



AVG Email Server Edition 2012

Manual del usuario

Revisión del documento 2012.06 (2/28/2012)

Copyright AVG Technologies CZ, s.r.o. Reservados todos los derechos.
El resto de marcas comerciales son propiedad de sus respectivos propietarios.

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

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

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



Contenido

1. Introducción	4
2. Requisitos de instalación de AVG	5
2.1 Sistemas operativos compatibles	5
2.2 Servidores de correo electrónico compatibles	5
2.3 Requisitos de hardware	5
2.4 Desinstalar versiones anteriores	5
2.5 Service Packs de MS Exchange	6
3. Proceso de instalación de AVG	7
3.1 Inicio de la instalación	7
3.2 Active su licencia	8
3.3 Seleccione el tipo de instalación	9
3.4 Instalación personalizada - Opciones personalizadas	10
3.5 Finalización de la instalación	11
4. Analizador de correo electrónico para MS Exchange Server 2007/2010	13
4.1 Información general	13
4.2 Analizador de correo electrónico para MS Exchange (AT enrutador)	16
4.3 Analizador de correo electrónico para MS Exchange (AT SMTP)	17
4.4 Analizador de correo electrónico para MS Exchange (VSAPI)	18
4.5 Acciones de detección	21
4.6 Filtrado de mensajes	22
5. Analizador de correo electrónico para MS Exchange Server 2003	24
5.1 Información general	24
5.2 Analizador de correo electrónico para MS Exchange (VSAPI)	27
5.3 Acciones de detección	30
5.4 Filtrado de mensajes	31
6. AVG for Kerio MailServer	33
6.1 Configuración	33
6.1.1 Antivirus	33
6.1.2 Filtro de adjuntos	33
7. Cómo configurar Anti-Spam	37
7.1 Interfaz de Anti-Spam	37



7.2 Principios de Anti-Spam	39
7.3 Configuración de Anti-Spam	39
7.3.1 Asistente de entrenamiento de Anti-Spam	39
7.3.2 Seleccionar carpeta con mensajes	39
7.3.3 Opciones de filtrado de mensajes	39
7.4 Rendimiento	44
7.5 RBL	45
7.6 Lista blanca	46
7.7 Lista negra	47
7.8 Configuración de experto	48
8. Administrador de configuraciones de AVG	49
9. Preguntas más frecuentes (FAQ) y soporte técnico	52



1. Introducción

Este manual del usuario proporciona documentación completa sobre **AVG Email Server Edition 2012**.

Enhorabuena por adquirir AVG Email Server Edition 2012.

AVG Email Server Edition 2012 es un software de la gama de productos galardonados de AVG que están diseñados para darle tranquilidad a usted y total seguridad a su servidor. Al igual que el resto de productos AVG, **AVG Email Server Edition 2012** se ha rediseñado íntegramente, de arriba a abajo, para proporcionar la reconocida y acreditada protección de seguridad de AVG de forma novedosa, más eficiente y fácil de usar.

AVG ha sido diseñado y desarrollado para proteger su actividad informática y de red. Disfrute la experiencia de una protección total con AVG.

Nota: esta documentación contiene una descripción de las características específicas de *E-mail Server Edition*. Para obtener información acerca de otras características de AVG, consulte la guía del usuario de *Internet Security Edition*, que contiene todos los detalles necesarios. Puede descargar la guía desde <http://www.avg.com>.



2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG Email Server Edition 2012 se ha diseñado para proteger servidores de correo electrónico con los siguientes sistemas operativos:

- Windows 2008 Server Edition (x86 y x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Servidores de correo electrónico compatibles

Son compatibles los siguientes servidores de correo electrónico:

- MS Exchange 2003 Server
- MS Exchange 2007 Server
- MS Exchange 2010 Server
- Kerio MailServer: versión 6.7.2 y superior

2.3. Requisitos de hardware

Requisitos de hardware mínimos para **AVG Email Server Edition 2012**:

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

Requisitos de hardware recomendados para **AVG Email Server Edition 2012**:

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

2.4. Desinstalar versiones anteriores

Si tiene instalada una versión más antigua de AVG Email Server, necesitará desinstalarla de forma manual antes de instalar **AVG Email Server Edition 2012**. Debe realizar de forma manual la desinstalación de la versión anterior, utilizando la funcionalidad estándar de Windows.

- Desde el menú de inicio **Inicio/Configuración/Panel de control/Agregar o quitar**



programas, seleccione el programa correcto de la lista de software instalado. También puede desinstalarla, y quizás con mayor facilidad, a través del menú **Inicio/Todos los programas/AVG/Uninstall AVG**.

- Si ha utilizado anteriormente la versión AVG 8.x o anterior, no olvide desinstalar también los complementos individuales del servidor.

Nota: *será necesario reinstalar el servicio de almacenamiento durante el proceso de desinstalación.*

Complemento de Exchange: ejecute `setupes.exe` con el parámetro `/uninstall` desde la carpeta en la que se instaló el complemento.

p. ej., C:\AVG4ES2K\setupes.exe /uninstall

Complemento de Lotus Domino/Notes: ejecute `setupln.exe` con el parámetro `/uninstall` desde la carpeta en la que se instaló el complemento.

p. ej., C:\AVG4LN\setupln.exe /uninstall

2.5. Service Packs de MS Exchange

No es necesario ningún Service Pack para MS Exchange 2003 Server; sin embargo, se recomienda mantener el sistema actualizado con los Service Packs y revisiones más recientes para obtener la máxima seguridad disponible.

Service Pack para MS Exchange 2003 Server (opcional):

<http://www.microsoft.com/exchange/evaluation/sp2/overview.msp>

Al comienzo de la instalación, se examinarán todas las versiones de las bibliotecas del sistema. Si resulta necesario instalar bibliotecas nuevas, el instalador añadirá a la extensión `.delete` al nombre de las antiguas. Se eliminarán al reiniciar el sistema.

Service Pack para MS Exchange 2007 Server (opcional):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>



3. Proceso de instalación de AVG

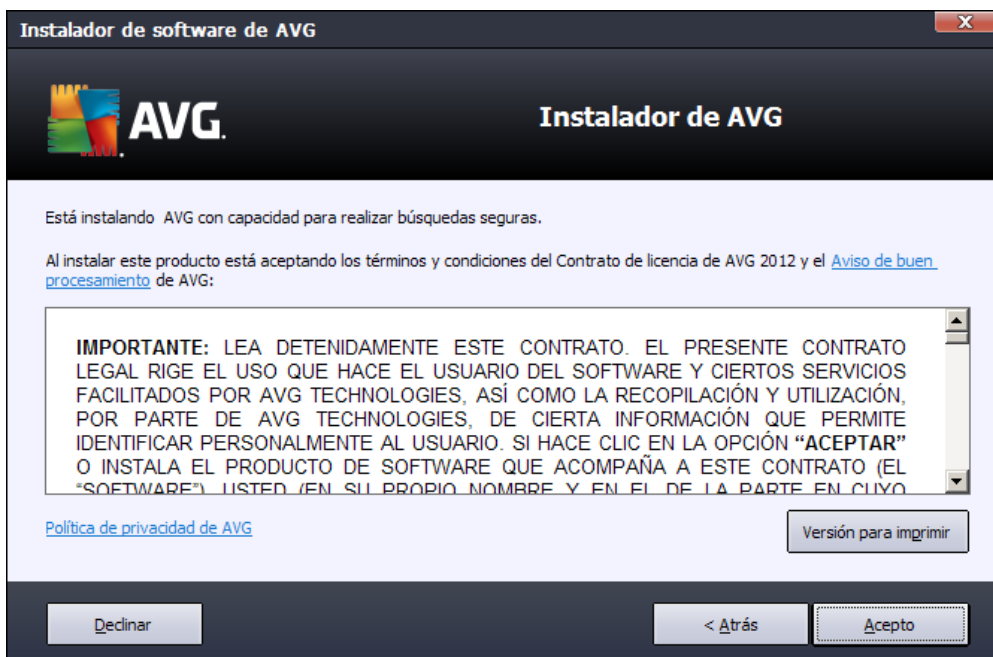
Para instalar AVG en su equipo, debe obtener el archivo de instalación más reciente. Puede utilizar el archivo de instalación del CD que forma parte de la edición en caja, aunque este archivo podría estar obsoleto. Por este motivo, se recomienda obtener en línea el archivo de instalación más reciente. Puede descargar el archivo del [sitio web de AVG](http://www.avg.com/download?prd=msw) (en <http://www.avg.com/download?prd=msw>)

Nota: hay dos paquetes de instalación disponibles para su producto; para sistemas operativos de 32 bits (señalados como x86) y para sistemas operativos de 64 bits (señalados como x64). Asegúrese de utilizar el paquete de instalación adecuado para su sistema operativo específico.

Durante el proceso de instalación se le solicitará el número de licencia. Asegúrese de tenerlo a mano antes de comenzar la instalación. El número figura en el paquete del CD. Si compró su copia de AVG en línea, el número de licencia se le habrá enviado por correo electrónico.

Una vez que haya descargado y guardado el archivo de instalación en el disco duro, puede iniciar el proceso de instalación. La instalación es una secuencia de ventanas de cuadro de diálogo con una breve descripción de lo que se debe hacer en cada paso. A continuación ofrecemos una explicación de cada ventana de cuadro de diálogo:

3.1. Inicio de la instalación



El proceso de instalación se inicia con la ventana de cuadro de diálogo **Bienvenido**. Aquí puede seleccionar el idioma que se utilizará en el proceso de instalación y leer las condiciones de la licencia. Utilice el botón **Versión para imprimir** para abrir el texto de la licencia en una nueva ventana. Pulse el botón **Acepto** para confirmar y pasar al cuadro de diálogo siguiente.

Atención: podrá elegir más idiomas para la interfaz de la aplicación durante el proceso de

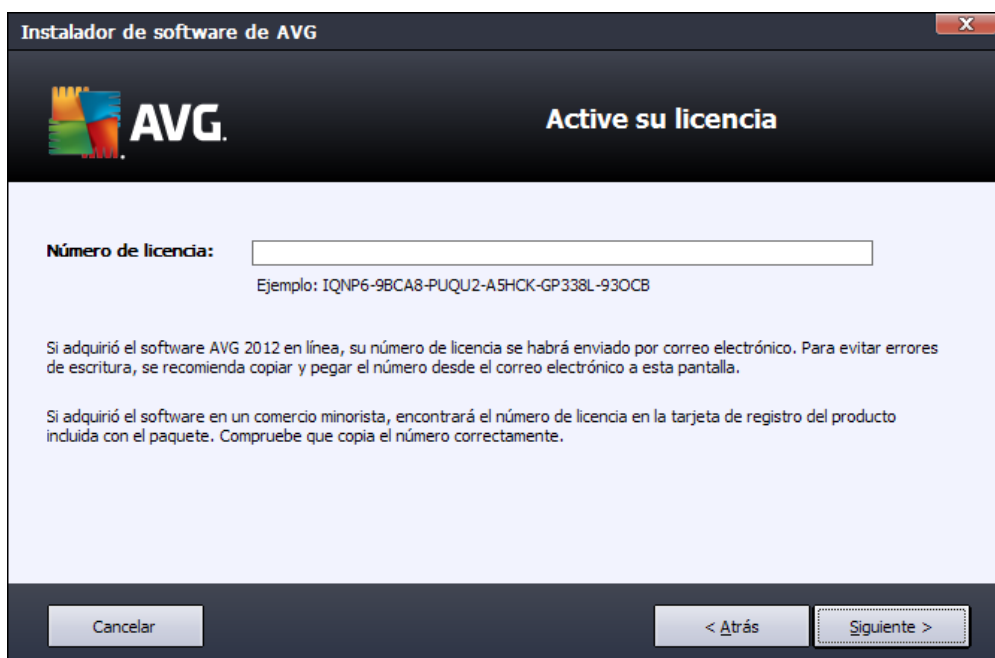


instalación.

3.2. Active su licencia

En el cuadro de diálogo **Active su licencia** debe introducir su número de licencia.

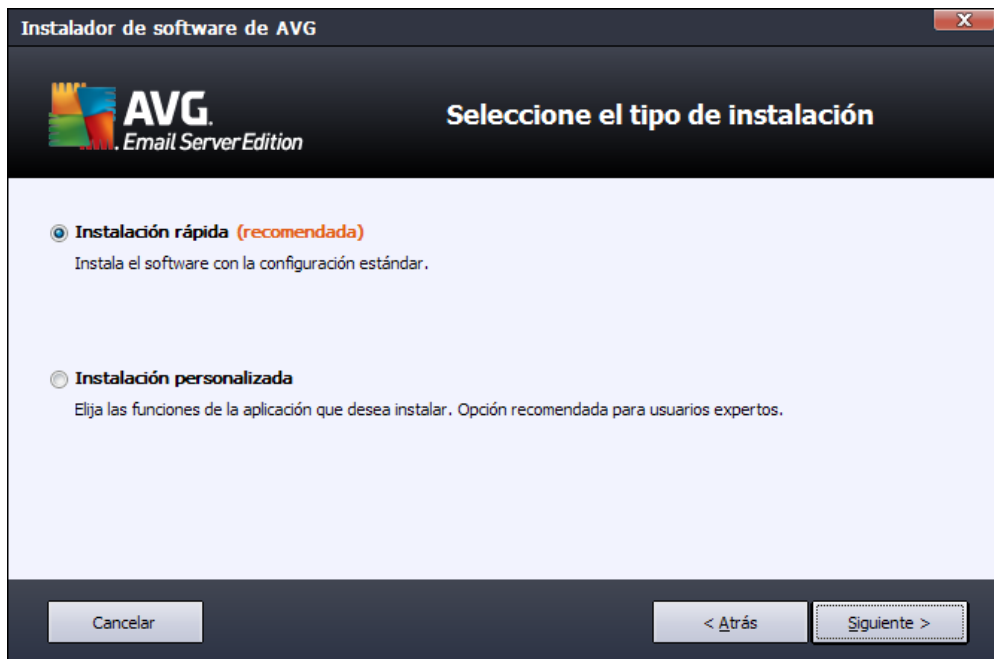
Escríbalo en el campo de texto **Número de licencia**. El número de licencia se encontrará en el correo electrónico de confirmación que recibió tras la compra en línea de AVG. Debe introducir el número tal como figura. Si cuenta con el formato digital del número de licencia (en el correo electrónico), se recomienda usar el método copiar y pegar para insertarlo.



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



3.3. Seleccione el tipo de instalación

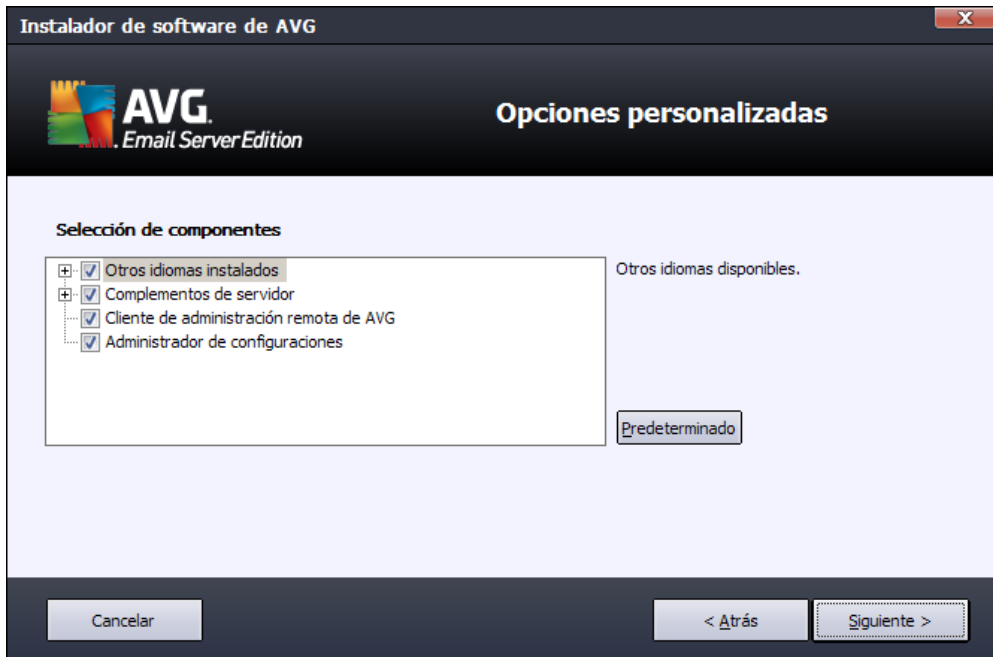


El cuadro de diálogo **Seleccione el tipo de instalación** permite elegir entre dos opciones de instalación: **Instalación rápida** e **Instalación personalizada**.

Para la mayoría de los usuarios, se recomienda seleccionar la opción estándar **Instalación rápida**, la cual instala AVG de manera totalmente automática con la configuración predefinida por el proveedor del programa. Esta configuración ofrece máxima seguridad con un uso óptimo de los recursos. En el futuro, si fuese necesario modificar la configuración, siempre tendrá la posibilidad de hacerlo directamente desde la aplicación AVG.

