ir al siguiente paso:

Este cuadro de diálogo incluye las siguientes opciones de configuración:

- ***Ubicación*** indica dónde se guardará físicamente la caja fuerte de datos. Busque un lugar adecuado en su disco, o bien, puede mantener la ubicación predefinida, que es la carpeta *Documentos*. Recuerde que una vez que ha creado una caja fuerte de datos, ya no puede cambiar su ubicación.
- ***Tamaño***: puede predefinir el tamaño de su caja fuerte de datos, que asignará el espacio necesario en el disco. El valor con el cual se configurará no debe ser ni demasiado pequeño *(no será suficiente para sus necesidades)*, ni demasiado grande *(ocupará demasiado espacio en el disco sin necesidad)*. Si ya sabe qué desea colocar en la caja fuerte de datos, puede ubicar todos los archivos en una carpeta y luego utilizar el vínculo ***Seleccionar una carpeta*** para calcular automáticamente el tamaño total. Sin embargo, más adelante podrá cambiar el tamaño, según sus necesidades.
- ***Acceso***: las casillas de verificación en esta sección le permiten crear accesos directos convenientes a su caja fuerte de datos.

Cómo utilizar su caja fuerte de datos

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



Para utilizar su nueva caja fuerte de datos, primero debe abrirla: haga clic en el botón ***Abrir Ahora***. Después de hacerlo, la caja fuerte de datos aparece en su equipo como un nuevo disco virtual. Asígnele una letra de su

elección del menú desplegable (*sólo se le permitirá seleccionar de discos actualmente libres*). Normalmente, no podrá elegir las letras C *(usualmente asignada a su disco duro)*, A *(unidad de disco flexible)* o D *(unidad de DVD)*. Recuerde que cada vez que desbloquee una caja fuerte de datos, podrá elegir una letra diferente para la unidad.

Cómo desbloquear su caja fuerte de datos

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

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

3.4.2. Protección de Navegación Web

El componente ***Protección de Navegación Web*** comprende dos servicios: ***LinkScanner Surf-Shield*** y ***Online Shield***:

- ***LinkScanner Surf-Shield*** le protege contra el creciente número de amenazas fugaces que aparecen en la Web. Estas amenazas pueden esconderse en cualquier tipo de sitio web, desde gubernamentales y de marcas grandes y reconocidas hasta de negocios pequeños, y rara vez permanecen allí por más de 24 horas. LinkScanner lo protege analizando las páginas web que se esconden en los vínculos de cualquier página web que esté viendo y se asegura de que sean seguras en el único momento en que verdaderamente importa: cuando está por hacer clic sobre ellas. ***LinkScanner Surf-Shield no 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 cuadro de diálogo puede encontrar los siguientes controles. Su funcionalidad es similar ya sea que pertenezcan a un servicio de seguridad o a otro *(LinkScanner Surf-Shield u Online Shield)*:

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.***

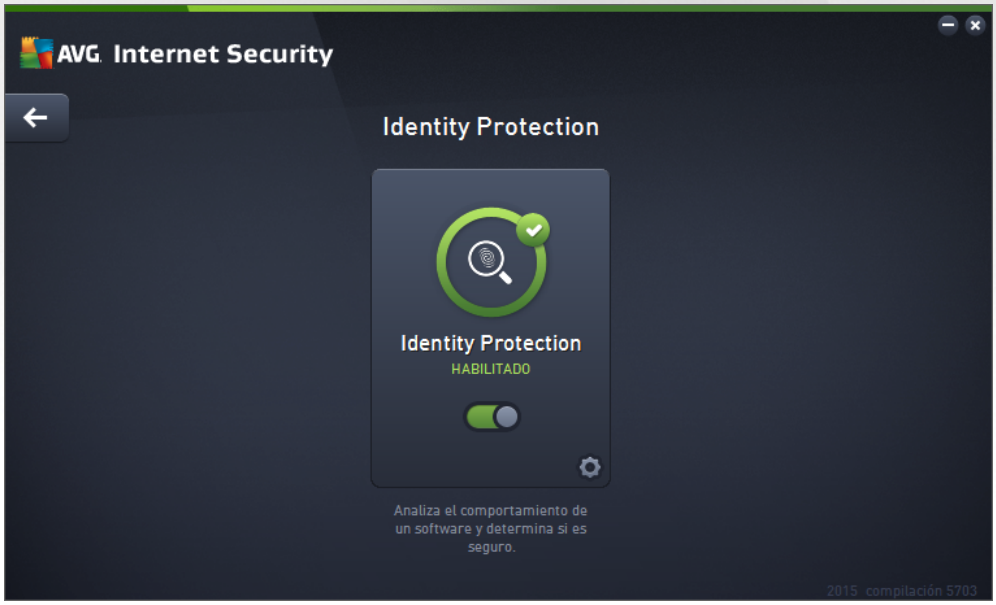
Configuración: haga clic en el botón para redireccionarse a la interfaz de configuración avanzada. De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, LinkScanner Surf-Shield u Online Shield. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG Internet Security 2015,** pero solamente se recomienda que lo hagan usuarios experimentados.

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

3.4.3. Identity Protection

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

- ***Identity Protection*** es un servicio anti-malware que ofrece protección contra todo tipo de malware (*spyware, bots, robo de identidad, ...*) 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 deshará los cambios que hayan podido realizarse en el sistema *(inyecciones de código, cambios del registro, apertura de puertos, etc.)*. No es necesario iniciar un análisis para estar protegido. Esta tecnología es muy proactiva, raras veces necesita actualización y siempre está de guardia.



Controles del cuadro de diálogo

En el cuadro de diálogo, 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 redireccionarse a la interfaz de configuración avanzada. De forma precisa, el cuadro de diálogo respectivo se abre y le permitirá configurar el servicio seleccionado, es decir, Identity Protection. En la interfaz de configuración avanzada, puede editar toda la configuración de cada servicio de seguridad dentro de **AVG Internet Security 2015,** pero solamente se recomienda que lo hagan usuarios experimentados.

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

Lamentablemente, en **AVG Internet Security 2015**, 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.

3.4.4. Protección del Correo Electrónico

El componente ***Protección del correo electrónico*** cubre los siguientes dos servicios de seguridad: ***Analizador de correo electrónico*** y ***Anti-Spam*** *(el servicio Anti-Spam sólo es accesible en las ediciones Internet Security y Premium Security)*.

- ***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.***

 ***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, 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 Internet Security 2015,** pero solamente se recomienda que lo hagan usuarios experimentados.

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

3.4.5. Firewall

Un ***firewall*** es un sistema que aplica una política de control de acceso entre dos o más redes bloqueando o permitiendo el tráfico. Cada firewall contiene un conjunto de reglas que protege la red interna de ataques que se originan desde *fuera (generalmente desde Internet) y* controla toda comunicación en cada puerto de red. La comunicación se evalúa según las reglas definidas y, así, se permite o prohíbe. Si el firewall reconoce cualquier intento de intrusión, "bloquea" el intento y no permite el acceso al equipo. El firewall está configurado para permitir o denegar la comunicación interna o externa *(bidireccional, de entrada o de salida)* mediante puertos definidos y para aplicaciones de software especificadas. Por ejemplo, el firewall puede configurarse para permitir que la información web entrante y saliente fluya únicamente mediante Microsoft Explorer. Cualquier intento de transmitir información web mediante otro navegador sería bloqueado. Protege su información personal para que no se envíe desde su equipo sin su autorización. Controla la forma en que su equipo intercambia datos con otros equipos a través de Internet o de una red local. Dentro de una organización, el firewall también protege a equipos individuales de posibles ataques iniciados por usuarios internos desde otros equipos en la red.

En **AVG Internet Security 2015**, el ***Firewall*** controla todo el tráfico en cada puerto de red de su equipo. El Firewall, de acuerdo con las reglas definidas, evalúa las aplicaciones que están ejecutándose en el equipo *(y desean conectarse a Internet o a una red local)* o las que abordan su equipo desde el exterior para intentar conectarse a él. Para cada una de estas aplicaciones, el Firewall permite o prohíbe la comunicación en los puertos de red. De forma predeterminada, si la aplicación es desconocida *(es decir, no tiene reglas de Firewall definidas)*, el Firewall le preguntará si desea permitir o bloquear el intento de comunicación.

AVG Firewall no está diseñado para proteger plataformas de servidor.

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

Nota: *Después de la instalación de su AVG Internet Security 2015 el componente Firewall puede solicitar que se reinicie el equipo. En ese caso, el cuadro de diálogo del componente aparece con la información de que es necesario reiniciar. Directamente en el cuadro de diálogo encontrará el botón* ***Reiniciar ahora****. Hasta que se reinicie el equipo, el componente Firewall no estará completamente activado. Además, todas las opciones de*

edición del cuadro de diálogo estarán desactivadas. Preste atención a esta advertencia y reinicie su equipo lo más pronto posible.

Modos de Firewall disponibles

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

- ***Automático***: en este modo, el Firewall maneja todas las redes de tráfico automáticamente. No se lo invitará a tomar decisiones. El Firewall permitirá la conexión para cada aplicación conocida y, al mismo tiempo, creará una regla para la aplicación que especifique que ésta siempre puede conectarse en el futuro. Para otras aplicaciones, el Firewall decidirá si se debe permitir la conexión o bloquearla en función del comportamiento de la aplicación. No obstante, en este tipo de situación, no se creará la regla y la aplicación se comprobará nuevamente cuando intente conectarse. El modo automático es discreto y se recomienda a la mayoría de los usuarios.

- ***Interactivo***: este modo es conveniente si desea controlar por completo todo el tráfico de la red hacia y desde su equipo. El Firewall supervisará y lo notificará sobre cada intento de comunicación o transferencia de datos, para que usted permita o bloquee el intento si lo considera adecuado. Recomendado sólo para usuarios avanzados.

- ***Bloquear acceso a internet***: la conexión a internet está bloqueada por completo, no puede acceder a internet y nadie desde afuera puede acceder a su equipo. Solamente para uso especial y breve.

- ***Desactivar la protección del Firewall (no recomendable)***: desactivar el Firewall permitirá todo el tráfico de la red hacia y desde su equipo. En consecuencia, esto lo hará vulnerable a los ataques de los hackers. Siempre considere esta opción cuidadosamente.

Tenga en cuenta un modo automático específico disponible también dentro del Firewall. Este modo se activa de manera silenciosa si se desactivan los componentes Equipo o Identity Protection y, por lo tanto, su equipo es más vulnerable. En estos casos, el Firewall sólo permitirá automáticamente aplicaciones conocidas y absolutamente seguras. Para todas las demás, le solicitará que tome una decisión. Esto se realiza para compensar los componentes de protección desactivados y mantener la seguridad de su equipo.

Recomendamos encarecidamente que no desactive el Firewall. No obstante, si necesariamente tiene que desactivar el componente Firewall, puede hacerlo seleccionando el modo de protección Desactivar Firewall en la lista anterior de modos de Firewall disponibles.

Controles del cuadro de diálogo

El cuadro de diálogo proporciona una descripción general de la información básica sobre el estado del componente Firewall:

- ***Modo Firewall***: proporciona información sobre el modo Firewall seleccionado actualmente. Utilice el botón ***Cambiar*** situado junto a la información proporcionada para cambiar a la interfaz de configuración de Firewall si desea cambiar el modo actual por otro *(para ver una descripción y recomendación sobre el uso de perfiles de Firewall, consulte el párrafo anterior)*.

- ***Uso compartido de archivos e impresoras***: informa si se permite en estos momentos el uso compartido de archivos e impresoras *(bidireccional)*. El uso compartido de archivos e impresoras

significa en realidad el uso compartido de archivos o carpetas que marque como "Compartidas" en Windows, unidades de disco comunes, impresoras, escáneres y dispositivos similares. El uso compartido de tales elementos es deseable dentro de redes que pueden considerarse seguras *(por ejemplo en el hogar, en el trabajo o en la escuela)*. Sin embargo, si está conectado a una red pública *(como la conexión wi-fi de un aeropuerto o la de un café con Internet)*, probablemente no desee compartir nada.

- ***Conectado a***: proporciona información sobre el nombre de la red a la que está conectado actualmente. Con Windows XP, el nombre de la red responde a la denominación que elija para la red específica cuando se conecte por primera vez. Con Windows Vista y superior, el nombre de la red se toma automáticamente del Centro de redes y recursos compartidos.

- ***Restablecer valores predeterminados***: presione este botón para reemplazar la configuración de Firewall actual y revertir a la configuración predeterminada en función de la detección automática.

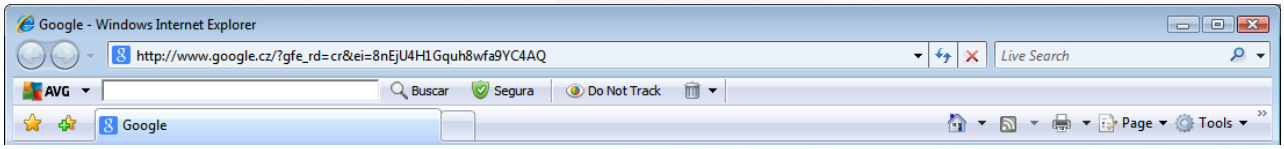
El cuadro de diálogo contiene los siguientes controles gráficos:

Configuración: haga clic en el botón para dirigirse a la interfaz de configuración de Firewall donde puede editar toda la configuración de Firewall. Sólo los usuarios experimentados pueden llevar a cabo cambios en la configuración.

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

3.5. 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 Internet Security 2015**, 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*) 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***.
- ***Contrato de Licencia de Usuario Final***: abre el sitio web de AVG en la página que muestra íntegramente el contrato de licencia relacionado con el uso de su **AVG Internet Security 2015**.
- ***Política de Privacidad***: abre el sitio web de AVG en la página donde puede encontrar el texto completo de la Política de Privacidad de AVG.
- ***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 cuadro de diálogo con información sobre el nivel de la amenaza actual (*Seguro*) de la página que está visitando. Esta breve descripción general se puede ampliar y muestra detalles completos de todas las actividades de seguridad relacionadas con la página, directamente en la ventana del navegador (*Informe del sitio web 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***.

- Botones de acceso directo para el acceso rápido a estas aplicaciones: ***Calculadora***, ***Bloc de notas***, ***Explorador de Windows***.

3.6. 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 sitos 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.

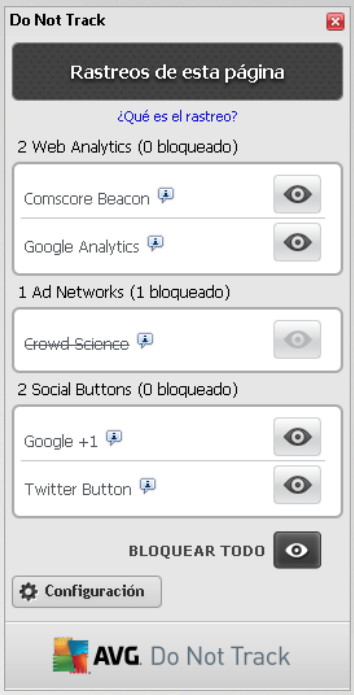
- ***AVG Do Not Track*** está habilitado de manera predeterminada, pero puede deshabilitarse fácilmente en cualquier momento. Puede encontrar instrucciones en el artículo de las FAQ que trata cómo deshabilitar la función AVG Do Not Track.

- 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.

3.6.1. 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).*

3.6.2. 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.

3.6.3. 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.

3.6.4. 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.

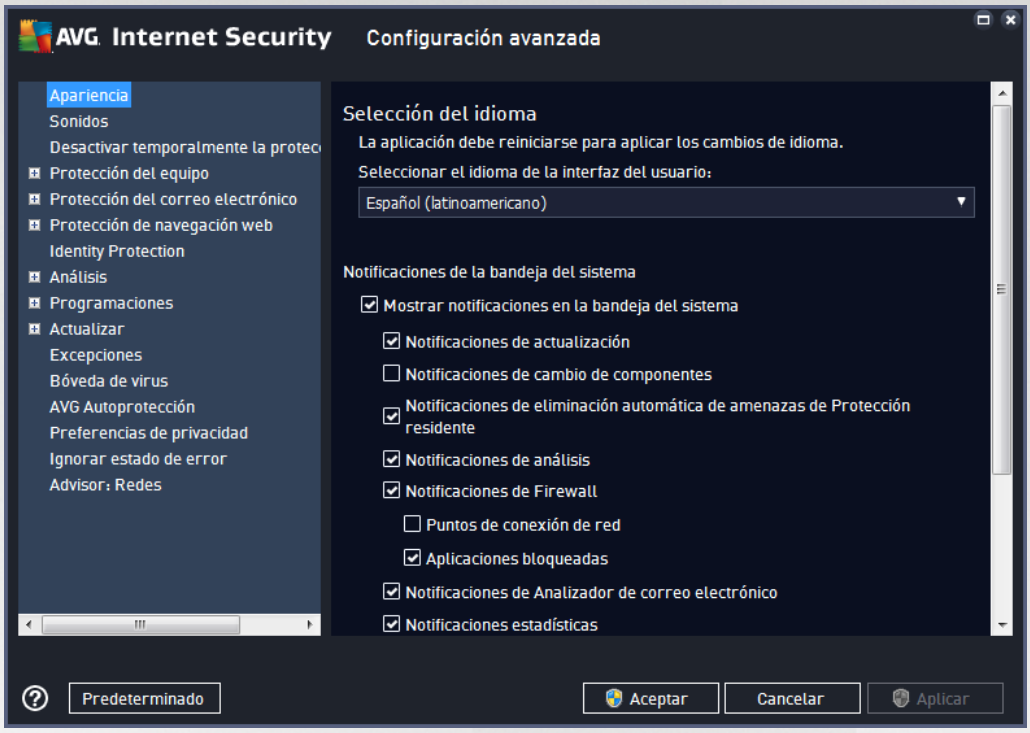
- ***Notificar a los sitios web...***: en esta sección puede activar o desactivar la opción ***Notificar a los sitios web que no deseo ser rastreado*** *(activada de forma predeterminada).* Mantenga esta opción marcada para confirmar que desea que ***Do Not Track*** informe a los proveedores de un servicio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

3.7. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **AVG Internet Security 2015** 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.

3.7.1. Apariencia

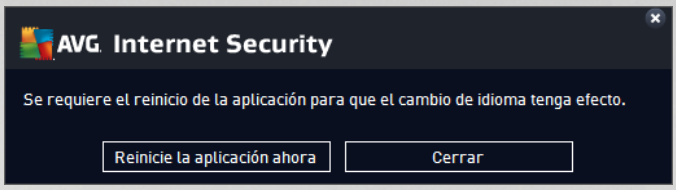
El primer elemento del árbol de navegación, ***Apariencia***, hace referencia a la configuración general de la interfaz del usuario **AVG Internet Security 2015**, y proporciona unas pocas opciones básicas del comportamiento de la aplicación:



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 Internet Security 2015**. 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 Internet Security 2015** 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 Internet Security 2015**
- Presione el botón ***Reiniciar AVG ahora*** para aceptar el reinicio del programa y espere un momento a que el cambio de idioma surta efecto:



Notificaciones de la bandeja del sistema

En esta sección, puede suprimir la visualización de las notificaciones de la bandeja del sistema sobre el estado de la aplicación **AVG Internet Security 2015**. 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 Internet Security 2015.** 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 Internet Security 2015)*, 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 Internet Security 2015**.
    - ***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 Internet Security 2015**.
    - ***Notificaciones de eliminación automática de amenazas de Protección Residente*** *(activada de forma predeterminada)*: decida si debe visualizarse o suprimirse la información relativa a los procesos de guardado, copia y apertura de archivos (*esta configuración sólo se muestra si la opción Autorreparar de Protección Residente está activada*).
    - Notificaciones de ***análisis*** *(activada de forma predeterminada)*: decida si debe visualizarse información sobre la ejecución automática del análisis programado, su progreso y resultados.
    - ***Notificaciones del Firewall*** *(activada de forma predeterminada)*: decida si debe visualizar información relativa al estado y los procesos relacionados con el Firewall, por ejemplo, las advertencias de activación o desactivación del componente, el posible bloqueo del tráfico, etc. . Este elemento proporciona dos opciones de selección más específicas *(para obtener una explicación detallada de cada una de ellas, consulte el capítulo Firewall de este documento)*:

        - ***Puntos de conexión de red*** *(desactivada de forma predeterminada)*: al conectarse a una red, Firewall informa si la conoce y cómo se deberá configurar el uso compartido de archivos e impresoras.

- ***Aplicaciones bloqueadas*** *(activada de manera predeterminada)*: cuando una aplicación desconocida o sospechosa está tratando de conectarse a una red, Firewall bloquea el intento y muestra una notificación. Esto es útil para mantenerlo informado, por lo tanto recomendamos que siempre mantenga la función activada.

- ***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 AVG Accelerator*** *(activada de forma predeterminada)*: decida si debe visualizarse información acerca de las actividades de ***AVG Accelerator***. ***AVG Accelerator*** es un servicio que mejora la reproducción de video en línea y que facilita la realización de descargas adicionales.

- ***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.

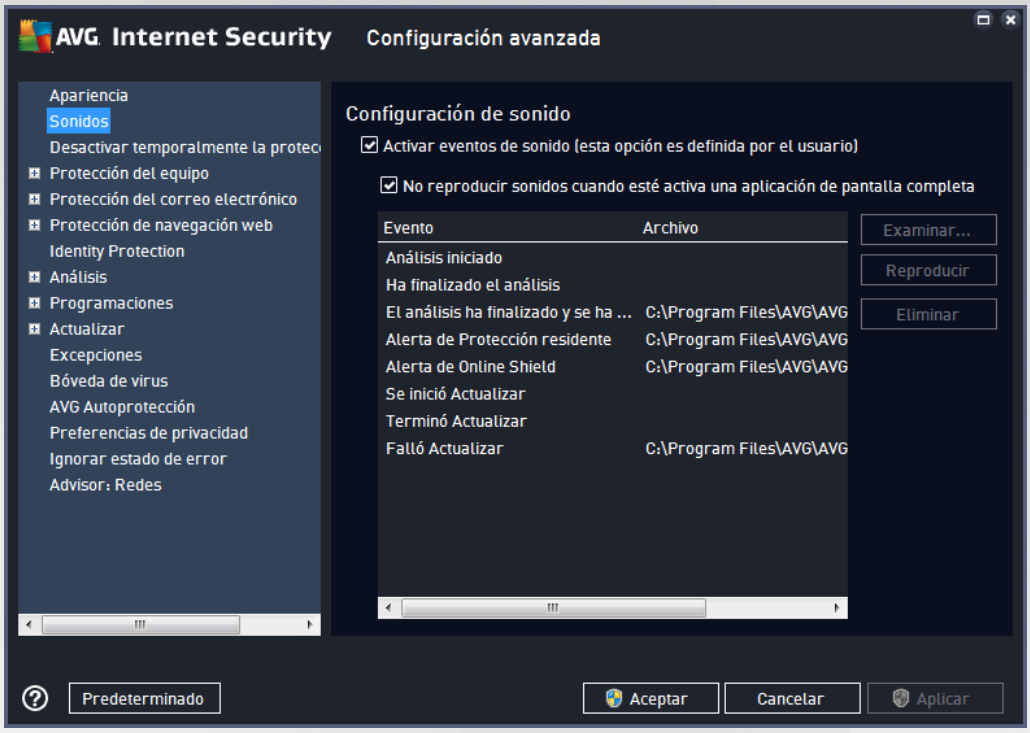
- ***Notificaciones de AVG Advisor*** *(activada de forma predeterminada):* decida si debe mostrar la información de las actividades de AVG Advisor en el panel deslizante en la bandeja del sistema.

