# AVG Email Server Edition 2012

## Manual do Utilizador

**Revisão do documento 2012.01 (7. 9. 2011)**

# Índice

# 1. Introdução

Este manual do utilizador disponibiliza informação completa para o **AVG Email Server Edition 2012**.

**Parabéns pela sua aquisição do AVG Email Server Edition 2012!**

O **AVG Email Server Edition 2012** é um entre um leque de premiados produtos AVG desenvolvidos para lhe proporcionar descanso e segurança absoluta para o seu servidor. Como todos os produtos AVG, o **AVG Email Server Edition 2012** foi completamente redesenhado, de raiz, para proporcionar a renomeada e acreditada protecção de segurança de uma forma nova, mais fácil de utilizar e mais eficiente.

O AVG foi concebido e desenvolvido para proteger o seu computador e actividade de rede. Desfrute da experiência da protecção total do AVG.

***Nota:*** *Esta documentação contém descrições de funcionalidades específicas da Versão Servidor de E-mail. Se precisar de informações sobre outras funcionalidades AVG, queira consultar o manual do utilizador da versão Internet Security, que contém todas as informações necessárias. Pode transferir o manual a partir de http://www.avg.com.*

# 2. Requisitos de Instalação do AVG

## 2.1. Sistemas Operativos Suportados

O **AVG Email Server Edition 2012** destina-se a proteger servidores de e-mail em execução nos seguintes sistemas operativos:

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

## 2.2. Servidores de E-mail Suportados

São suportados os seguintes servidores de e-mail:

- MS Exchange 2003 Server
- MS Exchange 2007 Server
- MS Exchange 2010 Server
- AVG para Kerio MailServer – versão 6.7.2 e superiores

## 2.3. Requerimentos de Hardware

Os requisitos mínimos de hardware para o **AVG Email Server Edition 2012** são:

- Intel Pentium CPU 1.5 GHz
- 500 MB de espaço livre no disco rígido (para propósitos de instalação)
- 512 MB de memória RAM

Os requisitos recomendados de hardware para o **AVG Email Server Edition 2012** são:

- Intel Pentium CPU 1.8 GHz
- 600 MB de espaço livre no disco rígido (para propósitos de instalação)
- 512 MB de memória RAM

## 2.4. Desinstalar Versões Anteriores

Se possuir uma versão anterior do AVG Email Server instalada, precisará de a desinstalar manualmente antes de instalar o **<%MAIN_PRODUCT_ NAME_IN_TEXT%>**. Deve desinstalar manualmente a versão anterior através das funcionalidades tradicionais do Windows.

- A partir do menu ***Iniciar/Definições/Painel de Controlo/Adicionar ou Remover Programas***

, seleccione o programa pretendido da lista de software instalado. Tenha atenção para seleccionar o programa AVG correcto para desinstalação. É necessário desinstalar a Email Server Edition antes de desinstalar a AVG File Server Edition.

- Quando tiver a Email Server Edition desinstalada, pode desinstalar a versão anterior do AVG File Server Edition. Pode fazê-lo através do menu ***Iniciar/Todos os programas/AVG/ Desinstalar o AVG***

- Se tiver usado o AVG 8.x ou uma versão anterior, não se esqueça de desinstalar também os plug-ins individuais do servidor.

  ***Nota:*** *Será necessário reiniciar o serviço store durante o processo de desinstalação.*

  ***Plug-in Exchange*** - execute o ficheiro setupes.exe com o parâmetro /uninstall a partir da pasta onde o plug-in foi instalado

  *ex., C:\AVG4ES2K\setupes.exe /uninstall*

  ***Plug-in Lotus Domino/Notes*** - execute o ficheiro setupln.exe com o parâmetro /uninstall a partir da pasta onde o plug-in foi instalado

  *ex., C:\AVG4LN\setupln.exe /uninstall*

## 2.5. Service Packs do MS Exchange

Para o Exchange 2003 Server não é necessário nenhum pacote de serviço adicional; no entanto, recomenda-se que mantenha o sistema actualizado com os pacotes de serviço e correcções mais recentes, de modo a obter a máxima segurança disponível.

**Service Pack para MS Exchange 2003 Server (opcional):**

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

No início da configuração, todas as versões das bibliotecas do sistema serão examinadas. Se for necessário instalar novas bibliotecas, o programa de instalação mudará o nome das versões anteriores com a extensão .delete. Estas versões serão eliminadas depois de o sistema reiniciar.

**Service Pack para MS Exchange 2007 Server (opcional):**

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

# 3. Processo de Instalação do AVG

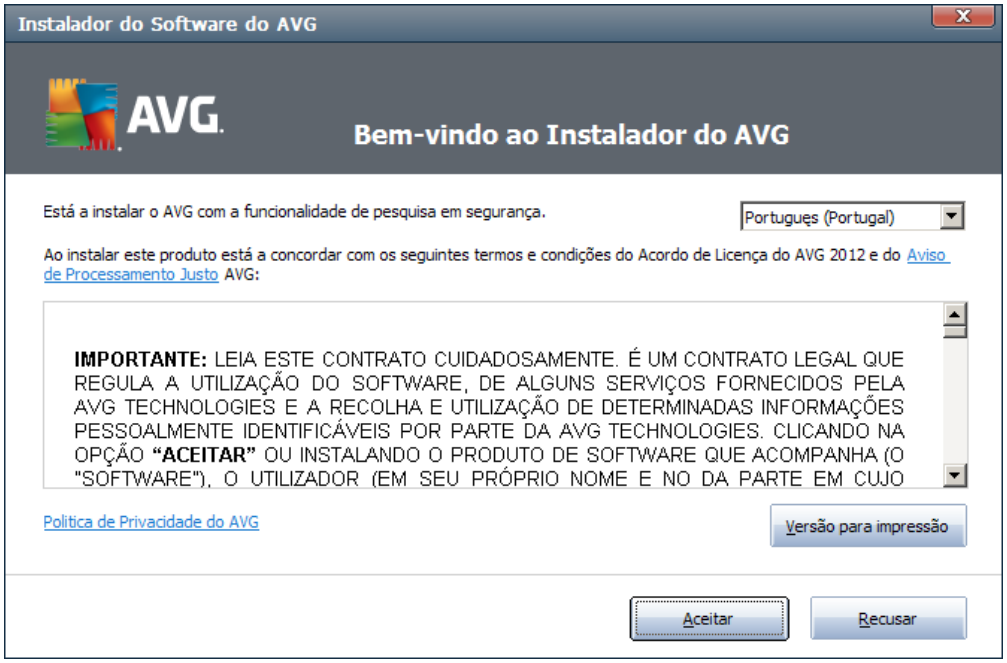
Para instalar o AVG no seu computador, precisa de obter o mais recente ficheiro de instalação. Pode utilizar o ficheiro de instalação a partir do CD facultado na caixa da sua edição, mas este ficheiro pode estar desactualizado. Como tal, recomendamos que obtenha o ficheiro de instalação mais recente ficheiro on-line. Pode transferir o ficheiro a partir do Website da AVG (em http://www.avg.com/download?prd=msw)

***Nota:*** *Existem dois pacotes de instalação disponíveis para o seu produto - para sistemas operativos de 32 bits (marcado como x86) e para sistemas operativos de 64 bits (marcado como x64). Certifique-se de que usa o pacote de instalação correcto para o seu sistema operativo específico..*

Durante o processo de instalação, ser-lhe-á solicitado o número de licença. Certifique-se de que o mesmo está disponível antes de iniciar a instalação. O número pode ser encontrado na embalagem do CD. Se tiver adquirido a sua cópia do AVG online, o número de licença foi-lhe enviado por e-mail.

Assim que tiver transferido e guardado o ficheiro de instalação no seu disco rígido, pode iniciar o processo de instalação. A instalação é uma sequência de janelas com uma breve descrição do que deve fazer em cada passo. De seguida facultamos uma explicação para cada janela:

## 3.1. Execução da Instalação



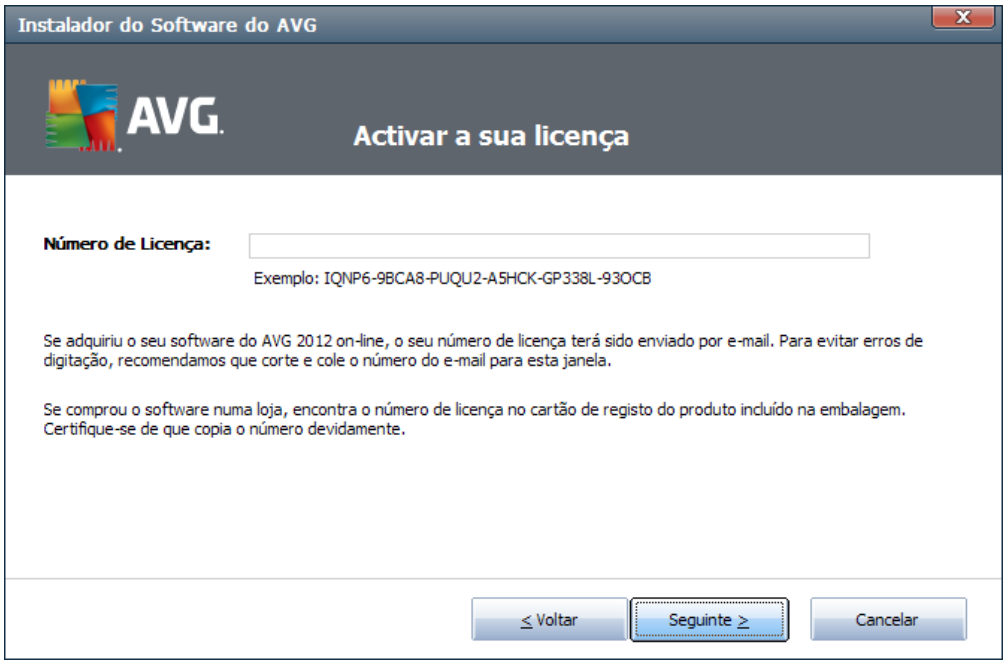

O processo de instalação inicia com a janela ***Bem-vindo***. Aqui pode seleccionar o idioma que será usado para o processo de instalação e ser-lhe-ão apresentadas as condições de licenciamento. Use o botão ***Versão de impressão*** para abrir o texto da licença numa nova janela. Depois clique no botão ***Aceito*** para confirmar e continue para a janela seguinte.

***Atenção:*** *Poderá escolher também idiomas adicionais para a interface da aplicação mais tarde durante o processo de instalação.*

## 3.2. Activar a sua licença

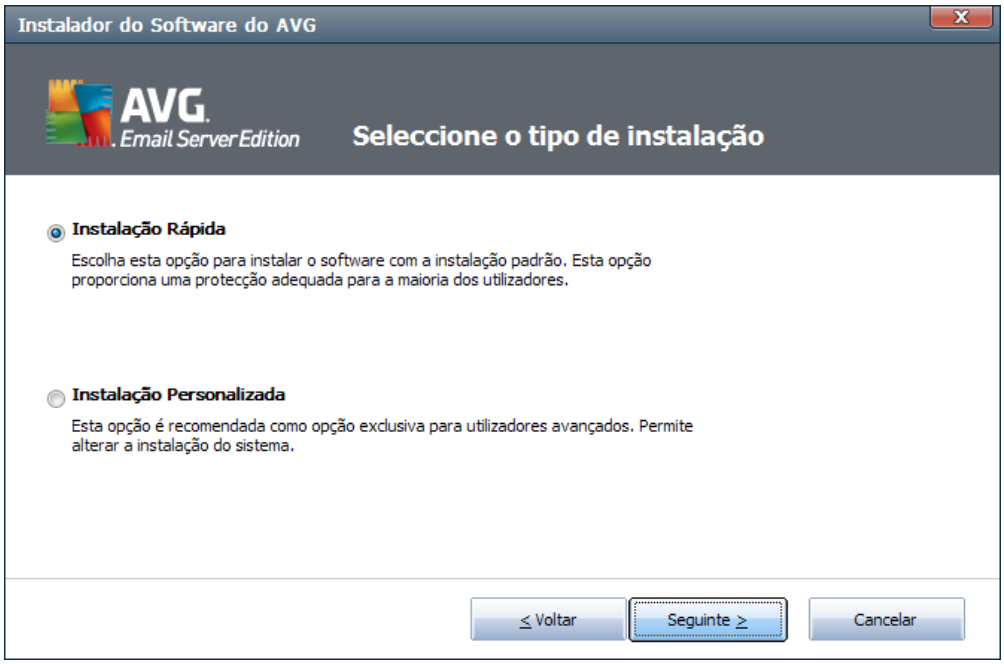
Na janela ***Activar a sua licença do*** tem de preencher o seu número de licença.

Introduza o seu número de licença no campo de texto ***Número de Licença*** . O número de licença estará no e-mail de confirmação que recebeu após comprar o seu AVG on-line. Tem de digitar o número exactamente conforme apresentado. Se o formulário digital do número de licença estiver disponível (na mensagem de e-mail), é recomendável que utilize o método copiar e colar para o inserir.




Clique no botão ***Seguinte*** para continuar o processo de instalação.

## 3.3. Seleccionar Tipo de Instalação

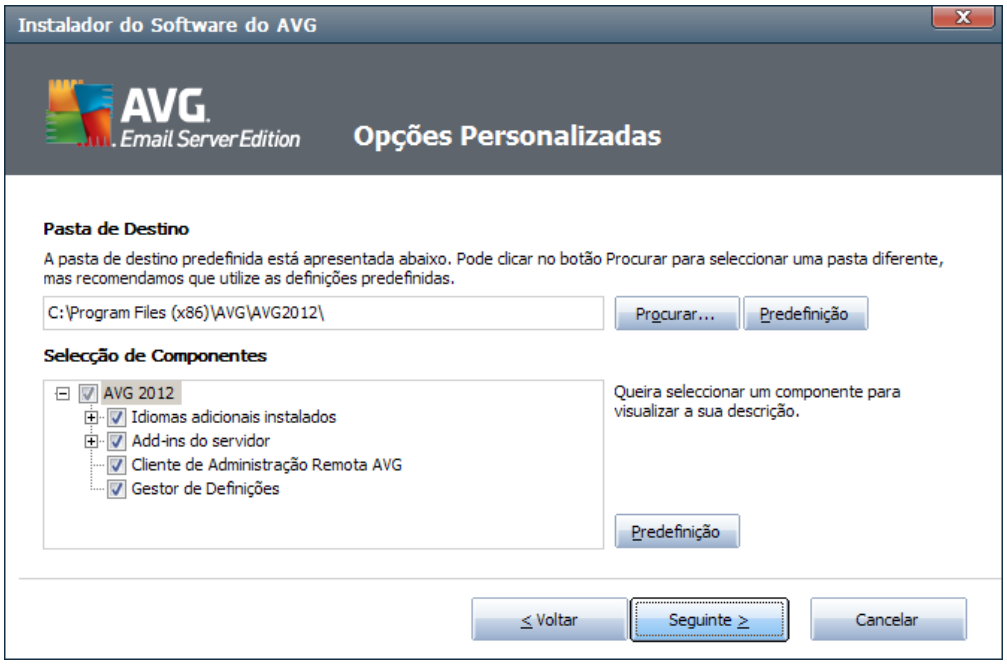



A janela ***Seleccione o tipo de instalação*** disponibiliza a possibilidade de duas opções de instalação: ***Instalação Rápida*** e ***Instalação Personalizada***.

Para a maioria dos utilizadores, é recomendável a ***Instalação Rápida***, que instala o AVG em modo totalmente automático com as definições predefinidas pelo fornecedor do programa. Esta configuração proporciona a segurança máxima combinada com uma utilização de recursos optimizada. Futuramente, se houver necessidade de alterar a configuração, tem sempre a possibilidade de o fazer directamente na aplicação AVG.

***A Instalação Personalizada*** só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o AVG com definições que não as padrão; ex. para corresponder a requisitos do sistema específicos.

## 3.4. Instalação Personalizada - Opções Personalizadas




A janela ***Pasta de destino***permite-lhe especificar a localização onde o AVG deverá ser instalado. O AVG será instalado por predefinição na pasta de ficheiros de programas localizada na unidade C:. Se quiser alterar esta localização, utilize o botão ***Procurar*** para visualizar a estrutura da unidade, e seleccione a pasta respectiva.

A secção ***Selecção de Componentes*** apresenta uma síntese de todos os componentes do AVG que podem ser instalados. Se as definições predefinidas não forem da sua conveniência, pode remover/adicionar componentes específicos.

***No entanto, só pode seleccionar entre os componentes que estão incluídos na edição do AVG que adquiriu. Só esses componentes serão facultados para instalação na janela de Selecção de Componentes!***

- ***Cliente de Administração Remota AVG*** - se pretender conectar o AVG a um Centro de Dados AVG (Edições de Rede do AVG), é necessário seleccionar esta opção.

  ***Nota:*** *Só os componentes do servidor presentes na lista podem ser geridos remotamente!*

- ***Gestor de Definições*** - é uma ferramenta, adequada principalmente para administradores de rede, que lhe permite copiar, editar e distribuir a configuração do AVG. A configuração pode ser guardada num dispositivo amovível (unidade flash USB, etc.) e depois aplicada manualmente, ou de qualquer outra forma, nos postos seleccionados.

- ***Idiomas Adicionais Instalados*** - pode definir o(s) idioma(s) em que o AVG deverá ter instalado(s). Marque o item ***Idiomas adicionais instalados*** e depois seleccione os idiomas pretendidos a partir do respectivo menu.

Síntese simplificada dos componentes individuais do servidor (***Add-ins do Servidor***):

- ***Servidor Anti-Spam para o MS Exchange***

  verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. Utiliza vários métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de protecção possível contra mensagens de e-mail indesejadas.

- ***Verificador de E-mail para o MS Exchange (routing Transport Agent)***

  Verifica todas as mensagens de e-mail de entrada, de saída e internas que passam pela função MS Exchange HUB.

  Disponível para o MS Exchange 2007/2010 e pode ser instalado apenas para a função HUB.