La **Instalación personalizada** sólo debería ser utilizada por usuarios expertos que tengan una razón válida para instalar AVG con una configuración diferente de la estándar. Por ejemplo, para adecuar el programa a necesidades específicas del sistema.

3.4. Instalación personalizada - Opciones personalizadas



El cuadro de diálogo **Carpeta de destino** le permite especificar la ubicación donde se debe instalar AVG. De manera predeterminada, AVG se instalará en la carpeta de archivos de programa situada en la unidad C:. Si desea cambiar esta ubicación, utilice el botón **Examinar** para mostrar la estructura de la unidad y seleccione la carpeta en cuestión.

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

Sin embargo, solamente puede seleccionar componentes incluidos en la edición de AVG que haya adquirido. Sólo se ofrecerá la posibilidad de instalar estos componentes específicos en el cuadro de diálogo Selección de componentes.

- **Cliente de Administración remota de AVG:** si planea conectar AVG a un Centro de datos de AVG (ediciones de red de AVG), tendrá que seleccionar esta opción.
- **Administrador de configuraciones:** es una herramienta adecuada principalmente para administradores de red que le permite copiar, editar y distribuir la configuración de AVG. La configuración se puede guardar en un dispositivo portátil (memoria flash USB, etc.) y luego aplicarse manualmente o de cualquier otra forma en las estaciones seleccionadas.
- **Otros idiomas instalados:** puede especificar en qué idiomas deberá instalarse AVG. Marque el elemento **Otros idiomas instalados** y luego seleccione los idiomas deseados del menú correspondiente.

Información básica de los componentes individuales del servidor (**Complementos de servidor**):

- **Servidor anti-spam para MS Exchange**



Comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como SPAM. Utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado.

- ***Analizador de correo electrónico para MS Exchange (agente de transporte enrutador)***

Comprueba todos los mensajes de correo electrónico entrantes, salientes e internos que van a través de la función HUB de MS Exchange.

Está disponible para MS Exchange 2007/2010 y sólo puede instalarse para la función HUB.

- ***Analizador de correo electrónico para MS Exchange (agente de transporte SMTP)***

Comprueba todos los mensajes de correo electrónico que llegan a través de la interfaz SMTP de MS Exchange.

Sólo está disponible para MS Exchange 2007/2010 y puede instalarse tanto para la función HUB como para la EDGE.

- ***Analizador de correo electrónico para MS Exchange (VSAPI)***

Comprueba todos los mensajes de correo electrónico almacenados en los buzones de los usuarios. Los virus detectados se mueven al Almacén de virus o se eliminan completamente.

Nota: existen distintas opciones disponibles para versiones diferentes de MS Exchange.

Continúe pulsando el botón ***Siguiente***.

3.5. Finalización de la instalación

Si ha seleccionado el módulo ***Componente Administración remota*** durante la selección de módulos, entonces la pantalla final le permitirá definir la cadena de conexión para conectarse a su Centro de datos de AVG.



Ahora AVG se ha instalado en el equipo y es totalmente funcional. El programa se ejecuta en segundo plano en modo completamente automático.

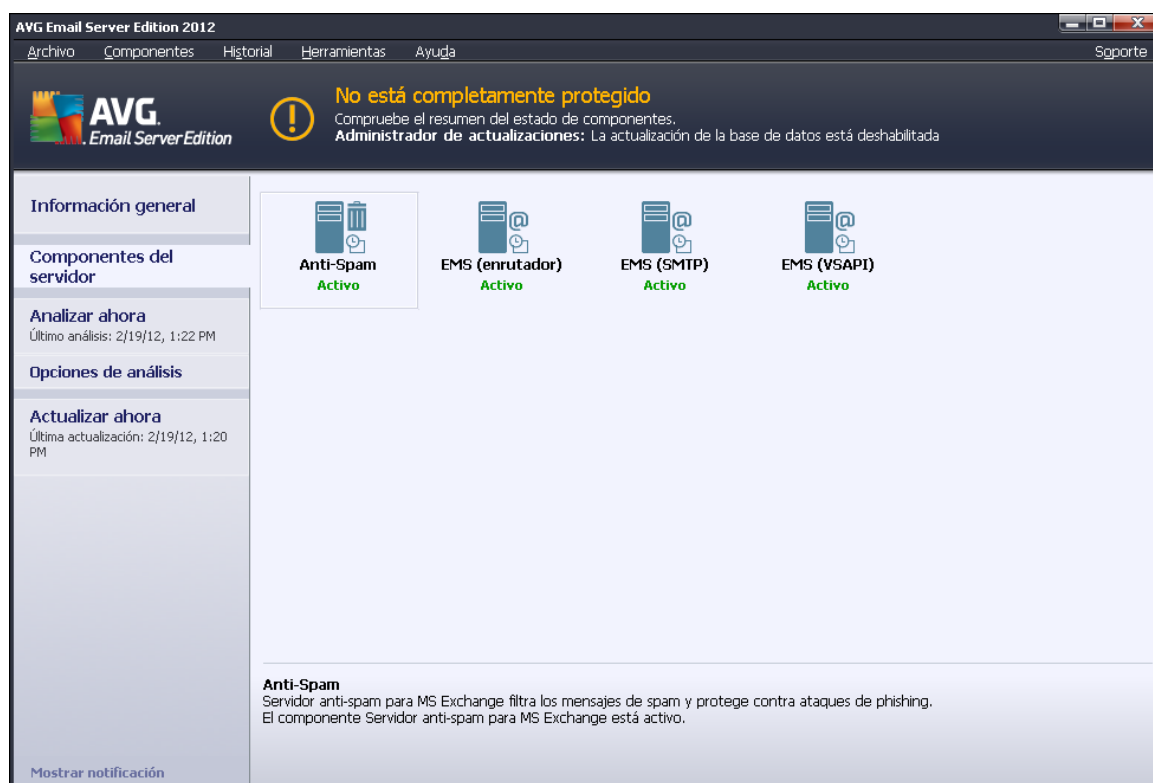
Para configurar de manera individual la protección para su servidor de correo electrónico, consulte el capítulo correspondiente:

- [*Analizador de correo electrónico para MS Exchange Server 2007/2010*](#)
- [*Analizador de correo electrónico para MS Exchange Server 2003*](#)
- [*AVG para Kerio MailServer*](#)

4. Analizador de correo electrónico para MS Exchange Server 2007

4.1. Información general

Las opciones de configuración de AVG para MS Exchange Server 2007/2010 están completamente integradas en AVG Email Server Edition 2012 como componentes del servidor.



Información básica de los componentes individuales del servidor:

- [**Anti-Spam - Servidor anti-spam para MS Exchange**](#)
Comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como SPAM. Utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado.
- [**EMS \(enrutador\) - Analizador de correo electrónico para MS Exchange \(agente de transporte enrutador\)**](#)
Comprueba todos los mensajes de correo electrónico entrantes, salientes e internos que van a través de la función HUB de MS Exchange.
Está disponible para MS Exchange 2007/2010 y sólo puede instalarse para la función HUB.
- [**EMS \(SMTP\) - Analizador de correo electrónico para MS Exchange \(agente de**](#)



[transporte SMTP\)](#)

Comprueba todos los mensajes de correo electrónico que llegan a través de la interfaz SMTP de MS Exchange.

Sólo está disponible para MS Exchange 2007/2010 y puede instalarse tanto para la función HUB como para la EDGE.

- **[EMS \(VSAPI\) - Analizador de correo electrónico para MS Exchange \(VSAPI\)](#)**

Comprueba todos los mensajes de correo electrónico almacenados en los buzones de los usuarios. Los virus detectados se mueven al Almacén de virus o se eliminan completamente.

Nota importante: *si decidió instalar y utilizar VSAPI en combinación con el agente de transporte enrutador en una función Hub Exchange, los mensajes de correo electrónico se analizarán dos veces. Para evitarlo, consulte el cuadro **No analizar los mensajes salientes (MS Exchange 2007/2010)** en la configuración de VSAPI (haga clic [aquí](#) para obtener más información).*

Haga clic en un componente requerido para abrir su interfaz. Con la excepción de Anti-Spam, todos los componentes tienen en común los botones de control y vínculos que se describen a continuación:

AVG Email Server Edition 2012

Archivo Componentes Historial Herramientas Ayuda Soporte

AVG
Email Server Edition

No está completamente protegido
Compruebe el resumen del estado de componentes.
Administrador de actualizaciones: La actualización de la base de datos está deshabilitada

Información general

Componentes del servidor

E-mail Scanner para MS Exchange (VSAPI)

Analizar ahora
Último análisis: 2/19/12, 1:22 PM

Opciones de análisis

Actualizar ahora
Última actualización: 2/19/12, 1:20 PM

Componente E-mail Scanner para MS Exchange (VSAPI)

Activo

Desde: 2/19/2012, 1:18 PM
Partes de correo electrónico comprobadas: **1604**

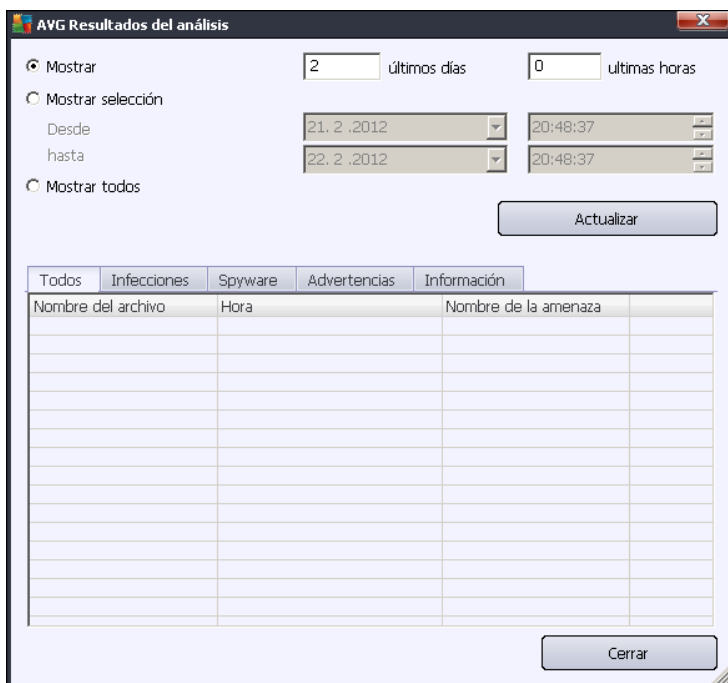
Amenazas detectadas:	0	PUP detectados:	0
Infecciones detectadas:	0	Información detectada:	0
Advertencias detectadas:	0		
Movidos al Almacén de virus:	0		
Eliminados:	0		
Omitidos:	0		

[Resultados del análisis](#), [Actualizar valores estadísticos](#), [Restablecer valores estadísticos](#)

Mostrar notificación Configuración Atrás

- **Resultados del análisis**

Abre un nuevo cuadro de diálogo donde puede revisar los resultados del análisis:



Aquí puede comprobar los mensajes, que aparecen divididos en varias fichas de acuerdo a su gravedad. Consulte la configuración de los componentes individuales para modificar la gravedad y el informe.

De manera predeterminada, únicamente se muestran los resultados de los últimos dos días. Puede cambiar el período visualizado modificando las opciones siguientes:

- **Mostrar últimos:** introduzca los días y horas deseados.
- **Mostrar selección:** elija un intervalo de fecha y hora personalizado.
- **Mostrar todos:** muestra los resultados para el período completo.

Utilice el botón **Actualizar** para volver a cargar los resultados.

- **Actualizar valores estadísticos:** actualiza las estadísticas mostradas más arriba.
- **Restablecer valores estadísticos:** pone a cero todas las estadísticas.

Los botones operativos son los siguientes:

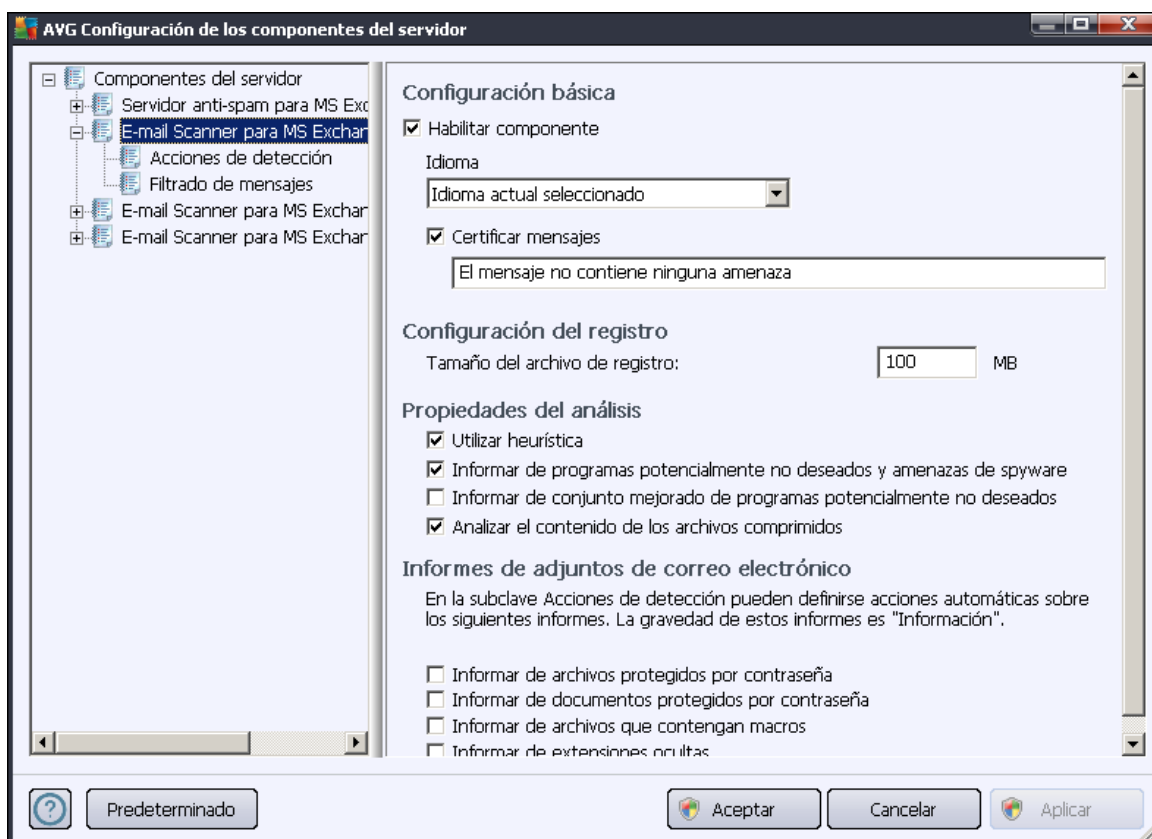
- **Configuración:** utilice este botón para abrir la configuración del componente.
- **Atrás:** pulse este botón para volver a la información general de los componentes del servidor.

Encontrará más información sobre las configuraciones individuales de todos los componentes en los capítulos que se encuentran a continuación.

4.2. Analizador de correo electrónico para MS Exchange (AT enrutador)

Para abrir la configuración del *Analizador de correo electrónico para MS Exchange (agente de transporte enrutador)*, seleccione el botón **Configuración** desde la interfaz del componente.

En la lista **Componentes del servidor**, seleccione el elemento *Analizador de correo electrónico para MS Exchange (AT enrutador)*:



La sección **Configuración básica** ofrece las opciones siguientes:

- **Habilitar componente:** quite la marca para desactivar todo el componente.
- **Idioma:** seleccione el idioma deseado del componente.
- **Certificar mensajes:** marque esta opción si desea añadir una nota de certificación a todos los mensajes analizados. Puede personalizar este mensaje en el siguiente campo.

La sección **Configuración del registro:**

- **Tamaño del archivo de registro:** elija el tamaño deseado del archivo de registro. Valor predeterminado: 100 MB.

La sección **Propiedades del análisis:**



- **Utilizar heurística:** marque esta casilla para activar el método de detección heurístico durante el análisis.
- **Informar de programas potencialmente no deseados y amenazas de spyware:** marque esta opción para informar sobre la presencia de programas potencialmente no deseados y spyware.
- **Informar de conjunto mejorado de programas potencialmente no deseados:** marque esta opción para detectar paquetes ampliados de spyware, es decir, programas perfectamente correctos y que no causan daño alguno cuando se adquieren directamente del fabricante, pero que pueden utilizarse más adelante para fines maliciosos (diversas barras de herramientas, etc.). Se trata de una medida adicional que aumenta aún más la seguridad y la comodidad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada. Nota: esta característica de detección es adicional a la opción anterior, por lo que si desea protección contra los tipos básicos de spyware, mantenga siempre activa la casilla anterior.
- **Analizar el contenido de los archivos comprimidos:** marque esta opción para permitir que el analizador busque también en los archivos comprimidos (zip, rar, etc.)

La sección **Informes de adjuntos de correo electrónico** le permite seleccionar sobre qué elementos deberá informarse durante el análisis. Si marca esta opción, cada mensaje de correo electrónico con dicho elemento contendrá la etiqueta [INFORMACIÓN] en el asunto del mensaje. Esta configuración es la predeterminada y puede modificarse fácilmente en la **sección Acciones de detección**, parte **Información** (consulte a continuación).