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 ***Activar el Modo de juego cuando se ejecute una aplicación de pantalla completa*** (*configuración predeterminada*).

3.7.2. Sonidos

En el cuadro de diálogo ***Configuración de Sonido***, puede especificar si desea que se le informe acerca de acciones específicas de **AVG Internet Security 2015** 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 en las que pueda resultar molesta *(consulte también la sección Modo de juego del capítulo Configuración Avanzada / Apariencia en este documento)*.

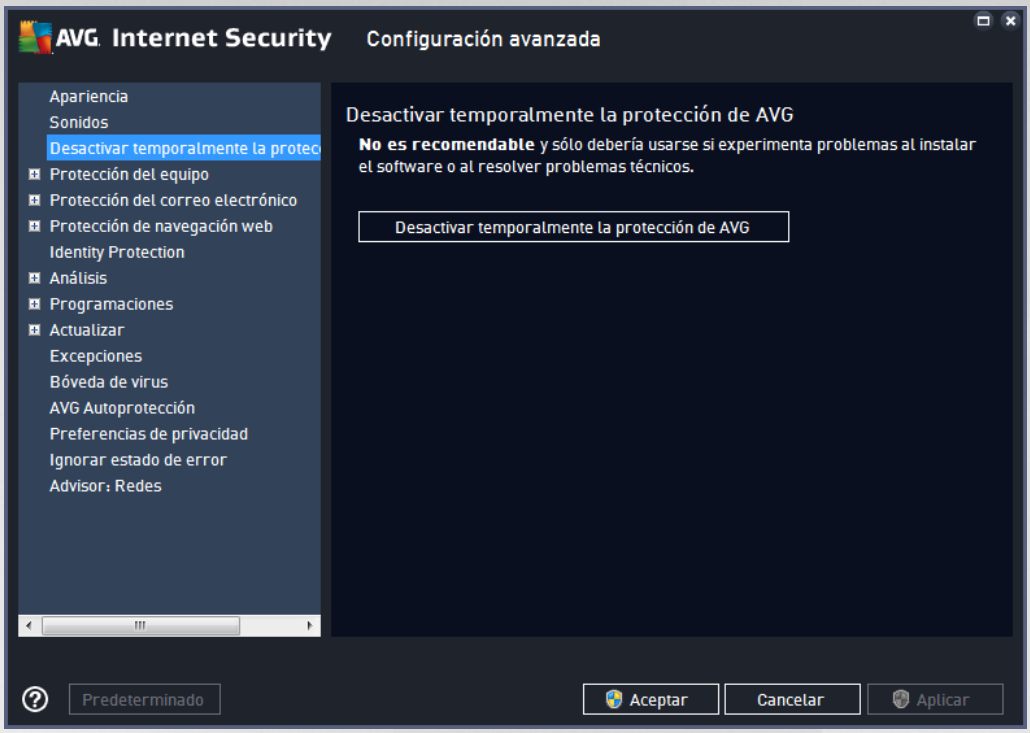
Botones de control

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

3.7.3. Desactivar temporalmente la protección de AVG

En el cuadro de diálogo ***Desactivar temporalmente la protección de AVG*** tiene la opción de desactivar toda la protección que proporciona **AVG Internet Security 2015** 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 Internet Security 2015** 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 desactivar la protección residente *(en el diálogo vinculado, desmarque primero el elemento **Activar la Protección Residente**)*. Si tiene que desactivar temporalmente **AVG Internet Security 2015**, 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.

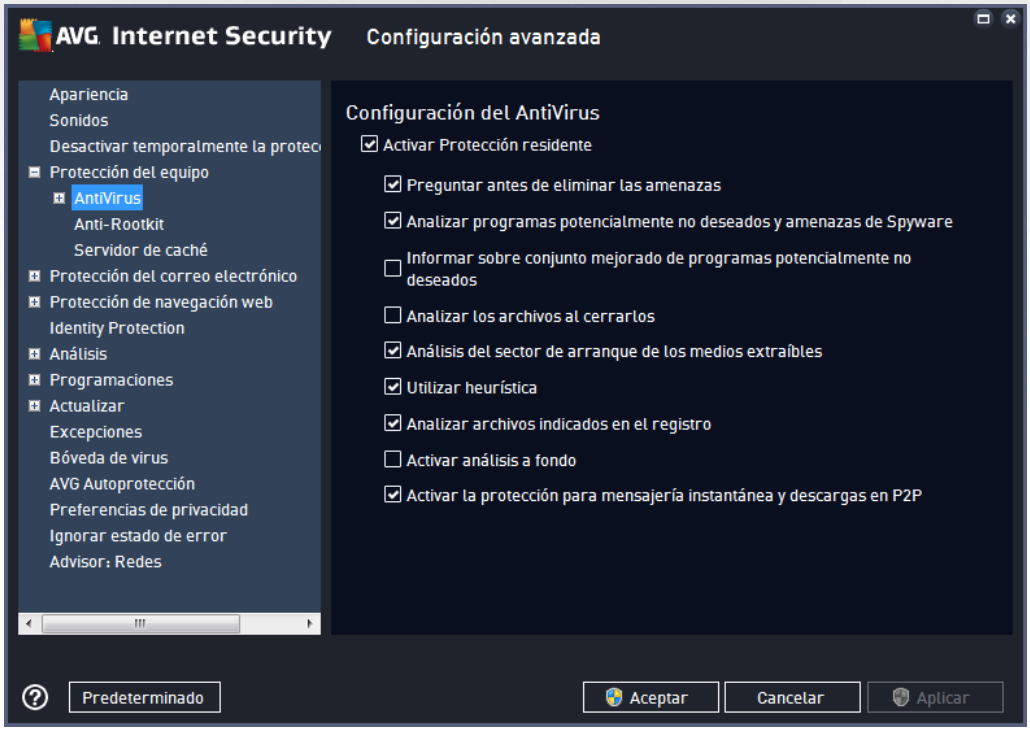
Cómo desactivar la protección de AVG

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 Internet Security 2015**. 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. Una opción separada para desactivar el componente ***Firewall*** está presente en el cuadro de diálogo ***Desactivar temporalmente la protección de AVG***. Marque la opción ***Desactivar protección de Firewall*** para hacerlo.

3.7.4. Protección del equipo

3.7.4.1. AntiVirus

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



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

residente se deben activar:

- ***Preguntar antes de eliminar las amenazas*** (*activada de forma predeterminada*): seleccione esta opción para que la Protección residente no realice ninguna acción de manera automática; si la selecciona, muestra un cuadro de diálogo que describe la amenaza detectada y le permite decidir qué debe hacer. Si deja la casilla sin seleccionar, **AVG Internet Security 2015** 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.

- ***Analizar el sector de arranque de los medios extraíbles*** (*activada por defecto*): seleccione esta opción para analizar los sectores de arranque de cualquier disco extraíble USB insertado, unidades de disco externas y cualquier otro medio extraíble en busca de amenazas.

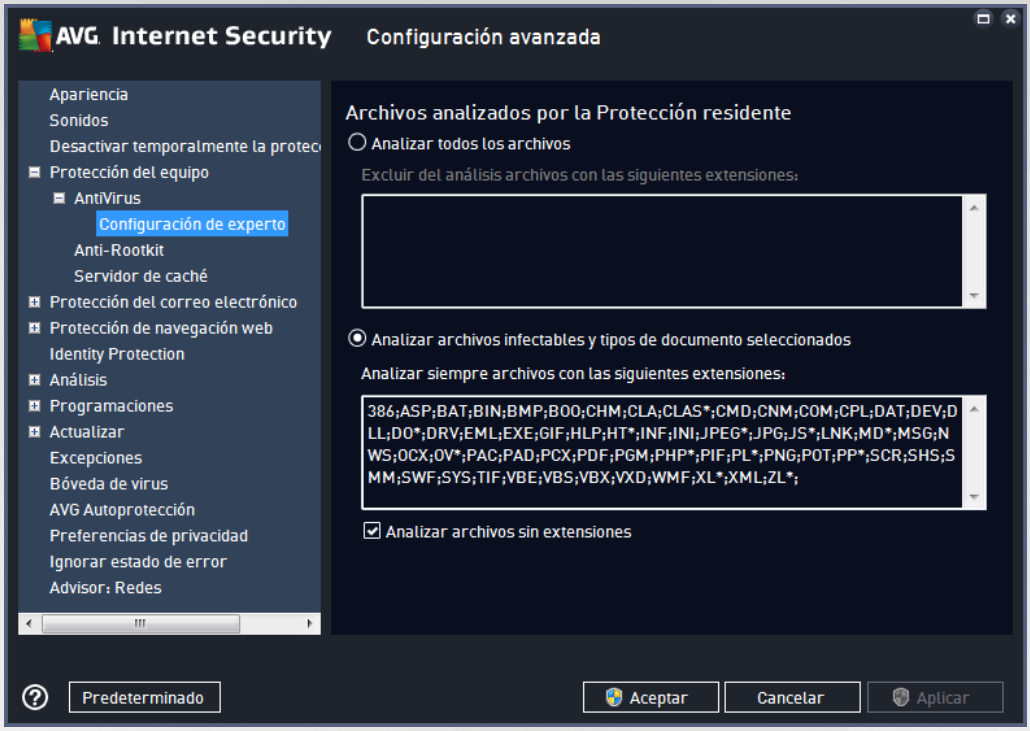
- ***Utilizar heurística*** (*activada de forma predeterminada*): el análisis heurístico *se utilizará para la detección (emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).

- ***Analizar archivos indicados en el registro*** (*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*):

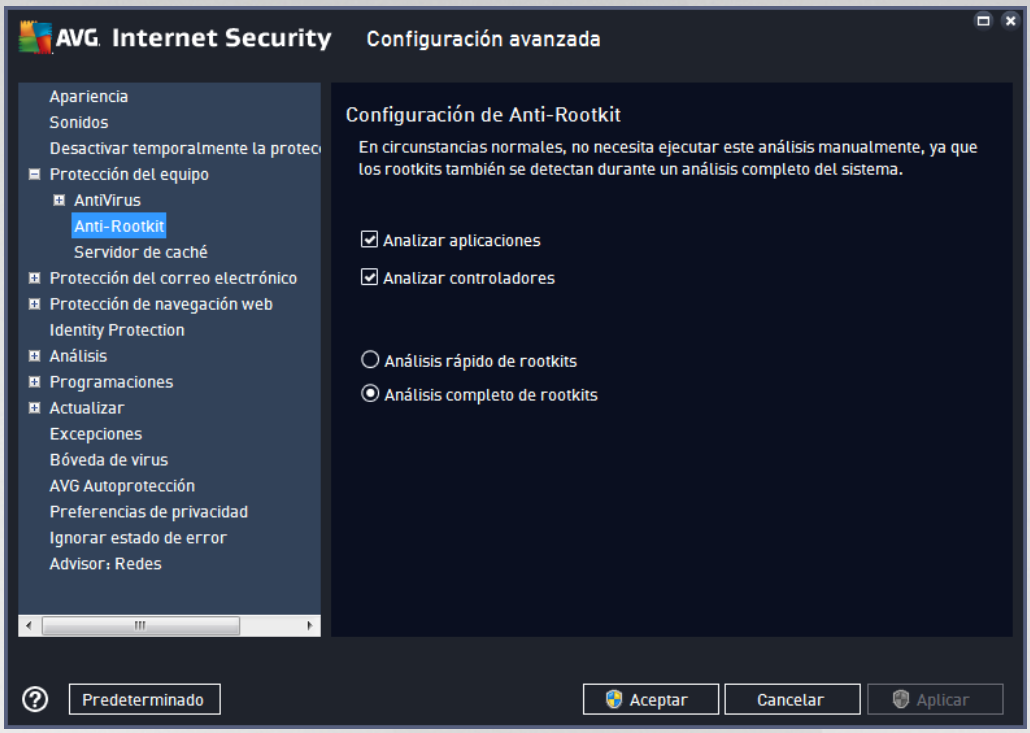


Marque la casilla de verificación respectiva para decidir si desea ***Analizar todos los archivos*** o solamente ***Analizar archivos infectables y tipos de documento seleccionados***. Para agilizar el análisis y proporcionar al mismo tiempo el nivel máximo de protección, recomendamos que conserve la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

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

3.7.4.2. Anti-Rootkit

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

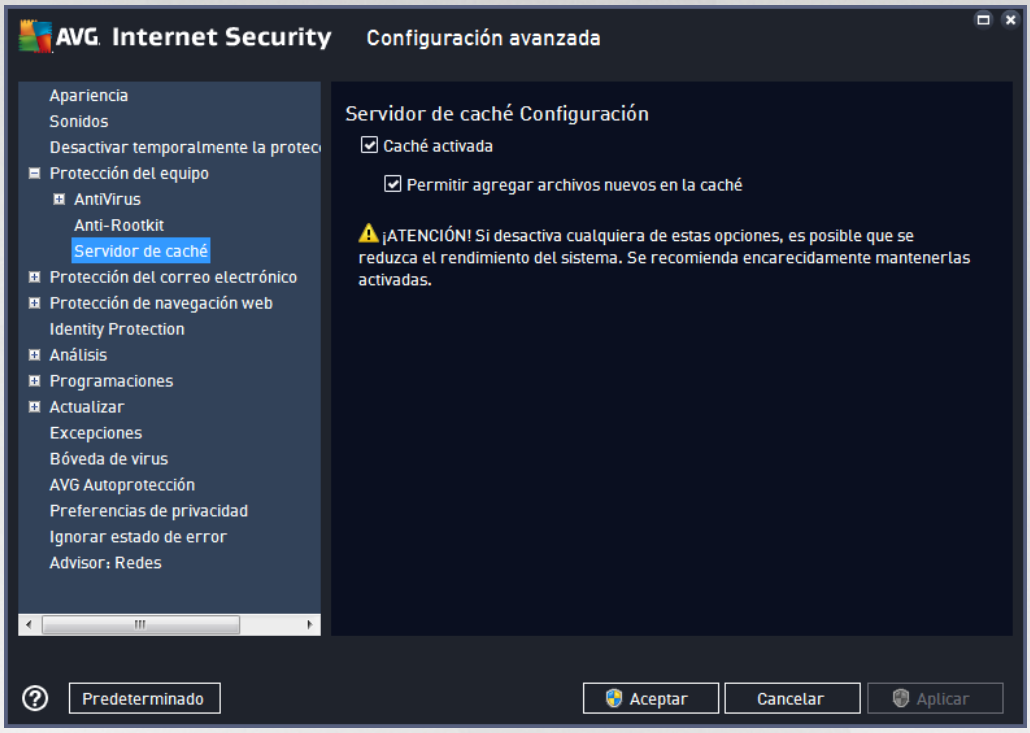


Analizar aplicaciones y ***Analizar controladores*** le permiten especificar en detalle qué debe incluirse en el análisis anti-rootkit. Esta configuración está diseñada para usuarios avanzados; le recomendamos mantener todas las opciones activadas. También puede seleccionar el modo de análisis de rootkits:

- ***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*)

3.7.4.3. Servidor de caché

El cuadro de diálogo ***Configuración del servidor de caché*** hace referencia al proceso del servidor de caché diseñado para aumentar la velocidad de todos los tipos de análisis de **AVG Internet Security 2015**:



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

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

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

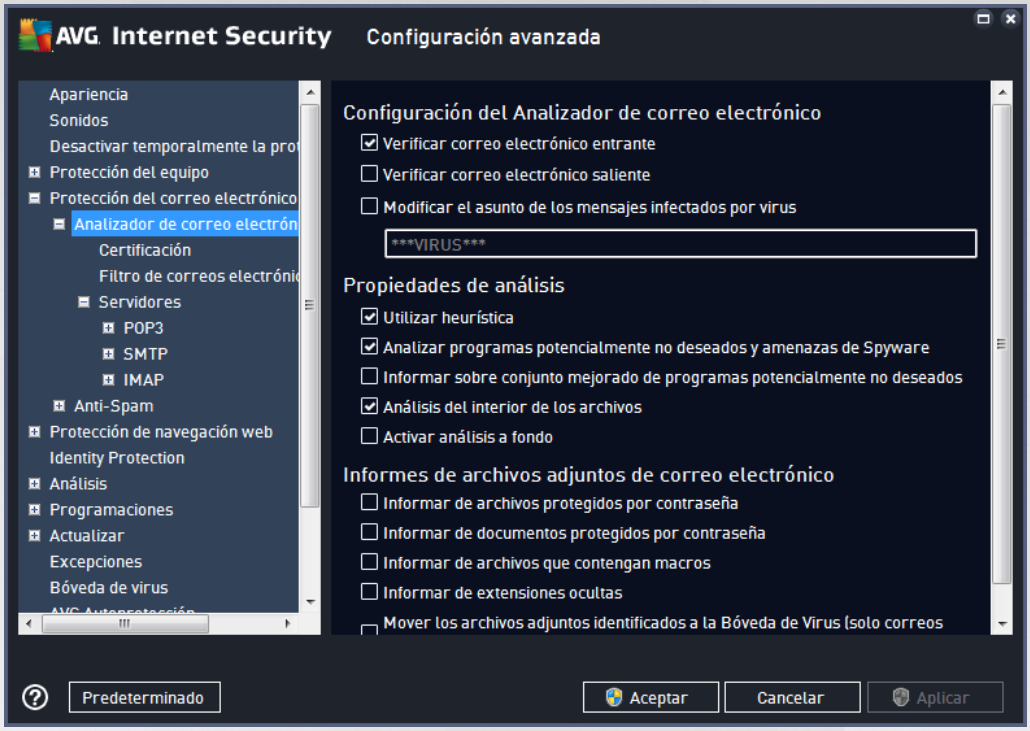
A menos que tenga un buen motivo para desactivar el servidor de caché, se recomienda especialmente que conserve la configuración predeterminada y deje las opciones activadas. De lo contrario, puede experimentar una disminución significativa en la velocidad y el rendimiento de su sistema.

3.7.5. Analizador de correos electrónicos

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

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

electrónicos.

- ***Analizar 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, sólo se agregará un texto de certificación al final del mensaje de correo electrónico, y todos esos informes se enumerarán en el cuadro de diálogo Detección mediante la Protección del correo electrónico:

- ***Notificar 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 notificarlos como potencialmente peligrosos.

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

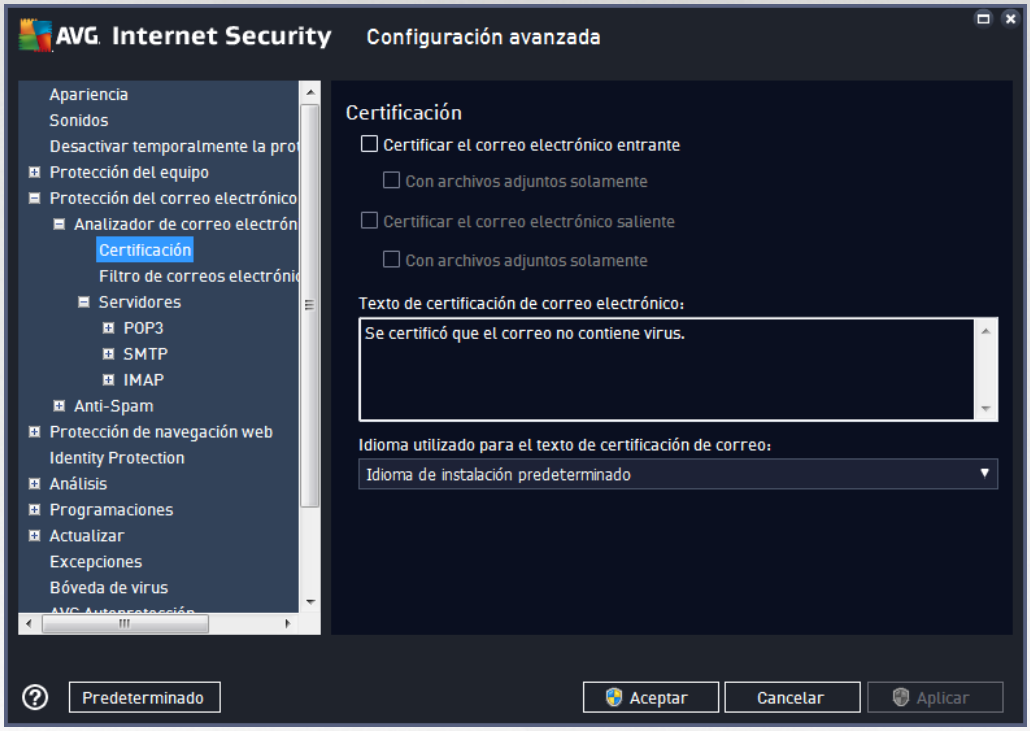
- ***Notificar archivos que contienen macros***: una macro es una secuencia predefinida de pasos encaminados a hacer que ciertas tareas sean más fáciles para el usuario *(las macros de MS Word son ampliamente conocidas*). Como tal, una macro puede contener instrucciones potencialmente peligrosas, y podría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

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

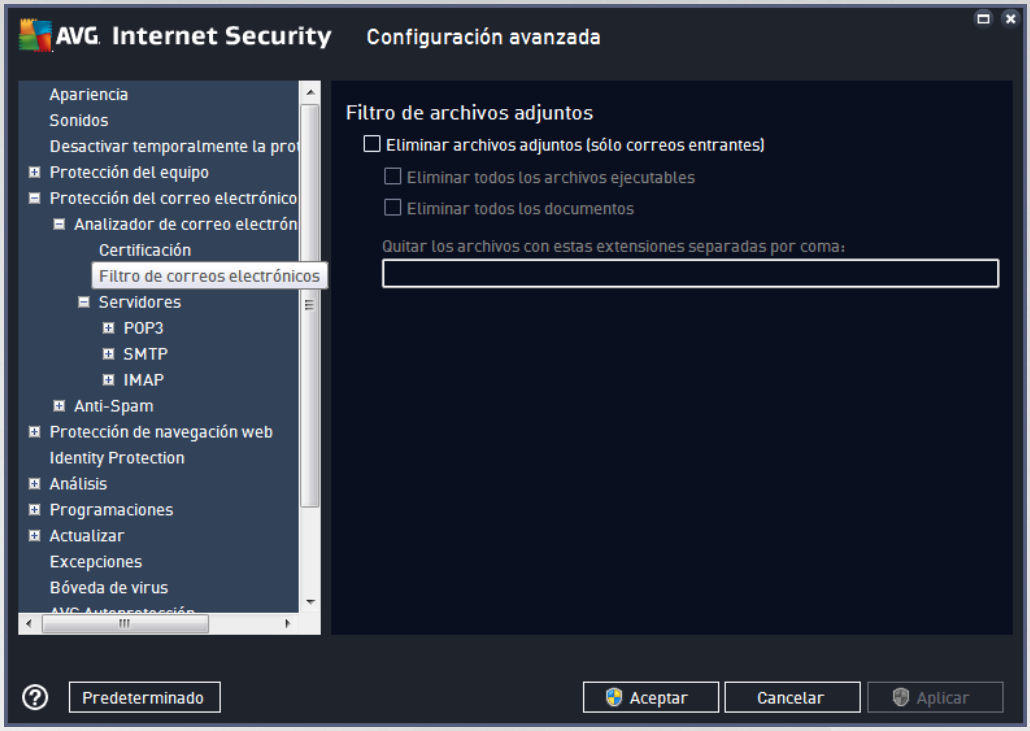
durante el análisis se identifica un mensaje en estas condiciones, defina si el objeto infeccioso detectado se debe mover a la Bóveda de virus.