- ***Verificador de E-mail para o MS Exchange (SMTP Transport Agent)***

  Verifica todas as mensagens que passam pela interface do MS Exchange SMTP.

  Disponível para o MS Exchange 207/2010 apenas e pode ser instalado para as funções EDGE e HUB.

- ***Verificador de E-mail para o MS Exchange (VSAPI)***

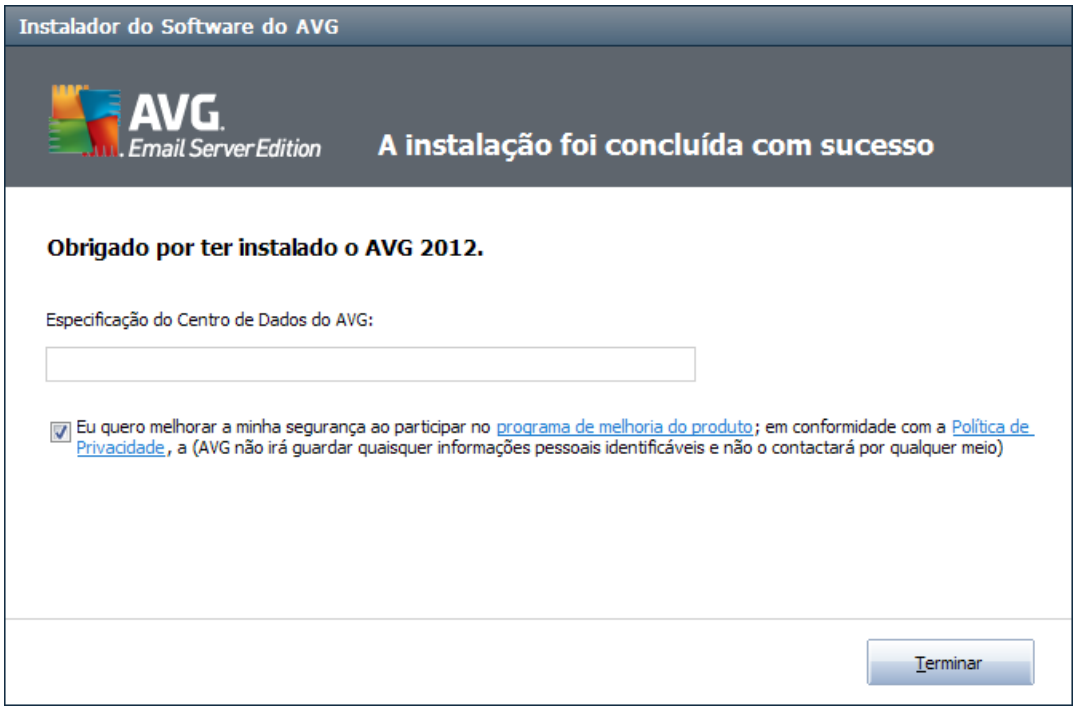
  Verifica todas as mensagens de e-mail guardadas nas caixas de correio dos utilizadores. Se for detectado algum vírus, será movido para a Quarentena de Vírus ou removido na totalidade.

***Nota:*** *Existem várias opções disponíveis para as várias versões do MS Exchange.*

Continue clicando no botão ***Seguinte***.

## 3.5. Conclusão da Instalação

Se tiver seleccionado o módulo ***Componente Administração Remota*** durante a selecção de módulos, pode definir neste ecrã a cadeia de caracteres de ligação ao seu Centro de Dados AVG.




O AVG está agora instalado no seu computador e totalmente funcional. O programa está em execução em segundo plano em modo completamente automático.

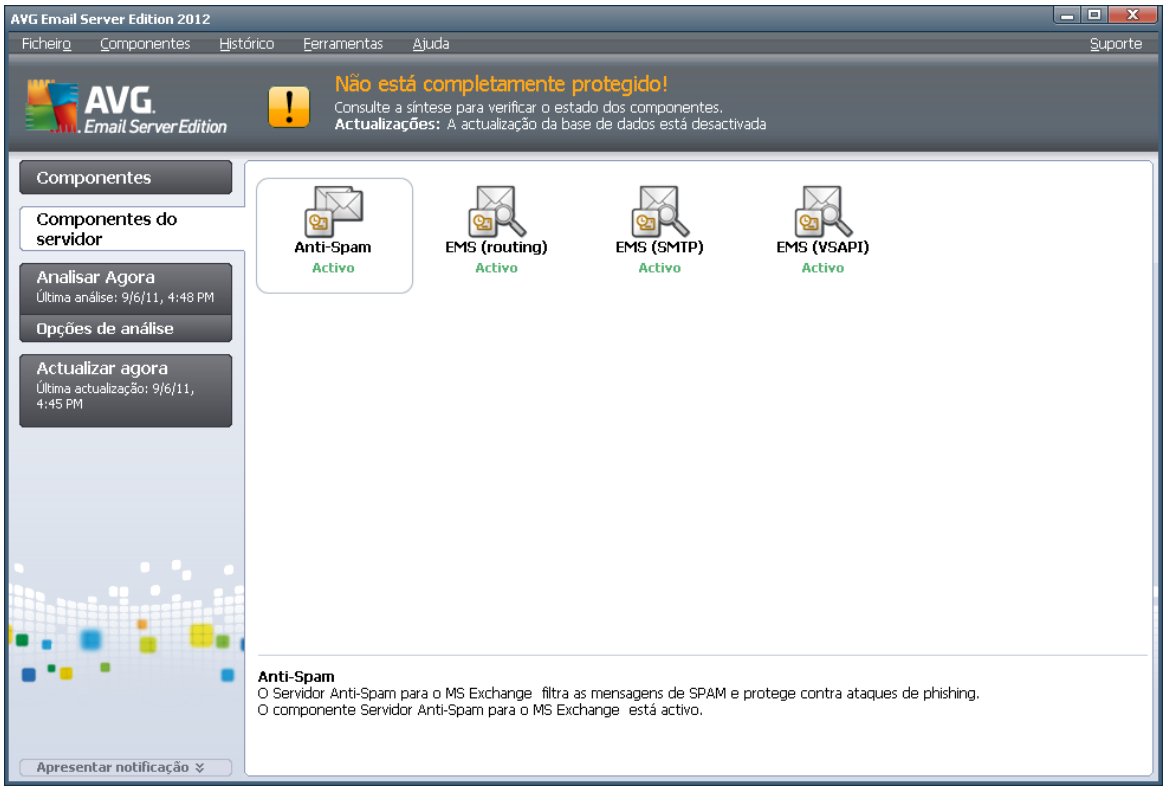
Para configurar individualmente a protecção do seu servidor de e-mail, consulte a secção correspondente:

- ***Verificador de E-mail para o Servidor MS Exchange 2007/2010***
- ***Verificador de E-mail para o Servidor MS Exchange 2003***
- ***AVG para Kerio MailServer***

# 4. Verificador de E-mail para o Servidor MS Exchange 2007/2010

## 4.1. Resumo

As opções de configuração do AVG para MS Exchange Server 2007/2010 estão completamente integradas no AVG Email Server Edition 2012 como componentes do servidor.




Síntese simplificada dos componentes individuais do servidor:

- ***Anti-Spam - Servidor Anti-Spam para o MS Exchange***

  verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. Utiliza vários métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de protecção possível contra mensagens de e-mail indesejadas.

- ***EMS (routing) - Verificador de E-mail para o MS Exchange (routing Transport Agent)***

  Verifica todas as mensagens de e-mail de entrada, de saída e internas que passam pela função MS Exchange HUB.

  Disponível para o MS Exchange 2007/2010 e pode ser instalado apenas para a função HUB.

- ***EMS (SMTP) - Verificador de E-mail para o MS Exchange (SMTP Transport Agent)***

Verifica todas as mensagens que passam pela interface do MS Exchange SMTP.

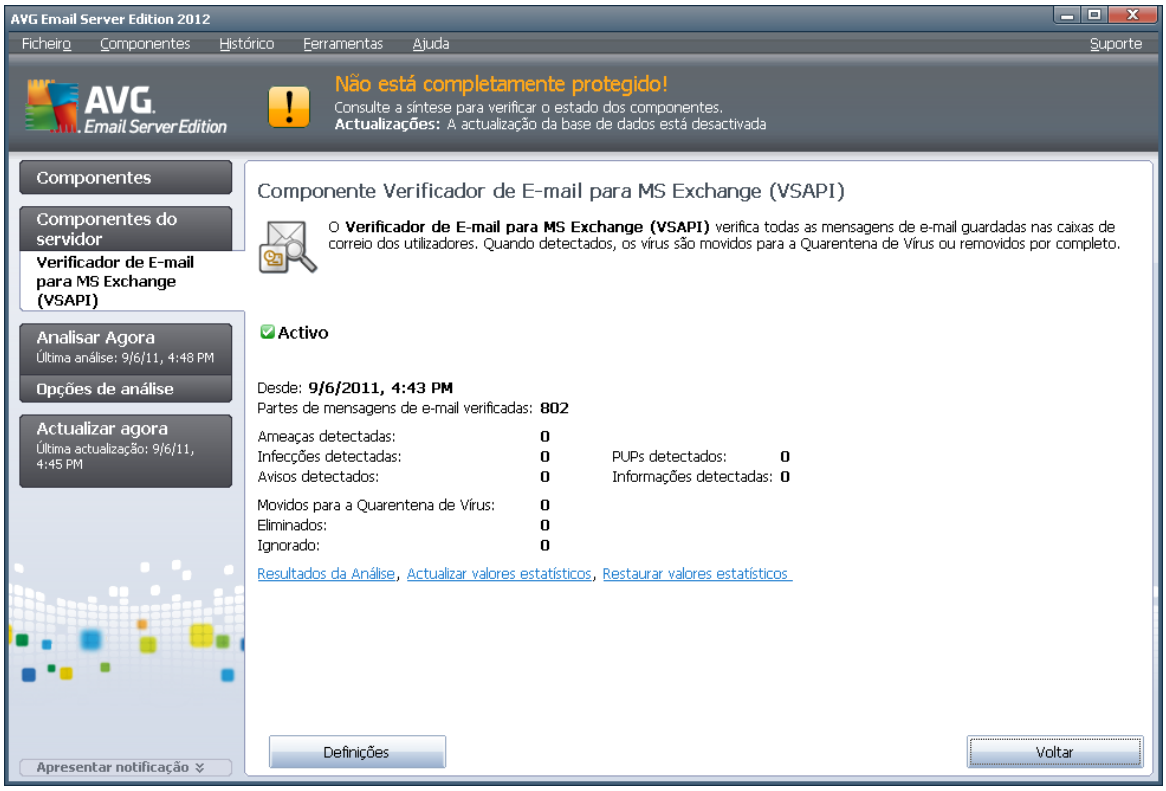
Disponível para o MS Exchange 207/2010 apenas e pode ser instalado para as funções EDGE e HUB.

- ***EMS (VSAPI) - Verificador de E-mail para o MS Exchange (VSAPI)***

  Verifica todas as mensagens de e-mail guardadas nas caixas de correio dos utilizadores. Se for detectado algum vírus, será movido para a Quarentena de Vírus ou removido na totalidade.

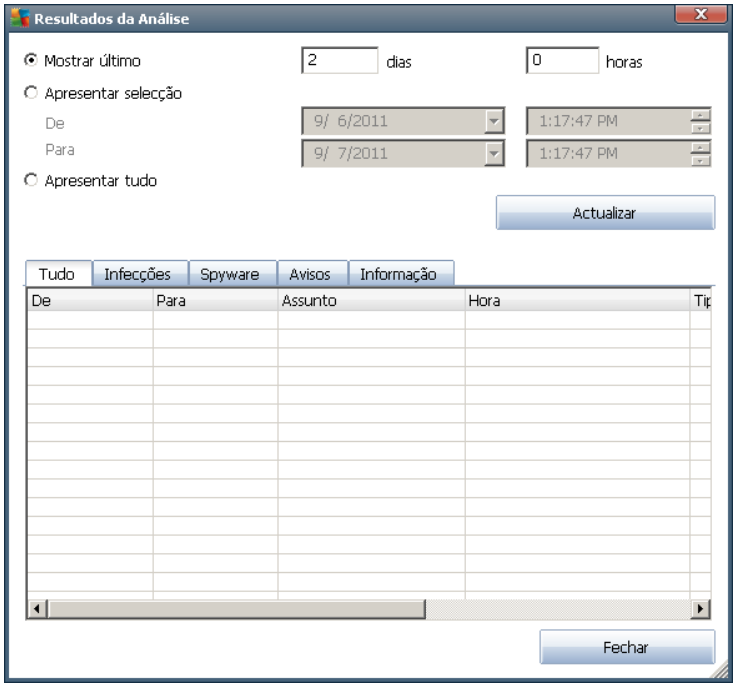
***Nota importante:*** *Se tiver optado pela instalação e utilização de VSAPI em conjunto com o agente routing transport numa função Hub Exchange, as suas mensagens de e-mail serão analisadas duas vezes. Para evitar esta situação, queira rever o capítulo* ***Informação técnica*** *abaixo para mais informações.*

Clique duas vezes sobe um componente para abrir a interface do mesmo. Com excepção do componente Anti-Spam, todos os componentes partilham os seguintes botões de controlo e ligações:




- ***Resultados da Análise***

  Abre uma nova janela onde pode rever os resultados da análise:




Aqui, pode verificar mensagens divididas em vários separadores de acordo com o nível de gravidade. Consulte a configuração dos componentes individuais para corrigir a gravidade e reportação.

Por predefinição, só são apresentados os resultados dos dois últimos dias. Pode alterar o período apresentado através da alteração das seguintes opções:

- ***Mostrar último*** - insira os dias e as horas pretendidas.
- ***Apresentar selecção*** - escolha uma hora pretendida e um intervalo de datas.
- ***Apresentar tudo*** - Apresenta resultados para todo o período.

Use o botão ***Actualizar*** para recarregar os resultados.

- ***Actualizar valores estatísticos*** - actualiza as estatísticas apresentadas acima.
- ***Restaurar valores estatísticos*** - restaura todas as estatísticas para zero.

Os botões activos são os seguintes:

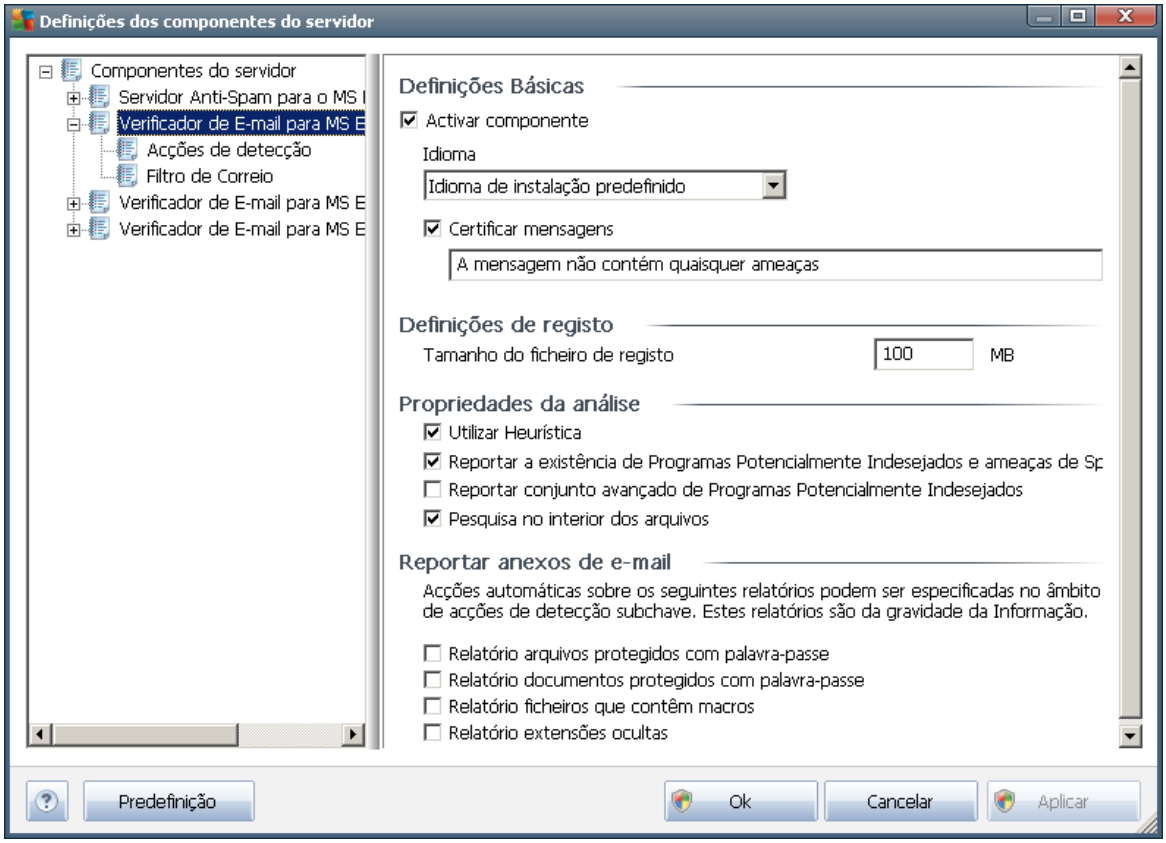
- ***Definições*** - use este botão para abrir as definições do componente.
- ***Retroceder*** - prima esta botão para regressar à Síntese de componentes do servidor.

Encontrará mais informações sobre definições individuais de todos os componentes nas secções abaixo.

## 4.2. Verificador de E-mail para o MS Exchange (routing TA)

Para aceder às definições do ***Verificador de e-mail para o MS Exchange (routing transport agent)***, seleccione o botão ***Definições*** na interface do componente.