Las opciones disponibles son las siguientes:

- **Informar de archivos protegidos por contraseña**
- **Informar de documentos protegidos por contraseña**
- **Informar de archivos que contengan macros**
- **Informar de extensiones ocultas**

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- [Acciones de detección](#)
- [Filtrado de mensajes](#)

4.3. Analizador de correo electrónico para MS Exchange (AT SMTP)

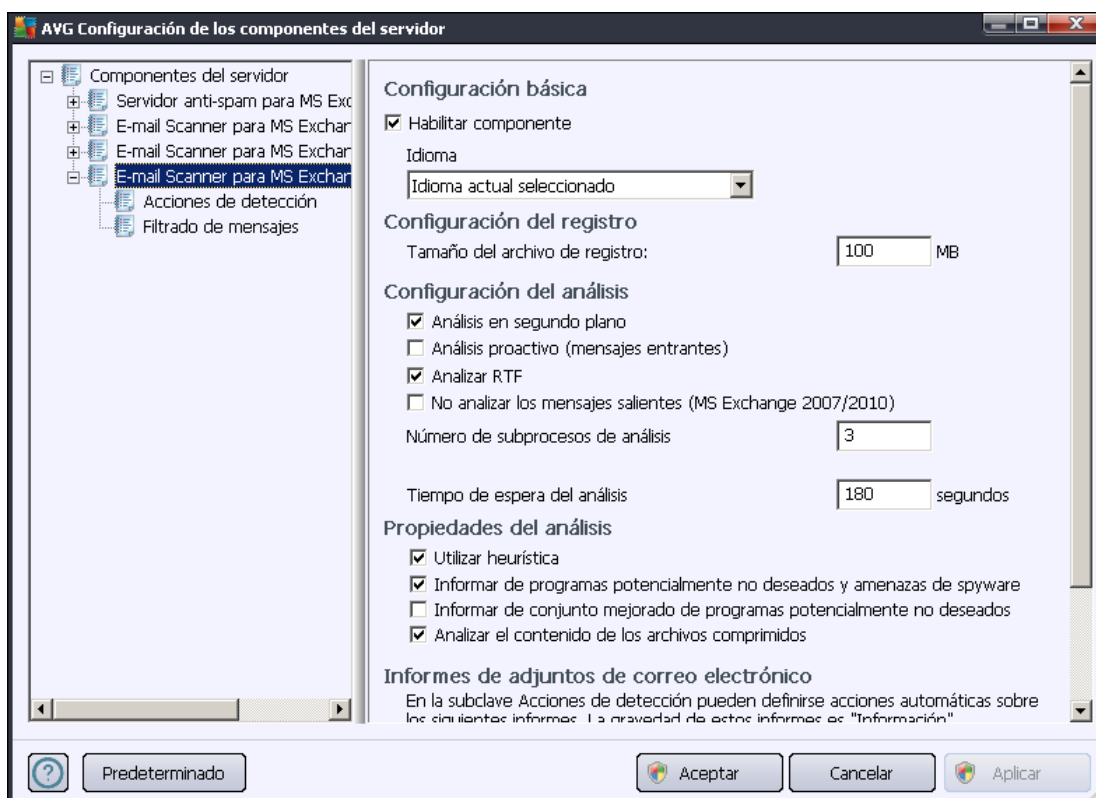
La configuración del **Analizador de correo electrónico para MS Exchange (agente de transporte SMTP)** es exactamente la misma que en el caso del agente de transporte enrutador. Para obtener más información, consulte más arriba el capítulo [Analizador de correo electrónico para MS Exchange \(AT enrutador\)](#).

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- [Acciones de detección](#)
- [Filtrado de mensajes](#)

4.4. Analizador de correo electrónico para MS Exchange (VSAPI)

Este elemento contiene la configuración del *Analizador de correo electrónico para MS Exchange (VSAPI)*.



La sección **Configuración básica** ofrece las opciones siguientes:

- **Habilitar componente:** quite la marca para desactivar todo el componente.
- **Idioma:** seleccione el idioma deseado del componente.

La sección **Configuración del registro:**

- **Tamaño del archivo de registro:** elija el tamaño deseado del archivo de registro. Valor predeterminado: 100 MB.

La sección **Configuración del análisis:**

- **Análisis en segundo plano:** aquí puede activar o desactivar el proceso de análisis en segundo plano. El análisis en segundo plano es una de las características de la interfaz de la aplicación VSAPI 2.0/2.5. Ofrece análisis mediante subprocessos para las bases de datos de



mensajería de Exchange. Cuando se encuentre en las carpetas de correo del usuario algún elemento que no haya sido analizado con la última actualización de la base de datos de virus de AVG, se enviará a AVG para Exchange Server para que se analice. El análisis y la búsqueda de objetos no examinados se realiza en forma paralela.

Para cada base de datos se utiliza un subproceso específico de baja prioridad, el cual garantiza que el resto de tareas (por ejemplo, el almacenamiento de mensajes en la base de datos de Microsoft Exchange) siempre tenga preferencia.

- **Análisis proactivo (mensajes entrantes)**

Aquí puede activar o desactivar la función de análisis proactivo de VSAPI 2.0/2.5. El análisis ocurre cuando se recibe un elemento en una carpeta sin que el cliente realice ninguna petición.

En cuanto los mensajes se envían al almacén de Exchange, pasan a estar en la cola del análisis global con baja prioridad (el máximo son 30 elementos). Se analizan según el orden de llegada. Si se accede a un elemento mientras todavía está en la cola, éste cambia a prioridad alta.

Nota: los mensajes de desbordamiento se enviarán al almacén sin analizar.

*Nota: aunque desactive las opciones **Análisis en segundo plano** y **Análisis proactivo**, el analizador en acceso estará activo cuando un usuario intente descargar un mensaje con el cliente MS Outlook.*

- **Analizar RTF:** aquí puede especificar si deberá analizarse o no el tipo de archivo RTF.
- **No analizar los mensajes salientes (MS Exchange 2007/2010):** con los componentes de servidor VSAPI y el Agente de transporte enrutador ([AT enrutador](#)) instalados (independientemente de que sea en un solo servidor o en dos servidores diferentes), puede ocurrir que el correo saliente se analice dos veces. El primer análisis lo realiza el analizador en acceso VSAPI, y el segundo, el Agente de transporte enrutador. Esto puede hacer que el servidor vaya más lento y provocar retrasos moderados al enviar correos electrónicos. Si está seguro de que ambos componentes del servidor están instalados y activos, puede evitar este análisis duplicado de los correos electrónicos salientes deshabilitando esta casilla de verificación y el analizador en acceso VSAPI.
- **Número de subprocesos de análisis:** de manera predeterminada, el proceso de análisis se realiza mediante subprocesos a fin de aumentar el rendimiento general del análisis al emplear cierto nivel de paralelismo. Aquí puede modificar el número de subprocesos.

El número predeterminado de subprocesos se computa como 2 veces el 'número de procesadores' + 1.

El número mínimo de subprocesos se computa como ('número de procesadores'+1) dividido entre 2.

El número máximo de subprocesos se computa como 'número de procesadores' multiplicado por 5 + 1.

Si el valor es el mínimo o menor, o el máximo o mayor, se utiliza el valor predeterminado.

- **Tiempo de espera del análisis:** el intervalo continuo máximo (en segundos) para que un



proceso acceda al mensaje que está siendo analizado (el valor predeterminado es de 180 segundos).

La sección **Propiedades del análisis**:

- **Utilizar heurística**: marque esta casilla para activar el método de detección heurístico durante el análisis.
- **Informar de programas potencialmente no deseados y amenazas de spyware**: marque esta opción para informar sobre la presencia de programas potencialmente no deseados y spyware.
- **Informar de conjunto mejorado de programas potencialmente no deseados**: marque esta opción para detectar paquetes ampliados de spyware, es decir, programas perfectamente correctos y que no causan daño alguno cuando se adquieren directamente del fabricante, pero que pueden utilizarse más adelante para fines maliciosos (diversas barras de herramientas, etc.). Se trata de una medida adicional que aumenta aún más la seguridad y la comodidad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada. Nota: esta característica de detección es adicional a la opción anterior, por lo que si desea protección contra los tipos básicos de spyware, mantenga siempre activa la casilla anterior.
- **Analizar el contenido de los archivos comprimidos**: marque esta opción para permitir que el analizador busque también en los archivos comprimidos (zip, rar, etc.)

La sección **Informes de adjuntos de correo electrónico** le permite seleccionar sobre qué elementos deberá informarse durante el análisis. La configuración predeterminada puede modificarse fácilmente en la **sección Acciones de detección**, parte **Información** (consulte a continuación).

Las opciones disponibles son las siguientes:

- **Informar de archivos protegidos por contraseña**
- **Informar de documentos protegidos por contraseña**
- **Informar de archivos que contengan macros**
- **Informar de extensiones ocultas**

Generalmente, algunas de estas funciones son extensiones del usuario de los servicios de interfaz de la aplicación VSAPI 2.0/2.5 para Microsoft. Para obtener más información sobre VSAPI 2.0/2.5, consulte los siguientes vínculos (y también los vínculos accesibles desde los indicados aquí):

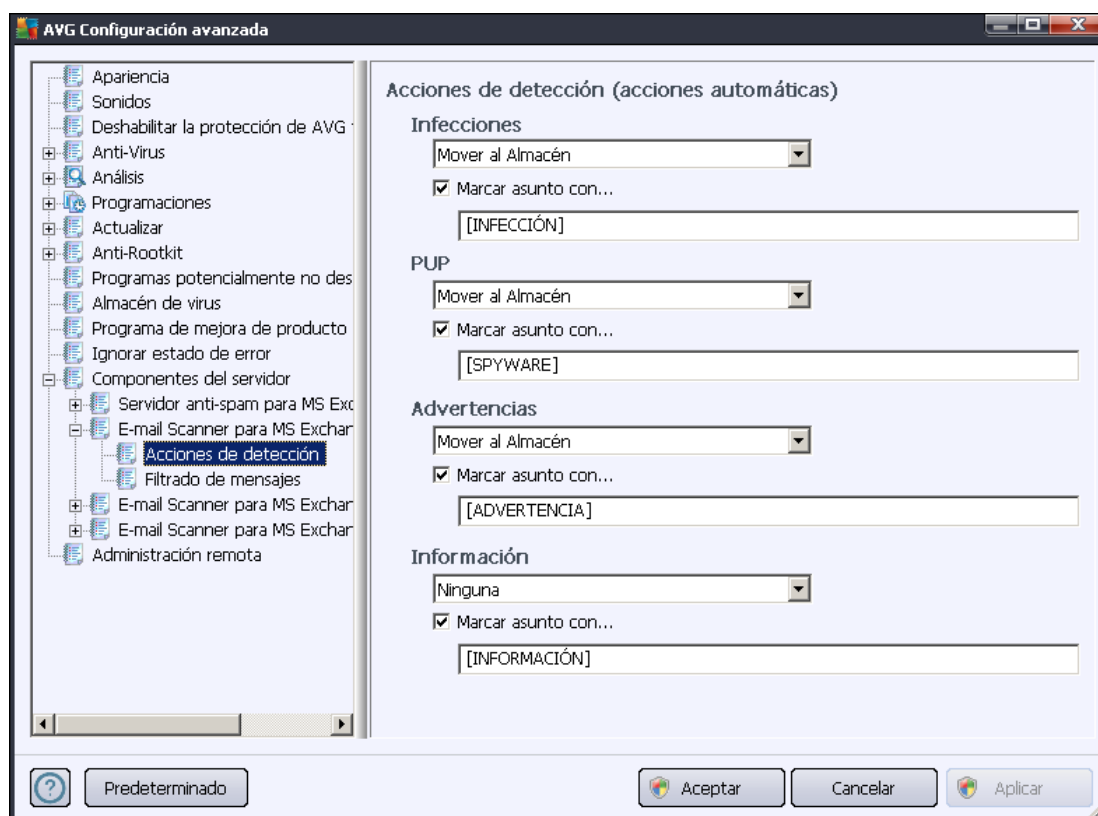
- <http://support.microsoft.com/default.aspx?scid=kb:en-us:328841&Product=exch2k>. Contiene información sobre la interacción entre Exchange y el software antivirus.
- <http://support.microsoft.com/default.aspx?scid=kb:en-us:823166>. Contiene información sobre características adicionales de VSAPI 2.5 en la aplicación Exchange 2003 Server.

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- **[Acciones de detección](#)**

- [Filtrado de mensajes](#)

4.5. Acciones de detección



En el subelemento **Acciones de detección** puede seleccionar las acciones automáticas que deberán llevarse a cabo durante el proceso de análisis.

Las acciones están disponibles para los siguientes elementos:

- **Infecciones**
- **PUP (Programas potencialmente no deseados)**
- **Advertencias**
- **Información**

Use el menú desplegable para seleccionar una acción para cada elemento:

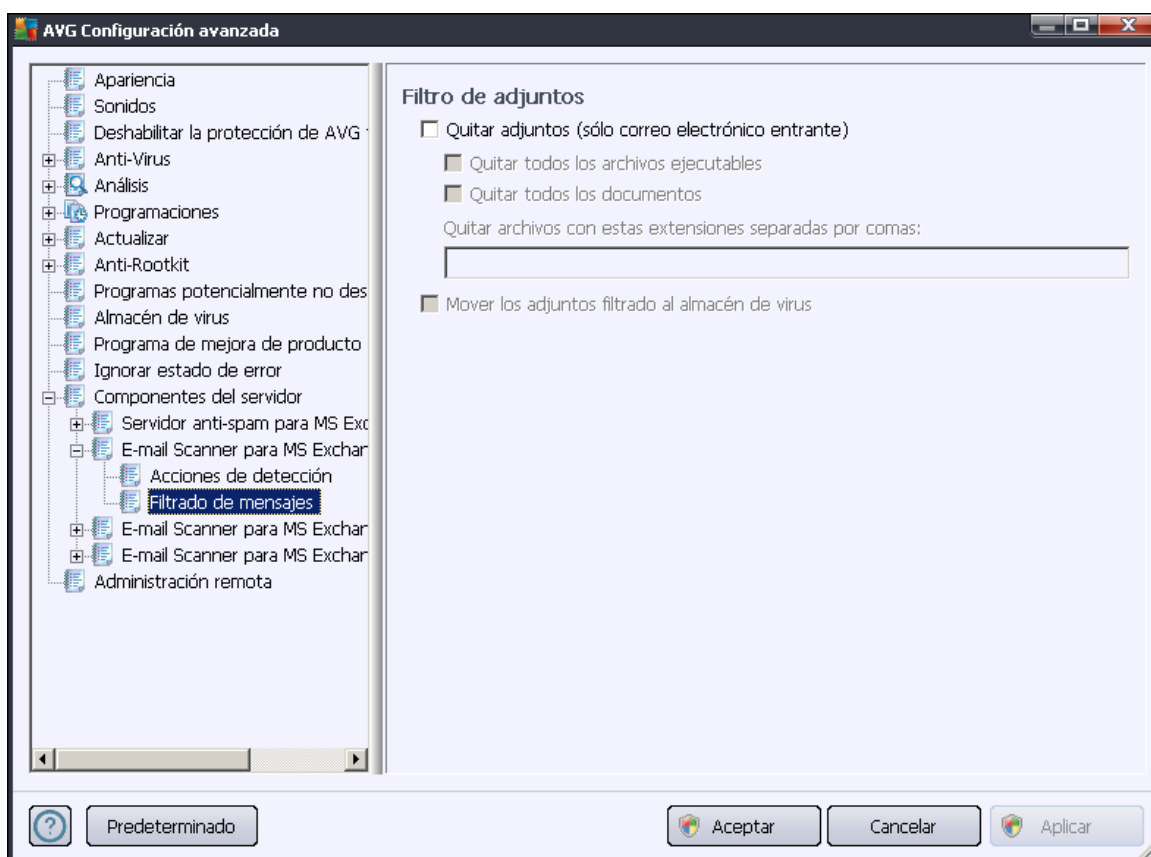
- **Ninguna:** no se llevará a cabo ninguna acción.
- **Mover al Almacén:** la amenaza en cuestión se enviará al Almacén de virus.
- **Quitar:** la amenaza en cuestión será eliminada.



Para seleccionar un texto personalizado para el asunto de los mensajes que contengan el elemento o amenaza en cuestión, marque la casilla **Marcar asunto con...** e introduzca el valor que desee.

Nota: la última característica mencionada no está disponible para el Analizador de correo electrónico para MS Exchange VSAPI.