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:

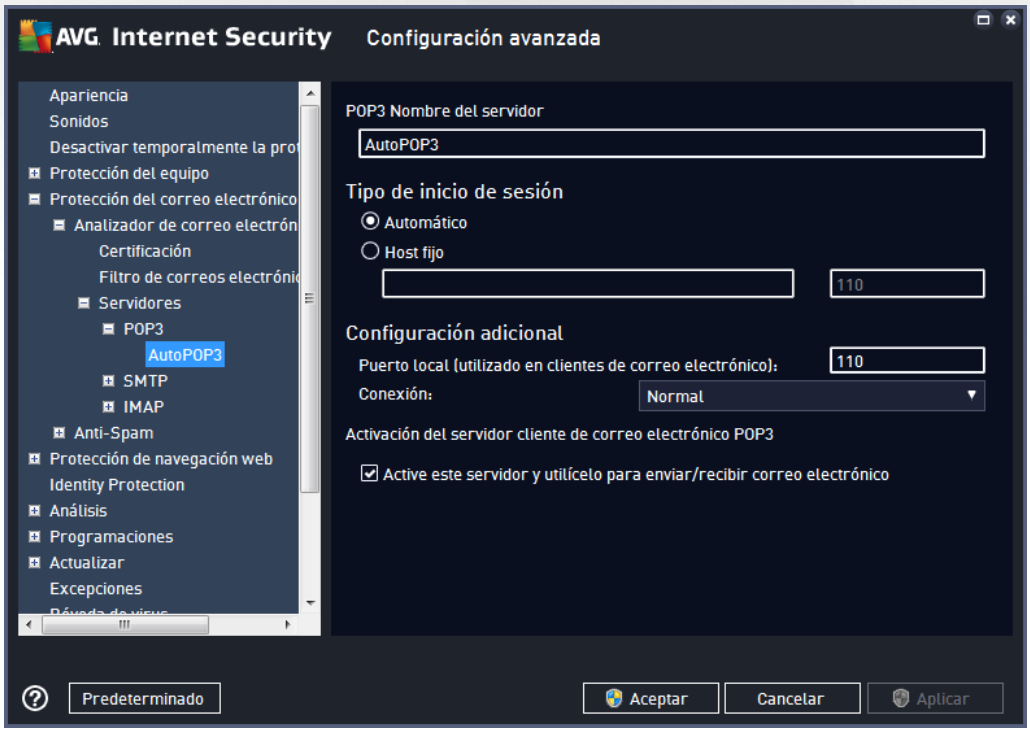
- ***Quitar todos los archivos ejecutables***: se eliminarán todos los archivos *.exe
- ***Quitar todos los documentos***: se eliminarán todos los archivos *.doc, *.docx, *.xls y *.xlsx
- ***Eliminar los archivos con las siguientes extensiones separadas por coma***: se eliminarán todos los archivos con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

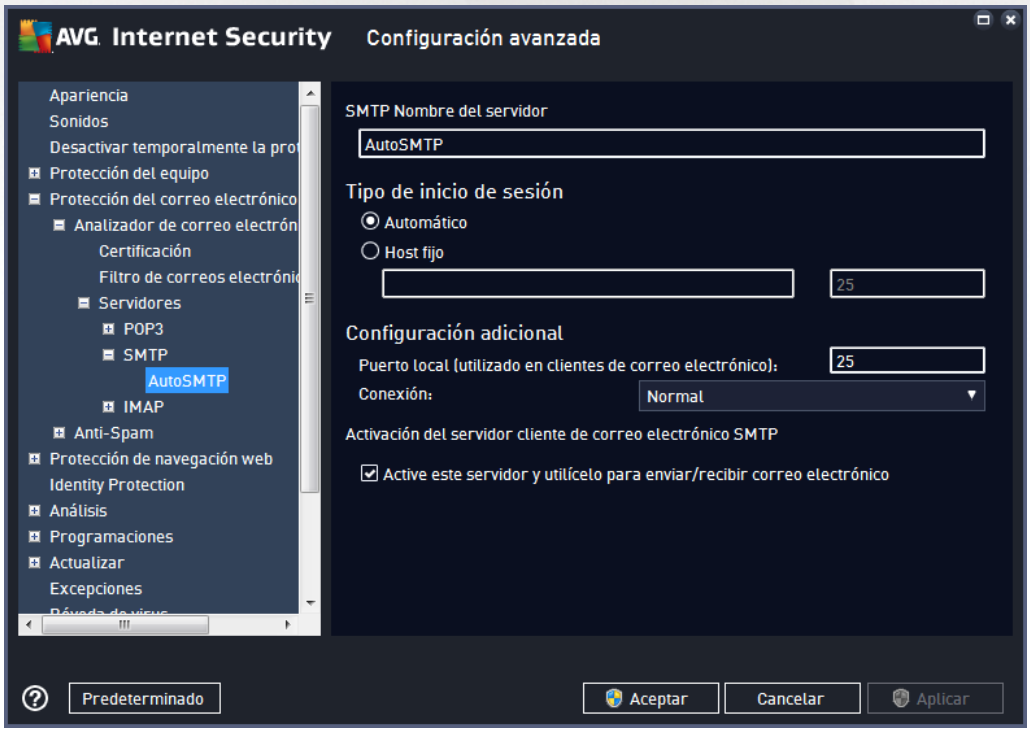


- ***Nombre del servidor POP3***: en este campo podrá especificar el nombre de los servidores nuevos

(*para agregar un servidor POP3, haga clic con el botón secundario del mouse en el elemento POP3 del menú de navegación de la izquierda*).

- ***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:

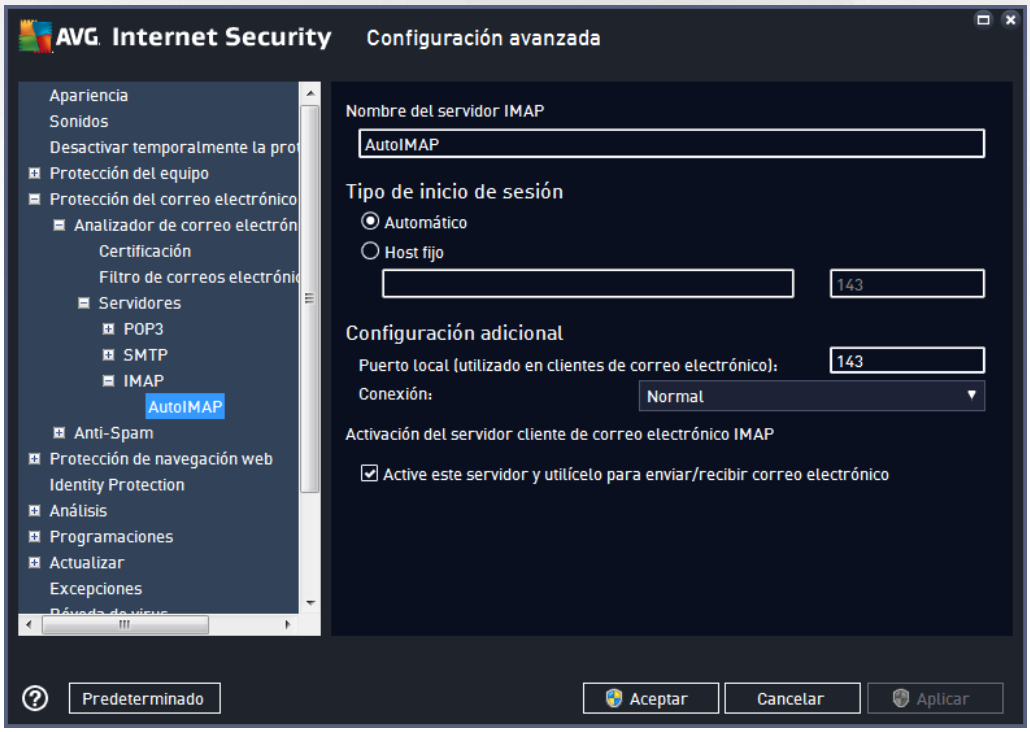


- ***Nombre del servidor SMTP***: en este campo podrá especificar el nombre de los servidores recién

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



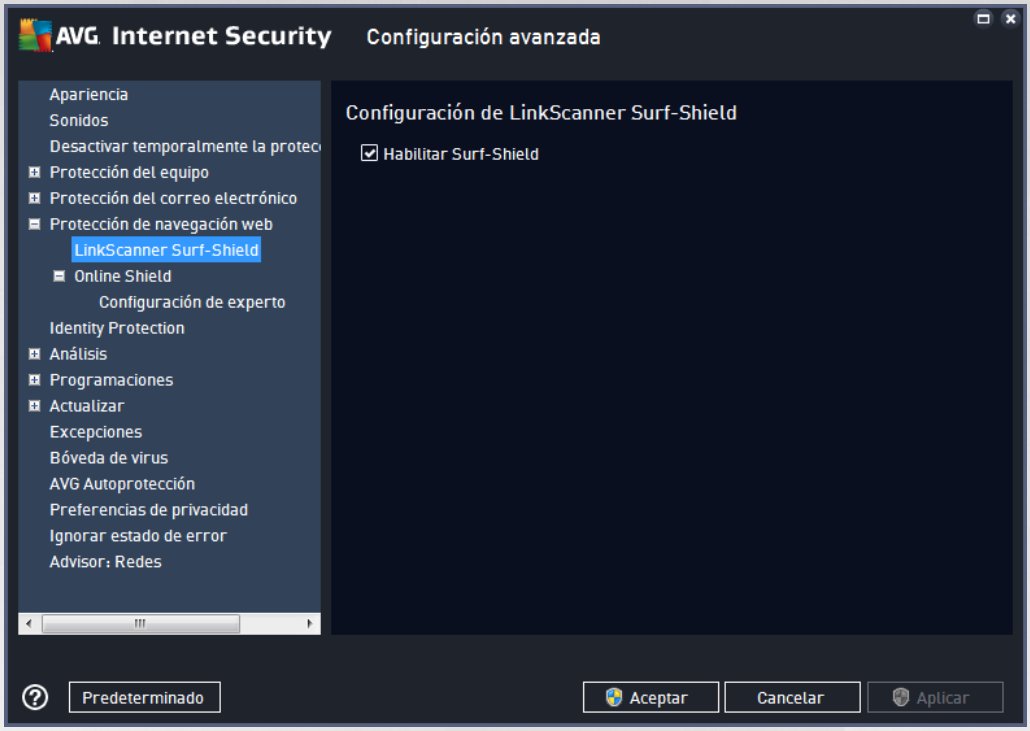
- ***Nombre del servidor IMAP***: en este campo podrá especificar el nombre de los servidores recién

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*).

- ***Tipo de Inicio de Sesión***: define el método para determinar el servidor de correo empleado para el correo saliente:
    - o ***Automático***: el inicio de sesión se efectuará automáticamente, según la configuración del cliente de correo electrónico.
    - o ***Host fijo***: en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (*por ejemplo, smtp.acme.com*), así como una dirección IP (*por ejemplo, 123.45.67.89*). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (*por ejemplo, imap.acme.com:8200*). El puerto estándar para comunicaciones IMAP es el 143.
- ***Configuración Adicional***: especifica los parámetros con mayor detalle:
    - o ***Puerto local utilizado***: especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Posteriormente deberá especificar en su aplicación de correo este puerto como puerto para la comunicación IMAP.
    - o ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (*normal/SSL/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.

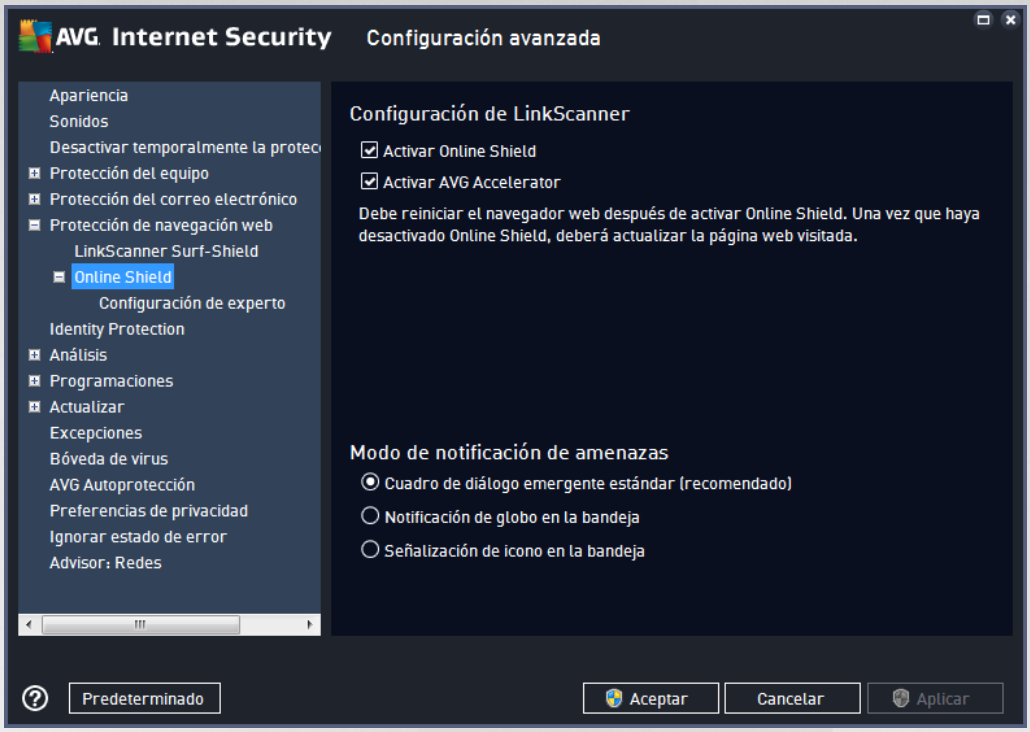
3.7.6. Protección de navegación web

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



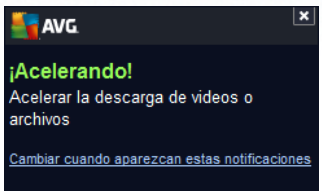
- ***Activar Surf-Shield*** (*activado de forma predeterminada):* protección (*en tiempo real*) activa contra sitios que amenazan la vulnerabilidad de la seguridad a medida que se accede a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido que amenaza la vulnerabilidad se bloquean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

3.7.6.1. Online Shield



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

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



Modo de notificación de amenazas

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

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

- ***Verificar archivos***: (*desactivado de manera predeterminada*): analiza el contenido de los archivos que pudieran existir en la página web que se visualizará.
- ***Analizar programas potencialmente no deseados y amenazas de Spyware***: (*activado de forma predeterminada*): seleccionar para activar el análisis de spyware, además de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen intencionalmente. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
- ***Informar sobre conjunto mejorado de 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.
- ***Utilizar heurística***: (*activado de forma predeterminada*): analiza el contenido de la página que se visualizará utilizando el método de análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*).
- ***Activar análisis a fondo***: (*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 el tráfico de red (TLS y SSL) cifrado_** (*activado por defecto*): dejar marcado para permitir a AVG analizar también toda la comunicación de red cifrada, es decir, las conexiones sobre protocolos de seguridad (SSL y su versión más reciente, TLS). Esto se aplica a sitios web que utilizan HTTPS y conexiones de clientes de correo electrónico que utilizan TLS/SSL. El tráfico protegido se descifra, se analiza para detectar malware y se vuelve a cifrar para devolverlo protegido a su computadora. Dentro de esta opción puede decidir ***incluir el tráfico de servidores con certificados de validación extendida (EV)*** y analizar también la comunicación de red cifrada de servidores con certificado de validación extendida. La emisión de un certificado de validación extendida requiere la validación extensiva a través de la autoridad de certificación y los sitios web operados conforme al certificado, por lo tanto, son mucho más confiables *(menos propensos a distribuir malware)*. Por este motivo, es posible que decida no analizar el tráfico proveniente de servidores con certificación de EV, lo cual hará que la comunicación cifrada sea moderadamente más rápida.

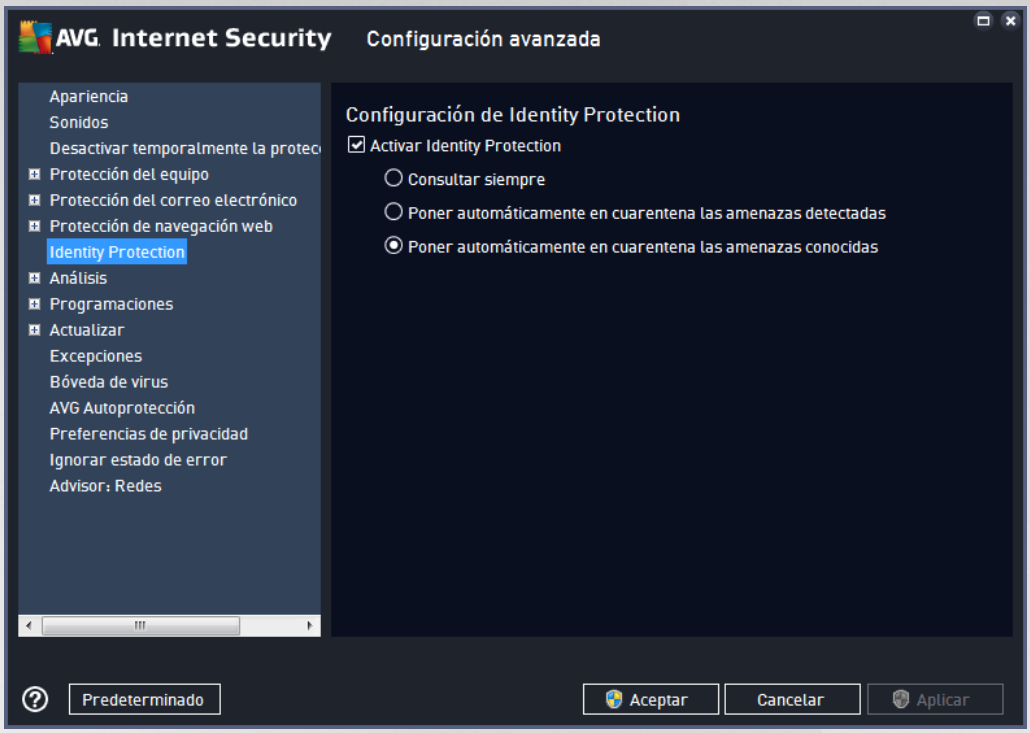
- **_Analizar archivos ejecutables descargados con Protección Residente_**: (*activado de forma predeterminada*): analizar archivos ejecutables *(generalmente archivos con extensiones exe, bat, com)* después de haberlos descargado. La Protección Residente analiza archivos antes de descargar para garantizar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

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

3.7.7. 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***: 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*** (*activada de forma predeterminada*): 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.

3.7.8. Análisis

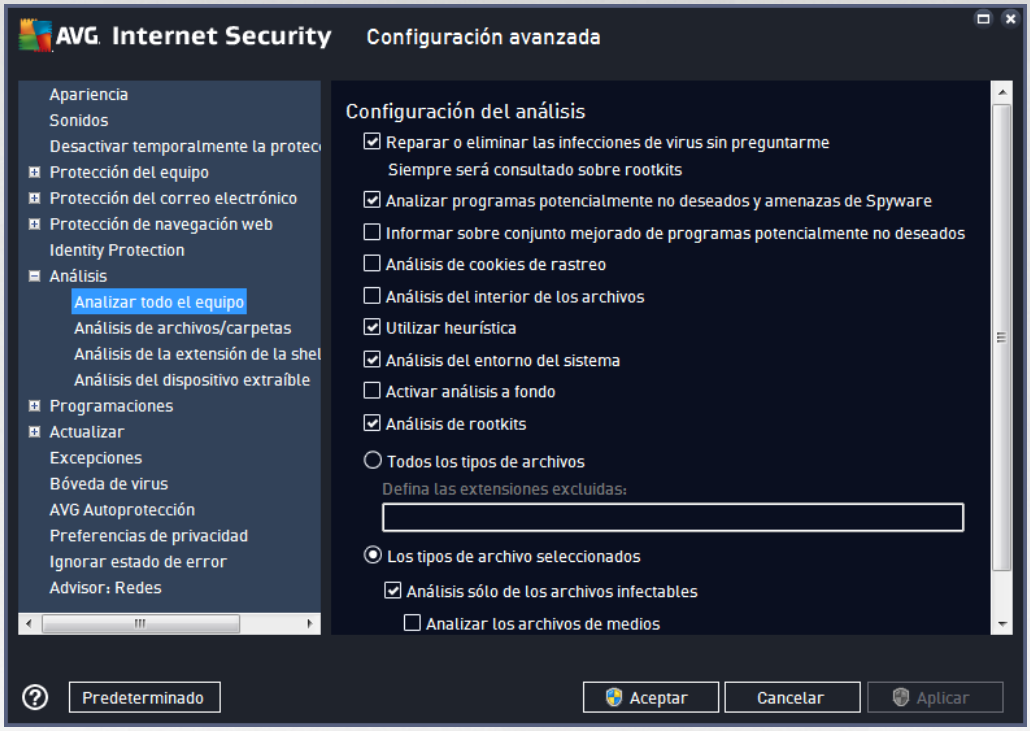
La configuración avanzada del análisis se divide en cuatro categorías con referencia a los tipos específicos de análisis definidos por el proveedor del software:

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

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

3.7.8.1. Análisis de todo el equipo

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



Configuración del análisis

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

- ***Reparar o eliminar las infecciones de virus sin preguntarme*** (*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 sobre conjunto mejorado de programas potencialmente no deseados*** (*desactivada de manera predeterminada*): marque esta opción para detectar paquetes extendidos de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear

programas legales, por lo que de forma predeterminada está desactivada.

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

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

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

- ***Analizar el entorno del sistema*** (*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.