A partir da lista de ***Componentes do servidor***, seleccione o item ***Verificador de E-mail para o MS Exchange (routing TA)***




A secção ***Definições Básicas*** contém as seguintes opções:

- ***Activar componente*** - desmarque para desactivar o componente.
- ***Idioma*** - seleccione o idioma pretendido para o componente.
- ***Certificar mensagens*** - marque esta opção se quiser adicionar uma nota de certificação a todas as mensagens analisadas. Pode personalizar a mensagem no campo seguinte.

A secção ***Definições de registo***:

- ***Tamanho do Ficheiro de registo*** - escolha um tamanho pretendido para o ficheiro de registo. Valor predefinido: 100 MB.

A secção ***Propriedades da análise***:

- ***Utilizar Heurística*** - marque esta caixa para activar o método de análise heurística durante a análise.

- ***Reportar a existência de Programas Potencialmente Indesejados e ameaças de Spyware*** - marque esta opção para reportar a presença de programas potencialmente indesejados e spyware.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** - marque para detectar pacotes alargados de spyware: programas que são perfeitamente seguros quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente, ou programas que são sempre seguros mas que podem ser indesejados (barras de ferramentas, etc.). Esta é uma medida adicional que aumenta o conforto e segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição. Nota: Esta funcionalidade de detecção é um complemento da opção anterior, portanto, se quiser protecção contra os tipos básicos de spyware, mantenha sempre a caixa anterior marcada.

- ***Analisar no interior de arquivos*** - marque esta opção para permitir que o verificador analise também no interior de arquivos (zip, rar, etc).

A secção ***Reportação de anexos de e-mail*** permite-lhe escolher os itens que deverão ser reportados durante a análise. Se marcada, cada e-mail com itens deste tipo conterá a etiqueta [INFORMAÇÃO] no assunto da mensagem. Esta é a configuração predefinida que pode ser facilmente corrigida na secção ***Acções de detecção***, opção ***Informação*** (veja abaixo).

Estão disponíveis as seguintes opções:

- ***Reportar arquivos protegidos por palavra-passe***

- ***Reportar documentos protegidos por palavra-passe***

- ***Reportar ficheiros que contenham macros***

- ***Reportar extensões ocultas***

Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Acções de detecção***

- ***Filtro de Correio***

## 4.3. Verificador de e-mail para o MS Exchange (SMTP TA)

A configuração do ***Verificador de e-mail para o MS Exchange (SMTP Transport Agent)*** é exactamente a mesma que para o Routing Transport Agent. Para mais informações, consulte a secção ***Verificador de e-mail para o MS Exchange (routing TA)*** acima.

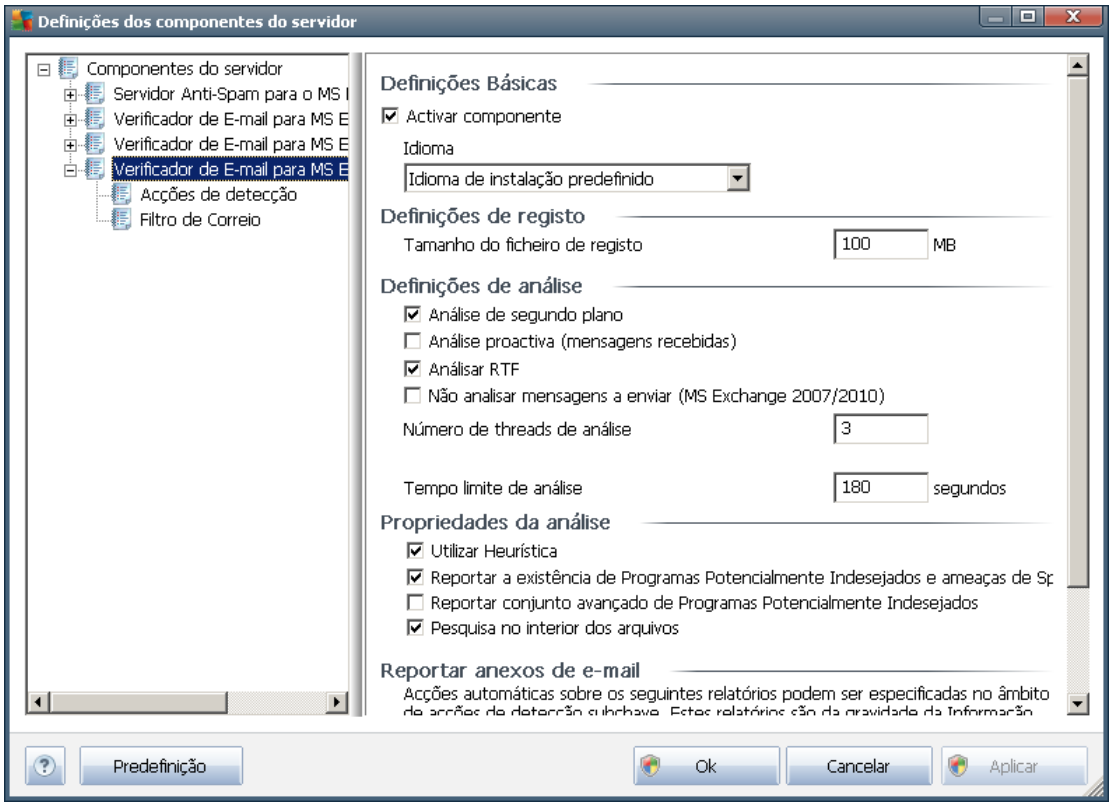
Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Acções de detecção***

- ***Filtro de Correio***

## 4.4. Verificador de E-mail para o MS Exchange (VSAPI)

Este item contém definições do ***Verificador de E-mail para o MS Exchange (VSAPI)***.




A secção ***Definições Básicas*** contém as seguintes opções:

- ***Activar componente*** - desmarque para desactivar o componente.
- ***Idioma*** - seleccione o idioma pretendido para o componente.

A secção ***Definições de registo***:

- ***Tamanho do Ficheiro de registo*** - escolha um tamanho pretendido para o ficheiro de registo. Valor predefinido: 100 MB.

A secção ***Definições de análise***:

- ***Análise em Segundo Plano*** – pode activar ou desactivar o processo de análise em segundo plano. A análise em segundo plano é uma das funcionalidades da interface de aplicação VSAPI 2.0/2.5. Permite a análise por tópicos das Bases de Dados de Mensagens do Exchange. Sempre que for encontrado um item que não tenha sido analisado com as mais recentes actualizações da base de dados de vírus nas pastas da caixa de correio do utilizador, será enviado ao AVG para Exchange / Server para ser analisado. A análise e a

procura de objectos não examinados são executadas em paralelo.

É usada uma classificação de prioridade baixa específica para cada base de dados, o que assegura que outras tarefas (ex. armazenamento de mensagens de e-mail na base de dados do Microsoft Exchange) são sempre executadas prioritariamente.

- ***Análise Pro-activa (mensagens de entrada)***

  Pode activar ou desactivar a função de análise pro-activa do VSAPI 2.0/2.5 aqui. . Esta análise ocorre quando um item é entregue numa pasta sem o pedido ter sido feito pelo cliente.

  Assim que as mensagens são submetidas para o Exchange, entram na fila de análise global com prioridade baixa (máximo de 30 itens). São analisados numa base de primeiro a entrar, primeiro a sair (FIFO). Se um item for acedido enquanto ainda estiver na fila, é passado para prioridade alta.

  ***Nota:*** *As mensagens que excedam o número limite continuarão para o Exchange sem serem analisadas.*

***Nota:*** *Mesma que desactive a* ***Análise em Segundo Plano*** *e a* ***Análise Pro-activa****, a análise aquando do acesso estará activa quando o utilizador tentar transferir uma mensagem com o cliente MS Outlook.*

- ***Analisar RTF*** - permite especificar se o tipo de ficheiro RTF deve ou não ser analisado.
- ***Número de Tópicos da Análise*** - por predefinição, a análise é processada por tópicos para aumentar o desempenho global da análise através de um certo nível de paralelismo. Neste campo, pode alterar a contagem dos tópicos.

  O número de tópicos predefinido é igual a 2 vezes o "número de processadores" + 1.

  O número mínimo de tópicos é computado como ('número de processadores'+1) dividido por 2.

  O número máximo de tópicos é computado como 'Número de processadores' multiplicado por 5 + 1.

  Se o valor for equivalente ao mínimo ou inferior, ou ao máximo ou superior, será usado o valor predefinido.

- ***Tempo Limite da Análise*** – o intervalo contínuo máximo (em segundos) para que um tópico aceda à mensagem que está a ser analisada (o valor predefinido é 180 segundos).

A secção ***Propriedades da análise***:

- ***Utilizar Heurística*** - marque esta caixa para activar o método de análise heurística durante a análise.

- ***Reportar a existência de Programas Potencialmente Indesejados e ameaças de Spyware*** - marque esta opção para reportar a presença de programas potencialmente indesejados e spyware.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** - marque para detectar pacotes alargados de spyware: programas que são perfeitamente seguros quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente, ou programas que são sempre seguros mas que podem ser indesejados (barras de ferramentas, etc.). Esta é uma medida adicional que aumenta o conforto e segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição. Nota: Esta funcionalidade de detecção é um complemento da opção anterior, portanto, se quiser protecção contra os tipos básicos de spyware, mantenha sempre a caixa anterior marcada.

- ***Analisar no interior de arquivos*** - marque esta opção para permitir que o verificador analise também no interior de arquivos (zip, rar, etc).

A secção ***Reportação de anexos de e-mail*** permite-lhe escolher os itens que deverão ser reportados durante a análise. A configuração predefinida pode ser facilmente corrigida na secção ***Acções de detecção***, opção ***Informação*** (veja abaixo).

Estão disponíveis as seguintes opções:

- ***Reportar arquivos protegidos por palavra-passe***

- ***Reportar documentos protegidos por palavra-passe***

- ***Reportar ficheiros que contenham macros***

- ***Reportar extensões ocultas***

Regra geral, algumas destas funcionalidades são extensões do utilizador dos serviços da interface da aplicação Microsoft VSAPI 2.0/2.5 Para obter informações detalhadas sobre o VSAPI 2.0/2.5, aceda a uma das seguintes hiperligações (e também às hiperligações acessíveis a partir das indicadas):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - para mais informações sobre o Exchange e interacção com software anti-vírus.

- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 para informações sobre funcionalidades do componente VSAPI 2.5 na aplicação Exchange 2003 Server.

Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Acções de detecção***

- ***Filtro de Correio***

## 4.5. Informação Técnica

Esta informação é relativa a uma situação de instalação e utilização simultânea de VSAPI e do Agente Routing Transport numa função Hub Exchange. Nesta situação, as suas mensagens de e-mail serão analisados duas vezes (primeiro pelo verificador de acesso VSAPI e depois pelo Agente Routing Transport).

Devido à forma como a interface VSAPI funciona, podem ocorrer algumas inconsistências nos resultados de análise, assim como uma utilização desnecessária dos recursos do sistema. Como tal, para evitar a duplicação das análises, recomendamos uma pequena correcção (veja abaixo) para resolver esta questão imediatamente.

***Nota:*** *O ajustamento do registo só é aconselhável para utilizadores experientes. Recomendamos que antes de editar o registo faça uma cópia de segurança e compreenda como o restaurar se ocorrer algum problema.*

Abra o Editor do registo (menu ***Iniciar/Executar*** do Windows, digite ***regedit*** e clique na tecla Enter). Navegue para o separador seguinte:

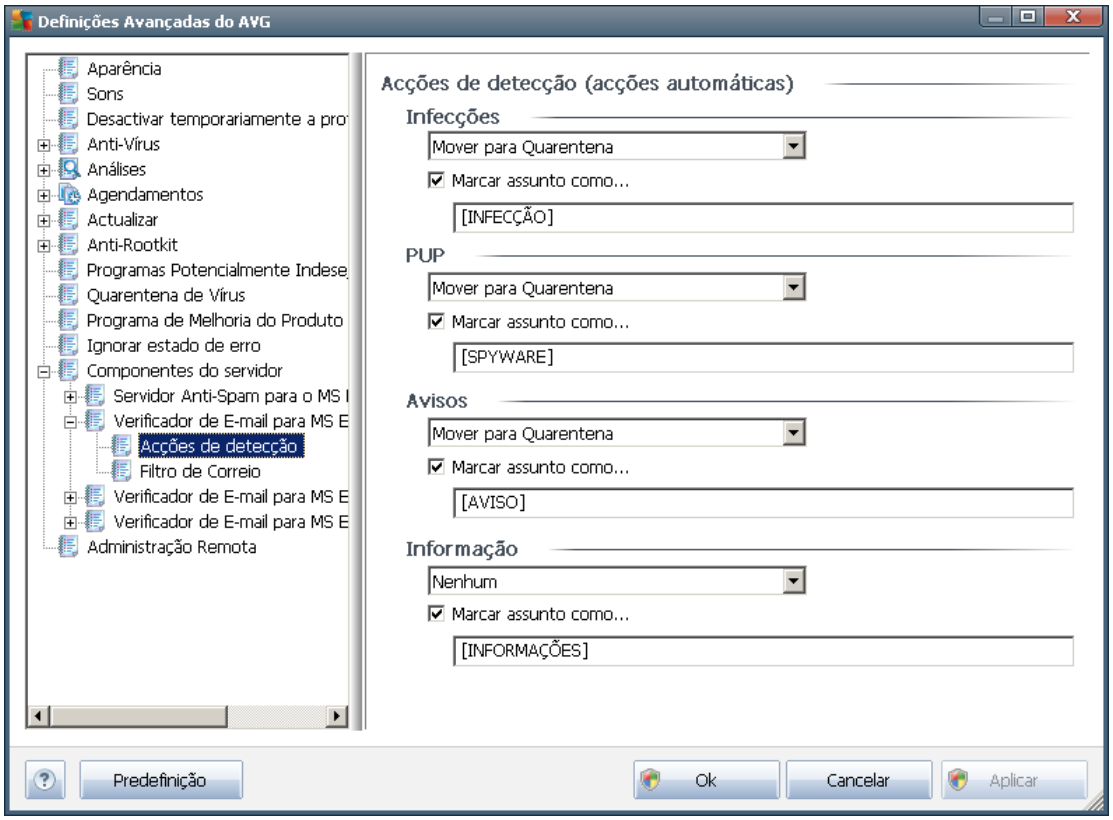
***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan***

Clique com o botão direito do rato na parte direita da janela e, a partir do menu de contexto, seleccione ***Novo valor/DWORD (32 bits)***. Nomeie o novo valor como ***TransportExclusion***. Clique duas vezes sobre o mesmo e altere o valor para ***1***.

Finalmente, para aplicar a alteração ao servidor MS Exchange, é necessário definir o valor ***ReloadNow*** para 1. Para o efeito, clique duas vezes sobre o mesmo e altere o valor.

Desta forma desactiva a análise de mensagens de saída por parte do verificador de acesso VSAPI. A alteração deverá ficar activo ao fim de alguns minutos.

## 4.6. Acções de detecção




No item secundário ***Acções de detecção***, pode escolher acções automáticas que deverão ser executadas durante o processo de análise

As acções estão disponíveis para os seguintes itens:

- ***Infecções***
- ***PUP (Programas Potencialmente Indesejados)***
- ***Avisos***
- ***Informações***

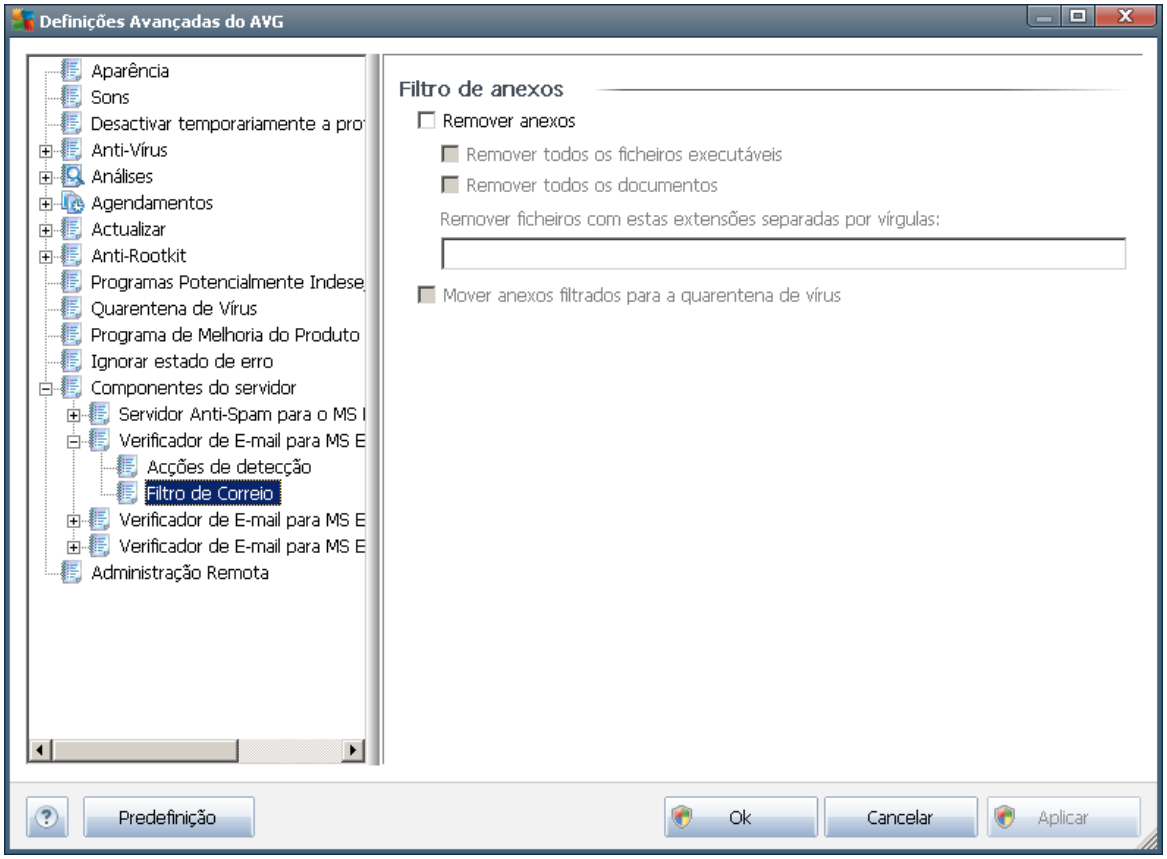
Use o menu pendente para escolher uma acção para cada item:

- ***Nenhuma*** - não será tomada nenhuma acção.
- ***Mover para a Quarentena*** - a ameaça em causa será movida para a Quarentena de Vírus.
- ***Remover*** - a ameaça em causa será removida.