4.6. Filtrado de mensajes



En el elemento secundario **Filtrado de mensajes** puede elegir los adjuntos que deben eliminarse automáticamente, si hay alguno. Las opciones disponibles son las siguientes:

- **Quitar adjuntos:** marque esta casilla para habilitar la característica.
- **Quitar todos los archivos ejecutables:** quita todos los archivos ejecutables.
- **Quitar todos los documentos:** quita todos los documentos.
- **Quitar archivos con estas extensiones separadas por comas:** complete la casilla con las extensiones de archivo que desea quitar automáticamente. Separe las extensiones con comas.
- **Mover los adjuntos filtrados al Almacén de virus:** marque esta opción si no desea que los adjuntos filtrados se eliminen completamente. Si esta casilla de verificación está marcada,



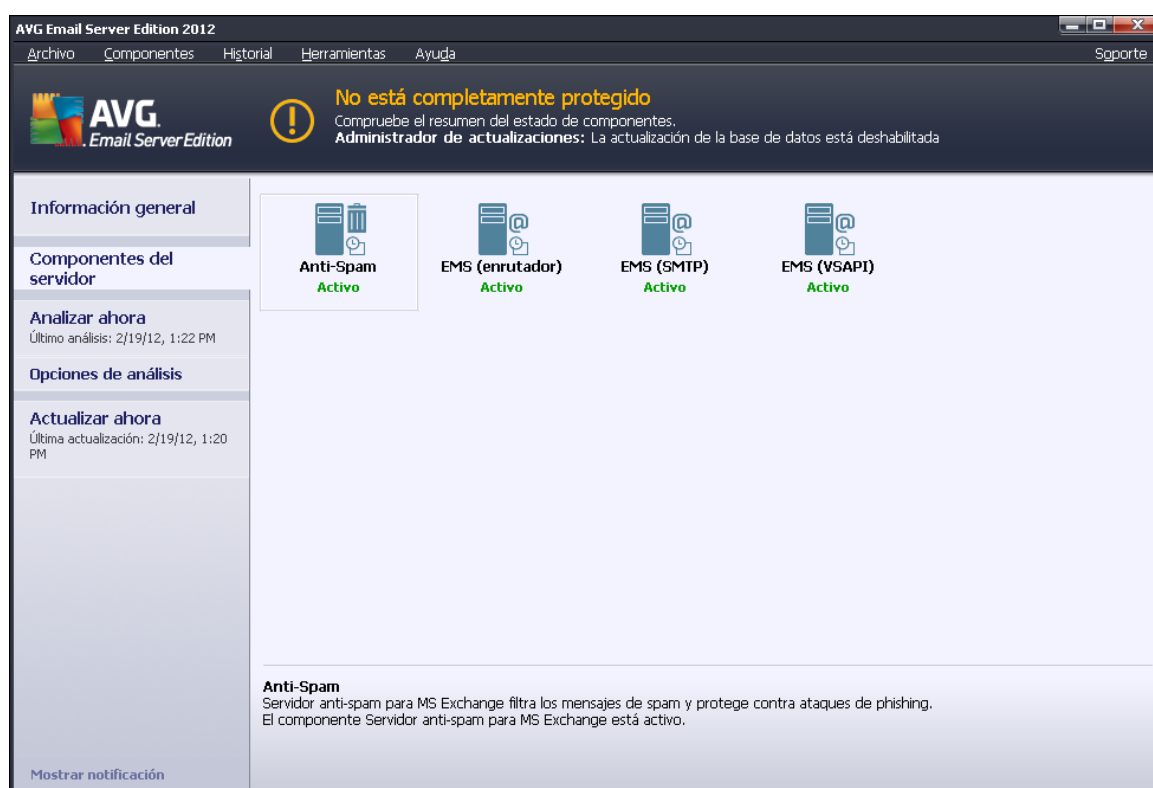
todos los adjuntos seleccionados en este cuadro de diálogo se enviarán automáticamente al entorno de cuarentena del Almacén de virus. Éste es un sitio seguro donde almacenar archivos potencialmente peligrosos: aquí puede visualizarlos y examinarlos sin que eso represente un peligro para el sistema. Puede acceder al Almacén de virus desde el menú superior de la interfaz principal de **AVG Email Server Edition 2012**. Simplemente, haga clic con el botón principal en el elemento **Historial** y seleccione el elemento **Almacén de virus** en el menú desplegable.



5. Analizador de correo electrónico para MS Exchange Server 2003

5.1. Información general

Las opciones de configuración del Analizador de correo electrónico para MS Exchange Server 2003 están completamente integradas en AVG Email Server Edition 2012 como un componente del servidor.



Los componentes del servidor incluyen las posibilidades siguientes:

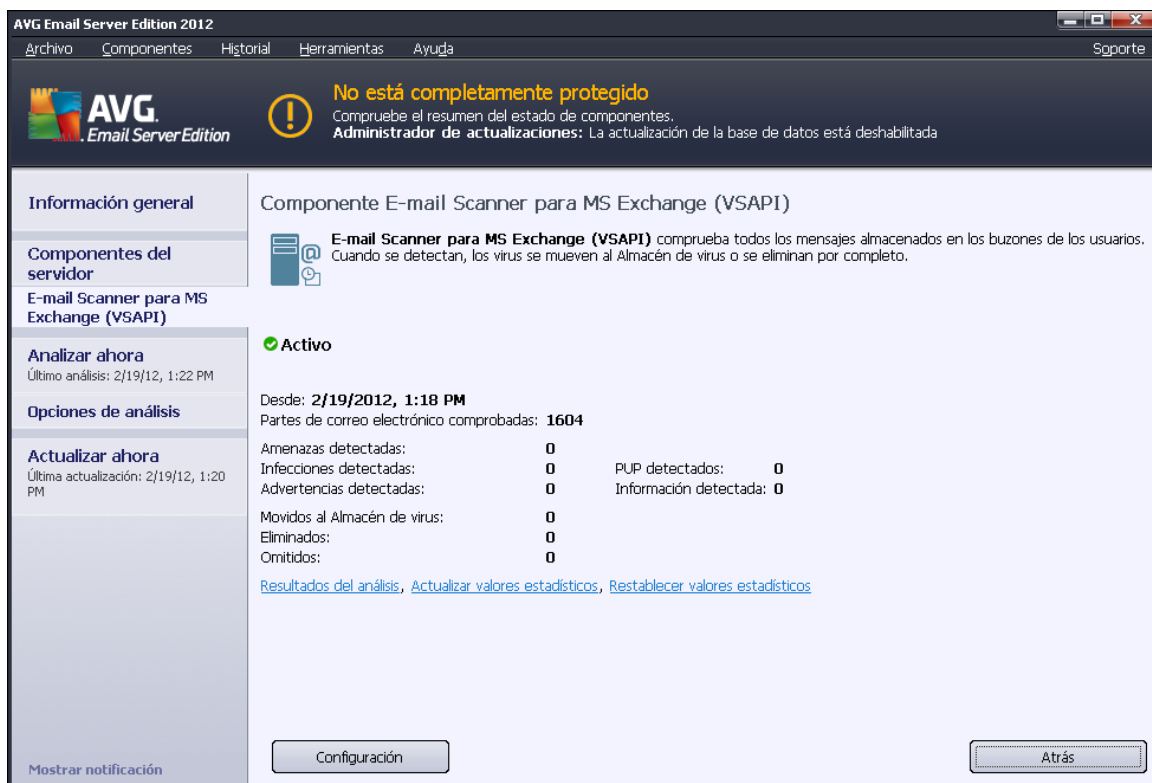
Información básica de los componentes individuales del servidor:

- [**Anti-Spam - Servidor anti-spam para MS Exchange**](#)
Comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como SPAM. Utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado.
- [**EMS \(VSAPI\) - Analizador de correo electrónico para MS Exchange \(VSAPI\)**](#)
Comprueba todos los mensajes de correo electrónico almacenados en los buzones de los usuarios. Los virus detectados se mueven al Almacén de virus o se eliminan completamente.

Haga clic en un componente requerido para abrir su interfaz. El **componente Anti-Spam** tiene su

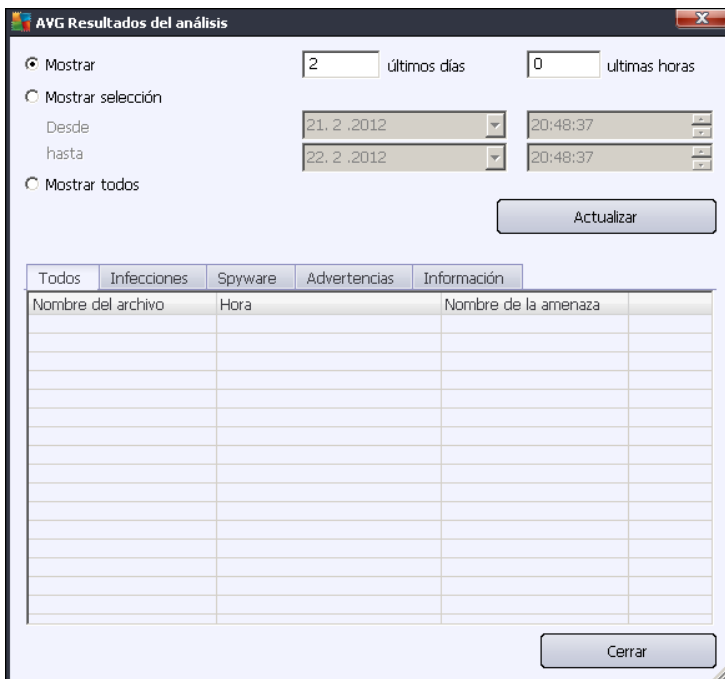


propia pantalla descrita en un [capítulo aparte](#). La interfaz del **Analizador de correo electrónico para MS Exchange (VSAPI)** dispone de los siguientes vínculos y botones de control:



- **Resultados del análisis**

Abre un nuevo cuadro de diálogo donde puede revisar los resultados del análisis:



Aquí puede comprobar los mensajes, que aparecen divididos en varias fichas de acuerdo a su gravedad. Consulte la configuración de los componentes individuales para modificar la gravedad y el informe.

De manera predeterminada, únicamente se muestran los resultados de los últimos dos días. Puede cambiar el período visualizado modificando las opciones siguientes:

- **Mostrar últimos:** introduzca los días y horas deseados.
- **Mostrar selección:** elija un intervalo de fecha y hora personalizado.
- **Mostrar todos:** muestra los resultados para el período completo.

Utilice el botón **Actualizar** para volver a cargar los resultados.

- **Actualizar valores estadísticos:** actualiza las estadísticas mostradas más arriba.
- **Restablecer valores estadísticos:** pone a cero todas las estadísticas.

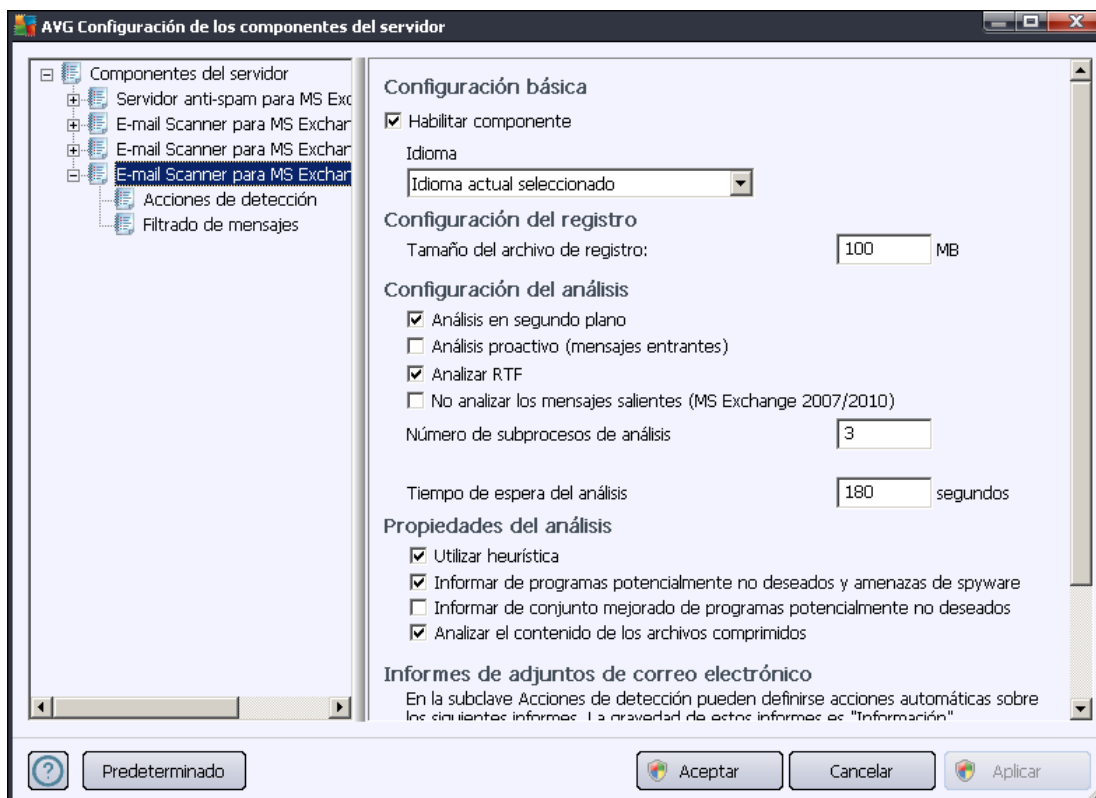
Los botones operativos son los siguientes:

- **Configuración:** utilice este botón para abrir la configuración del componente.
- **Atrás:** pulse este botón para volver a la información general de los componentes del servidor.

Encontrará más información sobre las configuraciones individuales de todos los componentes en los capítulos que se encuentran a continuación.

5.2. Analizador de correo electrónico para MS Exchange (VSAPI)

Este elemento contiene la configuración del *Analizador de correo electrónico para MS Exchange (VSAPI)*.



La sección **Configuración básica** ofrece las opciones siguientes:

- **Habilitar componente:** quite la marca para desactivar todo el componente.
- **Idioma:** seleccione el idioma deseado del componente.

La sección **Configuración del registro:**

- **Tamaño del archivo de registro:** elija el tamaño deseado del archivo de registro. Valor predeterminado: 100 MB.

La sección **Configuración del análisis:**

- **Análisis en segundo plano:** aquí puede activar o desactivar el proceso de análisis en segundo plano. El análisis en segundo plano es una de las características de la interfaz de la aplicación VSAPI 2.0/2.5. Ofrece análisis mediante subprocesos para las bases de datos de mensajería de Exchange. Cuando se encuentre en las carpetas de correo del usuario algún elemento que no haya sido analizado con la última actualización de la base de datos de virus de AVG, se enviará a AVG para Exchange Server para que se analice. El análisis y la búsqueda de objetos no examinados se realiza en forma paralela.



Para cada base de datos se utiliza un subproceso específico de baja prioridad, el cual garantiza que el resto de tareas (por ejemplo, el almacenamiento de mensajes en la base de datos de Microsoft Exchange) siempre tenga preferencia.

- **Análisis proactivo (mensajes entrantes)**

Aquí puede activar o desactivar la función de análisis proactivo de VSAPI 2.0/2.5. El análisis ocurre cuando se recibe un elemento en una carpeta sin que el cliente realice ninguna petición.

En cuanto los mensajes se envían al almacén de Exchange, pasan a estar en la cola del análisis global con baja prioridad (el máximo son 30 elementos). Se analizan según el orden de llegada. Si se accede a un elemento mientras todavía está en la cola, éste cambia a prioridad alta.

Nota: los mensajes de desbordamiento se enviarán al almacén sin analizar.

*Nota: aunque desactive las opciones **Análisis en segundo plano** y **Análisis proactivo**, el analizador en acceso estará activo cuando un usuario intente descargar un mensaje con el cliente MS Outlook.*

- **Analizar RTF:** aquí puede especificar si deberá analizarse o no el tipo de archivo RTF.
- **Número de subprocesos de análisis:** de manera predeterminada, el proceso de análisis se realiza mediante subprocesos a fin de aumentar el rendimiento general del análisis al emplear cierto nivel de paralelismo. Aquí puede modificar el número de subprocesos.

El número predeterminado de subprocesos se computa como 2 veces el 'número de procesadores' + 1.

El número mínimo de subprocesos se computa como ('número de procesadores'+1) dividido entre 2.

El número máximo de subprocesos se computa como 'número de procesadores' multiplicado por 5 + 1.

Si el valor es el mínimo o menor, o el máximo o mayor, se utiliza el valor predeterminado.

- **Tiempo de espera del análisis:** el intervalo continuo máximo (en segundos) para que un proceso acceda al mensaje que está siendo analizado (el valor predeterminado es de 180 segundos).

La sección **Propiedades del análisis:**

- **Utilizar heurística:** marque esta casilla para activar el método de detección heurístico durante el análisis.
- **Informar de programas potencialmente no deseados y amenazas de spyware:** marque esta opción para informar sobre la presencia de programas potencialmente no deseados y spyware.
- **Informar de conjunto mejorado de programas potencialmente no deseados:** marque esta opción para detectar paquetes ampliados de spyware, es decir, programas perfectamente



correctos y que no causan daño alguno cuando se adquieren directamente del fabricante, pero que pueden utilizarse más adelante para fines maliciosos (diversas barras de herramientas, etc.). Se trata de una medida adicional que aumenta aún más la seguridad y la comodidad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada. Nota: esta característica de detección es adicional a la opción anterior, por lo que si desea protección contra los tipos básicos de spyware, mantenga siempre activa la casilla anterior.