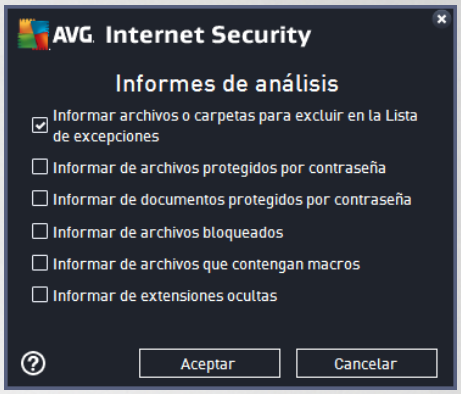
Ajustar el tiempo que tarda el análisis en completarse

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.

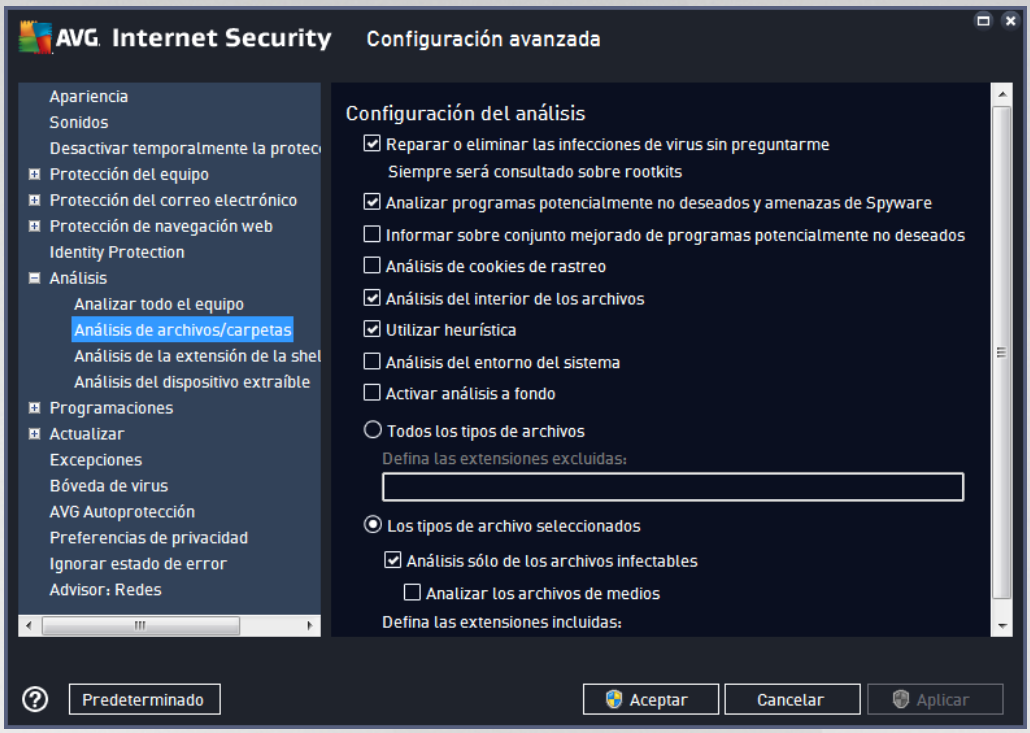
Configurar informes de análisis adicionales ...

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:



3.7.8.2. Análisis de archivos/carpetas

La interfaz de edición para ***Analizar Archivos o Carpetas Específicos*** es idéntica al cuadro de diálogo de edición Análisis completo del equipo. Todas las opciones de configuración son iguales; sin embargo, la configuración predeterminada es más estricta para el Análisis de Todo el Equipo:

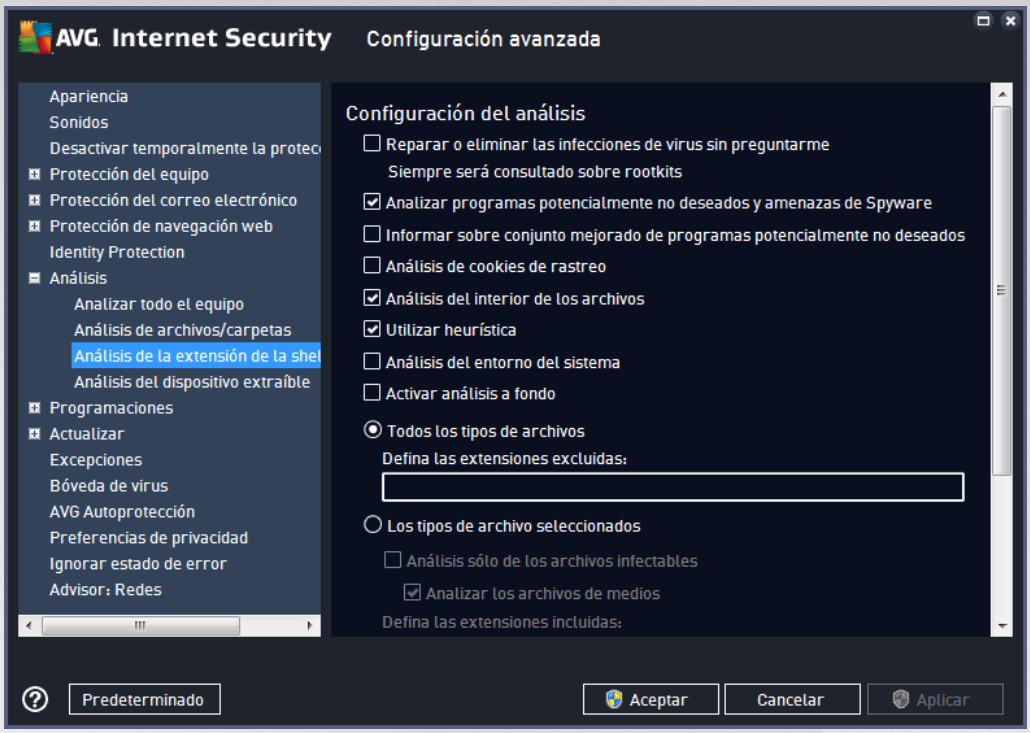


Todos los parámetros definidos en este diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con Análisis de archivos o carpetas específicos.

Nota: *para obtener una descripción de los parámetros específicos, consulte el capítulo Configuración Avanzada de AVG / Análisis / Análisis Completo del Equipo.*

3.7.8.3. Análisis de la extensión de la shell

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



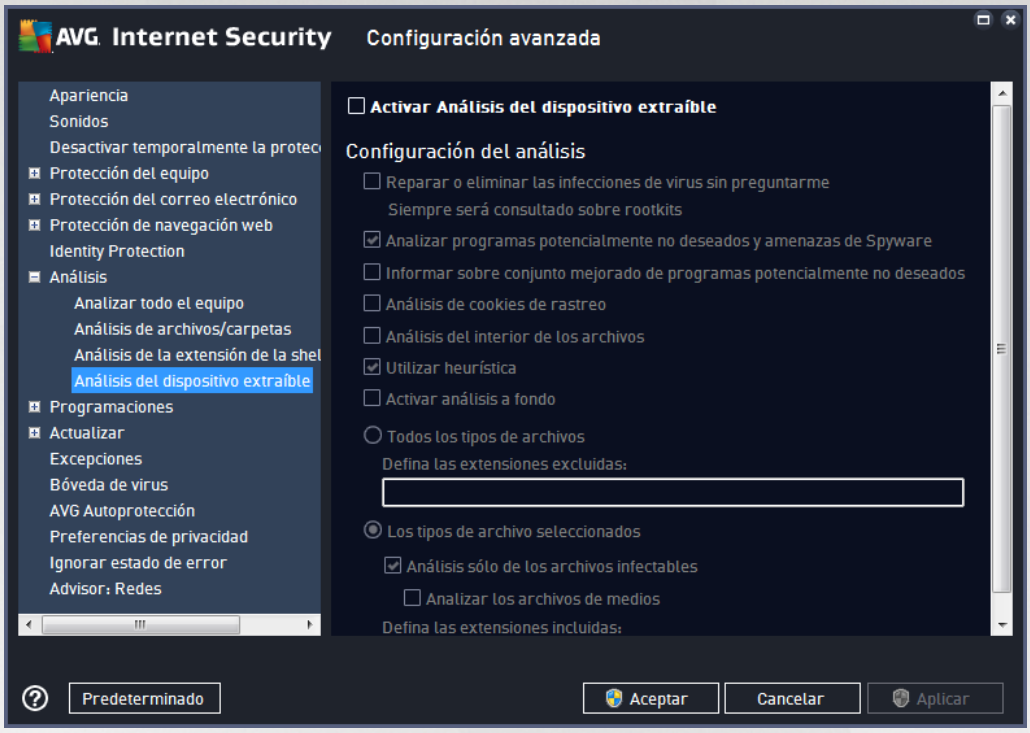
La lista de parámetros muestra parámetros idénticos a los que están disponibles para Analizar Todo el Equipo. Sin embargo, la configuración predeterminada es diferente (*por ejemplo, el análisis de todo el equipo no comprueba de manera predeterminada los archivos, pero sí analiza el entorno del sistema,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

Nota: *para obtener una descripción de los parámetros específicos, consulte el capítulo Configuración Avanzada de AVG / Análisis / Análisis Completo del Equipo.*

En comparación con el cuadro de diálogo Análisis Completo del Equipo, el cuadro de diálogo ***Análisis de Extensión de Consola*** también incluye la sección denominada ***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.

3.7.8.4. Análisis del dispositivo extraíble

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



El ***Análisis del dispositivo extraíble*** se inicia automáticamente cada vez que conecta algún dispositivo extraíble a 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 Completo del equipo.*

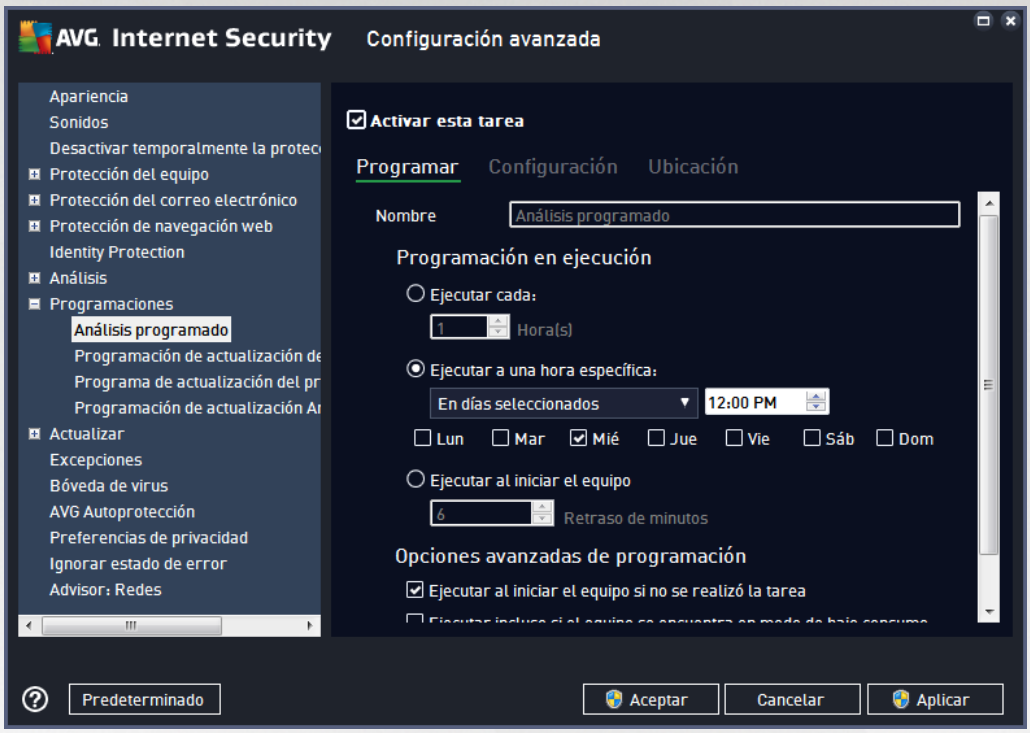
3.7.9. Programaciones

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

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

3.7.9.1. Análisis programado

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



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

Ejemplo: *No es adecuado llamar al análisis por el nombre "Nuevo análisis" o "Mi análisis" ya que estos nombres no hacen referencia a lo que el análisis realmente 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 sólo 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:

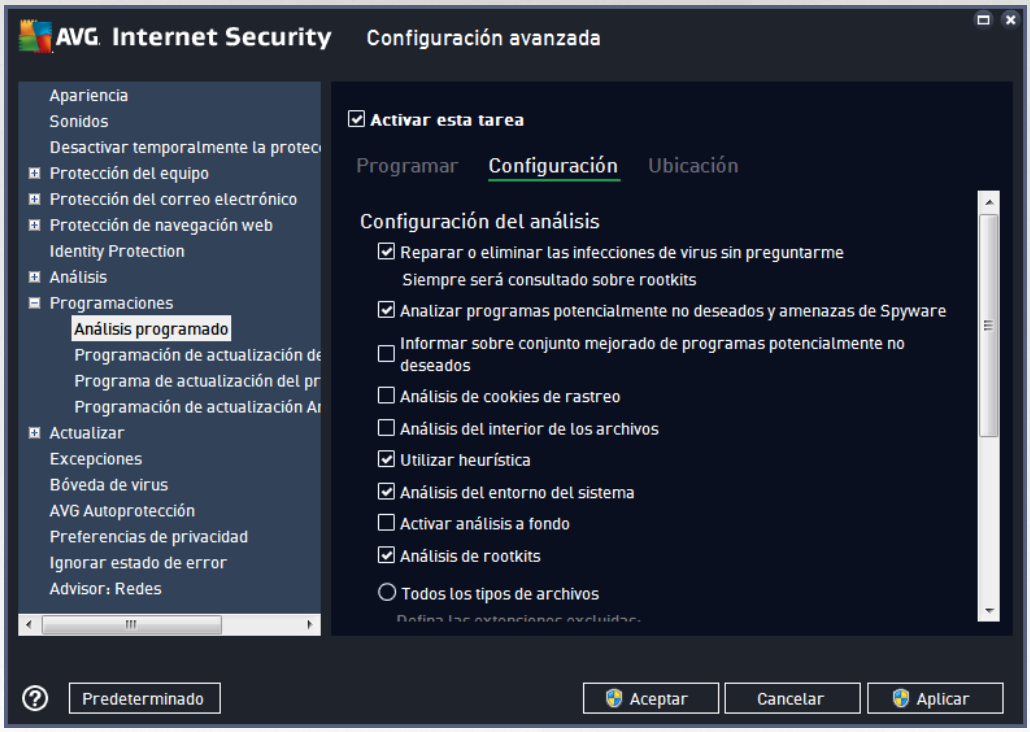
Programación en ejecución

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

Opciones avanzadas de programación

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

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



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

- ***Reparar 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 rastreo y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de sus carritos de compras electrónicos*).

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

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

- ***Análisis del entorno del sistema*** (*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.

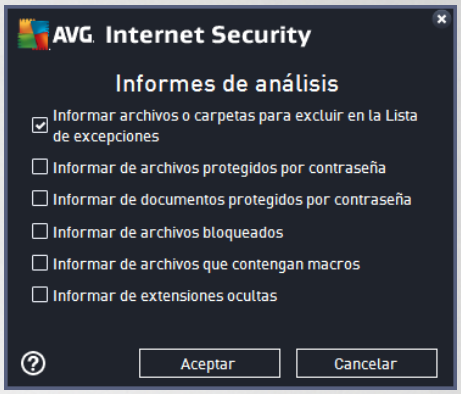
Ajustar el tiempo que tarda el análisis en completarse

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:



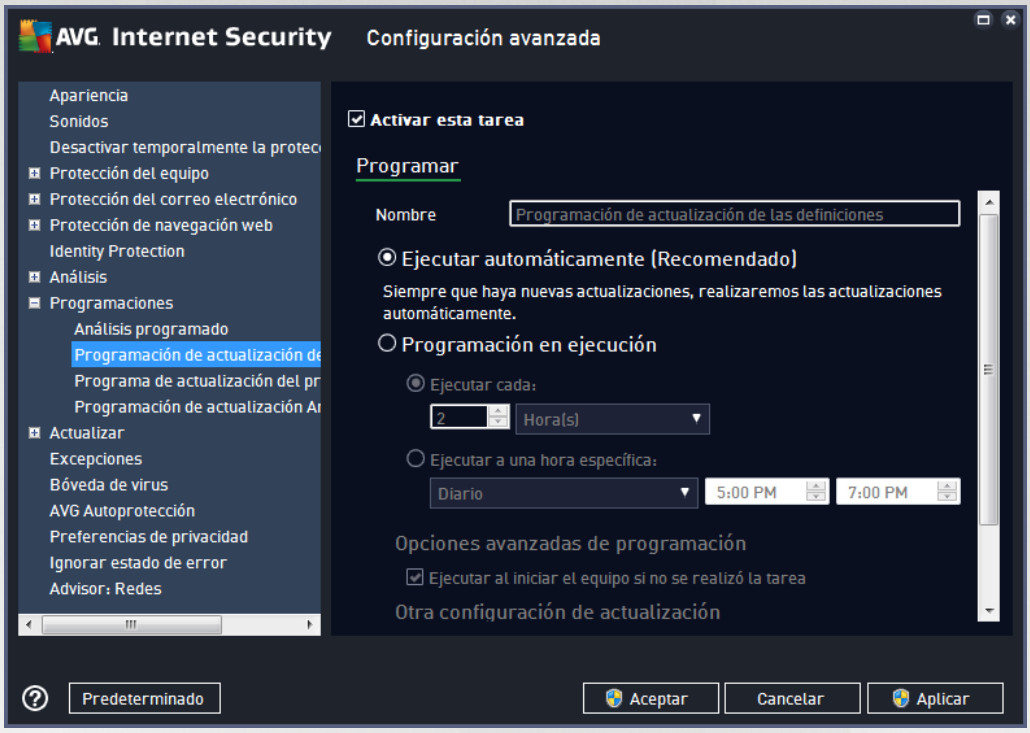
Opciones de apagado del equipo

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.

3.7.9.2. Programación de actualización de las definiciones

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



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

Programación en ejecución

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

Opciones avanzadas de programación

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

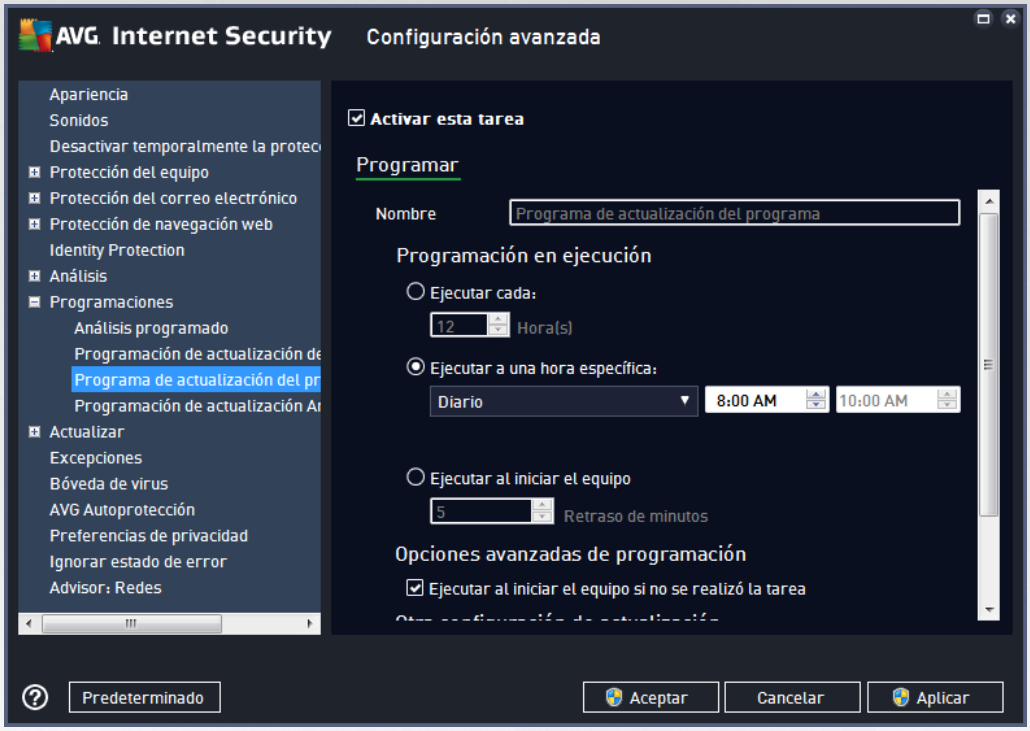
Otra configuración de actualización

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

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

3.7.9.3. 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 período de tiempo (***Ejecutar cada***) o definiendo una fecha y hora exactas (***Ejecutar en horas específicas***), o también definiendo un evento con el que se debe asociar la ejecución de la actualización (***Ejecutar al iniciar el 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

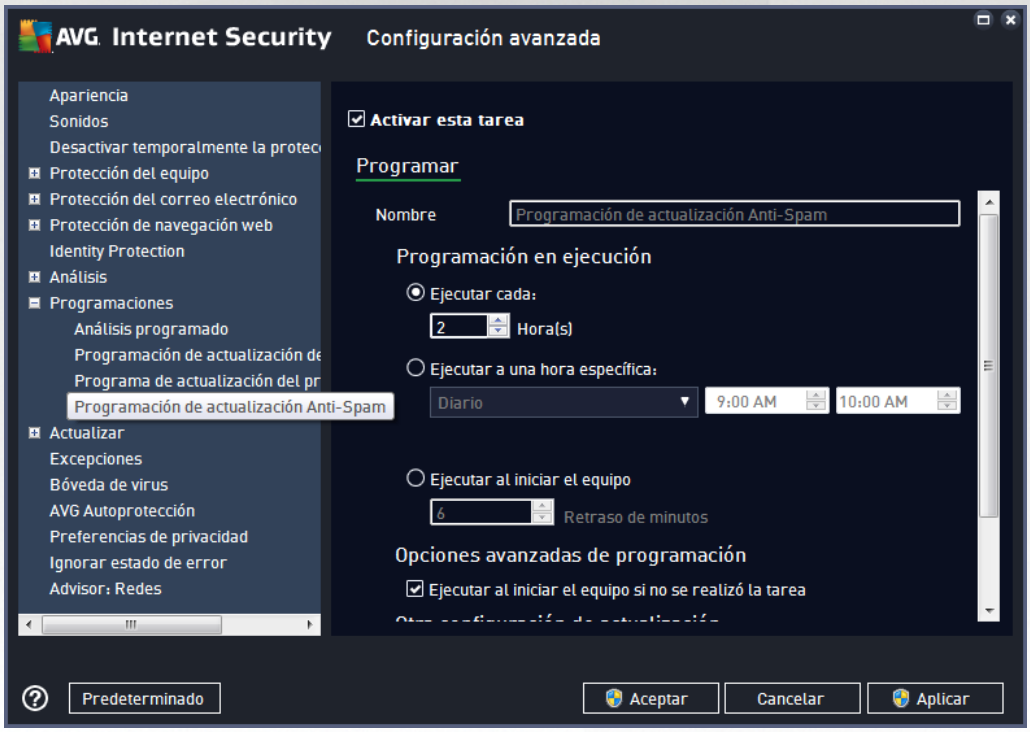
Marque la opción ***Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet*** para asegurarse de que, si se interrumpe la conexión a Internet y el proceso de actualización de Anti-

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 mayor prioridad y, por consiguiente, se interrumpirá el proceso de análisis. En ese caso, se le informará acerca del conflicto.*

3.7.9.4. Programación de actualización de Anti-Spam

Si es realmente necesario, puede quitar la marca del elemento ***Activar esta tarea*** para desactivar de forma temporal la actualización de Anti-Spam programada 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 todas las programaciones predeterminadas*) indica el nombre asignado a esta programación por proveedor de programación.