Para seleccionar um texto personalizado pata o campo Assunto das mensagens que contêm o item/ameaça, marque a caixa ***Marcar assunto com...*** e preencha o texto pretendido.

***Nota:*** *Esta funcionalidade não está disponível para o Verificador de e-mail para o MS Exchange VSAPI.*

## 4.7. Filtro de Correio




No item secundário ***Filtro de Correio***, pode escolher quais os anexos que devem ser automaticamente removidos, se quiser. Estão disponíveis as seguintes opções:

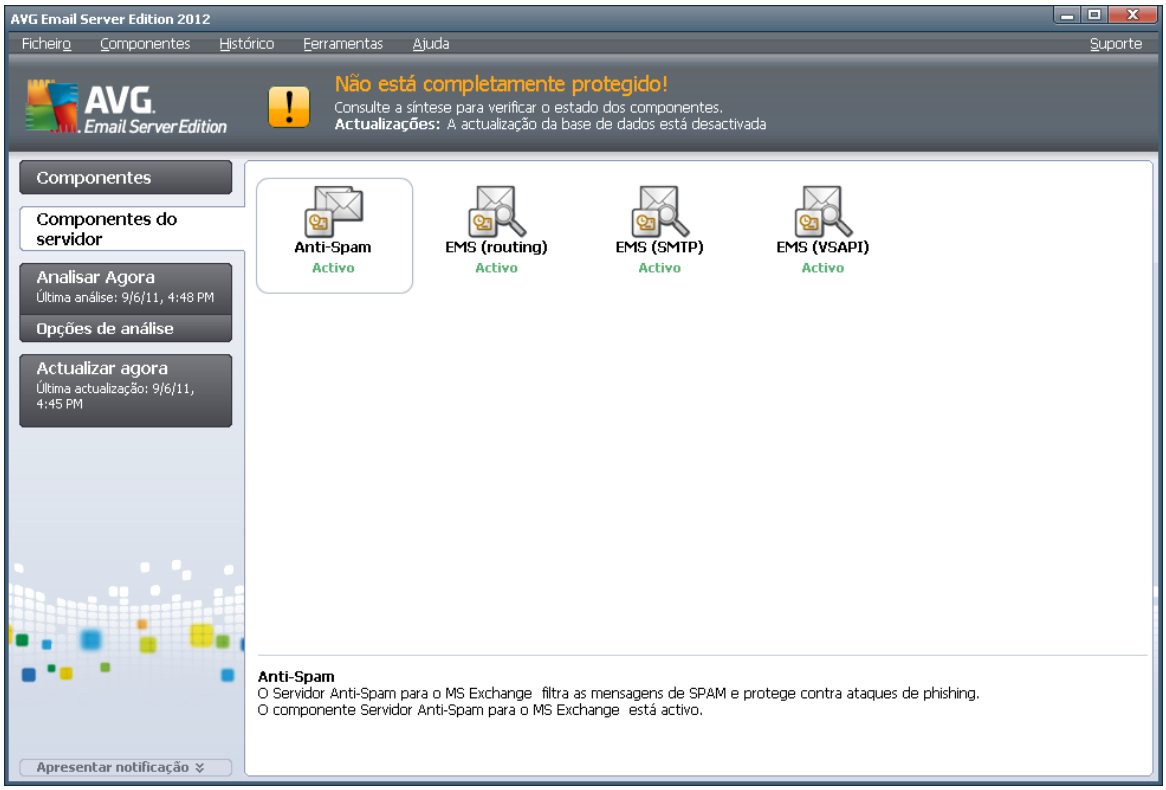
- ***Remover anexos*** - marque esta caixa para activar a funcionalidade.
- ***Remover todos os ficheiros executáveis*** - remover todos os executáveis.
- ***Remover todos os documentos*** - remover todos os documentos.
- ***Remover ficheiros com extensões separadas por vírgula*** - preencha esta caixa com extensões de ficheiros que queira que sejam automaticamente removidas. Separe as extensões com uma vírgula.
- ***Mover anexos filtrados para a quarentena de vírus*** - marque se não quiser que os anexos filtrados sejam definitivamente removidos. Com esta caixa marcada, todos os anexos seleccionados nesta janela serão automaticamente movidos para o ambiente da Quarentena de Vírus. É um local seguro para guardar ficheiros potencialmente maliciosos - pode aceder aos ficheiros e examiná-los sem colocar o sistema em perigo. A Quarentena de Vírus pode

ser acedida através do menu superior da interface principal do seu **AVG Email Server Edition 2012**. Basta clicar com o botão esquerdo do rato sobre o item ***Histórico*** e escolher o item ***Quarentena de Vírus*** a partir do menu de opções.

# 5. Verificador de E-mail para o Servidor MS Exchange 2003

## 5.1. Síntese

As opções de configuração do Verificador de E-mail para MS Exchange Server 2003 estão completamente integradas no AVG Email Server Edition 2012 como componente do servidor.




Os componentes do servidor incluem os seguintes:

Síntese simplificada dos componentes individuais do servidor:

- ***Anti-Spam - Servidor Anti-Spam para o MS Exchange***

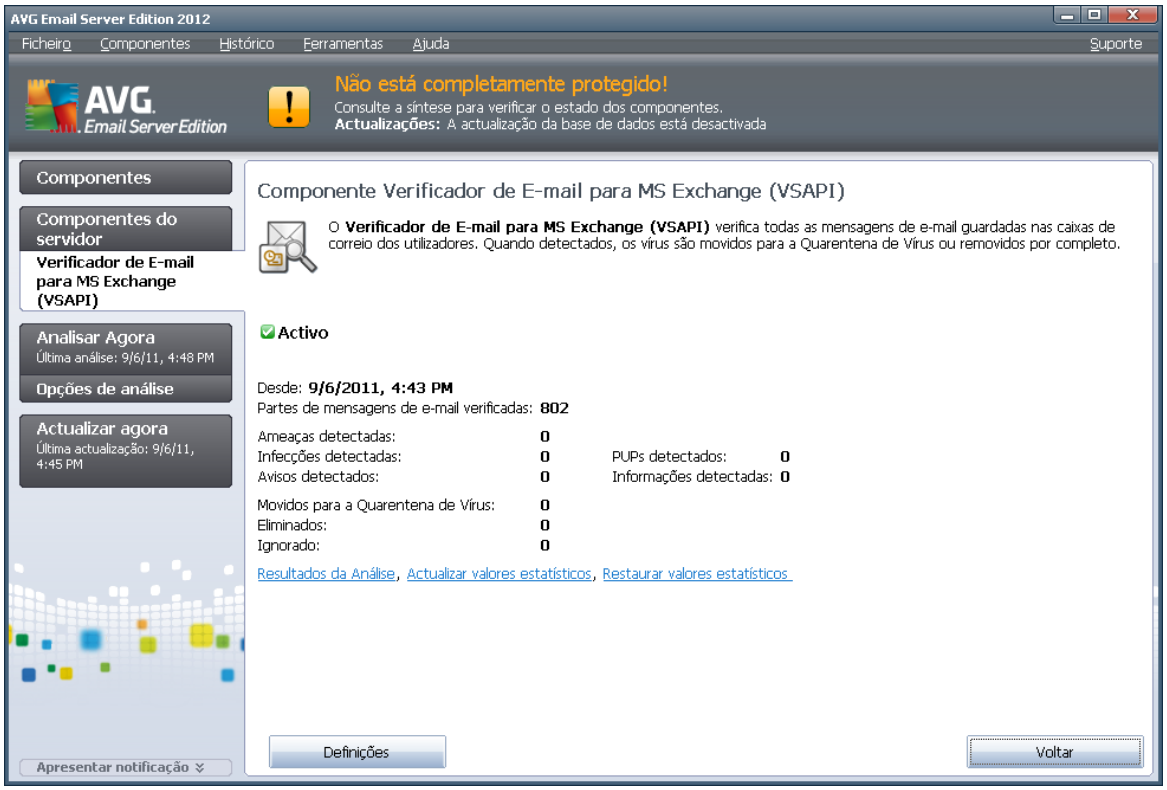
  verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. Utiliza vários métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de protecção possível contra mensagens de e-mail indesejadas.

- ***EMS (VSAPI) - Verificador de E-mail para o MS Exchange (VSAPI)***

  Verifica todas as mensagens de e-mail guardadas nas caixas de correio dos utilizadores. Se for detectado algum vírus, será movido para a Quarentena de Vírus ou removido na totalidade.

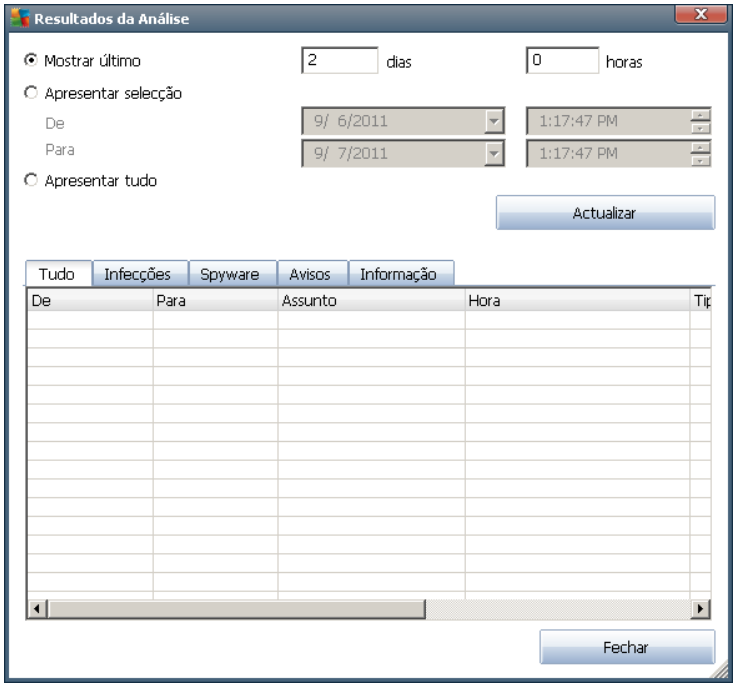
Clique duas vezes sobe um componente para abrir a interface do mesmo. O ***Componente Anti-Spam*** tem o seu ecrã exclusivo descrito num capítulo à parte. A interface do ***Verificador de E-mail***

***para MS Exchange (VSAPI)*** apresenta os seguintes botões de controlo e hiperligações:




- ***Resultados da Análise***

  Abre uma nova janela onde pode rever os resultados da análise:




Aqui, pode verificar mensagens divididas em vários separadores de acordo com o nível de gravidade. Consulte a configuração dos componentes individuais para corrigir a gravidade e reportação.

Por predefinição, só são apresentados os resultados dos dois últimos dias. Pode alterar o período apresentado através da alteração das seguintes opções:

- ***Mostrar último*** - insira os dias e as horas pretendidas.
- ***Apresentar selecção*** - escolha uma hora pretendida e um intervalo de datas.
- ***Apresentar tudo*** - Apresenta resultados para todo o período.

Use o botão ***Actualizar*** para recarregar os resultados.

- ***Actualizar valores estatísticos*** - actualiza as estatísticas apresentadas acima.
- ***Restaurar valores estatísticos*** - restaura todas as estatísticas para zero.

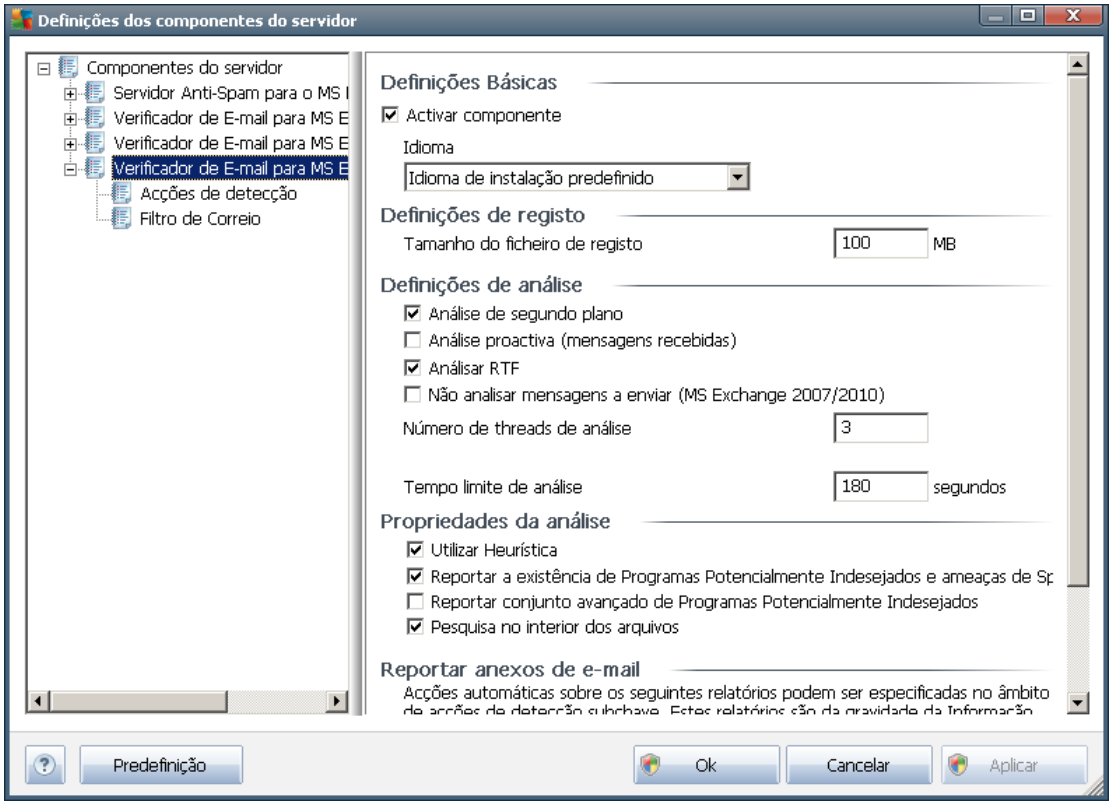
Os botões activos são os seguintes:

- ***Definições*** - use este botão para abrir as definições do componente.
- ***Retroceder*** - prima esta botão para regressar à Síntese de componentes do servidor.

Encontrará mais informações sobre definições individuais de todos os componentes nas secções abaixo.

## 5.2. Verificador de E-mail para o MS Exchange (VSAPI)

Este item contém definições do ***Verificador de E-mail para o MS Exchange (VSAPI)***.




A secção ***Definições Básicas*** contém as seguintes opções:

- ***Activar componente*** - desmarque para desactivar o componente.
- ***Idioma*** - seleccione o idioma pretendido para o componente.

A secção ***Definições de registo***:

- ***Tamanho do Ficheiro de registo*** - escolha um tamanho pretendido para o ficheiro de registo. Valor predefinido: 100 MB.

A secção ***Definições de análise***:

- ***Análise em Segundo Plano*** – pode activar ou desactivar o processo de análise em segundo plano. A análise em segundo plano é uma das funcionalidades da interface de aplicação VSAPI 2.0/2.5. Permite a análise por tópicos das Bases de Dados de Mensagens do Exchange. Sempre que for encontrado um item que não tenha sido analisado com as mais recentes actualizações da base de dados de vírus nas pastas da caixa de correio do utilizador, será enviado ao AVG para Exchange / Server para ser analisado. A análise e a procura de objectos não examinados são executadas em paralelo.

É usada uma classificação de prioridade baixa específica para cada base de dados, o que assegura que outras tarefas (ex. armazenamento de mensagens de e-mail na base de dados do Microsoft Exchange) são sempre executadas prioritariamente.

- ***Análise Pro-activa (mensagens de entrada)***

  Pode activar ou desactivar a função de análise pro-activa do VSAPI 2.0/2.5 aqui. . Esta análise ocorre quando um item é entregue numa pasta sem o pedido ter sido feito pelo cliente.

  Assim que as mensagens são submetidas para o Exchange, entram na fila de análise global com prioridade baixa (máximo de 30 itens). São analisados numa base de primeiro a entrar, primeiro a sair (FIFO). Se um item for acedido enquanto ainda estiver na fila, é passado para prioridade alta.

  ***Nota:*** *As mensagens que excedam o número limite continuarão para o Exchange sem serem analisadas.*

***Nota:*** *Mesma que desactive a* ***Análise em Segundo Plano*** *e a* ***Análise Pro-activa****, a análise aquando do acesso estará activa quando o utilizador tentar transferir uma mensagem com o cliente MS Outlook.*

- ***Analisar RTF*** - permite especificar se o tipo de ficheiro RTF deve ou não ser analisado.
- ***Número de Tópicos da Análise*** - por predefinição, a análise é processada por tópicos para aumentar o desempenho global da análise através de um certo nível de paralelismo. Neste campo, pode alterar a contagem dos tópicos.

  O número de tópicos predefinido é igual a 2 vezes o "número de processadores" + 1.

  O número mínimo de tópicos é computado como ('número de processadores'+1) dividido por 2.

  O número máximo de tópicos é computado como 'Número de processadores' multiplicado por 5 + 1.

  Se o valor for equivalente ao mínimo ou inferior, ou ao máximo ou superior, será usado o valor predefinido.

- ***Tempo Limite da Análise*** – o intervalo contínuo máximo (em segundos) para que um tópico aceda à mensagem que está a ser analisada (o valor predefinido é 180 segundos).

A secção ***Propriedades da análise***:

- ***Utilizar Heurística*** - marque esta caixa para activar o método de análise heurística durante a análise.