- **Analizar el contenido de los archivos comprimidos:** marque esta opción para permitir que el analizador busque también en los archivos comprimidos (zip, rar, etc.)

La sección **Informes de adjuntos de correo electrónico** le permite seleccionar sobre qué elementos deberá informarse durante el análisis. La configuración predeterminada puede modificarse fácilmente en la **sección Acciones de detección**, parte **Información** (consulte a continuación).

Las opciones disponibles son las siguientes:

- **Informar de archivos protegidos por contraseña**
- **Informar de documentos protegidos por contraseña**
- **Informar de archivos que contengan macros**
- **Informar de extensiones ocultas**

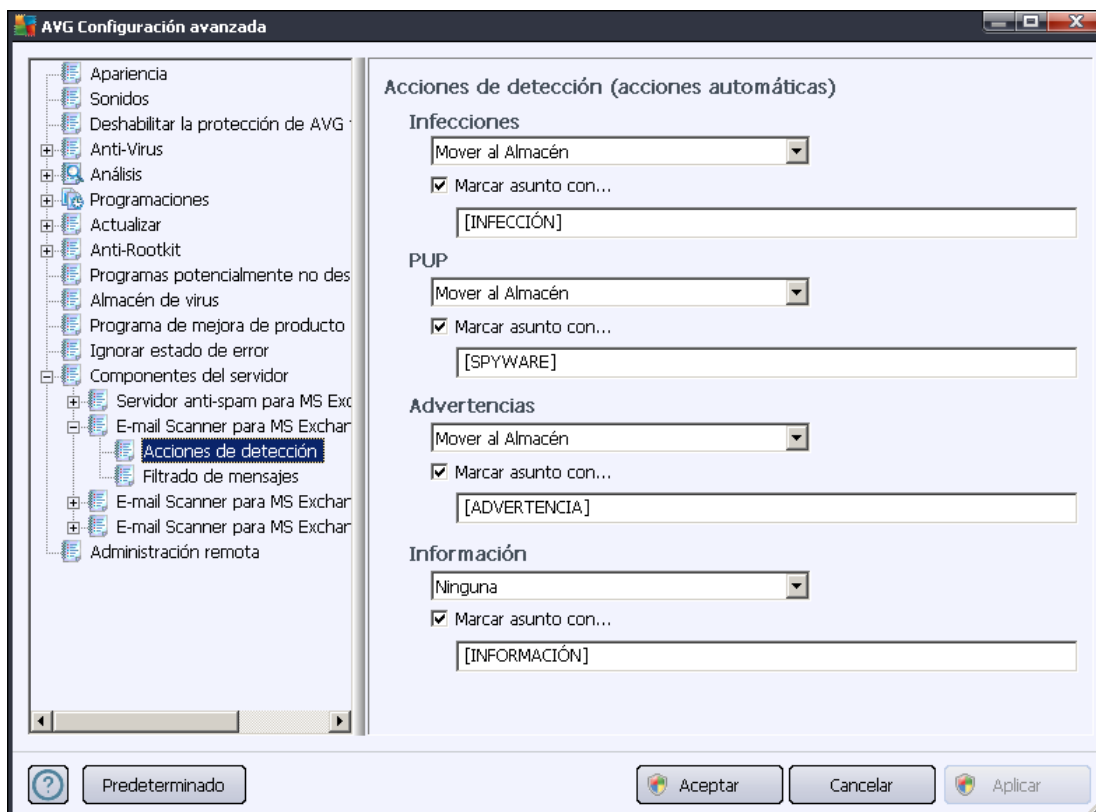
Generalmente, todas estas funciones son extensiones del usuario de los servicios de interfaz de la aplicación VSAPI 2.0/2.5 para Microsoft. Para obtener más información sobre VSAPI 2.0/2.5, consulte los siguientes vínculos (y también los vínculos accesibles desde los indicados aquí):

- <http://support.microsoft.com/default.aspx?scid=kb:en-us:328841&Product=exch2k>. Contiene información sobre la interacción entre Exchange y el software antivirus.
- <http://support.microsoft.com/default.aspx?scid=kb:en-us:823166>. Contiene información sobre características adicionales de VSAPI 2.5 en la aplicación Exchange 2003 Server.

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- [Acciones de detección](#)
- [Filtrado de mensajes](#)

5.3. Acciones de detección



En el subelemento **Acciones de detección** puede seleccionar las acciones automáticas que deberán llevarse a cabo durante el proceso de análisis.

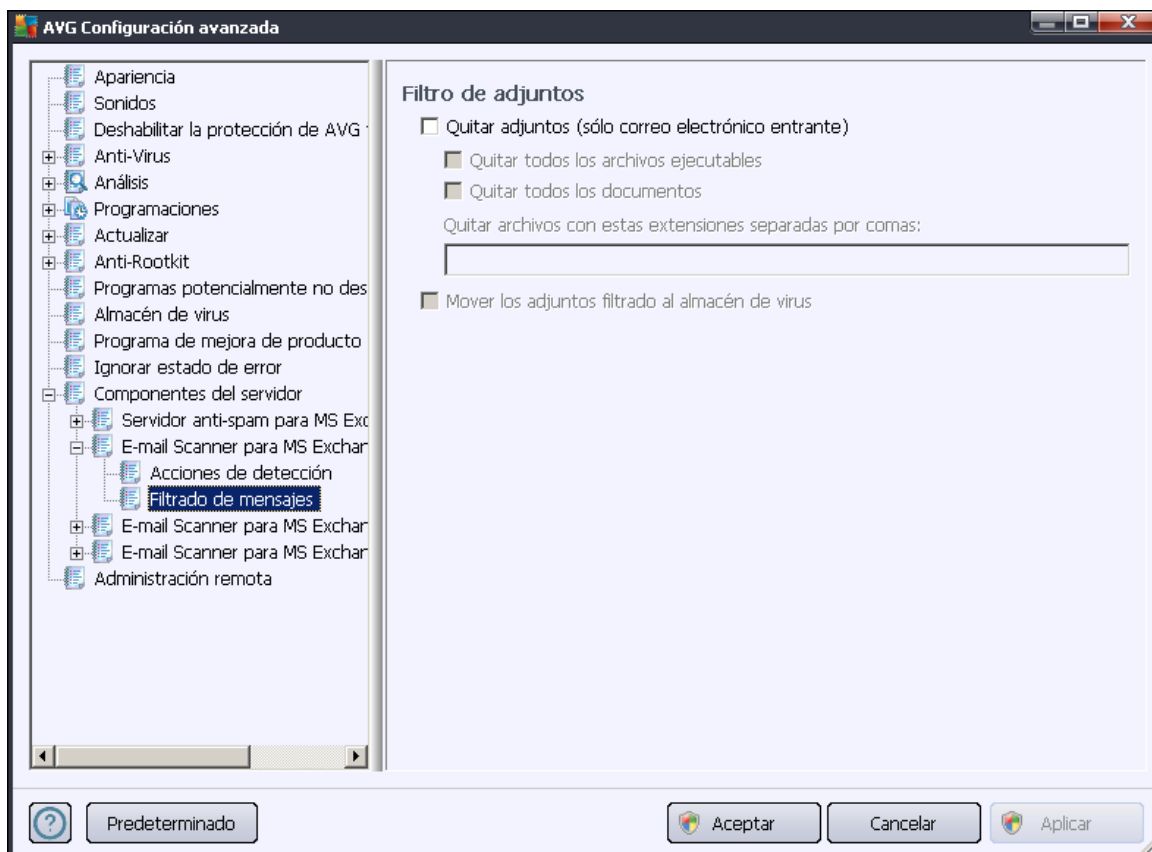
Las acciones están disponibles para los siguientes elementos:

- **Infecciones**
- **PUP (Programas potencialmente no deseados)**
- **Advertencias**
- **Información**

Use el menú desplegable para seleccionar una acción para cada elemento:

- **Ninguna:** no se llevará a cabo ninguna acción.
- **Mover al Almacén:** la amenaza en cuestión se enviará al Almacén de virus.
- **Quitar:** la amenaza en cuestión será eliminada.

5.4. Filtrado de mensajes



En el elemento secundario **Filtrado de mensajes** puede elegir los adjuntos que deben eliminarse automáticamente, si hay alguno. Las opciones disponibles son las siguientes:

- **Quitar adjuntos:** marque esta casilla para habilitar la característica.
- **Quitar todos los archivos ejecutables:** quita todos los archivos ejecutables.
- **Quitar todos los documentos:** quita todos los documentos.
- **Quitar archivos con estas extensiones separadas por comas:** complete la casilla con las extensiones de archivo que desea quitar automáticamente. Separe las extensiones con comas.
- **Mover los adjuntos filtrados al Almacén de virus:** marque esta opción si no desea que los adjuntos filtrados se eliminen completamente. Si esta casilla de verificación está marcada, todos los adjuntos seleccionados en este cuadro de diálogo se enviarán automáticamente al entorno de cuarentena del Almacén de virus. Éste es un sitio seguro donde almacenar archivos potencialmente peligrosos: aquí puede visualizarlos y examinarlos sin que eso represente un peligro para el sistema. Puede acceder al Almacén de virus desde el menú superior de la interfaz principal de **AVG Email Server Edition 2012**. Simplemente, haga clic con el botón principal en el elemento **Historial** y seleccione el elemento **Almacén de virus**

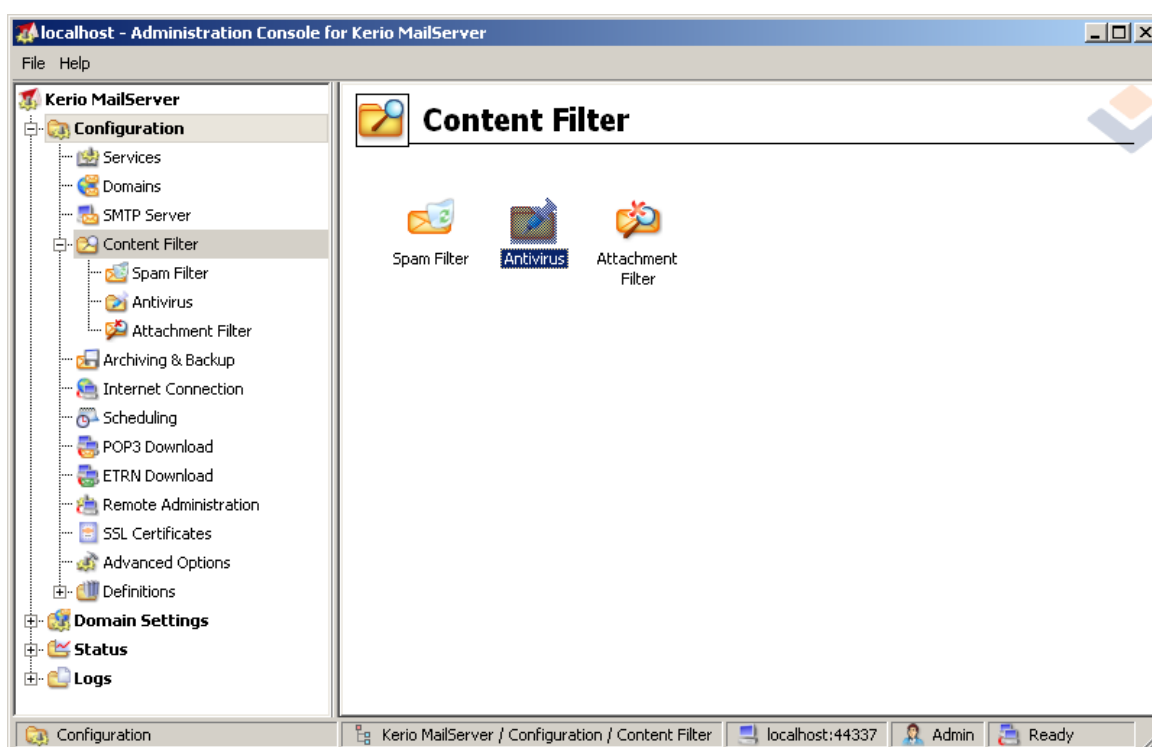


en el menú desplegable.

6. AVG for Kerio MailServer

6.1. Configuración

El mecanismo de protección del antivirus está integrado directamente en la aplicación de Kerio MailServer. Para activar la protección para correo electrónico de Kerio MailServer mediante el motor de análisis de AVG, inicie la aplicación Consola de administración de Kerio. En el árbol de control situado a la izquierda de la ventana de la aplicación, seleccione la subrama Filtro de contenido en la rama Configuración:

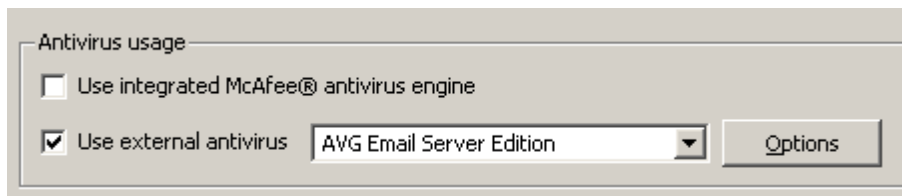


Si hace clic en Filtro de contenido, se mostrará un cuadro de diálogo con tres elementos:

- **Filtro de spam**
- [Antivirus](#) (consulte la sección **Antivirus**)
- [Filtro de archivos adjuntos](#) (consulte la sección **Filtro de archivos adjuntos**)

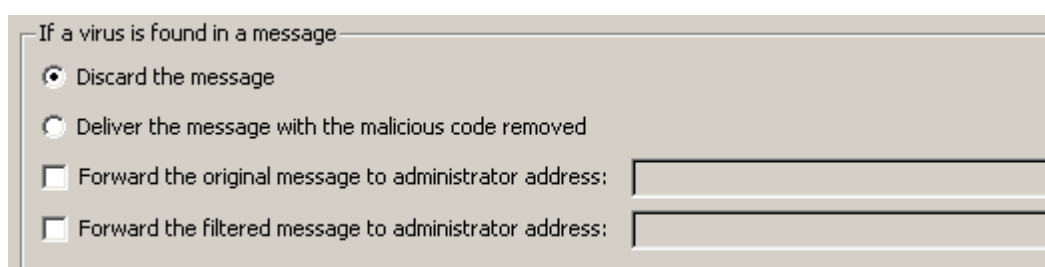
6.1.1. Antivirus

Para activar AVG para Kerio MailServer, seleccione la casilla Utilizar antivirus externo y elija el elemento AVG Email Server Edition en el menú de software externo, en la sección de uso del antivirus de la ventana de configuración:



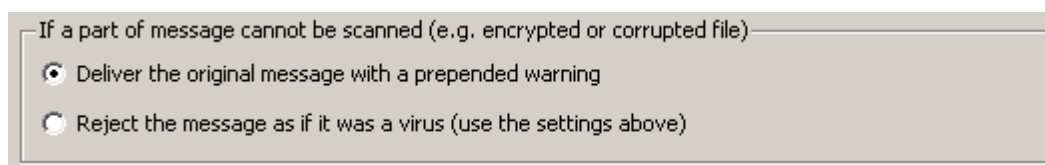
En la siguiente sección puede especificar lo que desea hacer con un mensaje infectado o filtrado:

- **Si se encuentra un virus en un mensaje**



Esta sección especifica la acción que se llevará a cabo cuando se detecte un virus en un mensaje o cuando un filtro de adjuntos filtre un mensaje:

- **Descartar mensaje:** si se selecciona, se eliminará el mensaje infectado o filtrado.
 - **Entregar mensaje después de quitar el código malicioso:** si se selecciona, el mensaje se entregará al receptor, pero sin el adjunto potencialmente dañino.
 - **Reenviar el mensaje original a la dirección del administrador:** si se selecciona, el mensaje infectado con virus se reenvía a la dirección especificada en el campo de texto de dirección
 - **Reenviar el mensaje filtrado a la dirección del administrador:** si se selecciona, el mensaje filtrado se reenvía a la dirección especificada en el campo de texto de dirección
- **Si no se puede analizar alguna parte del mensaje (p. ej., un archivo encriptado o dañado)**



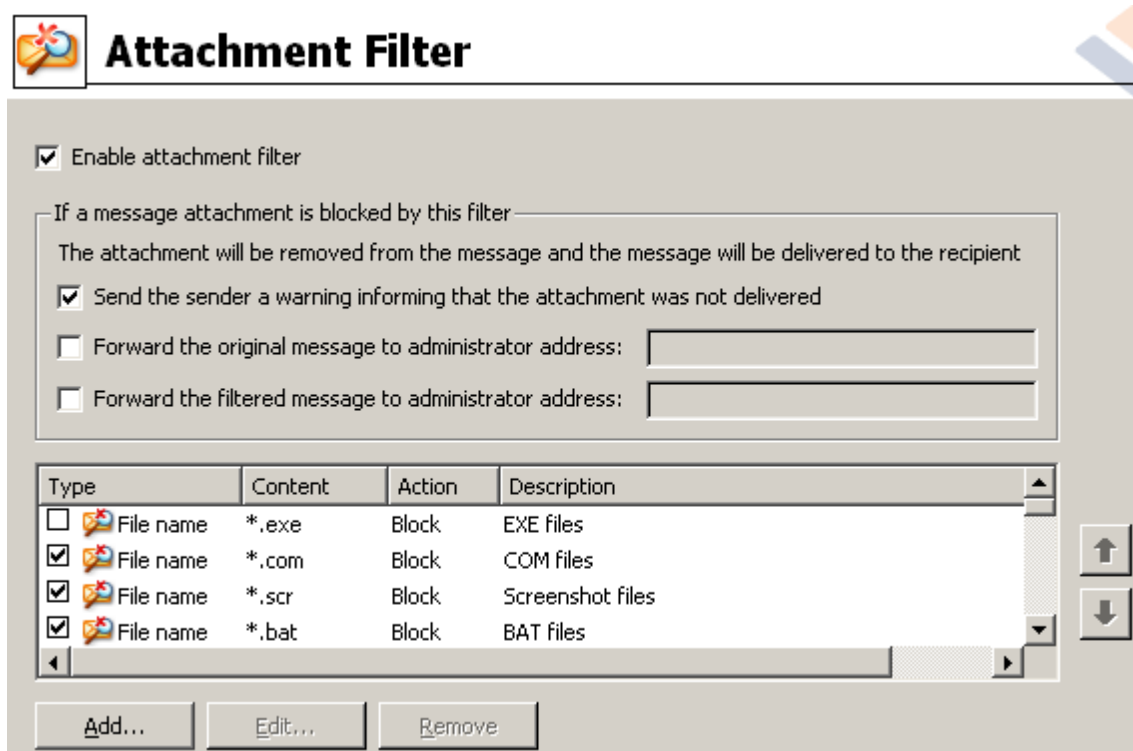
Esta sección especifica la acción que se realizará cuando no se puede analizar parte del mensaje o del archivo adjunto:

- **Entregar el mensaje original con un aviso preparado:** el mensaje (o archivo adjunto) se entregará sin comprobar. Se avisará al usuario de que el mensaje podría contener virus.