Programación en ejecución

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

Opciones avanzadas de programación

Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización de Anti-Spam si el

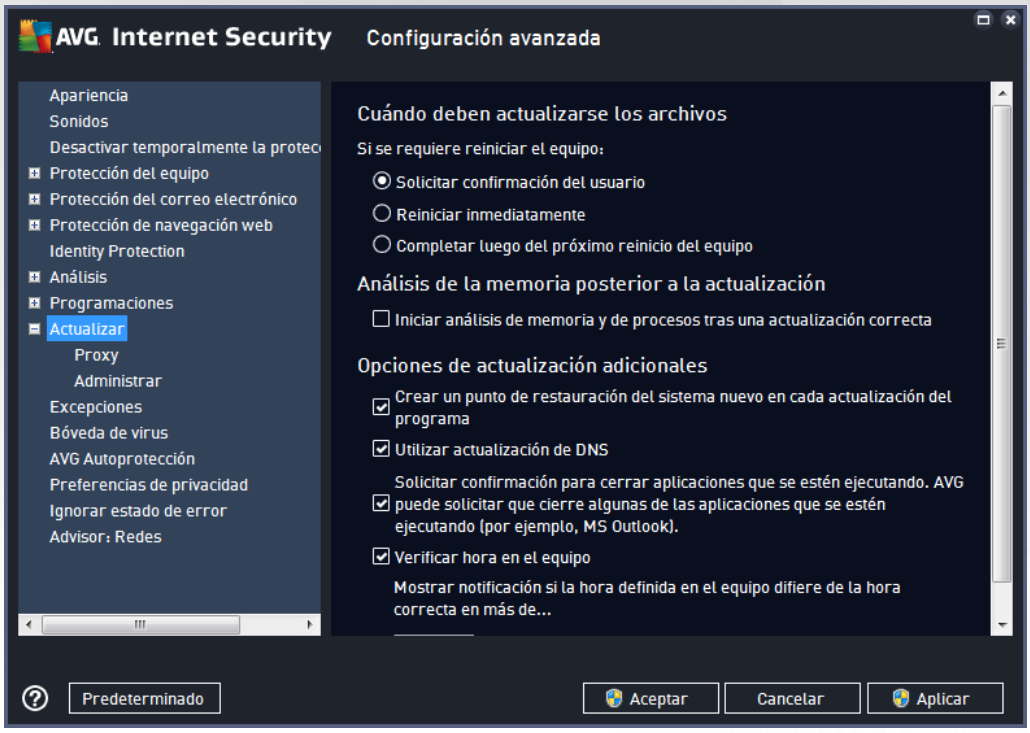
equipo se encuentra en modo de alimentación baja o totalmente apagado.

Otra configuración de actualización

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

3.7.10. Actualizar

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



Cuándo deben actualizarse los archivos

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

- ***Solicitar confirmación del usuario*** *(activada de forma predeterminada)*: se le pedirá que apruebe un reinicio 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 punto de restauración del sistema nuevo en cada actualización del programa*** (*activado de forma predeterminada*): antes de iniciar cada actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Se puede obtener acceso a esta opción mediante Inicio/Todos los programas/Accesorios/Herramientas del sistema/ Restaurar sistema, pero se recomienda que sólo los usuarios experimentados realicen cambios. Mantenga esta casilla seleccionada si desea hacer uso de esta funcionalidad.

- ***Utilizar actualización de DNS*** (*activado de manera predeterminada*): si este elemento está marcado, una vez que se inicia la actualización, su **AVG Internet Security 2015** 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 en el equipo*** (*activado de forma predeterminada*): 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.

3.7.10.1. 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.

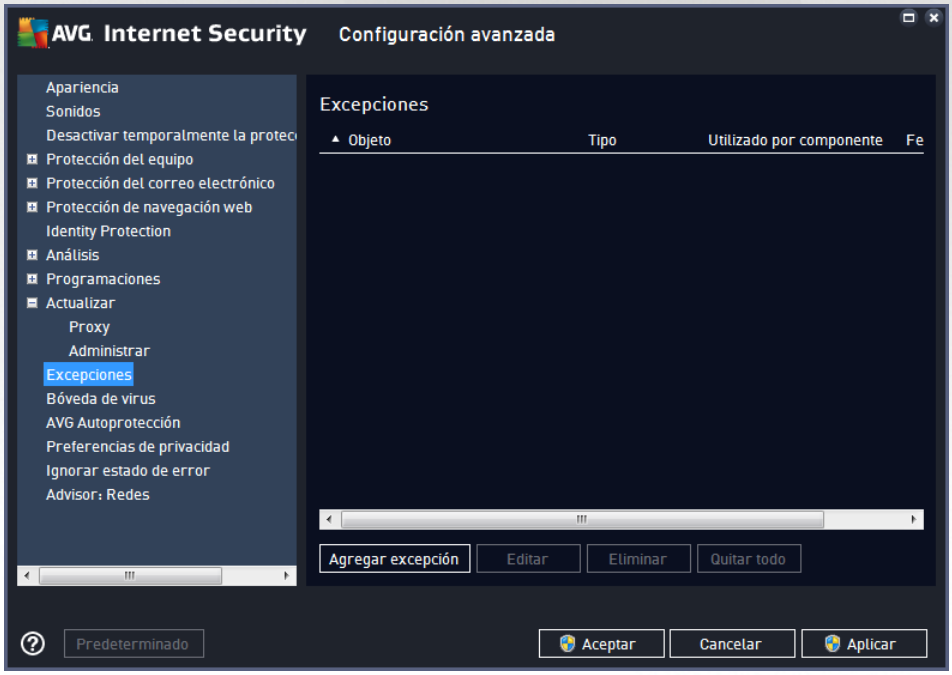
Configuración automática

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

3.7.10.2. Administrar

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

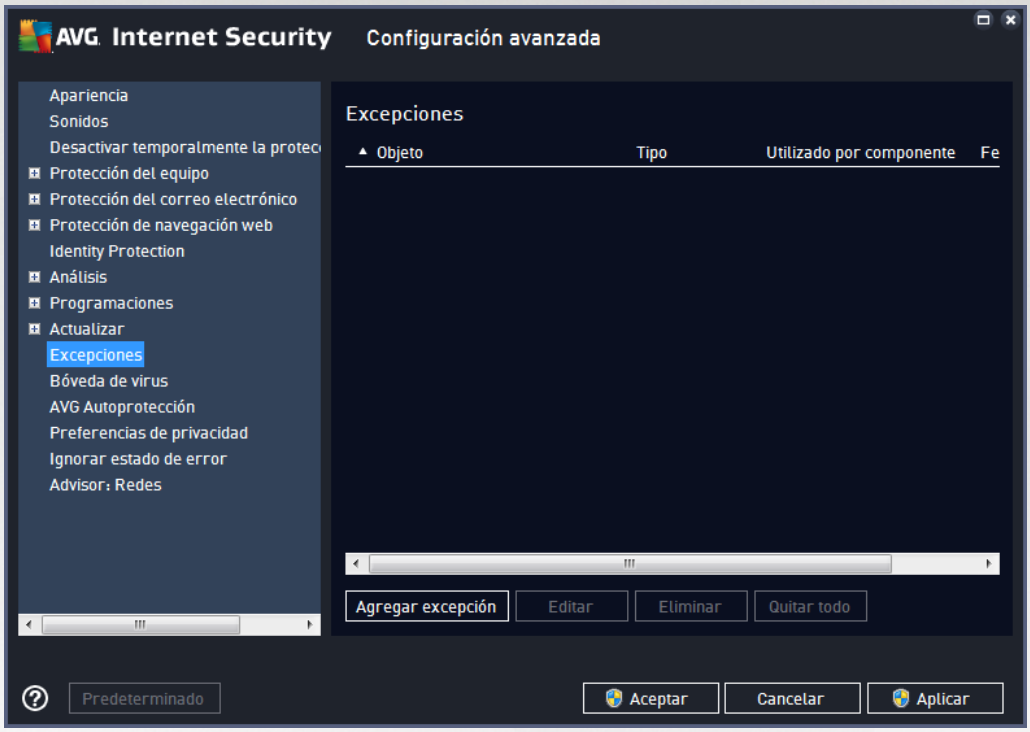


- ***Eliminar archivos de actualización temporales***: presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada estos archivos se guardan durante 30 días*)
- ***Revertir la base de datos de virus a la versión anterior***: presione este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

3.7.11. Excepciones

En el cuadro de diálogo ***Excepciones*** puede definir excepciones, es decir, elementos que **AVG Internet Security 2015** ignorará. Generalmente, deberá definir una excepción si AVG continúa detectando un programa o archivo como amenaza, o bloqueando un sitio web seguro como peligroso. Agregue ese archivo o sitio web a esta lista de excepciones, y AVG no le informará sobre él ni lo bloqueará más.

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



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

Botones de control

- ***Agregar excepción***: haga clic para abrir un nuevo cuadro de diálogo donde puede especificar el elemento que debe excluirse del análisis de AVG. En primer lugar, se lo invitará a definir el tipo de objeto, es decir, si se trata de una aplicación, un archivo, una carpeta, una URL o un certificado. A continuación, deberá examinar su disco para proporcionar la ruta de acceso al objeto respectivo o escribir la URL. Finalmente, puede seleccionar las funciones de AVG que deben ignorar el objeto seleccionado *(Protección Residente, Identity Protection, Análisis)*.

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

- ***Eliminar***: utilice este botón para cancelar una excepción previamente definida. Puede eliminarlas una por una, o resaltar un bloque de excepciones en la lista y cancelar las excepciones definidas. Después de cancelar la excepción, el archivo, carpeta o URL respectivo será comprobado por AVG

otra vez. Tenga en cuenta que sólo se quitará la excepción, no el archivo ni la carpeta.

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

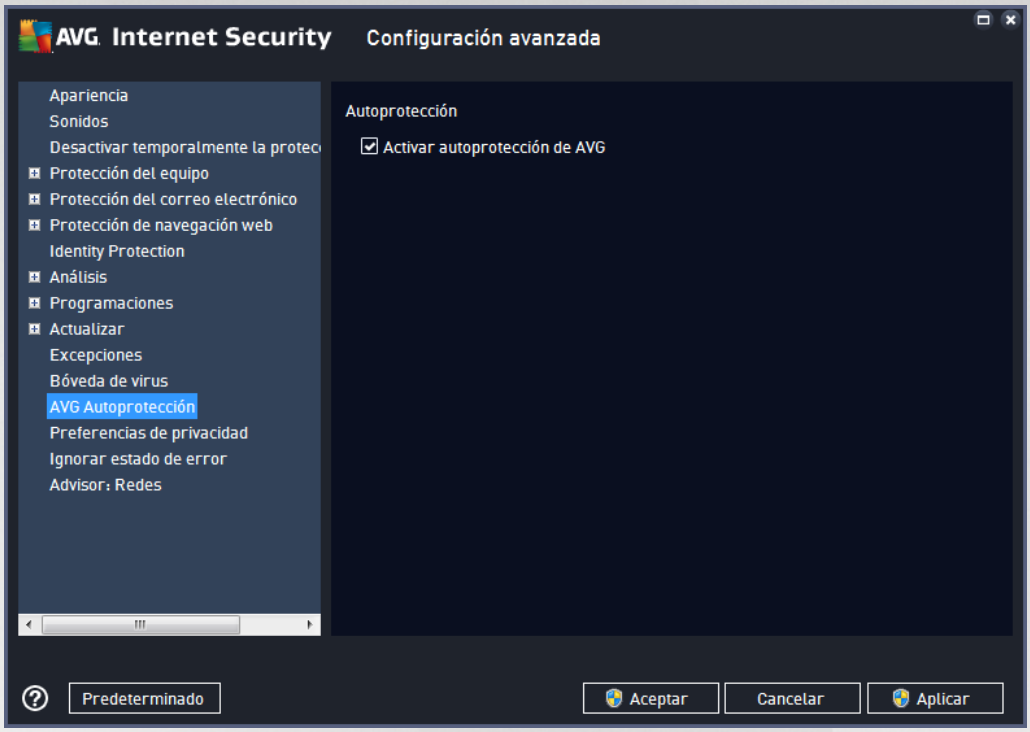
3.7.12. Bóveda de virus

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

- ***Limitar el Tamaño de la Bóveda de virus***: utilice el control deslizante para configurar el tamaño máximo de la Bóveda de Virus. El tamaño se especifica proporcionalmente en comparación con el tamaño del disco local.

- ***Eliminación automática de archivos***: en esta sección se define la longitud máxima de tiempo que los objetos deben almacenarse en la Bóveda de virus (***Eliminar archivos 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***).

3.7.13. Autoprotección AVG

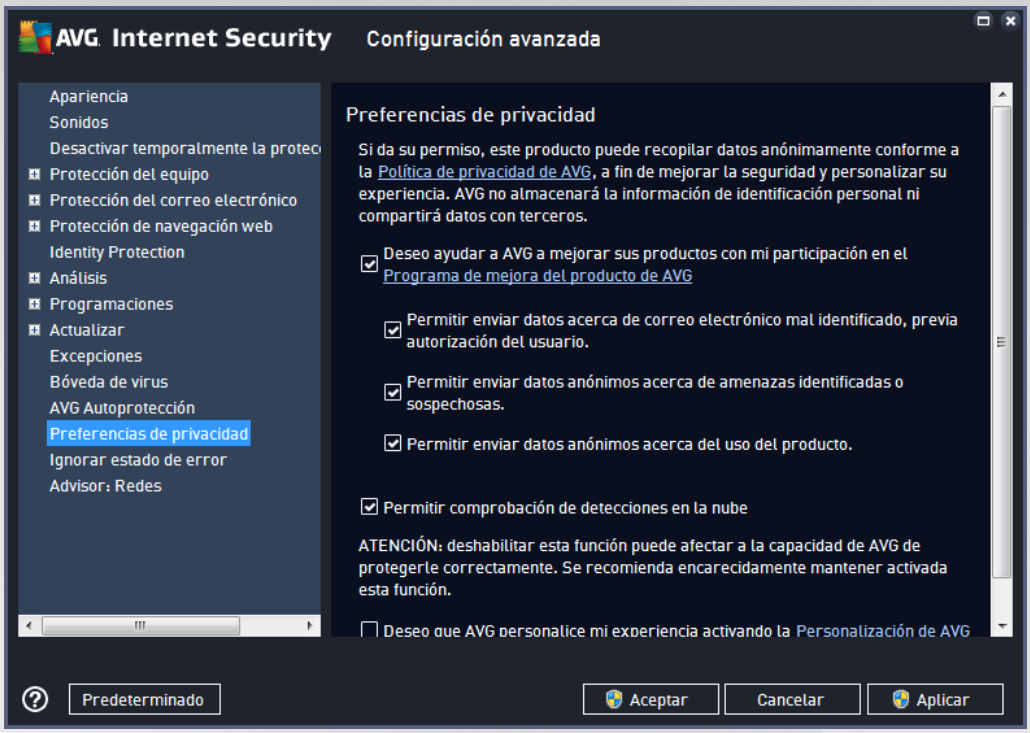


El elemento ***Autoprotección de AVG*** permite que **AVG Internet Security 2015** proteja sus propios procesos, archivos, claves de registro y controladores para que no se modifiquen ni desactiven. La razón principal para esta clase de protección es que algunas amenazas sofisticadas intentan desactivar la protección antivirus, y luego causan daño a su equipo libremente.

Recomendamos que esta función se mantenga activada.

3.7.14. Preferencias de privacidad

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



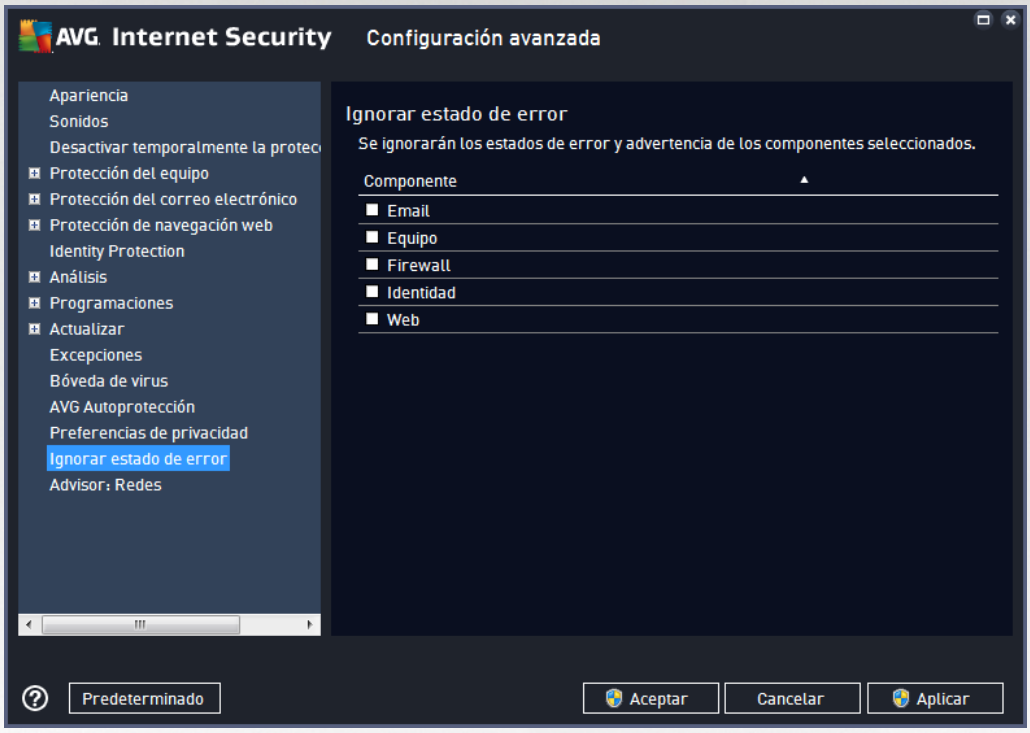
En el cuadro de diálogo, están disponibles las siguientes opciones de configuración:

- ***Deseo ayudar a AVG a mejorar 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 Internet Security 2015**, 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.
    - ***Permitir enviar datos acerca de correo electrónico mal identificado, previa autorización del usuario*** *(activada de forma predeterminada)*: envíe información sobre mensajes de correo electrónico identificados incorrectamente como spam, o sobre mensajes de spam no detectados por el servicio Anti-Spam. Al enviar este tipo de información, se 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 activando la Personalización de AVG*** *(desactivada de manera predeterminada)*: 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.

3.7.15. Ignorar estado de error

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



De manera predeterminada, ningún componente está seleccionado en esta lista. 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.

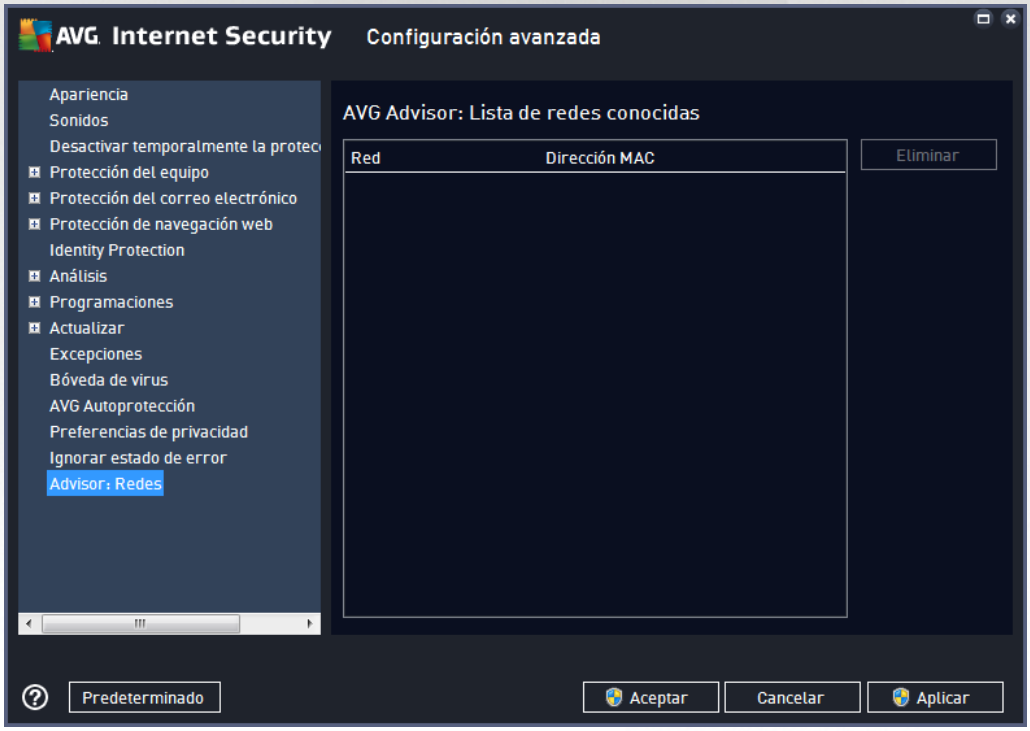
Para esta situación, dentro del cuadro de diálogo ***Ignorar estado de error*** puede seleccionar componentes que pueden estar en un estado de error (*o desactivado*) y de los cuales no desee recibir información. Presione

el botón ***Aceptar*** para confirmar.

3.7.16. 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.*

3.8. Configuración del Firewall

La configuración del Firewall se abre en una nueva ventana donde se pueden establecer parámetros muy avanzados del componente en varios cuadros de diálogo. La configuración del Firewall se abre en una nueva ventana donde puede editar los parámetros avanzados del componente en distintos cuadros de diálogo de configuración. La configuración puede mostrarse opcionalmente en el modo básico o experto. Cuando ingresa por primera vez a la ventana de configuración, se abre en la versión básica y proporciona opciones de edición de los siguientes parámetros:

- General

- Aplicaciones
- Uso compartido de archivos e impresoras

En la parte inferior del cuadro de diálogo podrá ver el botón ***Modo experto***. Presione el botón para mostrar otros elementos del cuadro de diálogo para una configuración de Firewall muy avanzada:

- Configuración avanzada
- Redes definidas
- Servicios de sistema
- Registros

3.8.1. General

El cuadro de diálogo ***Información general*** proporciona una descripción general de todos los modos de Firewall disponibles. La selección actual del modo de Firewall puede cambiarse si selecciona otro modo en el menú.