- ***Reportar a existência de Programas Potencialmente Indesejados e ameaças de Spyware*** - marque esta opção para reportar a presença de programas potencialmente indesejados e spyware.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** - marque para detectar pacotes alargados de spyware: programas que são perfeitamente seguros quando

adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente, ou programas que são sempre seguros mas que podem ser indesejados (barras de ferramentas, etc.). Esta é uma medida adicional que aumenta o conforto e segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição. Nota: Esta funcionalidade de detecção é um complemento da opção anterior, portanto, se quiser protecção contra os tipos básicos de spyware, mantenha sempre a caixa anterior marcada.

- ***Analisar no interior de arquivos*** - marque esta opção para permitir que o verificador analise também no interior de arquivos (zip, rar, etc).

A secção ***Reportação de anexos de e-mail*** permite-lhe escolher os itens que deverão ser reportados durante a análise. A configuração predefinida pode ser facilmente corrigida na secção ***Acções de detecção***, opção ***Informação*** (veja abaixo).

Estão disponíveis as seguintes opções:

- ***Reportar arquivos protegidos por palavra-passe***
- ***Reportar documentos protegidos por palavra-passe***
- ***Reportar ficheiros que contenham macros***
- ***Reportar extensões ocultas***

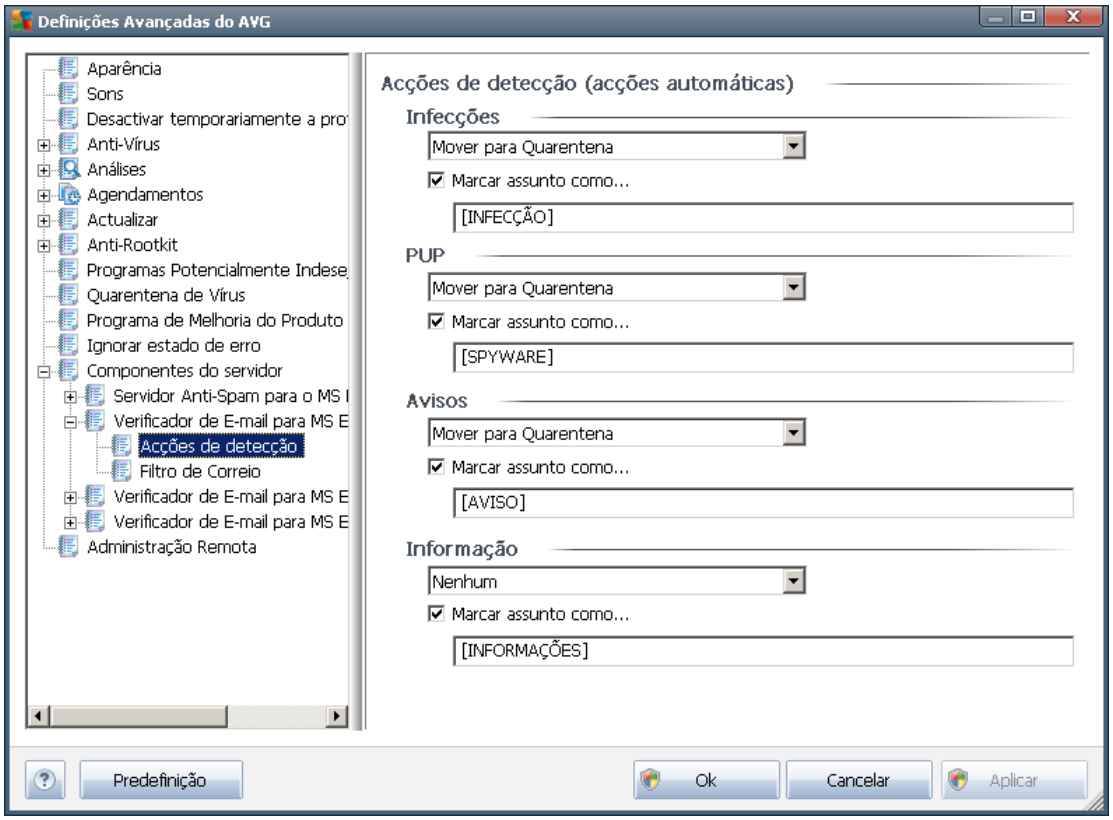
Regra geral, todas estas funcionalidades são extensões do utilizador dos serviços da interface da aplicação Microsoft VSAPI 2.0/2.5 Para obter informações detalhadas sobre o VSAPI 2.0/2.5, aceda a uma das seguintes hiperligações (e também às hiperligações acessíveis a partir das indicadas):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - para mais informações sobre o Exchange e interacção com software anti-vírus.
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 para informações sobre funcionalidades do componente VSAPI 2.5 na aplicação Exchange 2003 Server.

Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Acções de detecção***
- ***Filtro de Correio***

## 5.3. Acções de detecção




No item secundário ***Acções de detecção***, pode escolher acções automáticas que deverão ser executadas durante o processo de análise

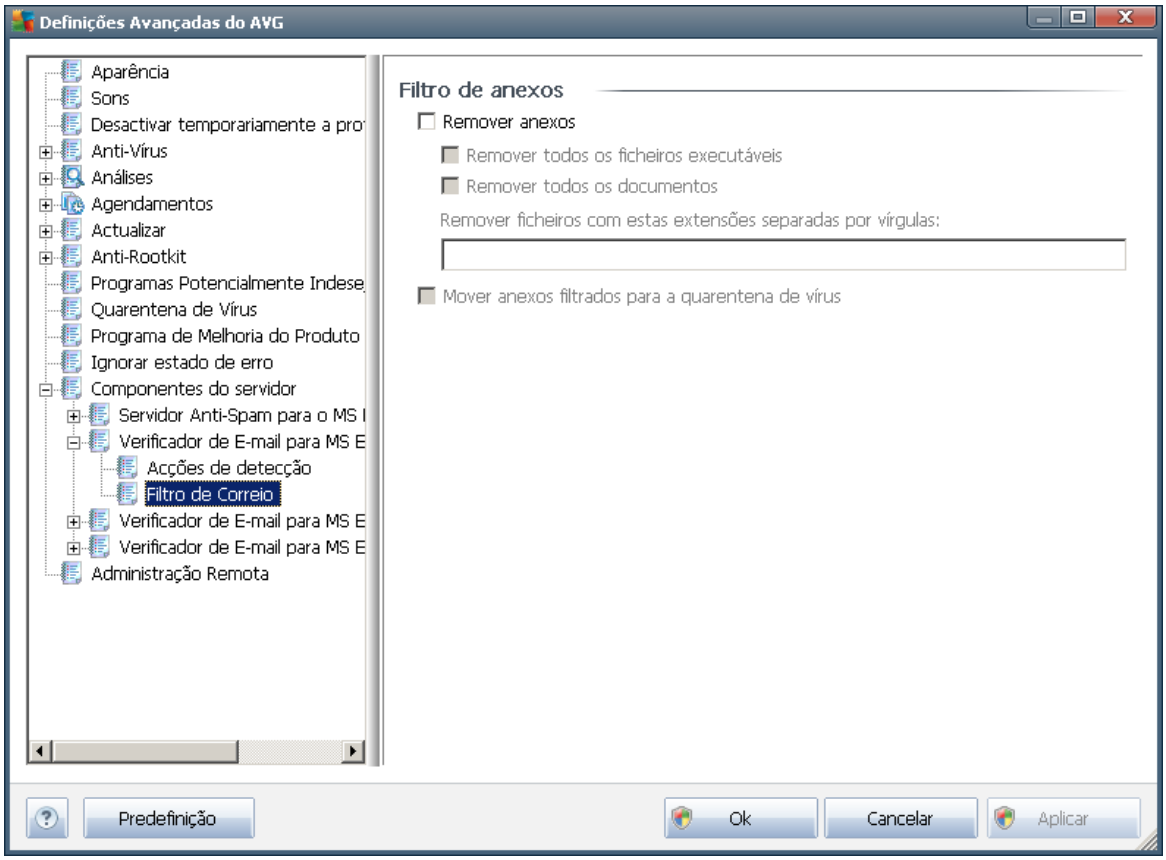
As acções estão disponíveis para os seguintes itens:

- ***Infecções***
- ***PUP (Programas Potencialmente Indesejados)***
- ***Avisos***
- ***Informações***

Use o menu pendente para escolher uma acção para cada item:

- ***Nenhuma*** - não será tomada nenhuma acção.
- ***Mover para a Quarentena*** - a ameaça em causa será movida para a Quarentena de Vírus.
- ***Remover*** - a ameaça em causa será removida.

## 5.4. Filtro de Correio



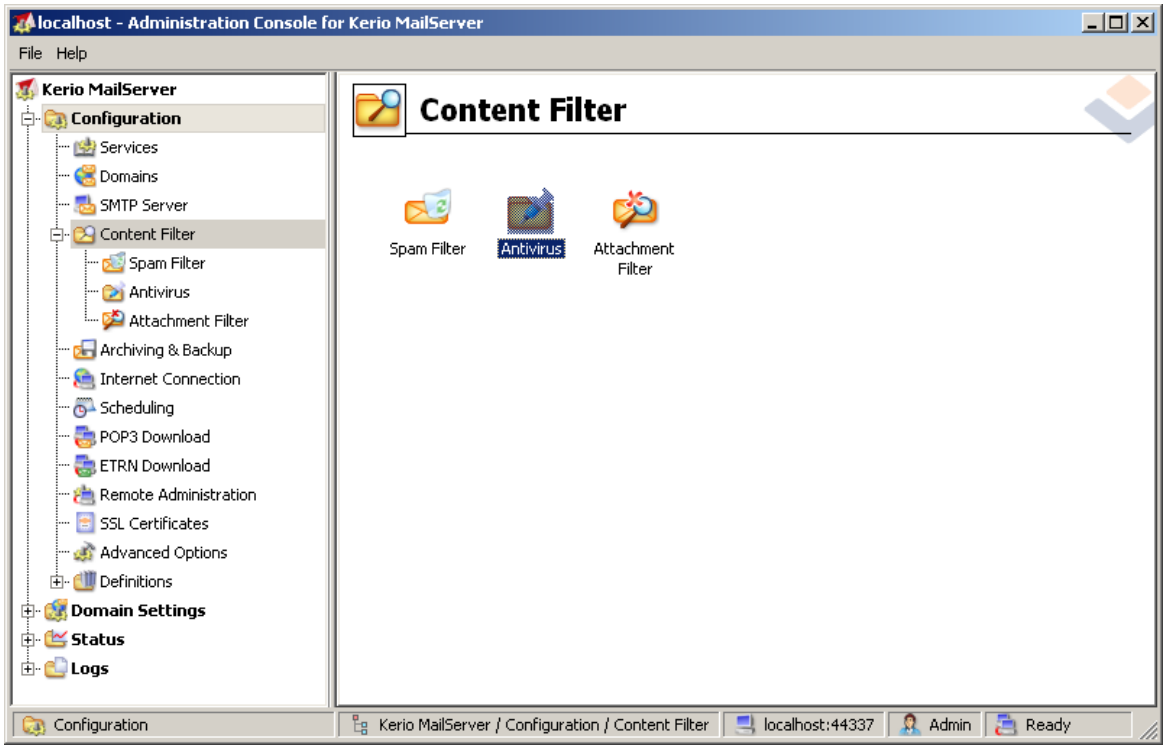

No item secundário ***Filtro de Correio***, pode escolher quais os anexos que devem ser automaticamente removidos, se quiser. Estão disponíveis as seguintes opções:

- ***Remover anexos*** - marque esta caixa para activar a funcionalidade.
- ***Remover todos os ficheiros executáveis*** - remover todos os executáveis.
- ***Remover todos os documentos*** - remover todos os documentos.
- ***Remover ficheiros com extensões separadas por vírgula*** - preencha esta caixa com extensões de ficheiros que queira que sejam automaticamente removidas. Separe as extensões com uma vírgula.
- ***Mover anexos filtrados para a quarentena de vírus*** - marque se não quiser que os anexos filtrados sejam definitivamente removidos. Com esta caixa marcada, todos os anexos seleccionados nesta janela serão automaticamente movidos para o ambiente da Quarentena de Vírus. É um local seguro para guardar ficheiros potencialmente maliciosos - pode aceder aos ficheiros e examiná-los sem colocar o sistema em perigo. A Quarentena de Vírus pode ser acedida através do menu superior da interface principal do seu **AVG Email Server Edition 2012**. Basta clicar com o botão esquerdo do rato sobre o item ***Histórico*** e escolher o item ***Quarentena de Vírus*** a partir do menu de opções.

# 6. AVG para Kerio MailServer

## 6.1. Configuração

O mecanismo de protecção antivírus está integrado directamente na aplicação do Kerio MailServer. Para activar a protecção de e-mail do Kerio MailServer pelo componente de análise AVG, inicie a aplicação Consola de Administração Kerio. Na árvore de controlo situada no lado esquerdo da janela da aplicação, seleccione o ramo secundário Filtro de Conteúdos no ramo Configuração:

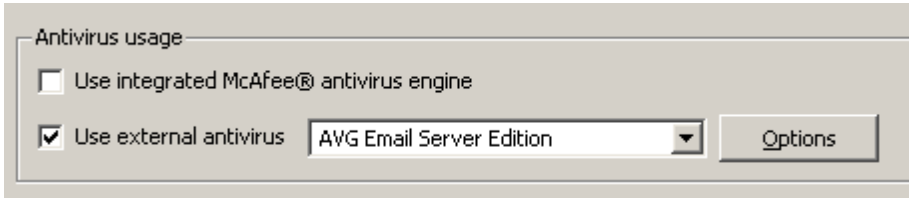



Se clicar no item Filtro de conteúdo, será apresentada uma janela com três itens:

- ***Filtro Anti-spam***
- ***Anti-vírus*** (consulte a secção ***Anti-vírus***)
- ***Filtro de anexos*** (consulte a secção ***Filtro de anexos***)

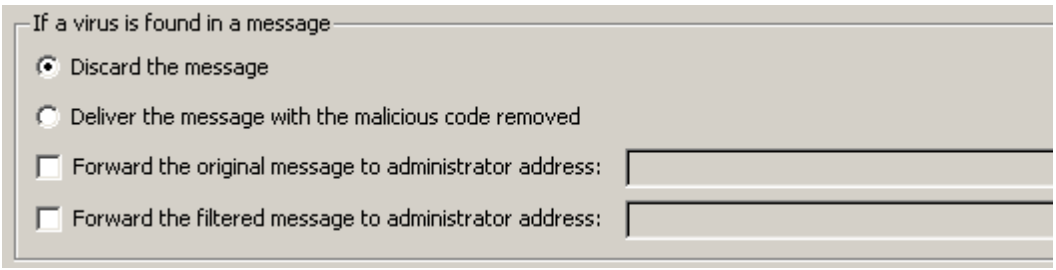
### 6.1.1. Antivírus

Para activar o AVG para Kerio MailServer, seleccione a caixa Utilizar antivírus externo e seleccione a edição AVG Email Server no menu de software externo do quadro Utilização Antivírus da janela de configuração:




Na secção seguinte, especifique o procedimento para uma mensagem infectada ou filtrada:

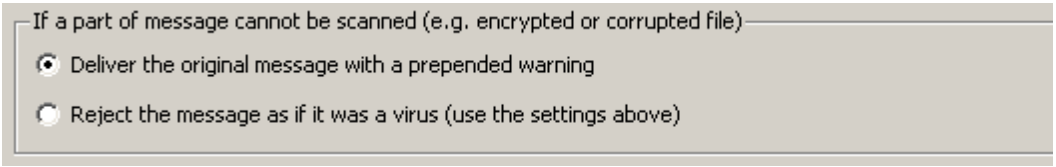
- ***Se for detectado um vírus numa mensagem***




Este quadro especifica a acção a executar quando é detectado um vírus numa mensagem ou quando uma mensagem é filtrada por um filtro de anexos:

  - ***Eliminar a mensagem*** – se seleccionada, a mensagem infectada ou filtrada será eliminada.
  - ***Entregar a mensagem com o código malicioso removido*** – se seleccionada, a mensagem será entregue ao destinatário, mas sem o anexo potencialmente perigoso.
  - ***Reencaminhar a mensagem original para o endereço do administrador*** – se seleccionada, a mensagem infectada com vírus será reencaminhada para o endereço especificado no campo de texto do endereço
  - ***Reencaminhar a mensagem filtrada para o endereço do administrador*** – se seleccionada, a mensagem filtrada será reencaminhada para o endereço especificado no campo de texto do endereço.