- **Rechazar el mensaje si era un virus:** el sistema reaccionará de la misma forma que cuando se detecta un virus (es decir, el mensaje se entregará sin archivo adjunto o se rechazará). Esta opción es segura, pero será prácticamente imposible enviar archivos protegidos por contraseña.

6.1.2. Filtro de adjuntos

En el menú Filtro de adjuntos, hay una lista de varias definiciones de adjuntos:



Puede habilitar o deshabilitar el filtrado de los adjuntos de correo seleccionando la casilla Habilitar filtro de adjuntos. Puede cambiar la siguiente configuración de forma opcional:

- **Enviar un aviso al remitente informando de que el adjunto no se ha entregado**
El remitente recibirá un aviso de Kerio MailServer informándole de que ha enviado un mensaje con un virus o un adjunto bloqueado.
- **Reenviar el mensaje original a la dirección del administrador**
El mensaje se reenviará (tal como está, con el adjunto infectado o prohibido) a una dirección de correo electrónico definida, independientemente de que se trate de una dirección local o externa.
- **Reenviar el mensaje filtrado a la dirección del administrador**
Se reenviará el mensaje sin el adjunto infectado o prohibido a la dirección de correo especificada (aparte de las acciones seleccionadas más abajo). Esto se puede utilizar para

verificar el funcionamiento correcto del antivirus y/o el filtro de adjuntos.

En la lista de extensiones, cada elemento tiene cuatro campos:

- **Tipo:** especificación del tipo de adjunto, determinado por la extensión dada en el campo Contenido. Tipos posibles son el nombre de archivo o MIME. Puede seleccionar la casilla correspondiente en este campo para incluir o no el elemento en el filtrado de adjuntos.
- **Contenido:** se puede introducir una extensión para incluirla en el filtrado. Aquí se pueden utilizar caracteres comodín reconocidos por el sistema (por ejemplo, la cadena "*.doc.*" significa cualquier archivo con extensión .doc, y cualquier otra extensión que la siga).
- **Acción:** defina la acción que se debe realizar con el adjunto específico. Las posibles acciones son Acepto (se acepta el adjunto) y Bloquear (se realizará una acción, según lo que se haya definido sobre la lista de adjuntos deshabilitados).
- **Descripción:** en este campo se define la descripción del adjunto.

Para quitar un elemento de la lista hay que pulsar el botón Quitar. Puede añadir otro elemento a la lista pulsando el botón **Agregar....** O bien puede editar un registro existente pulsando el botón **Editar....** A continuación, aparece la siguiente ventana:



- En el campo Descripción puede escribir una descripción corta del adjunto que se debe filtrar.
- En el campo "Si un mensaje contiene un adjunto donde" puede seleccionar el tipo de adjunto (Nombre de archivo o MIME). También puede elegir una extensión en particular de la lista de extensiones ofrecida, o bien escribir directamente el carácter comodín para la extensión.

En el campo "Entonces" puede decidir si desea bloquear el adjunto definido o aceptarlo.



7. Cómo configurar Anti-Spam

7.1. Interfaz de Anti-Spam

The screenshot shows the AVG Email Server Edition 2012 interface. At the top, there is a menu bar with 'Archivo', 'Componentes', 'Historial', 'Herramientas', 'Ayuda', and 'Soporte'. Below the menu bar, there is a warning message: 'No está completamente protegido' with a yellow exclamation mark icon. The main content area is titled 'Componente Servidor anti-spam para MS Exchange'. It includes a description of the component, its status (Active), and a table of statistics. The statistics table shows the version (6.4.0), the last update of the database (Friday, July 01, 2011, 1:00 AM), and the number of messages checked, spam detected, and phishing emails found, all reported as 0 since 2/19/2012, 1:18 PM. There are also links for 'Resultados del análisis', 'Actualizar valores estadísticos', and 'Restablecer valores estadísticos'. At the bottom, there is a checkbox for 'Habilitar Anti-Spam' which is checked, and buttons for 'Configuración', 'Guardar cambios', and 'Cancelar'.

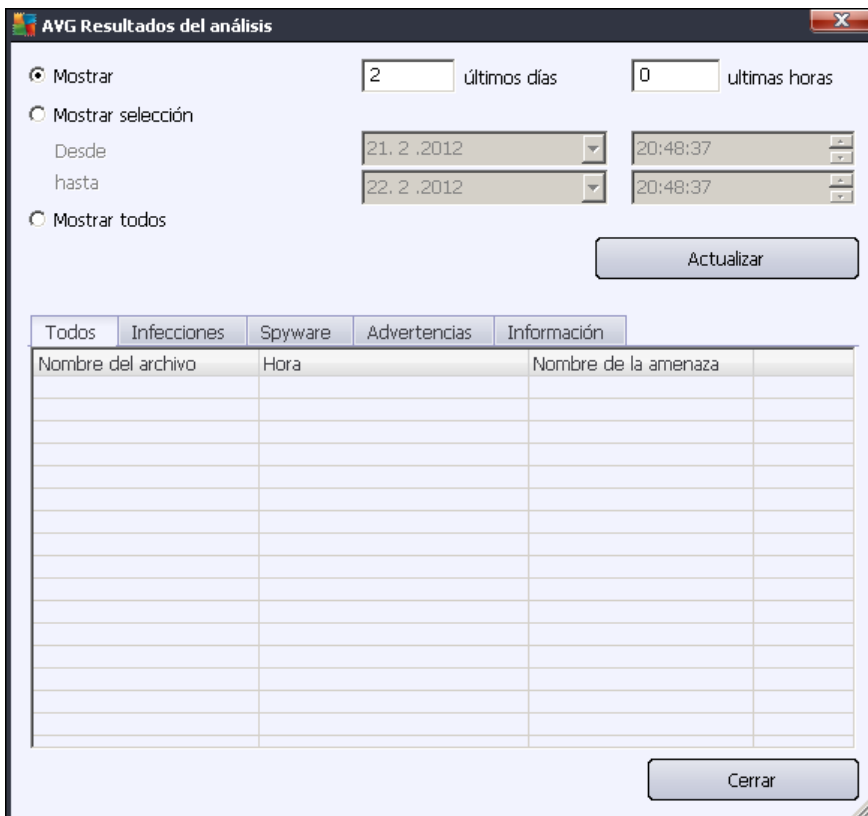
Componente Servidor anti-spam para MS Exchange	
Servidor anti-spam para MS Exchange comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como spam. Utiliza diversos métodos de análisis ofreciendo la máxima protección posible.	
● Activo	
Versión del componente:	6.4.0
Última actualización de la base de datos:	Friday, July 01, 2011, 1:00 AM
Mensajes de correo electrónico comprobados:	0 desde 2/19/2012, 1:18 PM
Mensajes de spam detectados:	0 desde 2/19/2012, 1:18 PM
Correos electrónicos con Phishing encontrados:	0 desde 2/19/2012, 1:18 PM

El cuadro de diálogo del componente del servidor **Anti-Spam** se ubica en la sección **Componentes del servidor** (menú izquierdo). Contiene información breve sobre la funcionalidad del componente del servidor, su estado actual (*El componente Servidor anti-spam para MS Exchange está activo.*) y algunas estadísticas.

Vínculos disponibles:

- **Resultados del análisis**

Abre un nuevo cuadro de diálogo donde puede revisar los resultados del análisis anti-spam:



The screenshot shows a window titled "AVG Resultados del análisis". It features three radio button options: "Mostrar" (selected), "Mostrar selección", and "Mostrar todos". The "Mostrar" option has two input fields: "2" for "últimos días" and "0" for "últimas horas". The "Mostrar selección" option has two date-time pickers: "Desde" (21. 2 .2012 20:48:37) and "hasta" (22. 2 .2012 20:48:37). Below these is an "Actualizar" button. A tabbed interface at the bottom includes tabs for "Todos", "Infecciones", "Spyware", "Advertencias", and "Información". Under the "Todos" tab is a table with columns: "Nombre del archivo", "Hora", and "Nombre de la amenaza". The table is currently empty. A "Cerrar" button is located at the bottom right.

Aquí puede comprobar los mensajes detectados como spam (mensajes no deseados) o como phishing (intentos de robar sus datos personales, datos bancarios, identidad, etc.). De manera predeterminada, únicamente se muestran los resultados de los últimos dos días. Puede cambiar el período visualizado modificando las opciones siguientes:

- **Mostrar últimos:** introduzca los días y horas deseados.
- **Mostrar selección:** elija un intervalo de fecha y hora personalizado.
- **Mostrar todos:** muestra los resultados para el período completo.

Utilice el botón **Actualizar** para volver a cargar los resultados.

- **Actualizar valores estadísticos:** actualiza las estadísticas mostradas más arriba.
- **Restablecer valores estadísticos:** pone a cero todas las estadísticas.

La sección **Configuración de Anti-spam** del cuadro de diálogo contiene una sola casilla de verificación: **Habilitar Anti-spam**. Deje en blanco esta casilla para deshabilitar la protección de Anti-spam (es decir, desactivar todo el componente). Puede volver a activar la protección de Anti-spam mediante la misma casilla de verificación o marcando una casilla de verificación similar en [Configuración de Anti-spam](#).

Los botones operativos son los siguientes:

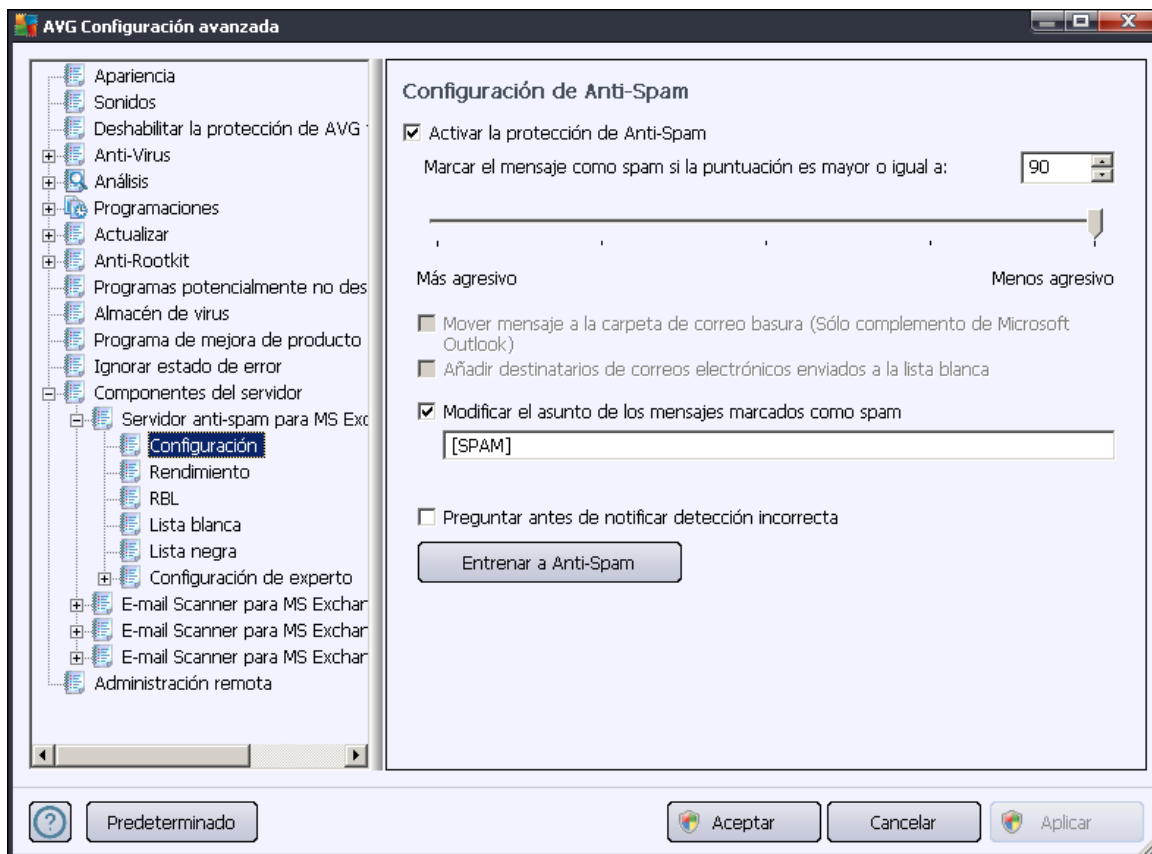
- **Configuración:** utilice este botón para abrir [Configuración de Anti-Spam](#).
- **Atrás:** pulse este botón para volver a la información general de los componentes del servidor.

7.2. Principios de Anti-Spam

El spam se refiere al correo electrónico no solicitado, generalmente anunciando un producto o servicio, que se envía masiva y simultáneamente a un gran número de direcciones de correo electrónico, llenando los buzones de los destinatarios. El spam no hace referencia al correo comercial legítimo al que los consumidores dan su consentimiento. El spam no solamente es molesto, sino que también suele ser fuente de estafas, virus o contenidos ofensivos.

Anti-Spam comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como spam. Utiliza varios métodos de análisis para procesar cada mensaje, ofreciendo la máxima protección posible contra el correo no deseado.

7.3. Configuración de Anti-Spam



En el cuadro de diálogo **Configuración básica de Anti-Spam** puede marcar la casilla **Activar la**



protección de Anti-Spam para permitir o prohibir el análisis anti-spam de la comunicación por correo electrónico.

En este cuadro de diálogo, también puede seleccionar valores de puntuación más o menos agresivos. El filtro **Anti-Spam** asigna una puntuación a cada mensaje (*es decir, el grado de similitud del contenido del mensaje con el spam*) en función de diversas técnicas de análisis dinámico. Puede ajustar la configuración de **Marcar el mensaje como spam si la puntuación es mayor o igual a** introduciendo el valor (50 a 90) o moviendo el control deslizante a la derecha o izquierda.

A continuación se ofrece un resumen del umbral de puntuación:

- **Valor 90:** la mayoría de los mensajes de correo electrónico entrantes se entregarán normalmente (sin ser marcados como [spam](#)). El [spam](#) más fácilmente identificable se filtrará, pero una cantidad importante de [spam](#) se seguirá permitiendo.
- **Valor 80-89:** los mensajes de correo electrónico con alta probabilidad de ser [spam](#) se filtrarán. También pueden filtrarse erróneamente algunos mensajes que no son spam.
- **Valor 60-79:** considerada como una configuración bastante agresiva. Los mensajes que posiblemente puedan ser [spam](#) se filtrarán. Es probable que también se retengan mensajes que no son spam.
- **Valor 50-59:** configuración muy agresiva. Es probable que los mensajes de correo electrónico que no son spam se identifiquen como mensajes de [spam](#) auténticos. Este intervalo no se recomienda para uso normal.