No obstante, el proveedor del software ha configurado todos los componentes de AVG Internet Security 2015 para que ofrezcan un rendimiento óptimo. No modifique la configuración predeterminada salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cambios en la configuración!

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

- ***Automático***: en este modo, el Firewall maneja todas las redes de tráfico automáticamente. No se lo invitará a tomar decisiones. El Firewall permitirá la conexión para cada aplicación conocida y, al mismo tiempo, creará una regla para la aplicación que especifique que ésta siempre puede conectarse en el futuro. Para otras aplicaciones, el Firewall decidirá si se debe permitir la conexión o bloquearla en función del comportamiento de la aplicación. No obstante, en este tipo de situación, no se creará la regla y la aplicación se comprobará nuevamente cuando intente conectarse. ***El modo automático es discreto y se recomienda a la mayoría de los usuarios.***

- ***Interactivo***: este modo es conveniente si desea controlar por completo todo el tráfico de la red hacia y desde su equipo. El Firewall supervisará y lo notificará sobre cada intento de comunicación o transferencia de datos, para que usted permita o bloquee el intento si lo considera adecuado. Recomendado sólo para usuarios avanzados.

- ***Bloquear acceso a internet***: la conexión a internet está bloqueada por completo, no puede acceder a internet y nadie desde afuera puede acceder a su equipo. Solamente para uso especial y breve.

- ***Desactivar la protección de Firewall***: desactivar el Firewall permitirá todo el tráfico de la red hacia y desde su equipo. En consecuencia, esto lo hará vulnerable a los ataques de los hackers. Siempre considere esta opción cuidadosamente.

Tenga en cuenta un modo automático específico disponible también dentro del Firewall. Este modo se activa de manera silenciosa si se desactivan los componentes Equipo o Identity Protection y, por lo tanto, su equipo es más vulnerable. En estos casos, el Firewall sólo permitirá automáticamente aplicaciones conocidas y absolutamente seguras. Para todas las demás, le solicitará que tome una decisión. Esto se realiza para compensar los componentes de protección desactivados y mantener la seguridad de su equipo.

3.8.2. Aplicaciones

El cuadro de diálogo ***Aplicación*** enumera todas las aplicaciones que intentaron comunicarse utilizando la red, y los iconos para la acción asignada:

Las aplicaciones de la ***Lista de aplicaciones*** son las que se detectaron en su equipo (*y a las que se*

asignaron acciones respectivas). Se pueden utilizar los siguientes tipos de acciones:

- - permitir la comunicación para todas las redes
- - bloquear la comunicación
- - configuración avanzada definida

Tenga en cuenta que sólo se pueden detectar las aplicaciones ya instaladas. De manera predeterminada, cuando la aplicación nueva intenta conectarse a través de la red por primera vez, el Firewall crea una regla automáticamente de acuerdo con la Base de datos confiable o le solicita que confirme si desea permitir o bloquear la comunicación. En el segundo caso, podrá guardar la respuesta como regla permanente (que se mostrará entonces en este cuadro de diálogo).

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

Además de las aplicaciones, la lista también contiene dos elementos especiales. ***Las reglas prioritarias de aplicaciones*** (*en la parte superior de la lista*) son preferenciales y siempre se aplican antes que las reglas específicas de las aplicaciones. ***Otras reglas de aplicaciones*** (*en la parte inferior de la lista*) se utilizan como "último recurso" cuando no se aplican reglas específicas para la aplicación, por ejemplo, para una aplicación desconocida e indefinida. Seleccione la acción que debe activarse cuando dicha aplicación intente comunicarse a través de la red: Bloquear *(la comunicación se bloqueará siempre)*, Permitir *(la comunicación se permitirá en cualquier red)*, Preguntar *(se le invitará a decidir si la comunicación debe permitirse o bloquearse)*. ***Estos elementos tienen opciones de configuración diferentes a las de las aplicaciones comunes y sólo deben utilizarlos los usuarios experimentados. Se recomienda encarecidamente no modificar la configuración.***

Botones de control

La lista puede editarse utilizando los siguientes botones de control:

- ***Agregar***: abre un cuadro de diálogo para definir nuevas reglas de aplicación.
- ***Editar***: abre el mismo cuadro de diálogo con los datos proporcionados para editar el conjunto de reglas de una aplicación existente.
- ***Eliminar***: elimina la aplicación seleccionada de la lista.

3.8.3. Uso compartido de archivos e impresoras

El uso compartido de archivos e impresoras significa en realidad el uso compartido de archivos o carpetas que marque como "Compartidas" en Windows, unidades de disco comunes, impresoras, escáneres y dispositivos similares. El uso compartido de tales elementos es deseable dentro de redes que pueden considerarse seguras *(por ejemplo en el hogar, en el trabajo o en la escuela)*. Sin embargo, si está conectado a una red pública *(como la conexión wi-fi de un aeropuerto o la de un café con Internet)*, probablemente no desee compartir nada. AVG Firewall puede bloquear fácilmente o permitir el uso compartido y le permite guardar su elección para las redes que ya visitó.

En el cuadro de diálogo ***Uso compartido de archivos e impresoras*** puede editar la configuración del uso compartido de archivos e impresoras, y las redes conectadas actualmente. Con Windows XP, el nombre de la red responde a la denominación que elija para la red específica cuando se conecte por primera vez. Con Windows Vista y superior, el nombre de la red se toma automáticamente del Centro de redes y recursos compartidos.

3.8.4. Configuración avanzada

Las ediciones dentro del cuadro de diálogo Configuración avanzada deben realizarse SÓLO POR USUARIOS EXPERIMENTADOS.

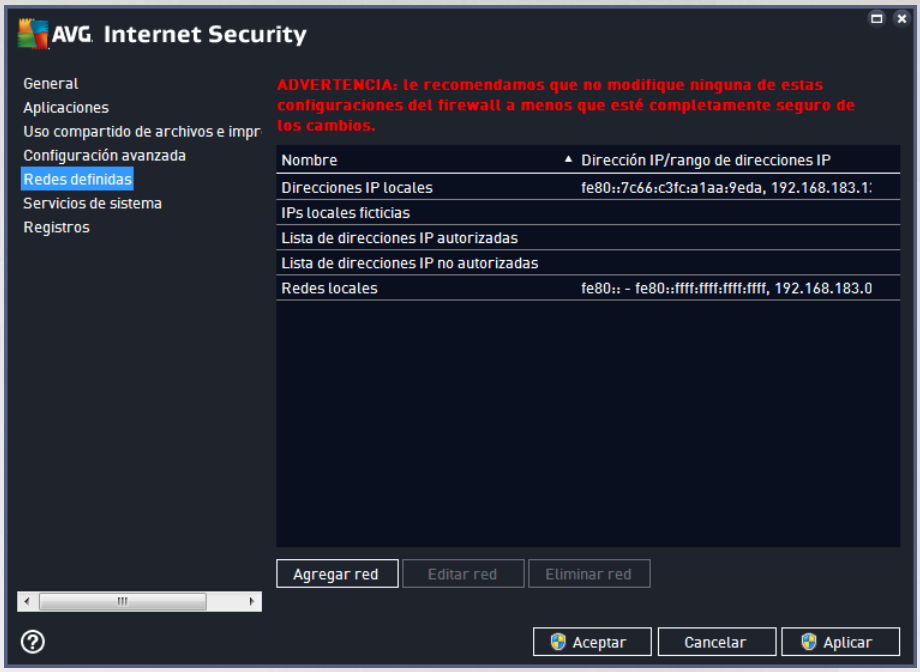
El cuadro de diálogo ***Configuración avanzada*** le permite activar o desactivar los siguientes parámetros de Firewall:

- ***Permitir todo tráfico desde y hacia máquinas virtuales que admite el Firewall***: se admite la conexión de red en máquinas virtuales como VMware.
- ***Permitir cualquier tráfico a redes privadas virtuales (VPN)***: se admiten conexiones VPN *(utilizadas para conectarse a computadoras remotas)*.
- ***Registrar trafico entrante/saliente desconocido***: todos los intentos de comunicación *(entrante / saliente)* de aplicaciones desconocidas se incluirán en el registro de Firewall.
- ***Desactivar la verificación de regla para todas las reglas de aplicación***: Firewall supervisa continuamente todos los archivos cubiertos por cada regla de aplicación. Cuando se produce una modificación del archivo binario, Firewall intentará una vez más confirmar la credibilidad de la aplicación a través medios estándares, es decir, verificando su certificado, buscándola en la base de datos de aplicaciones confiables, etc. Si no se puede considerar que la aplicación sea segura, Firewall tratará la aplicación según el modo seleccionado:
  - si Firewall se ejecuta en el ***modo Automático***, se permitirá la aplicación de forma predeterminada;
  - si Firewall se ejecuta en el ***modo Interactivo***, se bloqueará la aplicación y aparecerá un cuadro de diálogo de consulta que le solicitará al usuario que decida cómo se debería tratar la aplicación.

Por supuesto que el procedimiento deseado sobre cómo tratar una aplicación específica puede definirse por separado para cada aplicación en el cuadro de diálogo Aplicaciones.

3.8.5. Redes definidas

Las ediciones dentro del cuadro de diálogo Redes definidas deben realizarse SÓLO POR USUARIOS EXPERIMENTADOS.

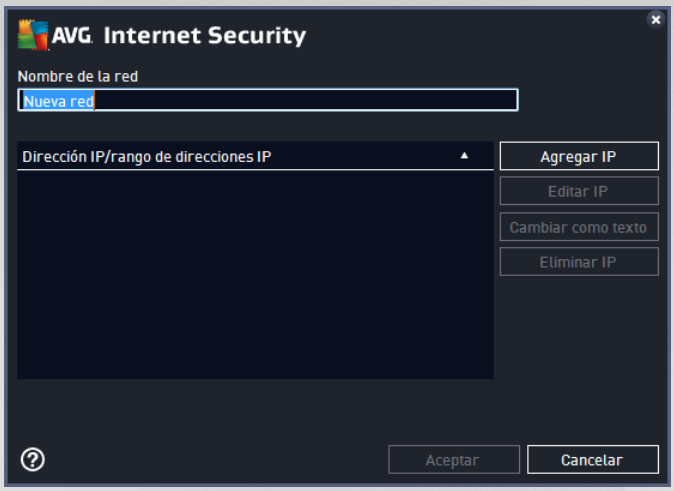


El cuadro de diálogo ***Redes definidas*** ofrece una lista de todas las redes a las que está conectado su equipo. La lista proporciona la siguiente información sobre cada red detectada:

- ***Redes***: proporciona una lista de los nombres de todas las redes a las que está conectado el equipo.
- ***Rango de direcciones IP***: cada red se detectará de forma automática y se especificará como un rango de direcciones IP.

Botones de control

- ***Agregar red***: abre una nueva ventana de diálogo donde puede editar parámetros para la red recientemente definida, es decir, proporcionar el ***nombre de la red*** y especificar el ***rango de direcciones IP***:

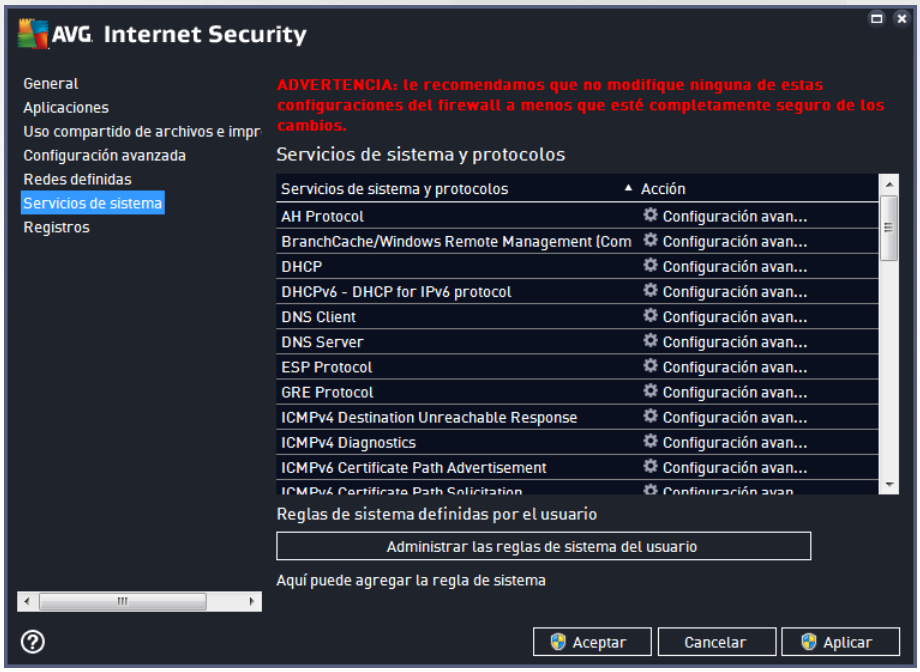


- ***Editar red***: abre la ventana del cuadro de diálogo ***Propiedades de la red*** (*ver arriba*), donde puede editar los parámetros de una red ya definida (*el cuadro de diálogo es idéntico al cuadro de diálogo para agregar una red nueva; consulte la descripción en el párrafo anterior*).

- ***Eliminar red***: elimina la referencia a una red seleccionada de la lista de redes.

3.8.6. Servicios de sistema

Se recomienda que SÓLO LOS USUARIOS EXPERTOS realicen cambios en el cuadro de diálogo Servicios de sistema y protocolos.



El cuadro de diálogo ***Servicios y protocolos de sistema*** muestra los servicios y protocolos estándar de Windows que pueden necesitar comunicarse a través de la red. La tabla tiene las siguientes columnas:

- ***La columna de servicios y protocolos del sistema*** muestra un nombre del servicio del sistema

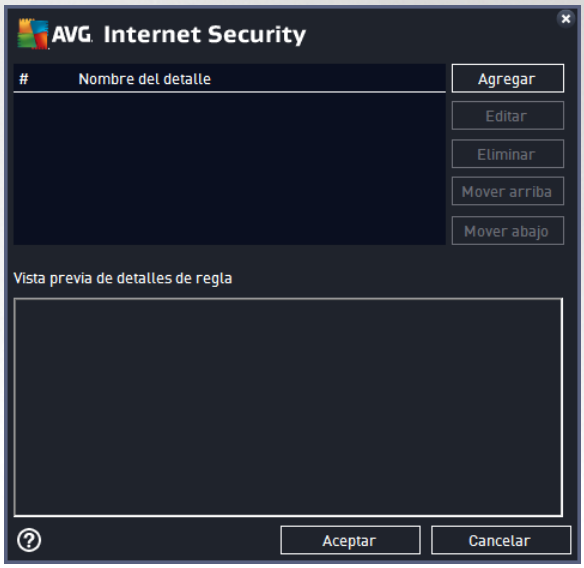
respectivo.

- ***Acción***: esta columna muestra un icono para la acción asignada:
  - o Permitir la comunicación para todas las redes
  - o Bloquear la comunicación

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

Reglas de sistema definidas por el usuario

Para abrir un cuadro de diálogo nuevo y definir su propia regla de servicio de sistema (*consulte la siguiente imagen*), presione el botón ***Administrar las reglas de sistema del usuario***. Se abre el mismo cuadro de diálogo si decide editar la configuración de cualquier elemento existente dentro de la lista de servicios y protocolos del sistema. La parte superior de este cuadro de diálogo muestra una descripción general sobre los detalles de la regla del sistema que se está editando; la sección inferior muestra el detalle seleccionado. Los detalles de una regla pueden editarse, agregarse o eliminarse mediante el botón correspondiente:



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

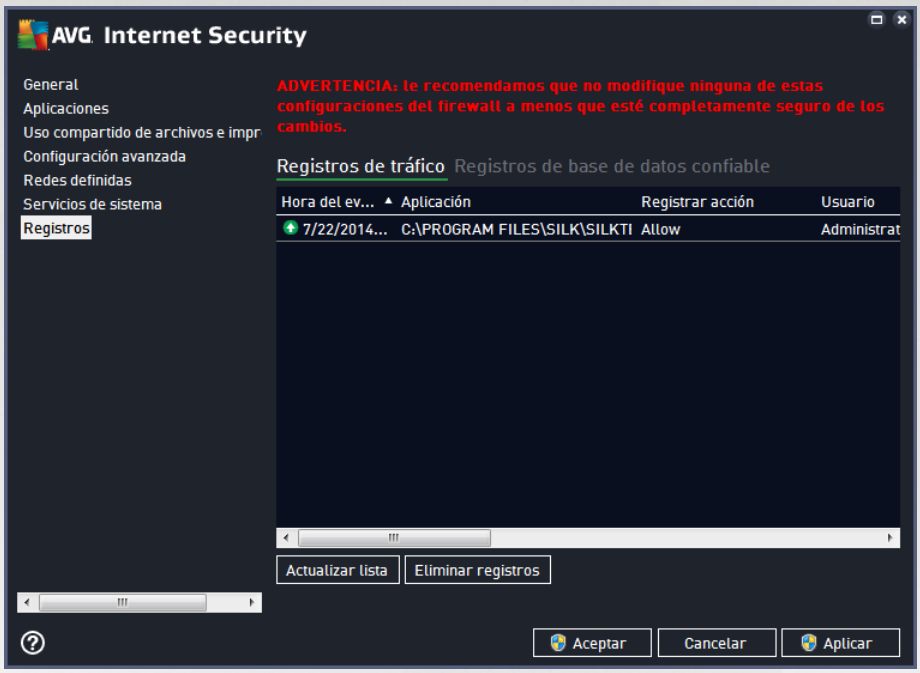
3.8.7. Registros

Las ediciones dentro del cuadro de diálogo Registros deben realizarse SÓLO POR USUARIOS EXPERIMENTADOS.

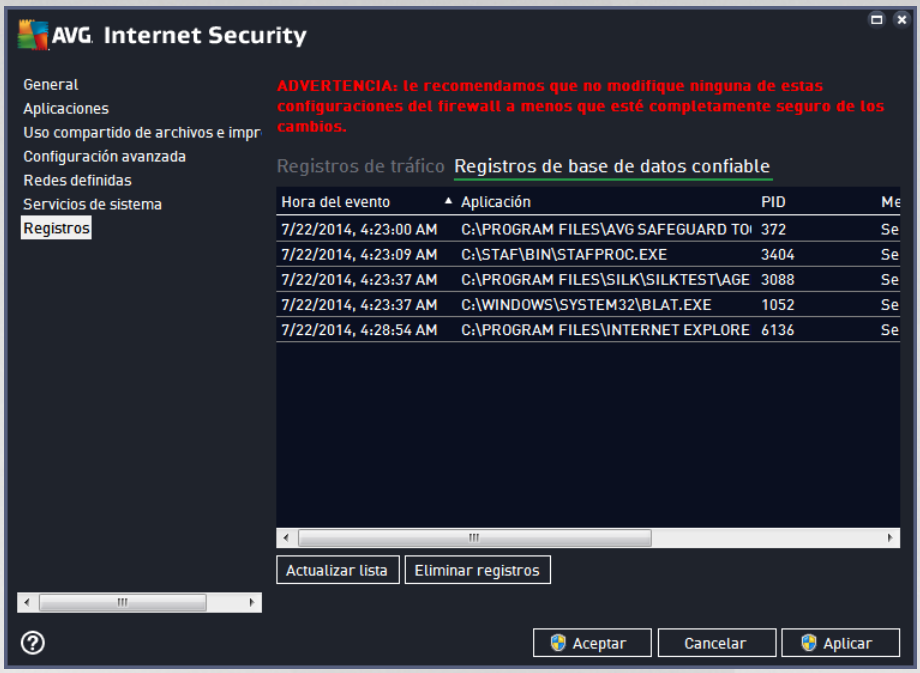
El cuadro de diálogo ***Registros*** le permite revisar la lista de todas las acciones y eventos registrados del

Firewall con una descripción detallada de los parámetros relevantes en dos pestañas:

- ***Registros de tráfico***: ofrece información acerca de las actividades de todas las aplicaciones que han intentado conectarse a la red. Encontrará para cada elemento información sobre la hora del evento, el nombre de la aplicación, la acción de registro correspondiente, el nombre de usuario, PID, dirección del tráfico, tipo de protocolo, números de los puertos remotos y locales, e información sobre la dirección IP local y remota.



- ***Registros de base de datos confiable***: la *Base de datos confiable* es la base de datos interna de AVG que recopila información acerca de aplicaciones certificadas y confiables a las que siempre se les puede permitir comunicarse en línea. La primera vez que una nueva aplicación intenta conectarse a la red (*es decir, aún no existen reglas del firewall especificadas para esta aplicación*), es necesario determinar si se le debe permitir la comunicación con la red. Primero, AVG busca en la *Base de datos confiable* y, si la aplicación se encuentra en la lista, se le concederá automáticamente acceso a la red. Sólo después de que se comprueba que no existe información disponible acerca de la aplicación en la base de datos, se le preguntará en un cuadro de diálogo independiente si desea permitir que la aplicación obtenga acceso a la red.



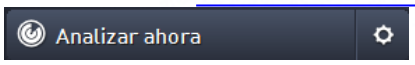
Botones de control

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

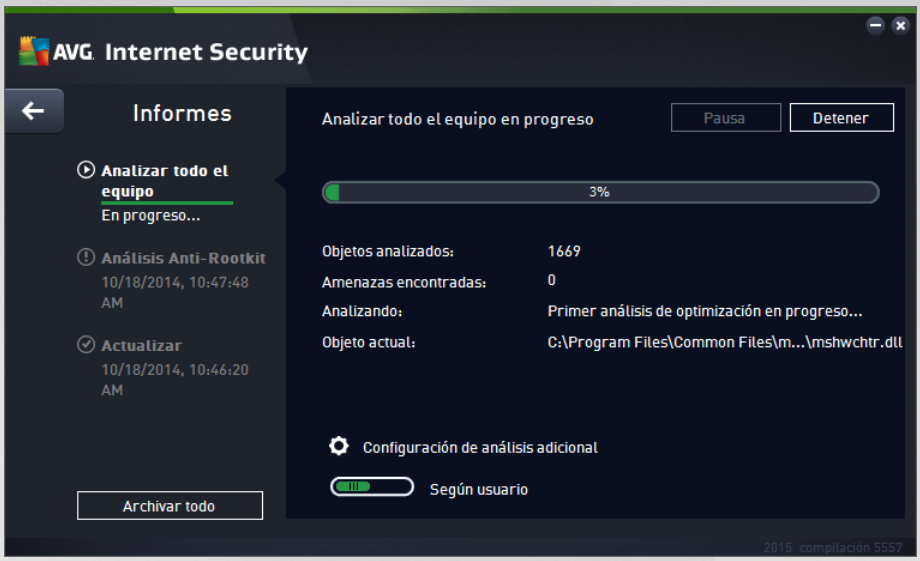
- ***Eliminar registros***: presione este botón para eliminar todas las entradas de la tabla.