- ***Se não for possível analisar uma parte da mensagem (por exemplo, um ficheiro encriptado ou danificado)***




Este quadro especifica a acção a executar se não for possível analisar uma parte da mensagem ou do anexo:

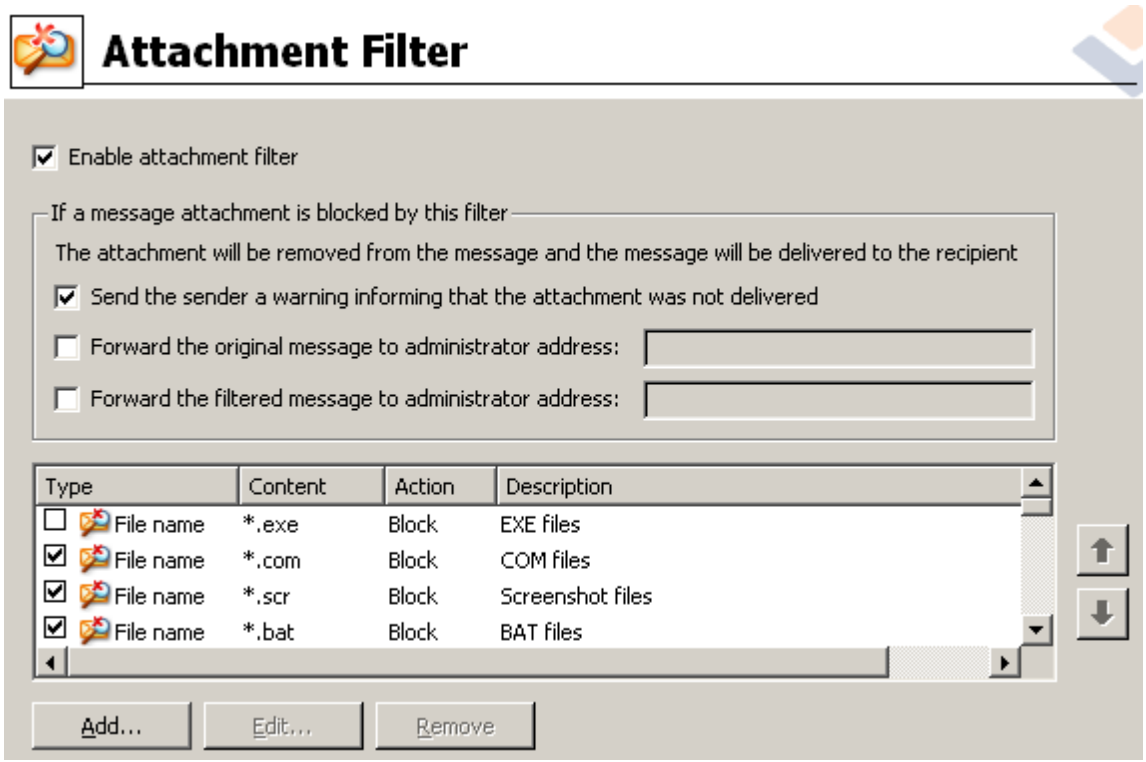
  - ***Entregar a mensagem original com um aviso preparado*** – a mensagem (ou anexo) será entregue sem ser analisada. O utilizador será avisado de que a mensagem ainda

pode conter vírus.

- ***Rejeitar a mensagem como se fosse um vírus*** – o sistema reagirá de forma idêntica a quando é detectado um vírus (ou seja, a mensagem será entregue sem nenhum anexo ou rejeitada). Esta opção é segura, mas o envio de arquivos protegidos por palavra-passe será virtualmente impossível.

### 6.1.2. Filtro de anexos

No menu Filtro de Anexos existe uma lista de várias definições de anexos:




Seleccione a caixa de verificação Activar filtro de anexos para activar/desactivar a filtragem de anexos de correio. Opcionalmente, pode alterar as seguintes definições:

- ***Enviar um aviso ao remetente a informar que o anexo não foi entregue***

  O remetente receberá um aviso do Kerio MailServer a informá-lo que enviou uma mensagem com um vírus ou um anexo bloqueado.

- ***Reencaminhar a mensagem original para o endereço do administrador***

  A mensagem será reencaminhada (tal como está – com o anexo infectado ou interdito) para um endereço de e-mail definido, local ou externo.

- ***Reencaminhar a mensagem filtrada para o endereço do administrador***

  A mensagem sem o anexo infectado ou interdito será (independentemente das acções

seleccionadas abaixo) reencaminhada para o endereço de e-mail especificado. Esta opção pode ser utilizada para verificar o funcionamento correcto do antivírus e/ou ou filtro de anexos.

Na lista de extensões, cada item tem quatro campos:

- ***Tipo*** – especificação do tipo de anexo determinado pela extensão fornecida do campo Conteúdo. Os tipos possíveis são Nome de ficheiro ou MIME. Seleccione a caixa respectiva neste campo para incluir/excluir o item da filtragem de anexos.
- ***Conteúdo*** - permite especificar uma extensão a filtrar. Pode utilizar caracteres universais do sistema operativo (por exemplo, a cadeia "*.doc.*" significa qualquer ficheiro com a extensão . doc e qualquer outra extensão subsequente).
- ***Acção*** – define a acção a executar com o anexo em causa. As acções possíveis são Aceitar (aceitar o anexo) e Bloquear (será executada uma acção conforme definido acima da lista de anexos desactivados).
- ***Descrição*** – a descrição do anexo é definida neste campo.

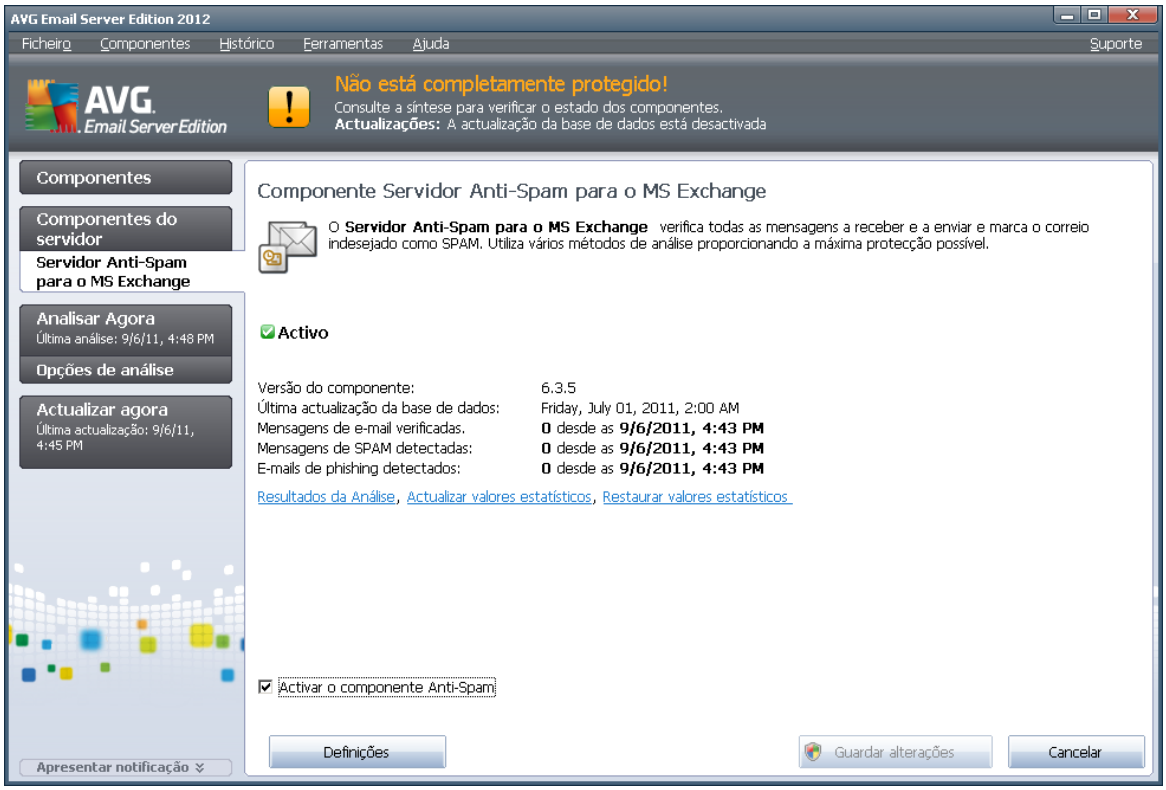
Para remover um item da lista, prima o botão Remover. Pode adicionar outro item à lista, prima o botão ***Adicionar....***. Ou, pode editar um registo existente clicando no botão ***Editar...***. Será apresentada a seguinte janela:


- No campo Descrição, escreva uma breve descrição do anexo a filtrar.
- No campo Se uma mensagem de correio contém um anexo em que, seleccione o tipo de anexo (Nome de ficheiro ou MIME). Também pode escolher uma extensão específica na lista de extensões fornecida ou digitar directamente os caracteres universais da extensão.

No campo Em seguida, decida se o anexo definido deve ser bloqueado ou aceite.

# 7. Configuração Anti-Spam

## 7.1. Interface do Anti-Spam

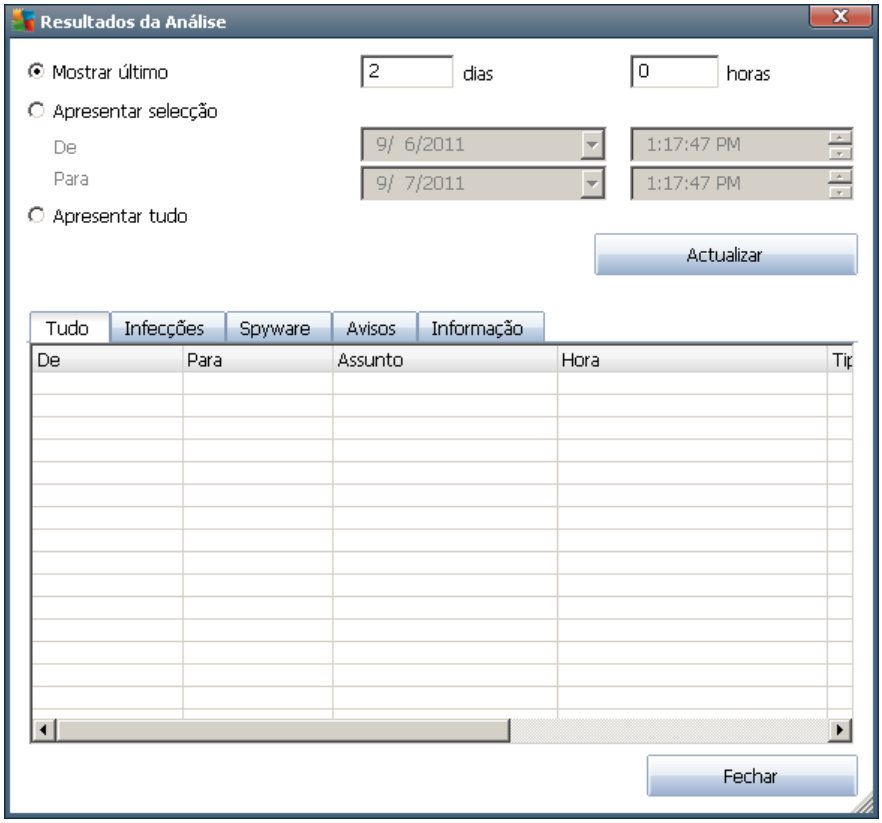



A janela do servidor ***Anti-Spam*** pode ser acedida através da secção ***Componentes do Servidor*** (menu esquerdo). Esta contém uma breve descrição da funcionalidade do componente servidor, informações sobre o seu estado actual (*O componente Servidor Anti-Spam para o MS Exchange está activo.* ), e algumas estatísticas.

Ligações disponíveis:

- ***Resultados da Análise***

  Abre uma nova janela onde pode rever os resultados da análise anti-spam:




Aqui pode verificar as mensagens detectadas como SPAM (mensagens indesejadas) ou Tentativa de Phishing (uma tentativa de roubo dos seus dados pessoais, informações bancárias, identidade, etc.). Por predefinição, só são apresentados os resultados dos dois últimos dias. Pode alterar o período apresentado através da alteração das seguintes opções:

- ***Mostrar último*** - insira os dias e as horas pretendidas.
- ***Apresentar selecção*** - escolha uma hora pretendida e um intervalo de datas.
- ***Apresentar tudo*** - Apresenta resultados para todo o período.

Use o botão ***Actualizar*** para recarregar os resultados.

- ***Actualizar valores estatísticos*** - actualiza as estatísticas apresentadas acima.
- ***Restaurar valores estatísticos*** - restaura todas as estatísticas para zero.

A secção **Definições do componente Anti-Spam** da janela contém uma única caixa ***Activar Anti-Spam***. Desmarque-a para desactivar a protecção Anti-Spam (ou seja, desactivar o componente por completo). A protecção Anti-Spam pode ser activada novamente por meio desta mesma caixa, ou marcando a caixa equivalente nas Definições do componente Anti-Spam.

Os botões activos são os seguintes:

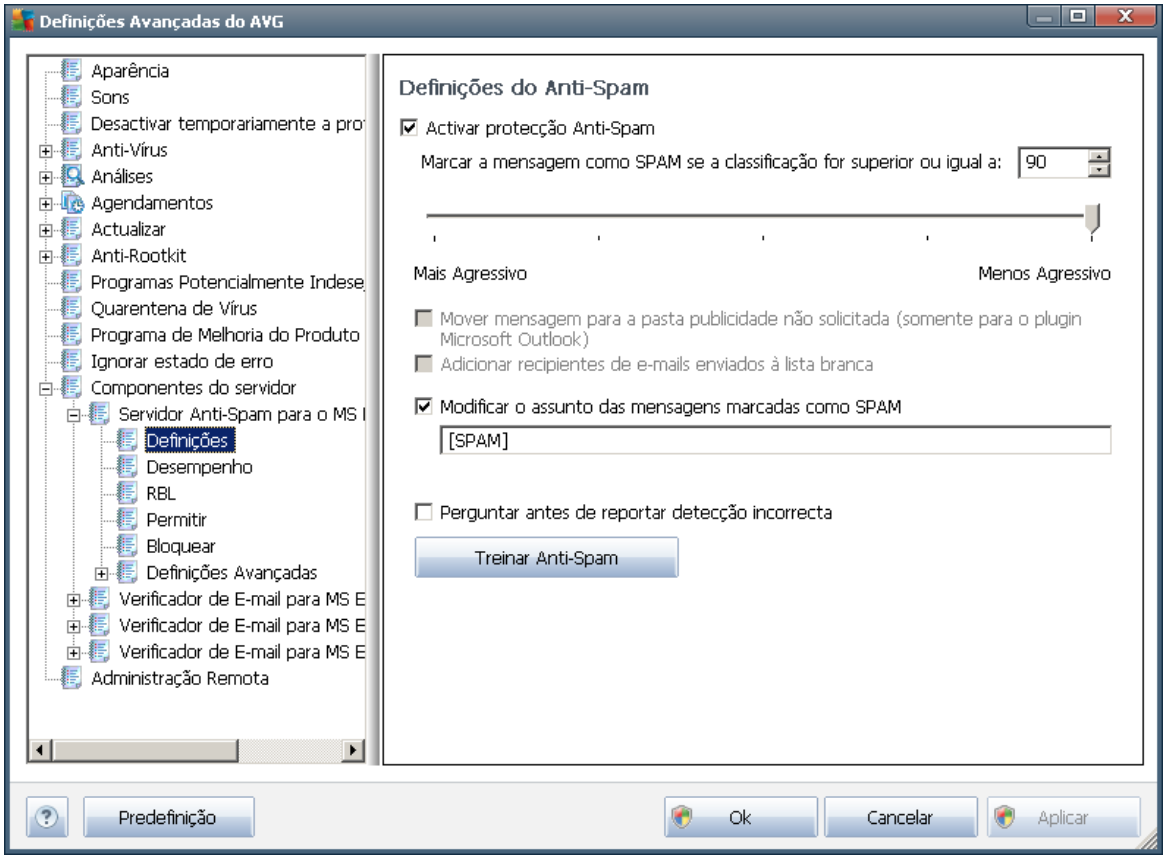
- ***Definições*** – use este botão para abrir as Definições Anti-Spam.
- ***Retroceder*** - prima esta botão para regressar à Síntese de componentes do servidor.

## 7.2. Princípios do Anti-Spam

Spam refere-se a correio não solicitado, que normalmente publicita um produto ou serviço, que é enviado em massa para um grande número de endereços de e-mail, sobrecarregando as caixas de correio dos destinatários. Spam não se refere a correio electrónico comercial legítimo, consentido pelos consumidores. Para além de aborrecedor, as mensagens de spam podem igualmente ser fonte de falcatruas, vírus ou conteúdo ofensivo.

***O componente Anti-Spam verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM.*** Utiliza vários métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de protecção possível contra mensagens de e-mail indesejadas.

## 7.3. Definições Anti-Spam




Na janela ***Definições básicas do componente Anti-Spam*** pode marcar a caixa ***Activar protecção Anti-Spam*** para permitir/interditar a análise anti-spam de comunicações de e-mail.

Nesta janela também pode seleccionar medidas de classificação mais ou menos agressivas. O filtro ***Anti-Spam***atribui uma classificação a cada mensagem ( *ou seja, o quão similar o conteúdo da mensagem é com SPAM*) baseado em várias técnicas de análise dinâmica. Pode ajustar a definição***Marcar mensagem como spam se a pontuação for superior ou igual a*** introduzindo um valor (*50 a 90*) ou fazendo deslizar o cursor para a esquerda ou para a direita.

Veja aqui uma revisão geral do limiar de classificação:

- ***Valor 90*** - A maioria das mensagens de e-mail a receber serão entregues normalmente (sem serem marcadas como spam). O spam mais facilmente identificado ***será filtrado, mas, mesmo assim, poderá passar uma quantidade significativa despam.
- ***Valor 80-89*** – As mensagens de e-mail passíveis de serem spamserão filtradas. É igualmente possível que algumas mensagens que não são spam sejam incorrectamente filtradas.
- ***Valor 60-79*** – Considerada uma configuração rigorosa. As mensagens de e-mail susceptíveis de serem spamserão filtradas. É muito provável que sejam igualmente filtradas mensagens que não são Spam.
- ***Valor 50-59*** – Configuração muito rigorosa. Existe uma forte probabilidade de considerar mensagens de e-mail que não são spam.como sendo spam. Este intervalo não é recomendado para uma utilização normal.