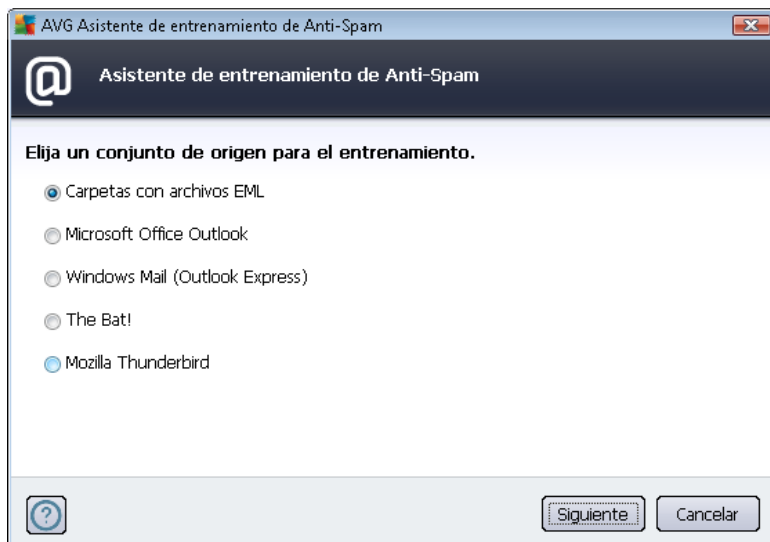
Posteriormente puede definir cómo se deben tratar los mensajes de [spam](#) detectados:

- **Modificar el asunto de los mensajes marcados como spam:** marque esta casilla si desea que todos los mensajes detectados como [spam](#) sean marcados con una palabra o carácter específico en el asunto del correo; el texto deseado se puede introducir en el campo de texto activo.
- **Preguntar antes de notificar detección incorrecta:** suponiendo que durante el proceso de instalación aceptara participar en el Programa de mejora de productos (este programa nos ayuda a recopilar información actualizada sobre las amenazas más recientes de parte de personas del mundo entero, lo cual nos permite ofrecer una mejor protección a todos nuestros usuarios), es decir, que aceptara informar a AVG sobre las amenazas detectadas. La notificación se procesa automáticamente. No obstante, puede marcar esta casilla de verificación para confirmar que desea ser consultado antes de informar a AVG sobre spam detectado con el fin de asegurarse de que el mensaje debe clasificarse realmente como spam.

El botón **Entrenar a Anti-Spam** abre el [Asistente de entrenamiento de Anti-Spam](#) descrito en detalle en el [siguiente capítulo](#).

7.3.1. Asistente de entrenamiento de Anti-Spam

El primer cuadro de diálogo del **Asistente de entrenamiento de Anti-Spam** le pide que seleccione el origen de los mensajes de correo electrónico que desea utilizar para el entrenamiento. Normalmente deseará utilizar correos electrónicos marcados incorrectamente como spam o mensajes de spam que no han sido reconocidos.



Puede elegir entre las siguientes opciones:

- **Un cliente específico de correo electrónico:** si utiliza uno de los clientes de correo electrónico enumerados (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), simplemente seleccione la opción correspondiente
- **Carpeta con archivos EML:** si utiliza cualquier otro programa de correo electrónico, deberá guardar previamente los mensajes en una carpeta determinada (*en formato .eml*) o asegurarse de que conoce la ubicación de las carpetas de mensajes de su cliente de correo electrónico. A continuación, seleccione **Carpeta con archivos EML**, que le permite localizar la carpeta deseada en el siguiente paso

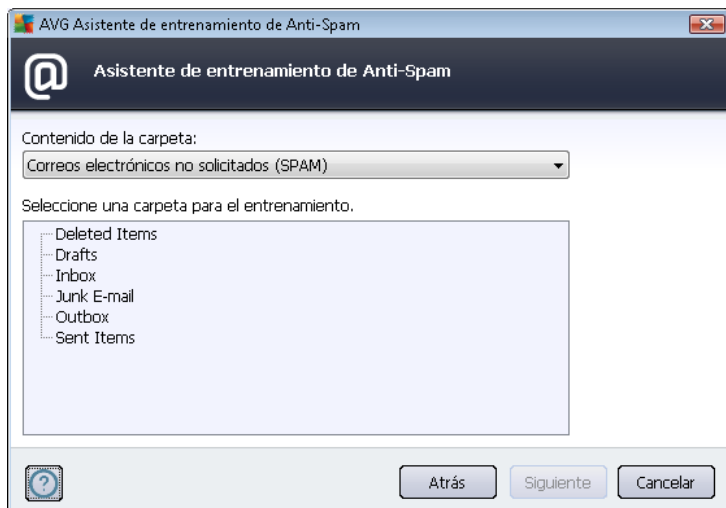
Para que el proceso de entrenamiento sea más rápido y fácil, se recomienda ordenar de antemano los correos electrónicos en las carpetas, de manera que la carpeta que utilice para el entrenamiento contenga solamente los mensajes de entrenamiento (deseados o no deseados). No obstante, esto no es necesario, ya que posteriormente podrá filtrar los correos electrónicos.

Seleccione la opción adecuada y haga clic en **Siguiente** para continuar con el asistente.

7.3.2. Seleccionar carpeta con mensajes

El cuadro de diálogo mostrado en este paso depende de su selección previa.

Carpetas con archivos EML



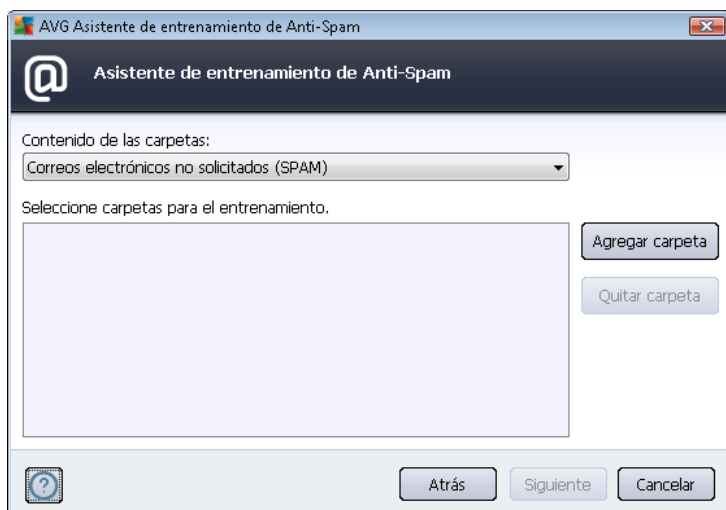
En este cuadro de diálogo, seleccione la carpeta con los mensajes que desea utilizar para el entrenamiento. Pulse el botón **Agregar carpeta** para localizar la carpeta con los archivos .eml (*mensajes de correo electrónico guardados*). A continuación, la carpeta seleccionada aparecerá en el cuadro de diálogo.

En el menú desplegable **Contenido de las carpetas**, defina una de las dos opciones: si la carpeta seleccionada contiene mensajes deseados (*HAM*) o no deseados (*SPAM*). Tenga en cuenta que podrá filtrar los mensajes en el paso siguiente, por lo que no es necesario que la carpeta contenga solamente los correos electrónicos para el entrenamiento. También puede quitar de la lista carpetas que no desee seleccionándolas y haciendo clic en el botón **Quitar carpeta**.

Cuando haya finalizado, haga clic en **Siguiente** y pase a [Opciones de filtrado de mensajes](#).

Cliente de correo electrónico específico

Cuando haya confirmado una de las opciones, aparecerá un nuevo cuadro de diálogo.

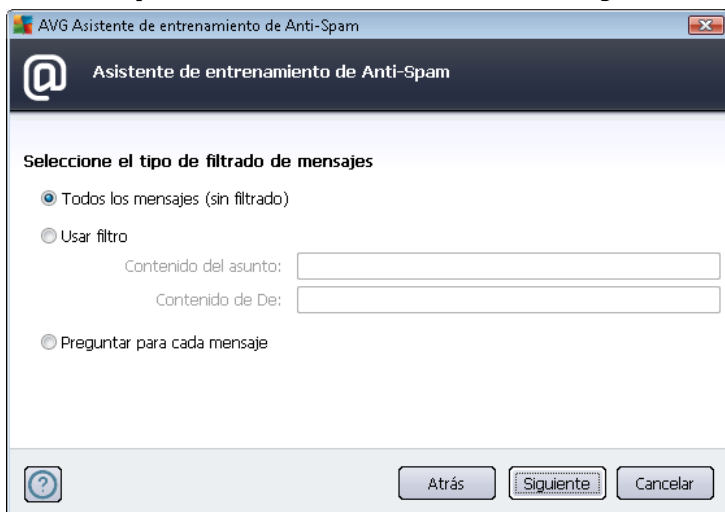


Nota: en el caso de Microsoft Office Outlook, se le solicitará primero que seleccione el perfil de MS Office Outlook que desee.

En el menú desplegable **Contenido de las carpetas**, defina una de las dos opciones: si la carpeta seleccionada contiene mensajes deseados (*HAM*) o no deseados (*SPAM*). Tenga en cuenta que podrá filtrar los mensajes en el paso siguiente, por lo que no es necesario que la carpeta contenga solamente los correos electrónicos para el entrenamiento. En la sección principal del cuadro de diálogo aparece un árbol de navegación del cliente de correo electrónico seleccionado. Localice en el árbol la carpeta deseada y resáltela con el ratón.

Cuando haya finalizado, haga clic en **Siguiente** y pase a [Opciones de filtrado de mensajes](#).

7.3.3. Opciones de filtrado de mensajes



En este cuadro de diálogo puede definir el filtrado de los mensajes de correo electrónico.

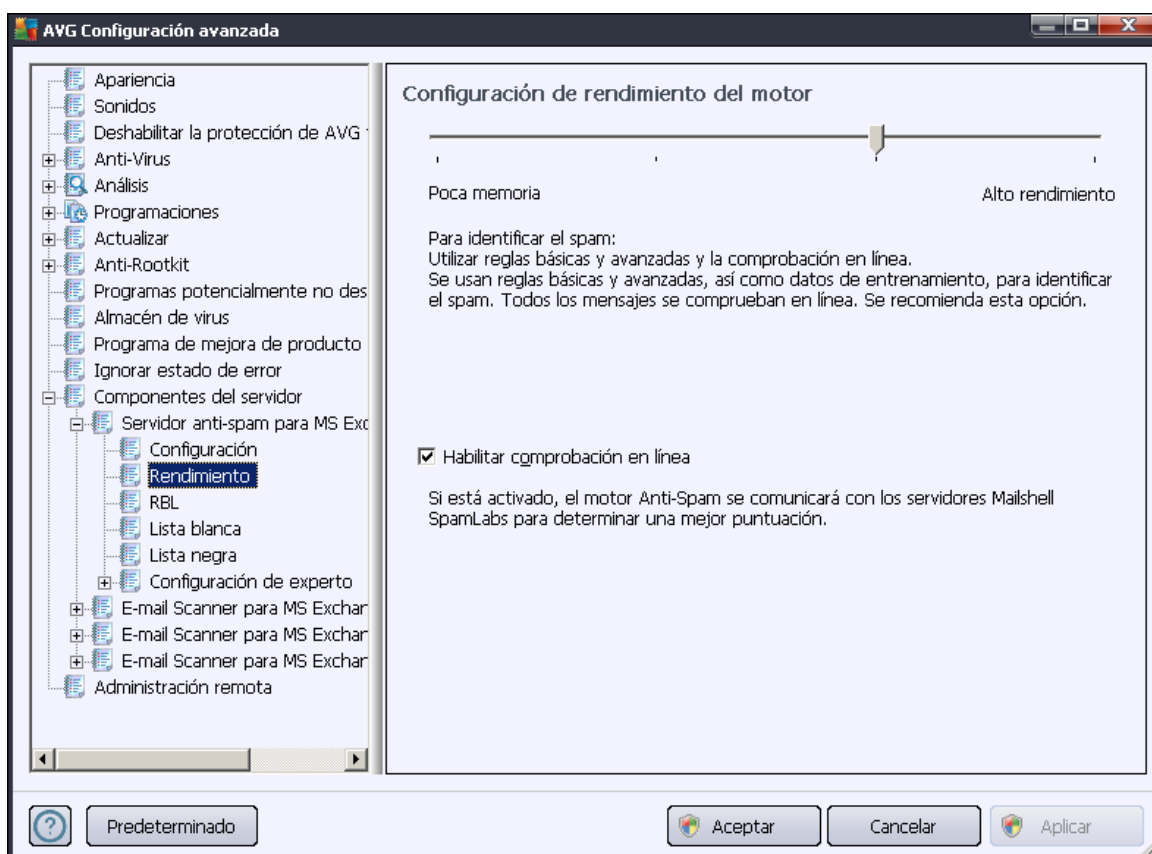
- **Todos los mensajes (sin filtrado):** si está seguro de que la carpeta seleccionada contiene solamente los mensajes que desea utilizar para el entrenamiento, seleccione la opción **Todos los mensajes (sin filtrado)**.
- **Usar filtro:** si prefiere un filtrado más avanzado, seleccione la opción **Usar filtro**. Puede escribir una palabra (*nombre*), parte de una palabra o una frase para buscar en el asunto del correo electrónico y/o el campo del remitente. Todos los mensajes que coincidan exactamente con los criterios introducidos se utilizarán para el entrenamiento sin necesidad de seguir interviniendo. Si rellena los dos campos de texto, también se usarán las direcciones que coincidan solamente con una de las condiciones.
- **Preguntar para cada mensaje:** si tiene dudas acerca de los mensajes que contiene la carpeta y desea que el asistente le pregunte sobre cada mensaje (*para que pueda indicar si desea utilizarlo para el entrenamiento o no*), seleccione la opción **Preguntar para cada mensaje**.

Cuando haya seleccionado la opción apropiada, haga clic en **Siguiente**. El siguiente cuadro de diálogo es meramente informativo y le indica que el asistente está preparado para procesar los mensajes. Para comenzar el entrenamiento, vuelva a hacer clic en el botón **Siguiente**. El



entrenamiento se iniciará según las condiciones seleccionadas con anterioridad.

7.4. Rendimiento



El cuadro de diálogo **Configuración de rendimiento del motor** (al que se accede mediante el elemento **Rendimiento** del panel de navegación izquierdo) ofrece la configuración de rendimiento del componente **Anti-Spam**. Mueva el control deslizante hacia la izquierda o la derecha para cambiar el nivel de rendimiento del análisis entre los modos **Poca memoria** / **Alto rendimiento**.

- **Poca memoria:** durante el proceso de análisis realizado para detectar [spam](#), no se utilizarán reglas. Sólo se emplearán datos de entrenamiento para la identificación. Este modo no se recomienda para uso común, a menos que el equipo cuente con escasos recursos de hardware.
- **Alto rendimiento:** este modo consumirá una gran cantidad de memoria. Durante el proceso de análisis realizado para detectar [spam](#), se emplearán las siguientes características: reglas y caché de base de datos de [spam](#), reglas básicas y avanzadas, direcciones IP de remitentes que envían spam y bases de datos de remitentes que envían spam.

El elemento **Habilitar comprobación en línea** está activado de manera predeterminada. En consecuencia, se obtiene una detección más precisa del [spam](#) gracias a la comunicación con los servidores [Mailshell](#); es decir, los datos analizados se compararán con el contenido de la base de

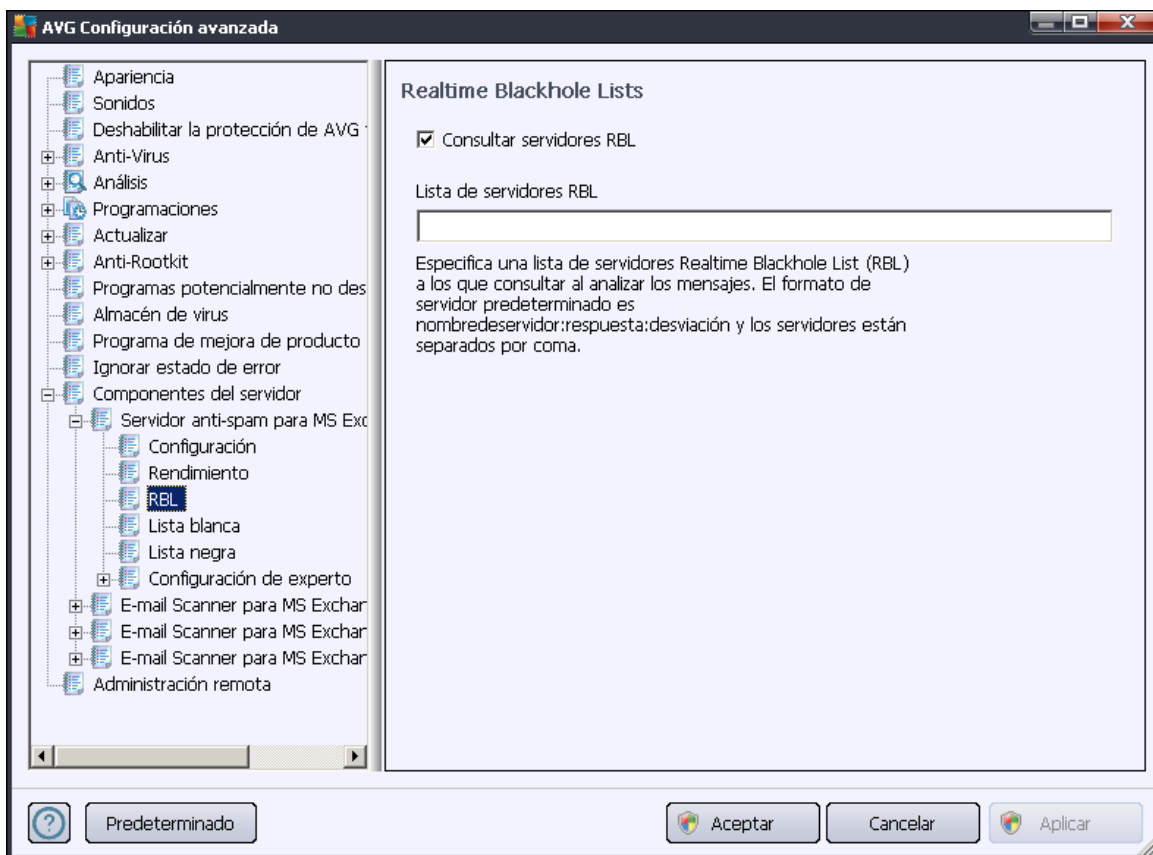


datos de [Mailshell](#) en línea.