3.9. Análisis de AVG

De forma predeterminada, **AVG Internet Security 2015** 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 Internet Security 2015**, 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 administrar 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*, irá al cuadro de diálogo de configuración del análisis de todo el equipo.

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

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

3.9.1. Análisis predefinidos

Una de las funciones principales de **AVG Internet Security 2015** es el análisis a pedido. Los análisis a pedido están diseñados para analizar varias partes de su equipo cuando existen sospechas de una posible infección de virus. De todas formas, se recomienda llevar a cabo dichos análisis con regularidad aun si no cree que se vayan a detectar virus en su equipo.

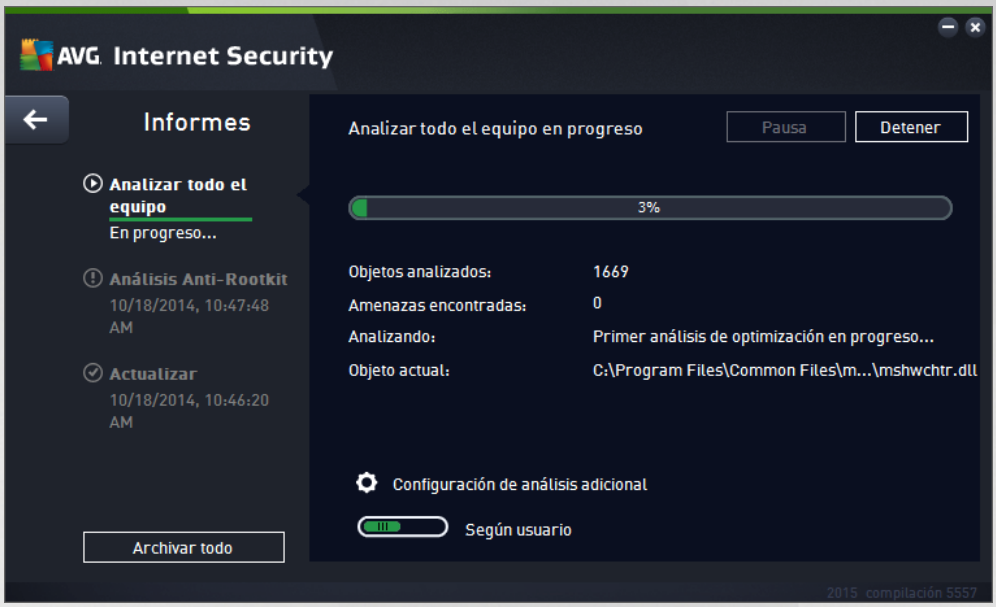
En **AVG Internet Security 2015** encontrará los siguientes tipos de análisis predefinidos por el proveedor del software:

3.9.1.1. 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.

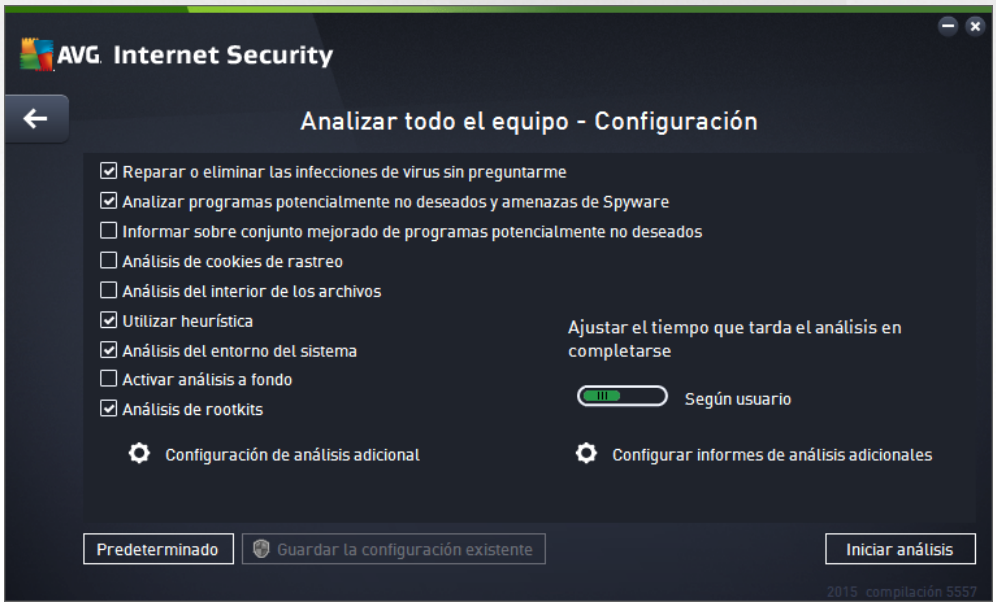
Ejecución del análisis

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 del 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, ...

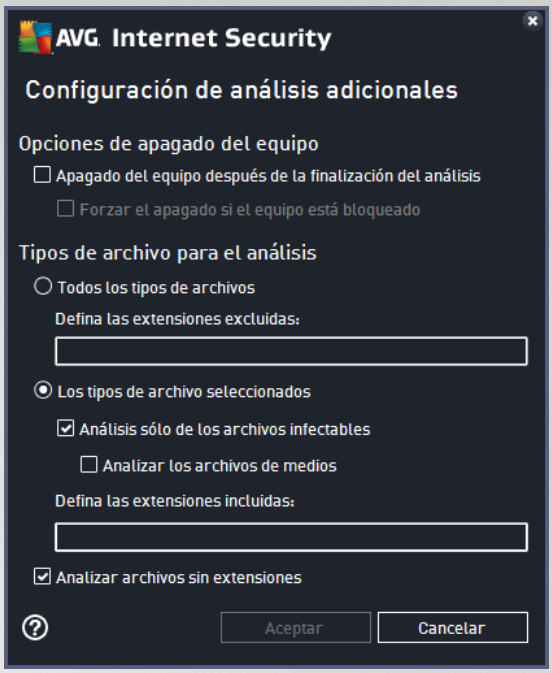
- ***Utilizar método heurístico*** (*activado de manera predeterminada*): el análisis heurístico (*la emulación dinámica de las instrucciones del objeto analizado en un entorno virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.

- ***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.

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

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



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

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

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

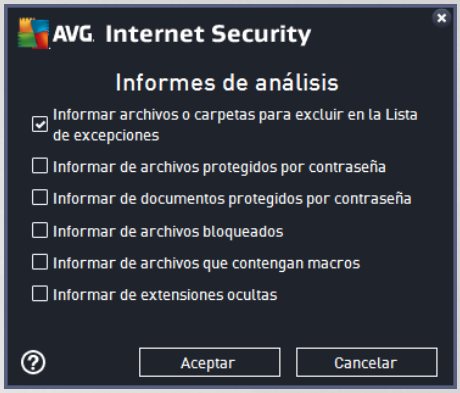
  - ***Tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos 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.*

3.9.1.2. Analizar carpetas o archivos

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

Ejecución del análisis

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

Edición de la configuración de análisis

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

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

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

- ***Analizar 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 del carrito de compras electrónico)*.

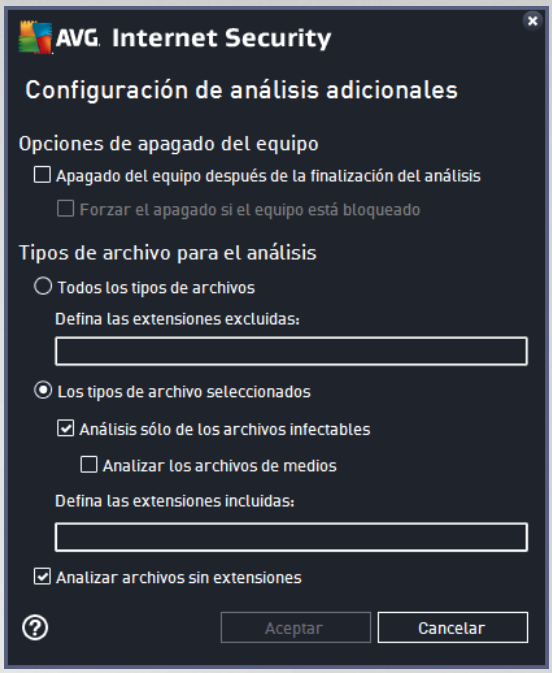
- ***Análisis del interior de los archivos*** (*activado de forma predeterminada*): Este parámetro define que el análisis debe comprobar todos los archivos almacenados dentro de archivos, por ej., ZIP, RAR, ...

- ***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;

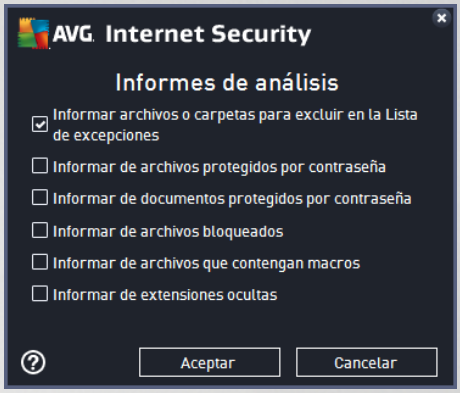
  - ***Tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos 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:



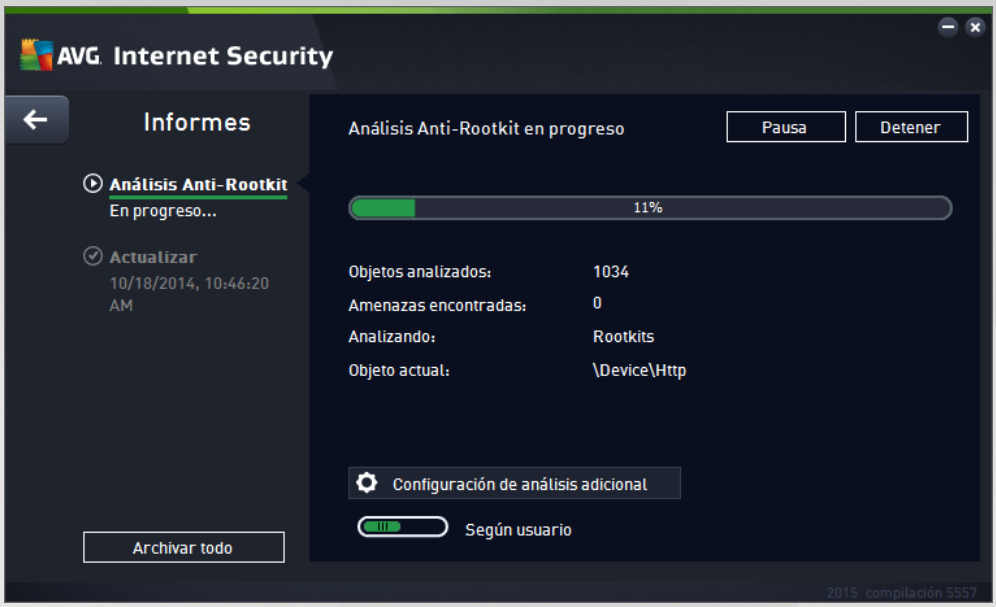
Advertencia: *Estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo Análisis de AVG / Programación de análisis / Cómo analizar. Si decide cambiar la configuración predeterminada de* ***Analizar carpetas o archivos específicos*** *puede guardar 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).*

3.9.1.3. Análisis del equipo en busca de rootkits

Analizar el equipo en busca de rootkits detecta y elimina con eficacia los rootkits peligrosos, es decir, los programas y las tecnologías que pueden camuflar la presencia de software malicioso en 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. El análisis puede detectar rootkits según un conjunto de reglas predefinido. Si se detecta un rootkit, no significa necesariamente que el equipo esté infectado. En ocasiones, los rootkits se utilizan como controladores o forman parte de aplicaciones correctas.

Ejecución del análisis

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



Edición de la configuración de análisis

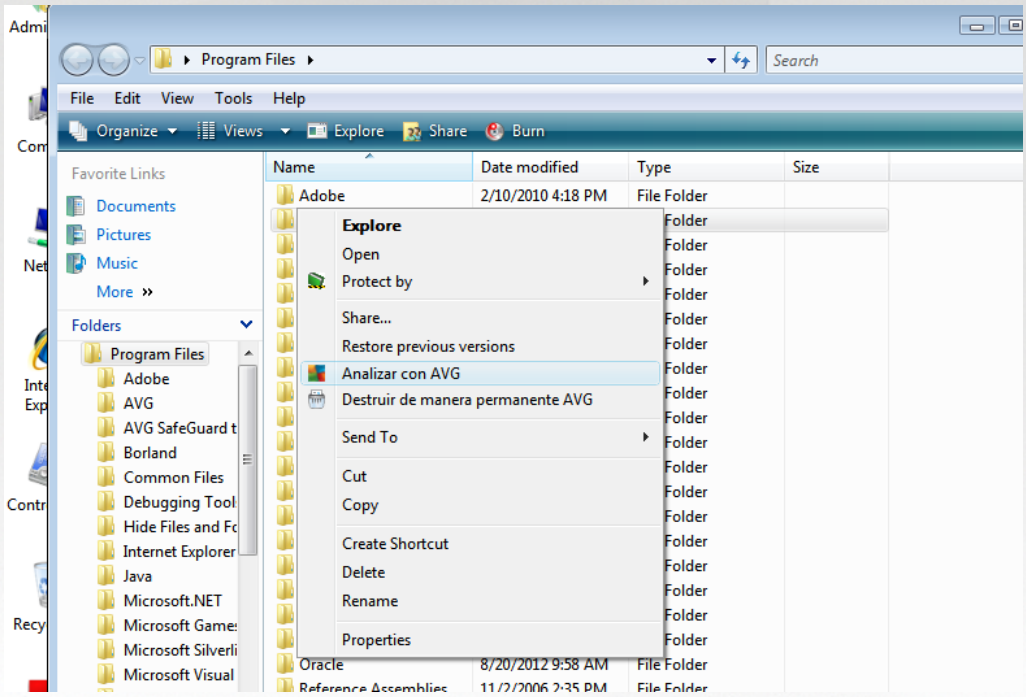
Puede editar la configuración del análisis Anti-Rootkit en el cuadro de diálogo ***Configuración Anti-Rootkit*** *(el cuadro de diálogo está disponible a través del vínculo Configuración para el análisis Analizar el equipo en busca de rootkits dentro del cuadro de diálogo Opciones de análisis).* ***Se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

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

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

3.9.2. Análisis en el Explorador de Windows

Además de los análisis predefinidos ejecutados para todo el equipo o sus áreas seleccionadas, **AVG Internet Security 2015** 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 Internet Security 2015**

3.9.3. Análisis desde línea de comandos

En **AVG Internet Security 2015** 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.

3.9.3.1. 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/

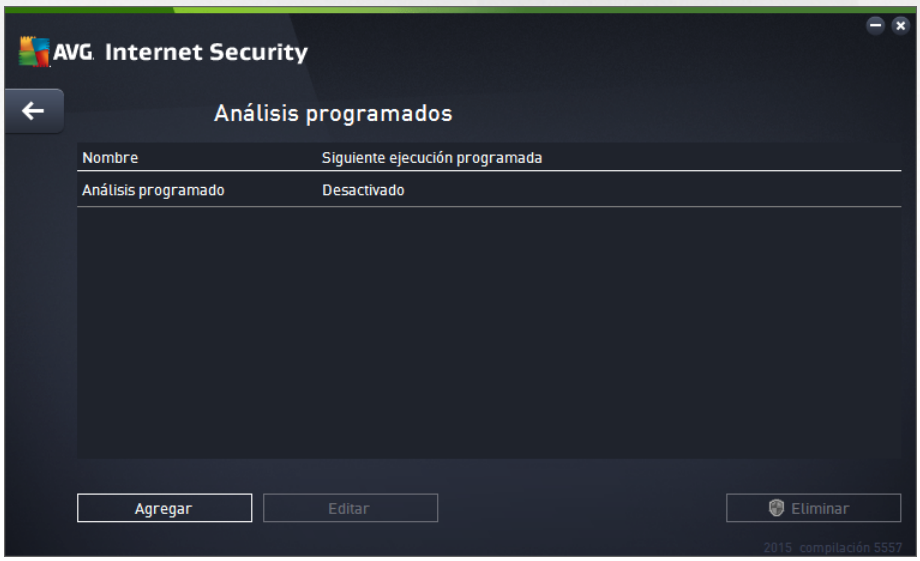
- /EXT Analizar estas extensiones /por ejemplo EXT=EXE,DLL/
- /NOEXT No analizar estas extensiones /por ejemplo NOEXT=JPG/
- /ARC Analizar archivos
- /CLEAN Borrar automáticamente
- /TRASH Mover los archivos infectados a la Bóveda de virus
- /QT Análisis rápido
- /LOG Generar un archivo de los resultados 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

3.9.4. Programación de análisis

Con **AVG Internet Security 2015** 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:



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

- 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.

3.9.4.1. Programar

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

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

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

3.9.4.2. 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 rastreo y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de sus carritos de compras electrónicos*).

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

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

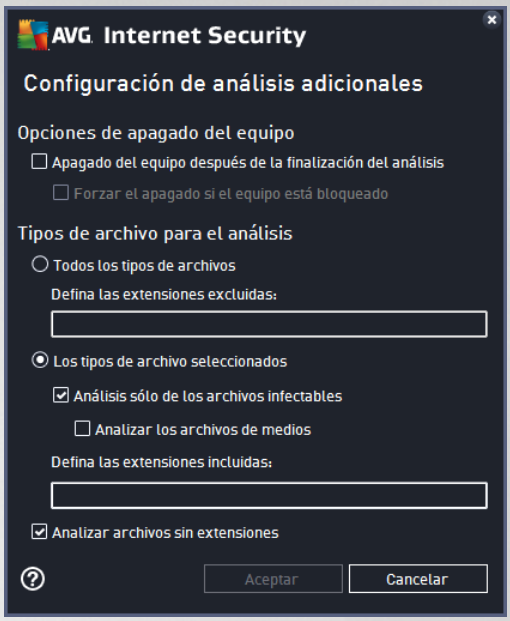
- ***Análisis del entorno del sistema*** (*activado de forma predeterminada*): el análisis también comprobará las áreas del sistema del equipo.

- ***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:

    - o ***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.

    - o ***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.

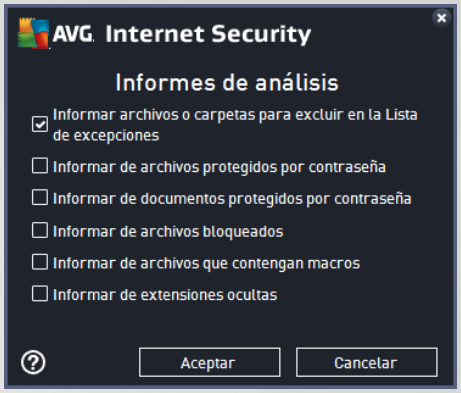
    - o De manera opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben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

3.9.4.3. 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*)

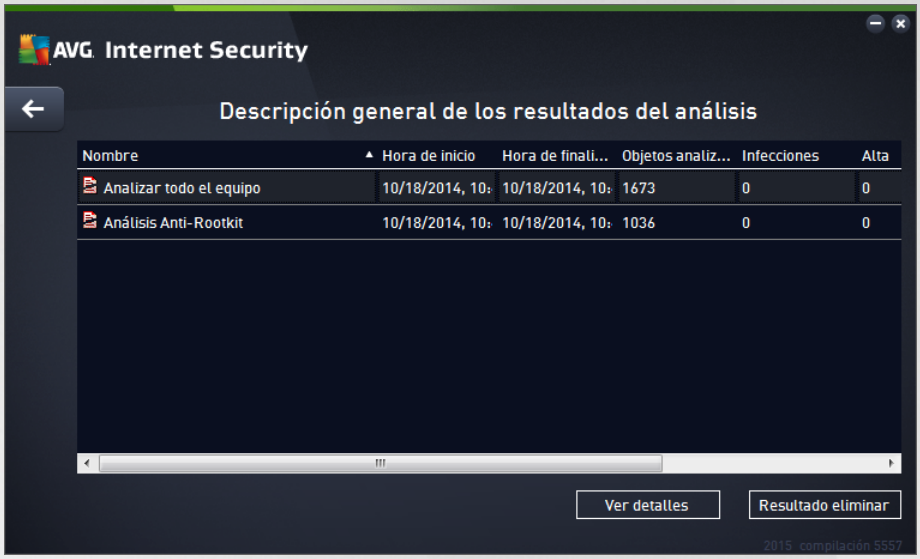
Controles en el diálogo

- ***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.

3.9.5. Resultados del análisis



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

- ***Icono***: la primera columna muestra un icono de información que describe el estado del análisis:
  - o No se han encontrado infecciones; análisis finalizado.
  - o No se han encontrado infecciones; análisis interrumpido antes de finalizar.
  - o Se han encontrado infecciones pero no se han reparado; análisis finalizado.
  - o Se han encontrado infecciones pero no se han reparado; análisis interrumpido antes de finalizar.
  - o Se han encontrado infecciones y se han reparado o removido; análisis finalizado.
  - o Se han encontrado infecciones y se han reparado o removido; 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.