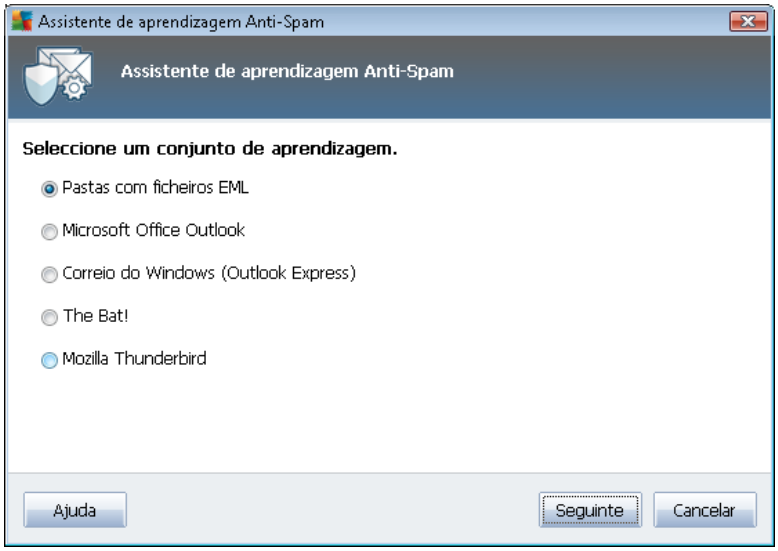
Pode ainda definir a forma como as mensagens de e-mail classificadas como spam devem ser tratadas:

- ***Modificar o assunto das mensagens marcadas como spam*** - seleccione esta caixa de verificação se quiser que todas as mensagens detectadas como sendo spam sejam marcadas com uma palavra ou carácter específico no campo de assunto da mensagem; o texto pretendido pode ser digitado no campo de texto activado.
- ***Perguntar antes de reportar detecção incorrecta*** - se tiver concordado com a participação no Programa de Melhoria do Produto durante o processo de instalação - este programa ajuda-nos a recolher informações actualizadas sobre as mais recentes ameaças de todos os participantes a nível mundial, e, em troca, temos a possibilidade de melhorar o produto para benefício de todos - ou seja, permitiu a reportação das ameaças detectadas à AVG. A reportação é processada automaticamente. No entanto, pode querer marcar esta caixa para confirmar que pretende ser inquirido antes da reportação de qualquer detecção de spam à AVG para assegurar que a mensagem deverá efectivamente ser classificada como spam.

O botão ***Treinar Anti-Spam*** abre o ***Assistente de aprendizagem do anti-spam*** descrito detalhadamente no capítulo seguinte.

## 7.3.1. Assistente de Aprendizagem Anti-Spam

A primeira janela do ***Assistente de Aprendizagem Anti-Spam*** solicita-lhe a origem de mensagens de e-mail que pretende utilizar para a aprendizagem. Regra geral, quererá usar mensagens de e-mail que não foram devidamente reconhecidas como SPAM, ou mensagens de spam que não foram reconhecidas.




Tem à sua disposição as seguintes opções a partir das quais escolher:

- ***Um cliente de e-mail específico*** - se usar um dos clientes de e-mail listados (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird* ), simplesmente seleccione a opção respectiva

- ***Pasta com ficheiros EML*** - Se utilizar outro programa de e-mail, deverá primeiro guardar as mensagens para uma pasta específica (no *formato.eml*), ou certificar-se de que conhece a localização das pastas das mensagens do seu cliente de e-mail. Depois seleccione***Pasta com ficheiros EML***, o que lhe permitirá localizar a pasta pretendida no próximo passo.

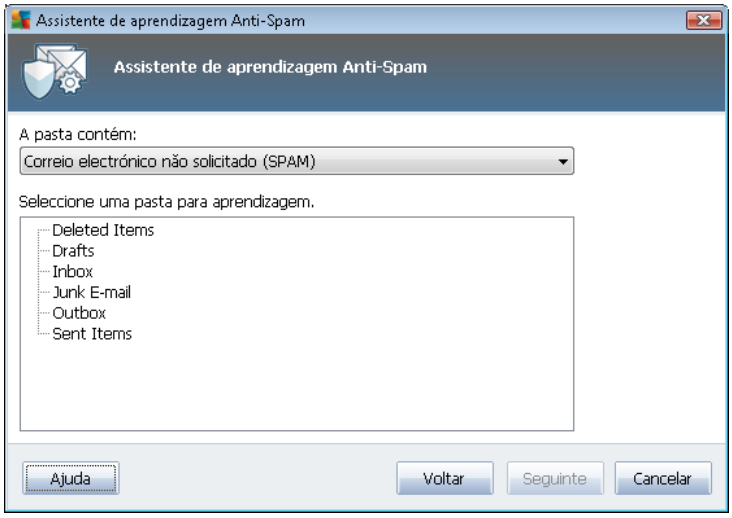
Para um processo de aprendizagem facilitado e mais rápido, é uma boa opção separar os e-mails nas pastas antecipadamente, de maneira a que a pasta que vai utilizar para a aprendizagem contenha só as mensagens de aprendizagem (sejam desejadas, ou indesejadas). No entanto, não é necessário, uma vez que poderá filtrar as mensagens de e-mail posteriormente.

Seleccione a opção apropriada e clique em ***Seguinte*** para continuar o assistente.

## 7.3.2. Selecciona Pasta com mensagens

A janela apresentada neste passo depende da sua selecção anterior.

**Pastas com ficheiros EML**



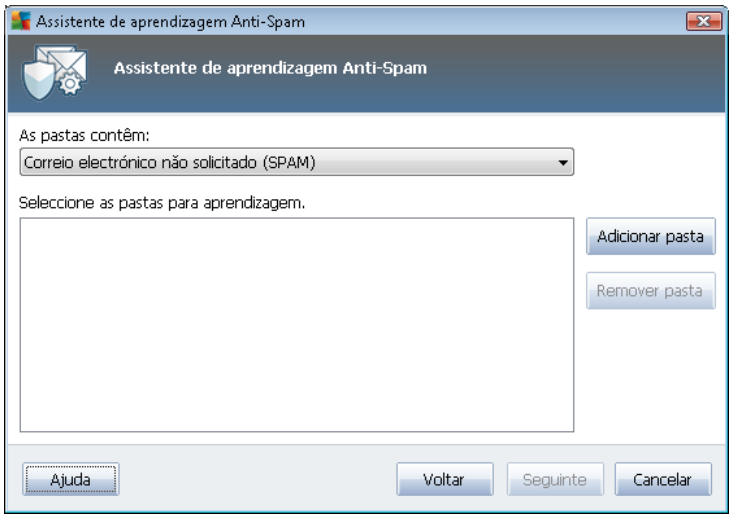

Nesta janela, por favor seleccione a pasta que contém as mensagens que pretende utilizar para a aprendizagem. Clique no botão ***Adicionar pasta*** para localizar a pasta com os ficheiros .eml ( *mensagens de e-mail guardadas*). A pasta seleccionada será então apresentada na janela.

Na Lista de opções ***Pastas contém:***, defina uma das seguintes opções - se a pasta seleccionada contém mensagens desejadas*(HAM)*), ou indesejadas (*SPAM*). Por favor tenha em atenção que poderá filtrar as mensagens no passo seguinte, portanto a pasta não tem necessariamente de conter só e-mails de aprendizagem. Também pode remover pastas seleccionadas indesejadas da lista clicando no botão ***Remover pasta***.

Quando tiver terminado, clique em***Seguinte*** e prossiga para as Opções de filtragem de mensagens.

## Cliente de e-mail específico

Assim que confirmar uma das opções, é apresentada uma nova janela.

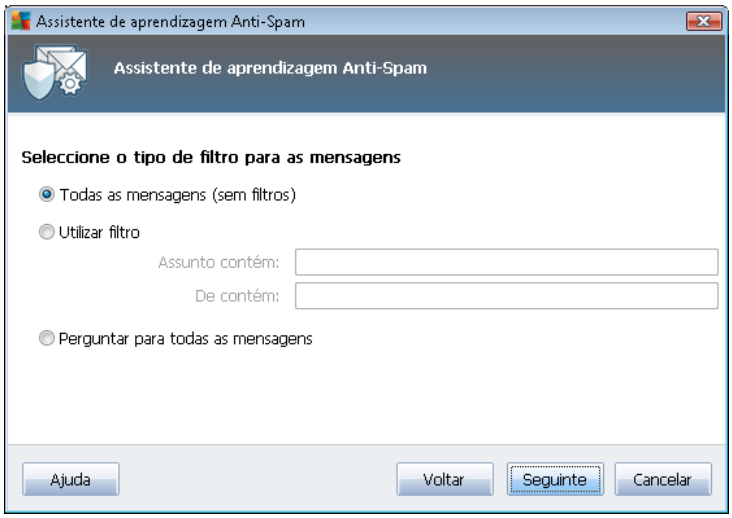


***Atenção:****No caso do Microsoft Office Outlook, será solicitado que seleccione o perfil do MS Office Outlook primeiro.*

Na Lista de opções ***Pastas contêm:***, defina uma das seguintes opções - se a pasta seleccionada contém mensagens desejadas*(HAM)*), ou indesejadas (*SPAM*). Por favor tenha em atenção que poderá filtrar as mensagens no passo seguinte, portanto a pasta não tem necessariamente de conter só e-mails de aprendizagem. Já existe uma árvore de navegação do cliente de e-mail seleccionado na secção principal da janela. Por favor localize a pasta pretendida na árvore e seleccione-a com o rato.

Quando tiver terminado, clique em***Seguinte*** e prossiga para as Opções de filtragem de mensagens.

## 7.3.3. Opções de filtragem de mensagens




Nesta janela, pode definir a filtragem das mensagens de e-mail.

- ***Todas as mensagens (sem filtragem)*** - Se tiver a certeza de que a pasta seleccionada contém apenas mensagens que quer utilizar para aprendizagem, seleccione a opção ***Todas as mensagens (sem filtragem)***.

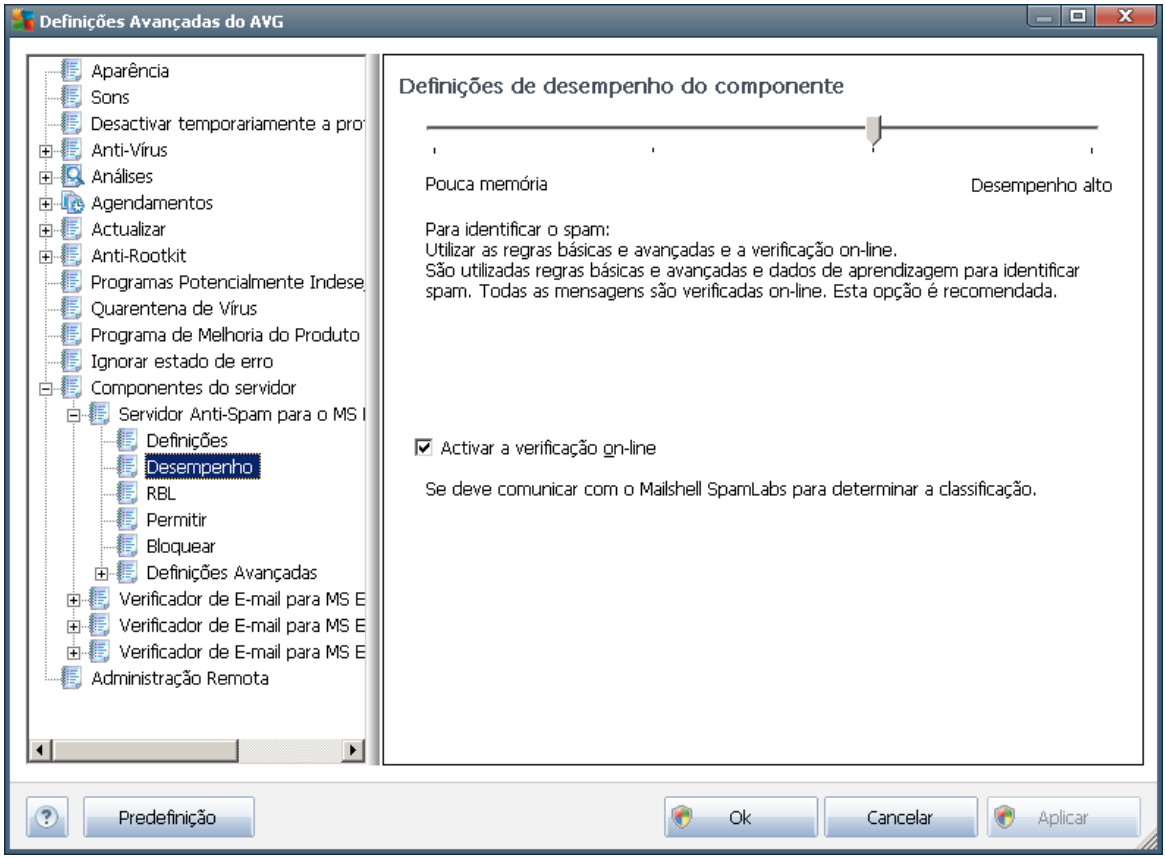
- ***Utilizar filtro*** - Para uma filtragem mais avançada, seleccione a opção ***Utilizar filtro***. Pode introduzir uma palavra (*nome*), parte de uma palavra, ou frase a ser procurada no campo assunto/e ou remetente do e-mail Todas as mensagens que correspondam ao critério com exactidão serão utilizadas para a aprendizagem, sem mais quaisquer interpelações. Quando preenche ambos os campos de texto, os endereços que correspondam a apenas uma das duas condições serão igualmente utilizados.

- ***Perguntar para cada mensagem*** - Se não tiver a certeza em relação às mensagens contidas na pasta, e se quiser que o Assistente o inquira em relação a cada mensagem *(para que possa determinar se a mensagem deve ser utilizada para aprendizagem ou não)*, seleccione a opção ***Perguntar para cada mensagem***.

Quando a opção apropriada tiver sido seleccionada, clique em ***Seguinte***. A janela seguinte será meramente informativa, informando-o que o assistente está pronto para processar as mensagens. Para iniciar a aprendizagem, clique no botão ***Seguinte*** novamente. A aprendizagem será então

iniciada de acordo com as condições previamente seleccionadas.

## 7.4. Desempenho




A janela ***Definições de desempenho do componente*** (*acessível via o item* ***Desempenho*** *na navegação à esquerda* ) faculta as definições de desempenho do componente ***Anti-Spam***. Desloque o cursor para a esquerda ou para a direita para alterar o nível de desempenho de análise estabelecido entre os modos ***Memória baixa*** / ***Elevado desempenho***.

- ***Memória baixa*** - não serão utilizadas quaisquer regras durante o processo de análise para identificar spam. Serão utilizados apenas dados de aprendizagem para identificação. Este modo não é recomendado para uso comum, a não ser que o hardware do computador seja muito fraco.

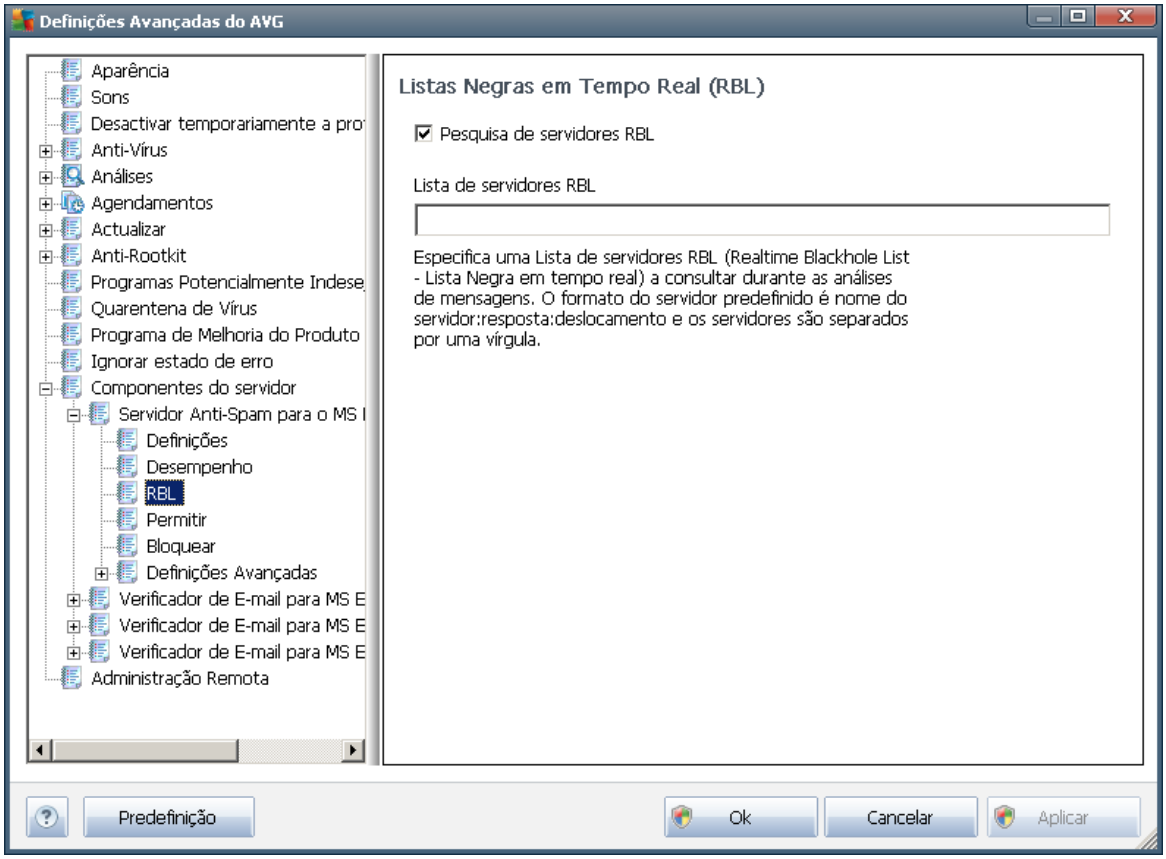
- ***Alto desempenho*** - este modo requer uma grande quantidade de memória. Durante o processo de análise para identificar spam, serão utilizadas as seguintes características: regras e cache de base de dados despam, regras básicas e avançadas, endereços IP de remetentes de spam e bases de dados de remetentes de spam.

O item ***Activar verificação on-line*** está activado por predefinição. Resulta numa detecção de spam mais precisa via comunicação com os servidores Mailshell, ou seja, os dados analisados serão comparados com as bases de dados on-lineMailshell.

***Normalmente é recomendável que mantenha as definições predefinidas e só as altere se tiver uma razão válida para o fazer. Quaisquer alterações à configuração devem ser efectuadas exclusivamente por utilizadores avançados!***

## 7.5. RBL

O item ***RBL*** abre uma janela de edição apelidada ***Listas Negras em Tempo Real (RBL)***:




Nesta janela pode activar/desactivar a função ***Pesquisa de servidores RBL***.