En términos generales, se recomienda mantener la configuración predeterminada y cambiarla únicamente si existe algún motivo que en verdad justifique hacerlo. Cualquier cambio en la configuración sólo debe ser realizado por usuarios expertos.

7.5. RBL

El elemento **RBL** abre un cuadro de diálogo de edición llamado **Realtime Blackhole Lists**:



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

Un servidor RBL (*Realtime Blackhole List*) es un servidor DNS con una extensa base de datos de remitentes que se sabe suelen enviar correo no deseado (spam). Cuando esta característica está activada, todos los mensajes de correo electrónico se verifican comparándolos con la base de datos del servidor RBL y se marcan como [spam](#) si coinciden con alguna de las entradas de la base de datos.

Las bases de datos de los servidores RBL contienen las últimas huellas dactilares de spam, actualizadas al minuto, lo que proporciona una detección del [spam](#) sumamente precisa y eficiente. Esta característica es útil en especial para aquellos usuarios que reciben grandes cantidades de correo no deseado que el motor Anti-Spam normalmente no detecta.



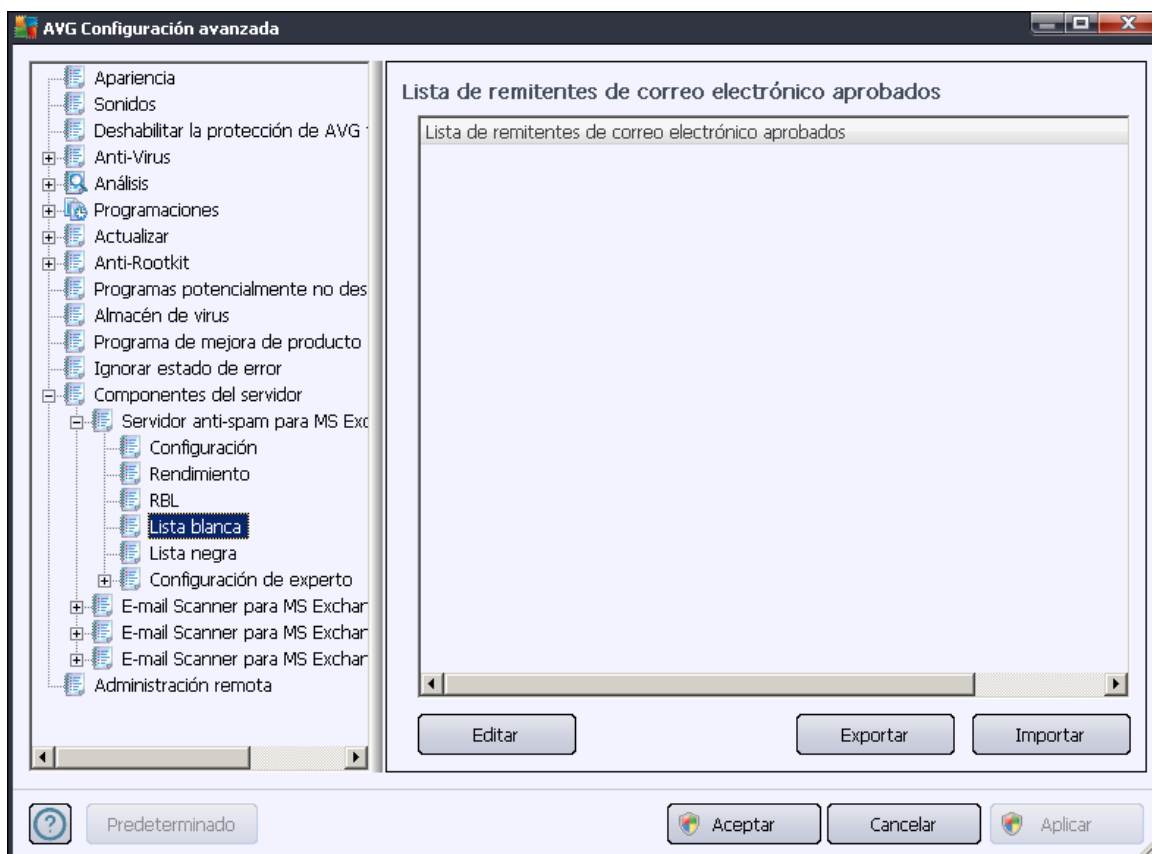
La **lista de servidores RBL** le permite definir ubicaciones específicas de los servidores RBL. De manera predeterminada, se especifican dos direcciones de servidores RBL. Le recomendamos que mantenga la configuración predeterminada a menos que sea un usuario experimentado y necesite realmente cambiar esta configuración.

Nota: el hecho de habilitar esta característica puede hacer que el proceso de recepción de correos electrónicos se vuelva más lento en algunos sistemas y configuraciones, dado que se debe verificar cada mensaje según la base de datos del servidor RBL.

No se envía ningún dato personal al servidor.

7.6. Lista blanca

El elemento **Lista blanca** abre un cuadro de diálogo que incluye una lista global de direcciones de remitentes de correo electrónico y nombres de dominio aprobados cuyos mensajes nunca se marcarán como [spam](#).



En la interfaz de edición puede compilar una lista de remitentes de los que tiene la seguridad que nunca le enviarán mensajes no deseados ([spam](#)). Del mismo modo, puede compilar una lista de nombres de dominio completos (por ejemplo, [avg.com](#)), que sabe que no generan mensajes de spam.

Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras

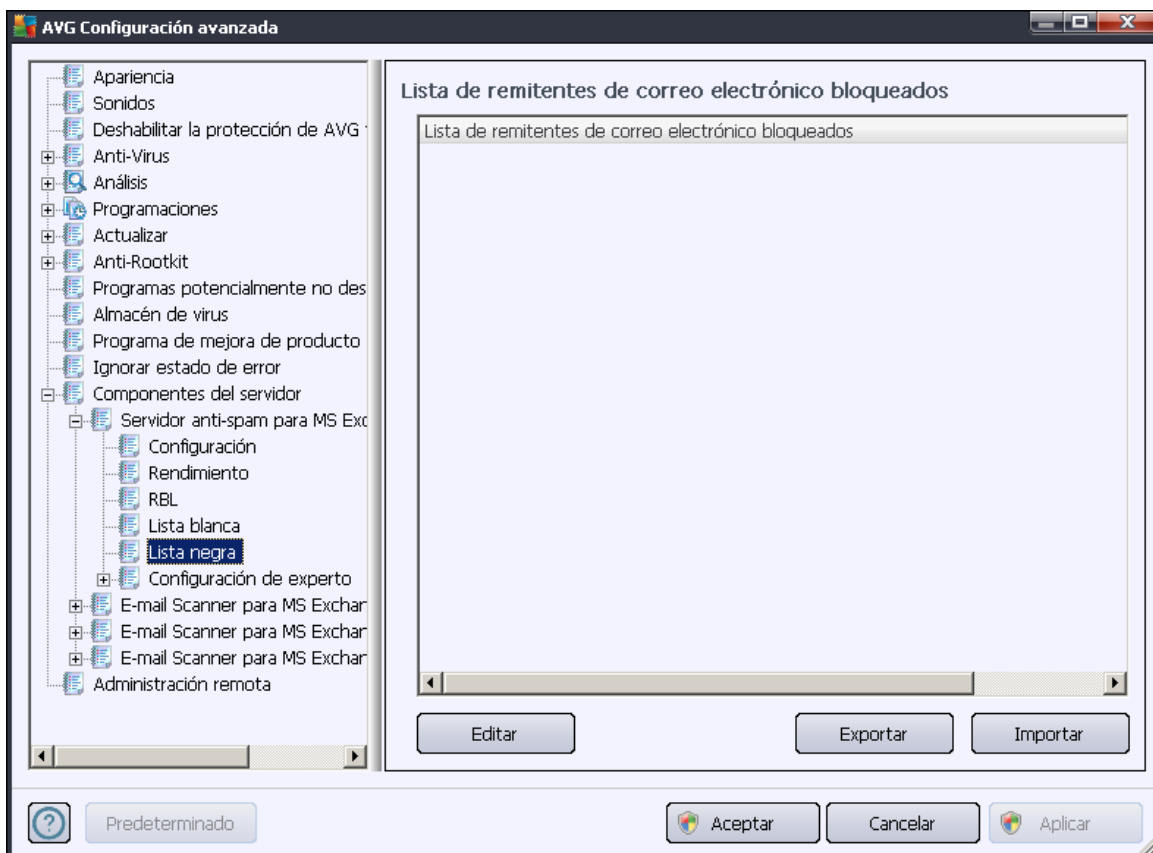


diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo. Los botones de control disponibles son los siguientes:

- **Editar:** pulse este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (también puede *copiar y pegar*). Inserte un elemento (remitente, nombre de dominio) por línea.
- **Importar:** puede importar las direcciones de correo electrónico existentes seleccionando este botón. El archivo de entrada puede ser un archivo de texto (en texto sin formato, y el contenido debe tener sólo un elemento (dirección o nombre de dominio) por línea) o un archivo WAB, o bien puede realizar la importación desde la libreta de direcciones de Windows o Microsoft Office Outlook.
- **Exportar:** si por algún motivo decide exportar los registros, puede hacerlo pulsando este botón. Todos los registros se guardarán en un archivo de texto sin formato.

7.7. Lista negra

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



En la interfaz de edición puede compilar una lista de remitentes de los que espera recibir mensajes



no deseados ([spam](#)). Del mismo modo, puede compilar una lista de nombres de dominio completos (por ejemplo, *empresadespam.com*) de los que espera o recibe mensajes de spam. Todo el correo electrónico procedente de las direcciones o de los dominios enumerados se identificará como spam.

Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo. Los botones de control disponibles son los siguientes:

- **Editar:** pulse este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (también puede *copiar y pegar*). Inserte un elemento (remitente, nombre de dominio) por línea.
- **Importar:** puede importar las direcciones de correo electrónico existentes seleccionando este botón. El archivo de entrada puede ser un archivo de texto (en texto sin formato, y el contenido debe tener sólo un elemento (dirección o nombre de dominio) por línea) o un archivo WAB, o bien puede realizar la importación desde la libreta de direcciones de Windows o Microsoft Office Outlook.
- **Exportar:** si por algún motivo decide exportar los registros, puede hacerlo pulsando este botón. Todos los registros se guardarán en un archivo de texto sin formato.

7.8. Configuración de experto

Normalmente se recomienda mantener la configuración predeterminada y cambiarla sólo si se tiene un motivo válido para hacerlo. Cualquier cambio en la configuración sólo debe ser realizado por usuarios expertos.

Si aún cree que necesita modificar la configuración de Anti-Spam al nivel más experto, siga las instrucciones proporcionadas directamente en la interfaz de usuario. En cada cuadro de diálogo encontrará una única característica específica que podrá editar y cuya descripción siempre se incluye en el propio cuadro:

- **Caché:** huella dactilar, reputación del dominio, LegitRepute
- **Entrenamiento:** máximo de palabras, umbral de autoentrenamiento, relevancia
- **Filtrado:** lista de idiomas, lista de países, direcciones IP aprobadas, direcciones IP bloqueadas, países bloqueados, conjuntos de caracteres bloqueados, suplantación de remitentes
- **RBL:** servidores RBL, múltiples coincidencias, umbral, tiempo de espera, máximo de direcciones IP
- **Conexión a Internet:** tiempo de espera, servidor proxy, autenticación de proxy

8. Administrador de configuraciones de AVG

El **Administrador de configuraciones de AVG** es una herramienta adecuada principalmente para redes más pequeñas que le permite copiar, editar y distribuir la configuración de AVG. La configuración se puede guardar en un dispositivo portátil (memoria flash USB, etc.) y luego aplicarse manualmente en las estaciones elegidas.

La herramienta está incluida en la instalación de AVG y disponible a través del menú Inicio de Windows:

Todos los programas/AVG 2012/Administrador de configuraciones de AVG



- **Configuración de AVG**

- **Editar la configuración de AVG:** use este vínculo para abrir el cuadro de diálogo de la configuración avanzada de AVG. Todos los cambios realizados aquí afectarán también la instalación local de AVG.
- **Cargar y editar la configuración de AVG:** si ya tiene un archivo de configuración de AVG (.pck), emplee este botón para abrir ese archivo y editarlo. Cuando confirme los cambios con el botón **Aceptar** o **Aplicar**, el archivo será sustituido por la nueva configuración.

- **Configuración de AVG Firewall**

Esta sección le permite hacer cambios en la configuración de Firewall de la instalación local de AVG o editar la configuración de Firewall ya preparada en un archivo de configuración de AVG (.pck). Sin embargo, dado que su AVG Email Server Edition 2012 no incluye el componente Firewall, los vínculos de esta sección se mostrarán atenuados y no funcionarán.

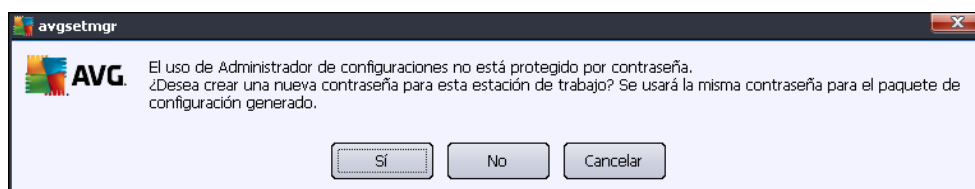


- **Opciones de carga**

- **Cargar una configuración guardada de AVG:** use este vínculo para abrir un archivo de configuración de AVG (.pck) y aplicarlo a la instalación local de AVG.

- **Opciones de almacenamiento**

- **Guardar la configuración local de AVG en un archivo:** use este vínculo para guardar el archivo de configuración de AVG (.pck) correspondiente a la instalación local de AVG. Si no ha establecido una contraseña para las acciones permitidas, puede que aparezca el siguiente cuadro de diálogo:



Responda **Sí** si desea definir ahora una contraseña para el acceso a los elementos permitidos y, a continuación, complete la información necesaria y confirme su selección. Responda **No** para omitir la creación de una contraseña y pasar a guardar la configuración local de AVG en un archivo.

- **Opciones de clonación**

- **Aplicar la misma configuración en toda la red:** este vínculo permite hacer una copia de la instalación local de AVG mediante la creación de un paquete de instalación con opciones personalizadas. La copia clonada incluye la mayoría de las configuraciones de AVG a excepción de lo siguiente:

- ✓ *Configuración de idioma*
- ✓ *Configuración de sonidos*
- ✓ *Lista de elementos permitidos y excepciones de programas potencialmente no deseados del componente Identity protection.*

Para proceder, seleccione primero la carpeta donde se guardará el script de instalación.



A continuación, seleccione del menú desplegable una de las siguientes opciones:

- ✓ *Instalación oculta*: no se mostrará ninguna información durante el proceso de instalación.
- ✓ *Mostrar el progreso de la instalación únicamente*: la instalación no requerirá la atención del usuario, pero el progreso será totalmente visible.
- ✓ *Mostrar el asistente de instalación*: la instalación será visible y el usuario tendrá que confirmar todos los pasos manualmente.

Utilice el botón **Descargar** para descargar el último paquete de instalación de AVG disponible directamente de la página web de AVG en la carpeta seleccionada, o bien coloque manualmente el paquete de instalación de AVG en esa carpeta.

Puede utilizar el botón **Proxy** para definir la configuración de un servidor proxy si su red así lo requiere para conectarse correctamente.

Al hacer clic en **Aceptar** empieza el proceso de clonación, que debería finalizar en breve. También puede aparecer un cuadro de diálogo solicitándole que establezca la contraseña para los elementos permitidos (consulte arriba). Cuando finalice, debería aparecer el archivo **AvgSetup.bat** en la carpeta seleccionada, junto a otros archivos. Si ejecuta el archivo **AvgSetup.bat**, se instalará AVG de acuerdo a los parámetros seleccionados arriba.



9. Preguntas más frecuentes (FAQ) y soporte técnico

En caso de que tenga algún problema con AVG, ya sea administrativo o técnico, consulte la sección **Preguntas más frecuentes** del sitio web de AVG (<http://www.avg.com>).

Si no consigue encontrar la solución de esta manera, póngase en contacto con el departamento de soporte técnico por correo electrónico. Utilice para ello el formulario de contacto que encontrará en el menú del sistema a través de **Ayuda / Obtener ayuda en línea**.