3.9.6. 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 sólo se muestra si se detectaron amenazas durante el análisis, y brinda información detallada sobre ellas:

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

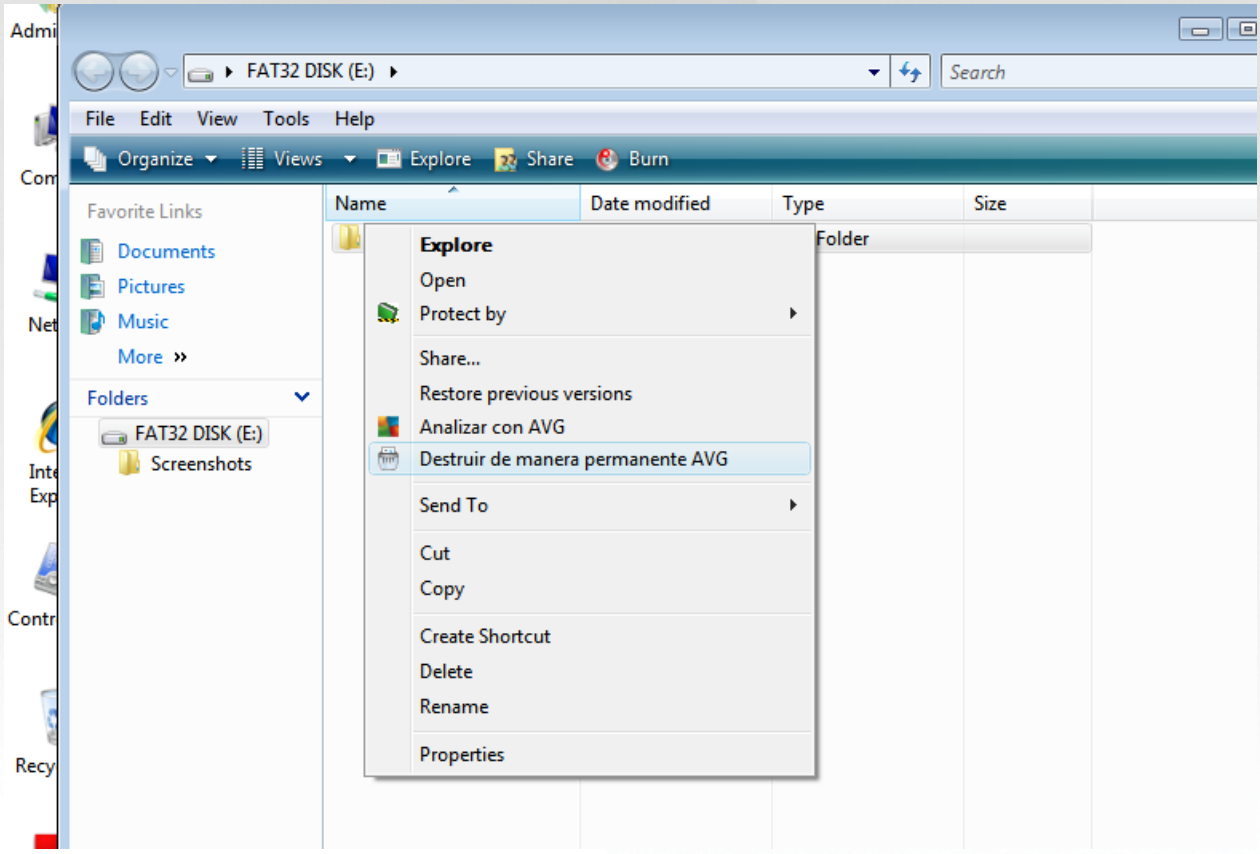
  Severidad media: generalmente son PUP *(programas potencialmente no deseados, como adware) o* cookies de rastreo

  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.

3.10. AVG File Shredder

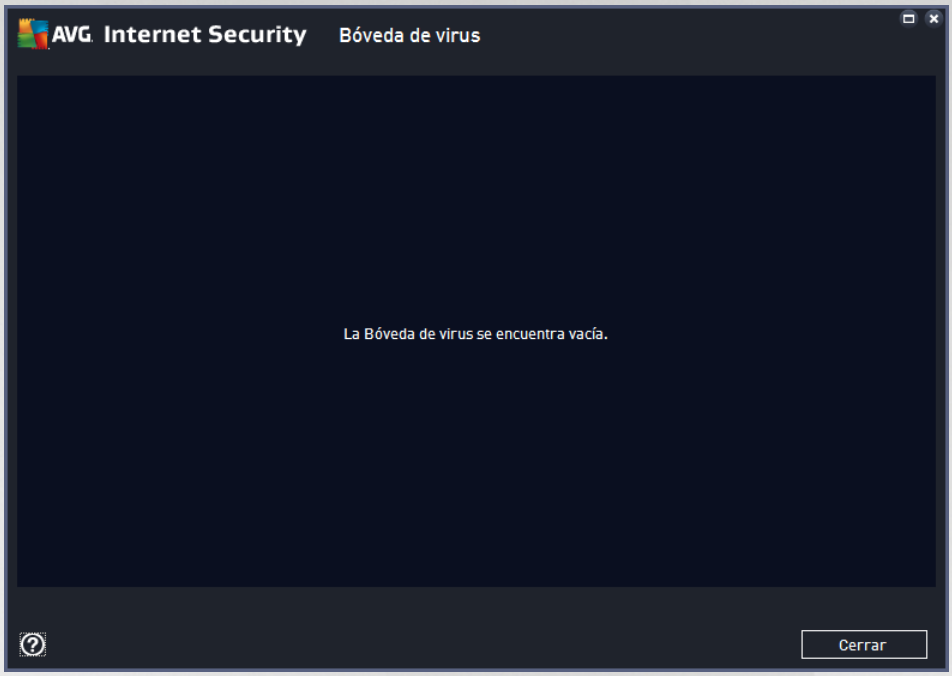
AVG File Shredder se ha diseñado para eliminar archivos de forma absolutamente segura, es decir, sin ninguna posibilidad de recuperarlos, ni siquiera con las herramientas de software avanzadas para este propósito.

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



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

3.11. 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 adición***: proporciona la fecha y hora en que se ha detectado y transferido el archivo sospechoso a la Bóveda de Virus.
- ***Amenaza***: si decide instalar el componente Identidad dentro de su **AVG Internet Security 2015**, se proporcionará una identificación gráfica de la gravedad de la detección en esta sección: desde inobjetable *(tres puntos verdes)* hasta muy peligroso *(tres puntos rojos)*. También encontrará información sobre el tipo de infección y su ubicación original. El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enclopedia de virus en línea.
- ***Fuente***: especifica qué componente de **AVG Internet Security 2015** ha detectado la amenaza en cuestión.
- ***Notificaciones***: en una situación inusual, pueden proporcionarse notas en esta columna con comentarios detallados de la amenaza en cuestión.

Botones de control

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

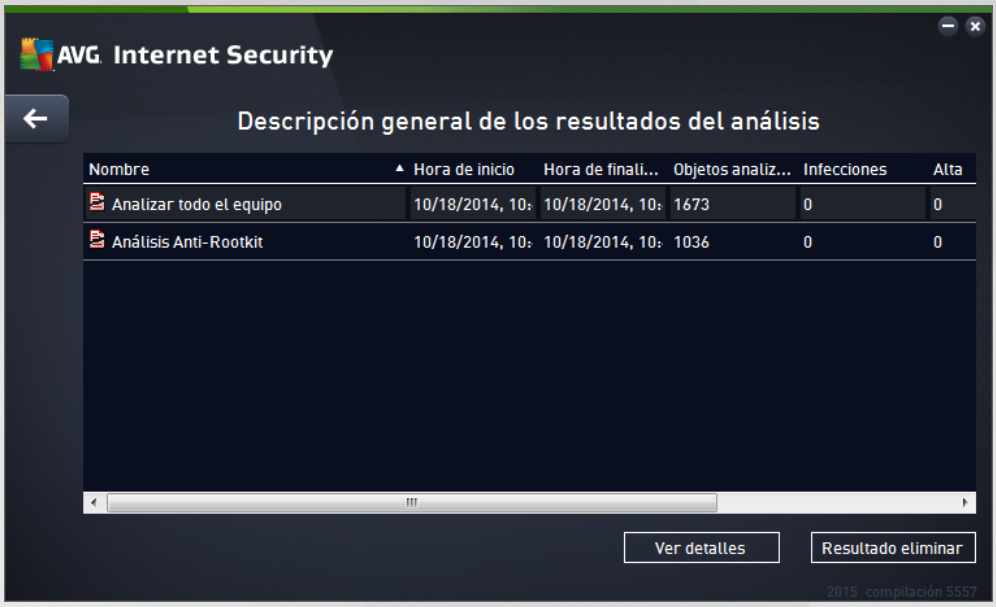
- ***Restaurar***: devuelve el archivo infectado a su ubicación original en el disco.
- ***Restaurar como***: mueve el archivo infectado a una carpeta seleccionada.
- ***Enviar para análisis***: el botón está activo sólo cuando se resalta un objeto en la lista de detecciones ubicada más arriba. En tal caso, tiene la opción de enviar la detección seleccionada a los laboratorios de virus de AVG en busca de análisis más detallados. Tenga en cuenta que esta característica debería servir principalmente para enviar falsos positivos, es decir, archivos que fueron detectados por AVG como infectados o sospechosos, pero que en realidad son inofensivos.
- ***Detalles***: para obtener información detallada sobre la cuarentena de amenazas específicas en la ***Bóveda de virus***, resalte el elemento seleccionado en la lista y haga clic en el botón ***Detalles*** para 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*).

3.12. 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
- Resultados de la Protección Residente
- Resultados de Protección del correo electrónico
- Configuración de Online Shield
- Historial de eventos
- Registro del Firewall

3.12.1. 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 Internet Security 2015**. 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***: estas columnas proporcionan la cantidad de infecciones eliminadas/totales encontradas de severidad alta y media, respectivamente
- ***Información***: información relacionada con el curso y el resultado del análisis *(normalmente 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

3.12.2. Resultados 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:

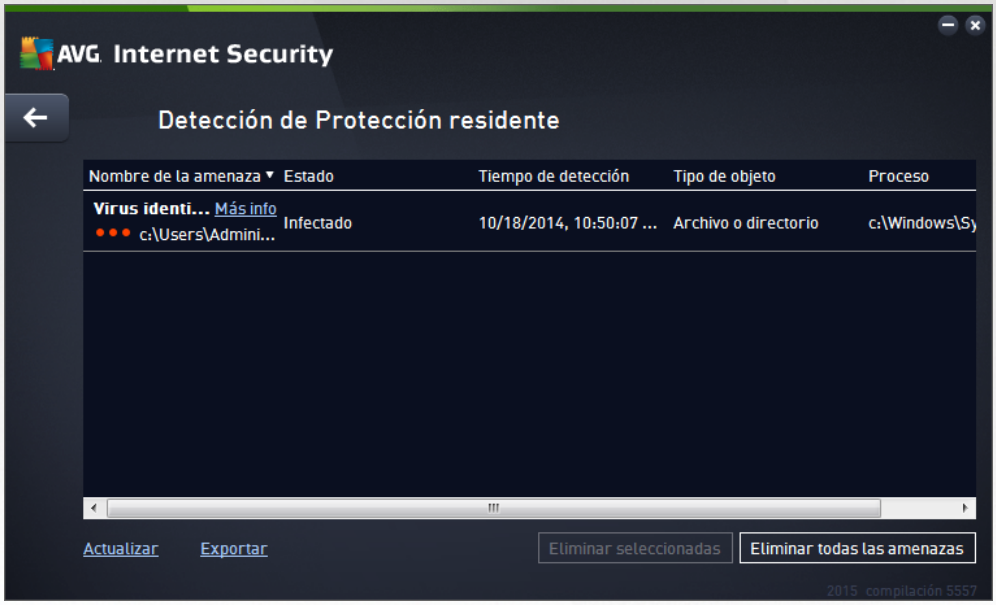
Dentro de este cuadro de diálogo de advertencia encontrará información sobre el objeto detectado y asignado al estado infectado (*Amenaza*), y algunos datos descriptivos sobre la infección reconocida (*Descripción*). El vínculo *Más información* lo lleva a una página que brinda información detallada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

Nota: *es posible que el tamaño del objeto detectado exceda el límite de espacio libre en la Bóveda de virus.*

Si es así, aparecerá un mensaje para informarle del problema cuando intente mover el objeto infectado a la Bóveda de virus. De todos modos, puede editar el tamaño de la Bóveda de virus. Este tamaño está definido como un porcentaje ajustable del tamaño real de su disco duro. Para aumentar el tamaño de la Bóveda de virus, vaya al cuadro de diálogo Bóveda de virus dentro de Configuración avanzada de AVG, utilizando la opción "Limitar el tamaño de la Bóveda de virus".

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

Dentro el cuadro de diálogo ***Detección de Protección residente*** hay una lista de todas las detecciones de Protección residente de las que se puede obtener una descripción general. Este cuadro de diálogo está disponible a través del elemento de menú ***Opciones / Historial / Detección de Protección residente*** en la navegación superior de la ventana principal de **AVG Internet Security 2015. 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 amenaza***: descripción (*posiblemente, incluso el nombre*) del objeto detectado y su ubicación. El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enclopedia de virus en línea.
- ***Estado***: acción realizada con el objeto detectado
- ***Tiempo de Detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de Objeto***: tipo del objeto detectado
- ***Proceso***: qué acción se 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 sólo esos elementos
- ***Eliminar todas las amenazas***: utilice el botón para eliminar todos los registros mencionados en este cuadro de diálogo
- : para regresar al cuadro de diálogo principal de AVG predeterminado *(descripción general de los componentes)*, utilice la flecha en la esquina superior izquierda de este cuadro de diálogo

3.12.3. Resultados de Identity Protection

Se puede acceder al cuadro de diálogo ***Resultados de Identity Protection*** a través del elemento de menú ***Opciones /Historial/Resultados de Identity Protection*** en la línea de navegación superior de la ventana principal de **AVG Internet Security 2015.**

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

- ***Nombre de la amenaza***: descripción *(posiblemente, incluso el nombre)* del objeto detectado y su ubicación. El vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enclopedia de virus en línea.
- ***Estado***: acción realizada con el objeto detectado
- ***Tiempo de Detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de Objeto***: tipo del objeto detectado
- ***Proceso***: qué acción se 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 dentro de la interfaz de ***Resultados de Identity Protection*** son:

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

3.12.4. Resultados de Protección del correo electrónico

Se puede acceder al cuadro de diálogo ***Resultados de Protección del correo electrónico*** a través del elemento de menú ***Opciones /Historial / Resultados de Protección del correo electrónico*** en la línea de navegación superior de la ventana principal de **AVG Internet Security 2015.**

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

- ***Nombre de la detección***: descripción *(posiblemente 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 mediante el 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

3.12.5. Configuración de Online Shield

Online Shield analiza el contenido de las páginas web visitadas y los archivos que puedan contener incluso antes de que se visualicen en el navegador web o de que se descarguen en 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 como infectado (*Amenaza*), y algunos datos descriptivos sobre la infección reconocida (*Nombre de objeto*). El vínculo *Más información* lo dirigirá a la enciclopedia de virus en línea, donde puede encontrar información detallada sobre la infección detectada, si es conocida. El cuadro de diálogo proporciona los siguientes elementos de control:

- ***Mostrar detalles***: haga clic en el vínculo para abrir una nueva ventana emergente donde podrá encontrar información acerca del proceso que se estaba ejecutando cuando se detectó la infección, y la identificación del proceso.
- ***Cerrar***: haga clic en el botón para cerrar el 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 Internet Security 2015**.

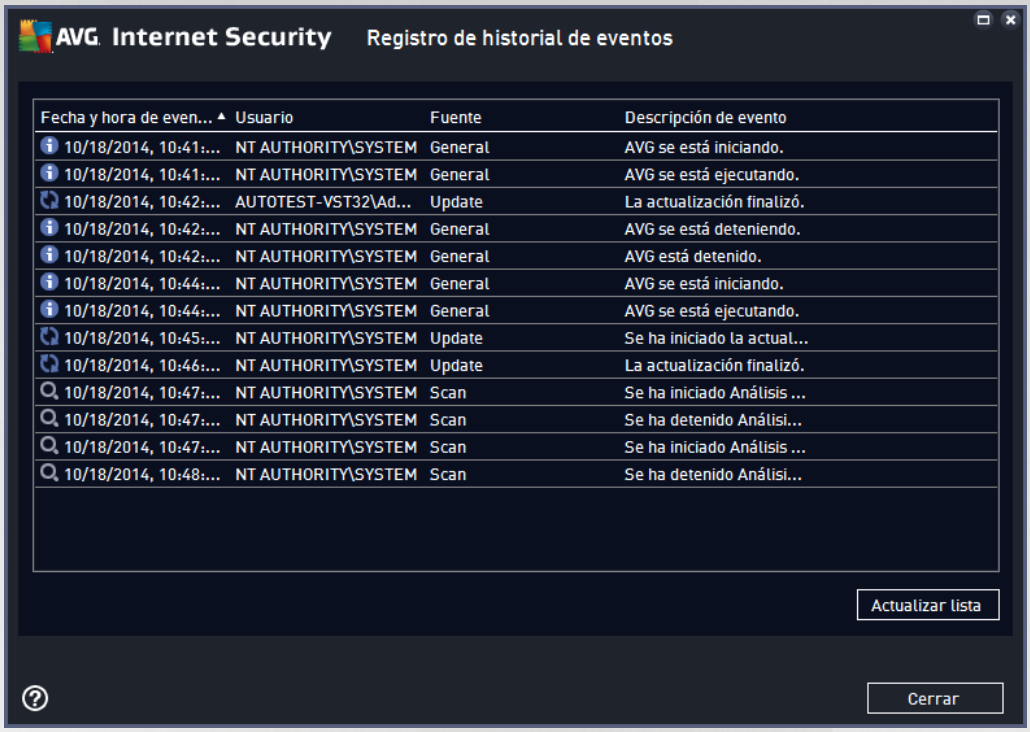
Para cada objeto detectado se proporciona la siguiente información:

- ***Nombre de la amenaza***: descripción (*posiblemente incluso el nombre*) del objeto detectado, y su origen (*página web*); el vínculo *Más información* lo lleva a una página que brinda información detallada sobre la amenaza detectada dentro de la enclopedia de virus en línea.
- ***Estado***: acción realizada con el objeto detectado
- ***Tiempo de Detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de Objeto***: tipo del objeto detectado

Botones de control

- ***Actualizar***: 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

3.12.6. Historial de Eventos



Se puede acceder al cuadro de diálogo ***Historial de eventos*** a través del elemento de menú ***Opciones/ Historial / Historial de Eventos*** en la línea de navegación superior de la ventana principal de **AVG Internet Security 2015**. En este cuadro de diálogo puede encontrar un resumen de los eventos importantes que se han producido durante el funcionamiento de **AVG Internet Security 2015**. 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

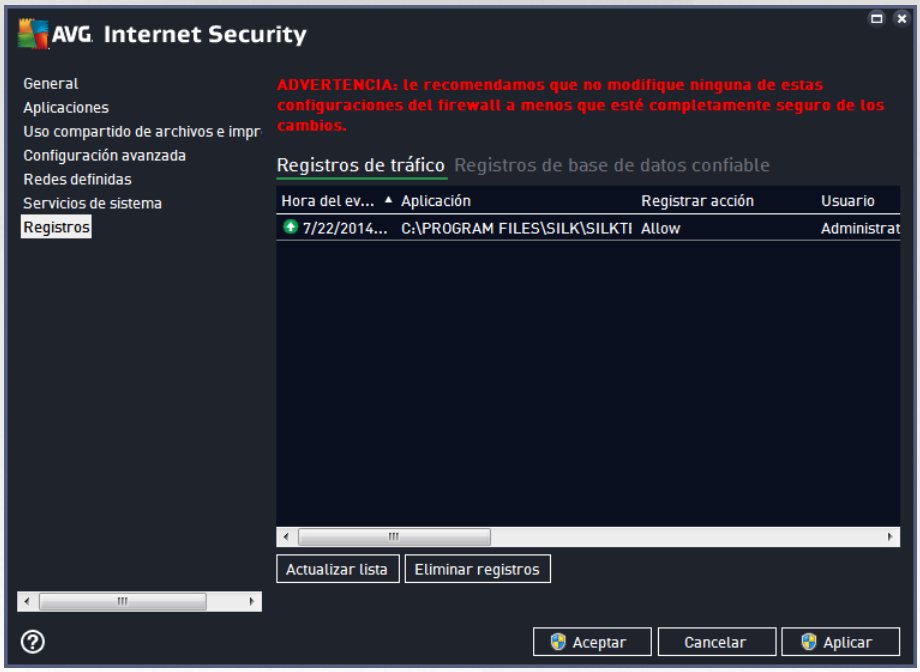
- ***Actualizar lista***: presione este botón para actualizar todas las entradas de la lista de eventos
- ***Cerrar***: presione el botón para regresar a la ventana principal de **AVG Internet Security 2015**

3.12.7. Registro del Firewall

Este cuadro de diálogo está diseñado para una configuración de experto, por lo que recomendamos que no cambie ninguna configuración a menos que esté absolutamente seguro del cambio.

El cuadro de diálogo ***Registros*** le permite revisar la lista de todas las acciones y eventos registrados del Firewall con una descripción detallada de los parámetros relevantes en dos pestañas:

- ***Registros de tráfico***: ofrece información acerca de las actividades de todas las aplicaciones que han intentado conectarse a la red. Encontrará para cada elemento información sobre la hora del evento, el nombre de la aplicación, la acción de registro correspondiente, el nombre de usuario, PID, dirección del tráfico, tipo de protocolo, números de los puertos remotos y locales, e información sobre la dirección IP local y remota.



- ***Registros de base de datos confiable***: la *Base de datos confiable* es la base de datos interna de AVG que recopila información acerca de aplicaciones certificadas y confiables a las que siempre se les puede permitir comunicarse en línea. La primera vez que una nueva aplicación intenta conectarse a la red (*es decir, aún no existen reglas del firewall especificadas para esta aplicación*), es necesario determinar si se le debe permitir la comunicación con la red. Primero, AVG busca en la *Base de datos confiable* y, si la aplicación se encuentra en la lista, se le concederá automáticamente acceso a la red. Sólo después de que se comprueba que no existe información disponible acerca de la aplicación en la base de datos, se le preguntará en un cuadro de diálogo independiente si desea permitir que la aplicación obtenga acceso a la red.

Botones de control

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

- ***Eliminar registros***: presione este botón para eliminar todas las entradas de la tabla.

3.13. 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 vulneren en el software y el sistema operativo. Diariamente aparecen nuevos virus, nuevo malware y nuevos ataques de hackers. Por ello, los proveedores de software generan constantes actualizaciones y parches de seguridad, con objeto de corregir las deficiencias de seguridad descubiertas.

Teniendo en cuenta la cantidad de nuevas amenazas para su equipo que surgen cada día y la velocidad a la que se propagan, es absolutamente esencial actualizar su **AVG Internet Security 2015** 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 Internet Security 2015** 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.

3.13.1. Ejecución de actualizaciones

Para proporcionar la seguridad máxima disponible, **AVG Internet Security 2015** 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 Internet Security 2015** 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
- Programación de actualización de Anti-Spam

3.13.2. Niveles de actualización

AVG Internet Security 2015 permite seleccionar dos niveles de actualización:

- ***Actualización de definiciones*** contiene los cambios necesarios para una protección antivirus, anti-spam y anti-malware confiable. Por lo general, no incluye cambios del código y sólo actualiza la base de datos de definiciones. Esta actualización se debe aplicar tan pronto como esté disponible.

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

Al programar una actualización, es posible 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 mayor prioridad y, por consiguiente, se interrumpirá el proceso de análisis. En ese caso, se le informará acerca del conflicto.*

3.14. Preguntas frecuentes y soporte técnico

Si tiene algún problema técnico o referente a la compra de la aplicación **AVG Internet Security 2015**, existen varios modos de buscar ayuda. Elija una de las opciones siguientes:

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

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

- ***Resolución de problemas en el archivo de ayuda***: Está disponible una sección de ***Resolución de problemas*** incluida en el archivo de ayuda **AVG Internet Security 2015** *(para abrir el archivo de ayuda, presione la tecla F1 en cualquier diálogo en la aplicación)*. Esta sección proporciona una lista de las situaciones que se producen con más frecuencia cuando un usuario desea obtener ayuda profesional sobre una cuestión técnica. Seleccione la situación que mejor describa su problema y haga clic en ella para abrir instrucciones detalladas que le permitan solucionarlo.

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

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

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