O servidor RBL (*Real-time Blackhole List)* é um servidor DNS com uma base de dados extensiva de remetentes de spam conhecidos. Quando esta funcionalidade está ligada, todas as mensagens de e-mail serão verificadas de acordo com a base de dados do servidor RBL e serão assinaladas como spam se forem idênticas a qualquer uma das entradas da base de dados.

As bases de dados dos servidores RBL contêm identificadores de spamactualizados ao minuto, para garantir a melhor e mais rigorosa detecção de spam. Esta funcionalidade é particularmente útil para utilizadores que recebem grandes quantidades de spam que o componente Anti-Spam normalmente não consegue detectar.

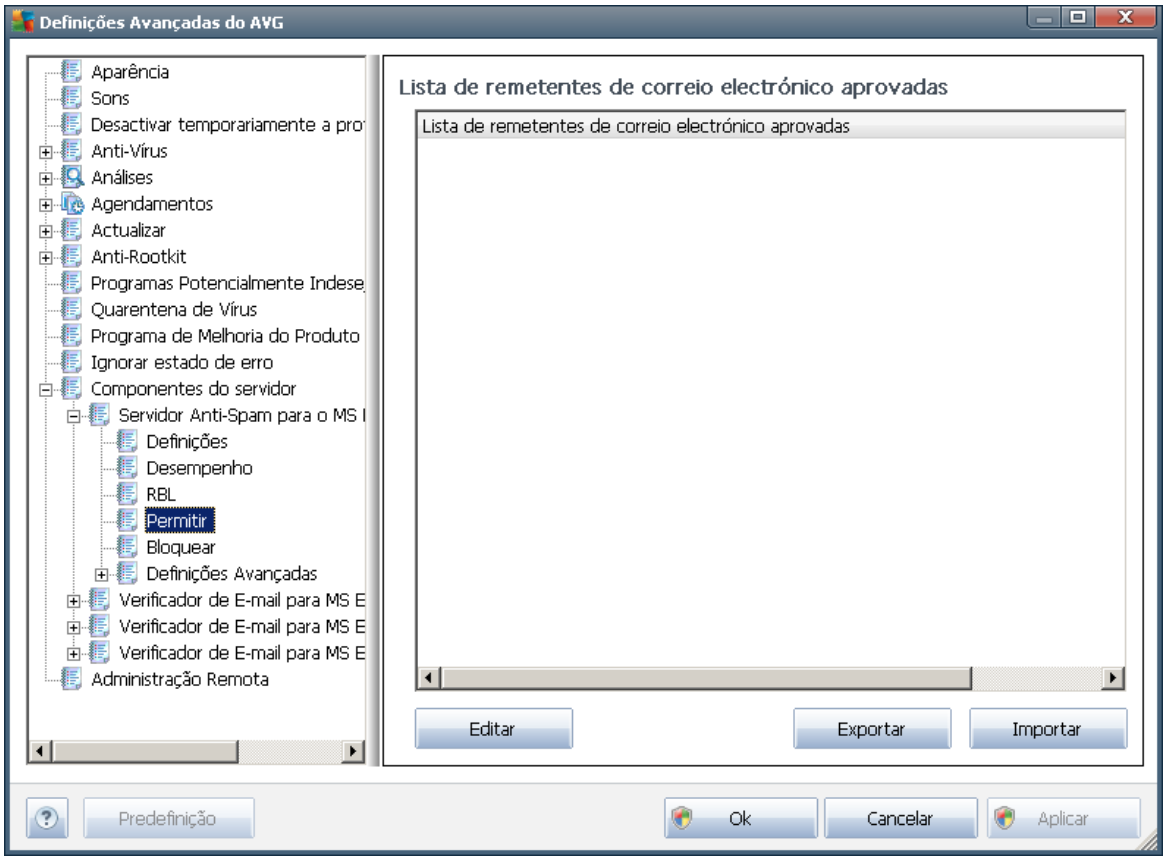
A ***lista de servidores RBL*** permite-lhe definir localizações específicas de servidores RBL. Por predefinição, são especificados dois endereços de servidores RBL. Recomendamos que mantenha as predefinições, a não ser que seja um utilizador experiente e precise de alterar estas definições!

***Atenção:****Activar esta funcionalidade pode tornar mais lento o processo de recepção de e-mail em alguns sistemas e configurações, uma vez que cada uma das mensagens tem de ser verificada de acordo com a base de dados do servidor RBL.*

***Não são enviados dados pessoais para o servidor!***

## 7.6. Lista Branca

O item ***Lista Branca*** abre uma janela com uma lista global de endereços de e-mail e de nomes de domínios aprovados cujas mensagens nunca serão assinaladas comospam.




Na interface de edição pode compilar uma lista de remetentes dos quais nunca espera receber mensagens indesejadas (spam). Pode ainda compilar uma lista de nomes de domínios completos (ex.*avg.com*, que sabe que não geram spam.

Quando já tiver uma lista de remetentes/ou nomes de domínio preparada, pode introduzi-los por meio de um dos seguintes métodos: via introdução directa de cada endereço de correio electrónico ou importando toda a lista de endereços de uma vez. Estão disponíveis os seguintes botões de controlo:

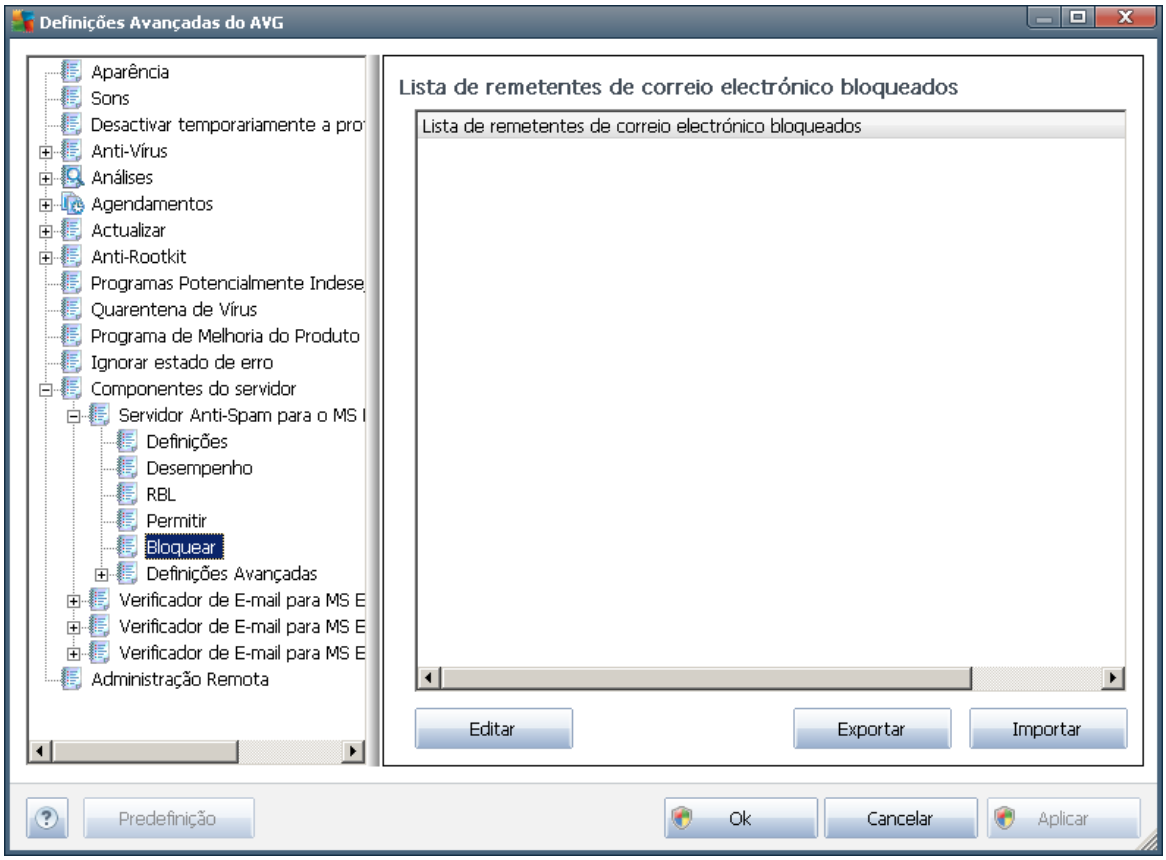
- ***Editar*** *– prima este botão para abrir uma janela onde pode inserir manualmente uma lista de endereços (também pode utilizar o método copiar e colar*). Insira um item (remetente, nome de domínio) por linha.

- ***Importar*** - pode importar os seus endereços de e-mail através deste botão. O ficheiro de origem pode ser um ficheiro de texto (no formato de texto simples, e o conteúdo só deve conter um item - endereço, nome de domínio - por linha), um ficheiro WAB, ou a importação pode ser efectuada a partir do Livro de Endereços do Windows ou do Microsoft Office Outlook.

- ***Exportar***- Se decidir exportar os registos para uma determinada finalidade, pode fazê-lo premindo este botão. Todos os registos serão guardados num ficheiro de texto simples.

## 7.7. Lista Negra

O item ***Lista Negra*** abre uma janela com uma lista global de endereços de e-mail e de nomes de domínios bloqueados cujas mensagens serão sempre assinaladas comospam.




Na interface de edição pode compilar uma lista de remetentes dos quais espera receber mensagens indesejadas (spam). Pode ainda compilar uma lista de nomes de domínios completos (ex. *spammingcompany.com*, dos quais recebe ou espera receber mensagens de spam. Todas as mensagens de e-mail dos endereços/domínios listados serão identificados como spam.

Quando já tiver uma lista de remetentes/ou nomes de domínio preparada, pode introduzi-los por meio de um dos seguintes métodos: via introdução directa de cada endereço de correio electrónico ou importando toda a lista de endereços de uma vez. Estão disponíveis os seguintes botões de controlo:

- ***Editar*** *– prima este botão para abrir uma janela onde pode inserir manualmente uma lista de endereços (também pode utilizar o método copiar e colar*). Insira um item (remetente, nome de domínio) por linha.

- ***Importar*** - pode importar os seus endereços de e-mail através deste botão. O ficheiro de origem pode ser um ficheiro de texto (no formato de texto simples, e o conteúdo só deve conter um item - endereço, nome de domínio - por linha), um ficheiro WAB, ou a importação pode ser efectuada a partir do Livro de Endereços do Windows ou do Microsoft Office Outlook.

- ***Exportar***- Se decidir exportar os registos para uma determinada finalidade, pode fazê-lo premindo este botão. Todos os registos serão guardados num ficheiro de texto simples.

## 7.8. Definições Avançadas

***Normalmente é recomendável que mantenha as definições predefinidas e só as altere se tiver uma razão válida para o fazer. Quaisquer alterações à configuração devem ser efectuadas exclusivamente por utilizadores avançados!***

Se contudo necessitar imperativamente de alterar a configuração do componente Anti-Spam nos módulos mais avançados, por favor siga as instruções facultadas na interface do utilizador. Regra geral, encontrará em cada janela uma única funcionalidade especifica e pode editá-la - a descrição da mesma está sempre incluída na própria janela:

- ***Memória Cache*** - identificação, reputação de domínio, LegitRepute

- ***Aprendizagem*** - máximo de entradas de palavras, limiar de auto-aprendizagem, peso

- ***Filtragem*** - lista de idiomas, lista de países, IPs aprovados, IPs bloqueados, países bloqueados, conjuntos de caracteres bloqueados, remetentes adulterados

- ***RBL*** - Servidores RBL, multi-correspondências, limiar, temporização, máximo de IPs

- ***Ligação à Internet***- tempo limite, servidor proxy, autenticação de servidor proxy

# 8. Gestor de Definições AVG

O ***Gestor de Definições AVG*** é uma ferramenta, adequada principalmente para redes mais pequenas, que lhe permite copiar, editar e distribuir a configuração do AVG. A configuração pode ser guardada num dispositivo amovível (Unidade flash USB, etc.) e depois aplicada manualmente nos postos seleccionados.

A ferramenta está incluída na instalação do AVG e disponível através do menu Iniciar do Windows:

***Todos os programas/AVG <%>/Gestor de Definições AVG***


- **Definições do AVG**
    - ***Editar as Definições do AVG*** - use este link para abrir uma janela com as definições avançadas do seu AVG local. Todas as alterações efectuadas aqui serão reflectidas na instalação local do AVG.
    - ***Carregar e editar as definições do AVG - se já possui um ficheiro de configuração AVG (.pck), use este botão para o abrir e editar.*** Depois de confirmar as alterações através do botão ***OK*** ou ***Aplicar, o ficheiro será substituído pelas novas definições!***
- **Definições da Firewall AVG**

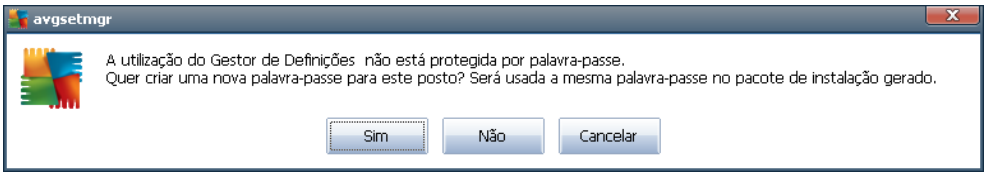
    *Esta secção permitir-lhe-ia fazer alterações às definições da Firewall da sua instalação local do AVG, ou editar as definições da Firewall num ficheiro de configuração (.pck) do AVG já preparado. No entanto, uma vez que o seu AVG Email Server Edition 2012 não inclui a componente Firewall, ambos os links são apresentados a cinzento e estão inactivos.*

- **Opções de Carregamento**

- ***Carregar um ficheiro de definições guardado para o AVG*** - use este link para abrir um ficheiro de configuração (.pck) do AVG e aplicá-lo à instalação local do AVG.

- **Opções de Salvaguarda**

  - ***Guardar as definições locais do AVG para um ficheiro*** - use este link para guardar o ficheiro de configuração (.pck) do AVG da instalação local do AVG. Se não tiver definido uma palavra-passe para as Acções permitidas, pode ser apresentada a seguinte janela:




  Responda ***Sim*** se pretender definir a palavra-passe para acesso aos Itens permitidos agora e depois preencha as informações solicitadas e confirme a sua escolha. Responda ***Não*** para saltar a criação da palavra-passe e continuar com a salvaguarda da configuração do AVG local para um ficheiro.

- **Opções de Clonagem**

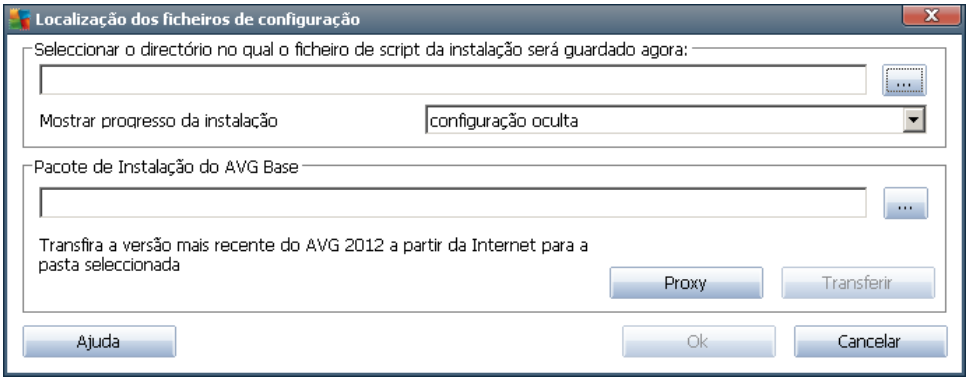
  - ***Aplicar definições idênticas ao longo da rede*** - ao clicar neste link, efectua uma cópia da instalação local do AVG ao criar um pacote de instalação com opções personalizadas. O clone inclui a maioria das definições do AVG, com excepção das seguintes:

    ✓ *Definições de idioma*

    ✓ *Definições de som*

    ✓ *Lista de permissões e excepções de programas potencialmente indesejados do componente Protecção de Identidade.*

  Para o efeito, primeiro seleccione a pasta onde o script de instalação deve ser guardado..



Depois, seleccione, a partir do menu pendente, uma das seguintes opções:

- ✓ *Instalação oculta* - não serão apresentadas quaisquer informações durante o processo de configuração.
- ✓ *Mostrar apenas o progresso da instalação* - a instalação não necessitará de qualquer intervenção do utilizador, mas o progresso será perfeitamente visível.
- ✓ *Mostrar o assistente de instalação* - a instalação será visível e o utilizador terá de confirmar todos os passos manualmente.

Use o botão ***Transferir*** para transferir o pacote de instalação do AVG mais recente directamente a partir do Website da AVG para a pasta seleccionada, ou coloque o pacote de instalação do AVG nessa pasta manualmente.

Pode usar o botão ***Proxy*** para definir as definições de um servidor proxy se a sua rede o solicitar para estabelecer ligação.

Ao clicar no botão ***OK***, o processo de clonagem inicia e deverá terminar em pouco tempo. Pode também ser apresentada uma janela a inquirir sobre a definição de uma palavra-passe para os Itens permitidos (veja acima). Uma vez concluído o processo, deverá haver um ficheiro ***AvgSetup.bat*** disponível na pasta seleccionada, assim como outros ficheiros. Se executar o ficheiro ***AvgSetup.bat***, este instalará o AVG em conformidade com os parâmetros escolhidos acima.

# 9. FAQ e Suporte Técnico

Se tiver qualquer tipo de problemas com o seu AVG, de natureza comercial ou técnica, por favor consulte a secção***Perguntas Frequentes (FAQ)*** do website da AVG emhttp://www.avg.com.

Se não conseguir obter ajuda por este meio, contacte o departamento de suporte técnico por e-mail. Por favor utilize o formulário de contacto acessível a partir do menu de sistema via ***Ajuda / Obtenha ajuda on-line***.