AVG Internet Security 2012

Manual do Utilizador

Revisão do documento 2012.20 (3/29/2012)

Índice

1. Introdução

Este manual do utilizador disponibiliza informação completa para o **AVG Internet Security 2012**.

O AVG Internet Security 2012 proporciona várias camadas de protecção para tudo o que faz online, o que significa que não tem de se preocupar com roubos de identidade, vírus, ou visitas a websites prejudiciais. A Rede de Protecção da Comunidade AVG e a Tecnologia de Protecção na Nuvem AVG estão incluídas, significando que compilamos as informações relativas às mais recentes ameaças e as partilhamos com a nossa comunidade, para garantir que o utilizador recebe a melhor protecção:

- Faça compras e operações bancárias online em segurança com a Firewall, o Anti-Spam e a Protecção de Identidade do AVG
- Mantenha-se protegido nas redes sociais com a Protecção nas Redes Sociais do AVG
- Navegue e pesquise com a confiança da protecção em tempo real do AVG LinkScanner

2. Requisitos de Instalação do AVG

2.1. Sistemas Operativos Suportados

O **AVG Internet Security 2012** destina-se a proteger postos de trabalho com os seguintes sistemas operativos:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 e x64, todas as edições)
- Windows 7 (x86 e x64, todas as edições)

(e service packs possivelmente superiores para sistemas operativos específicos)

***Nota**: O componente Protecção de Identidade não é suportado no Windows XP x64. Neste sistema operativo pode instalar o AVG Internet Security 2012 mas sem o componente PID.*

2.2. Requisitos Mínimos e Recomendados de Hardware

Requisitos mínimos de hardware para o **AVG Internet Security 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB de memória RAM
- 1000MB de espaço livre no disco rígido (para propósitos de instalação)

Requisitos recomendados de hardware para o **AVG Internet Security 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB de memória RAM
- 1550 MB de espaço livre no disco rígido (para propósitos de instalação)

3. Processo de Instalação do AVG

Onde é que obtenho o ficheiro de instalação?

Para instalar o **AVG Internet Security 2012** no seu computador, precisa de transferir o ficheiro de instalação mais recente. Para garantir que está a instalar a versão actualizada do **AVG Internet Security 2012**, recomendamos que transfira o ficheiro de instalação do Website da AVG (http://www.avg.com/). A secção ***Centro de Suporte / Transferências*** proporciona uma síntese estruturada dos ficheiros de instalação de cada edição do AVG.

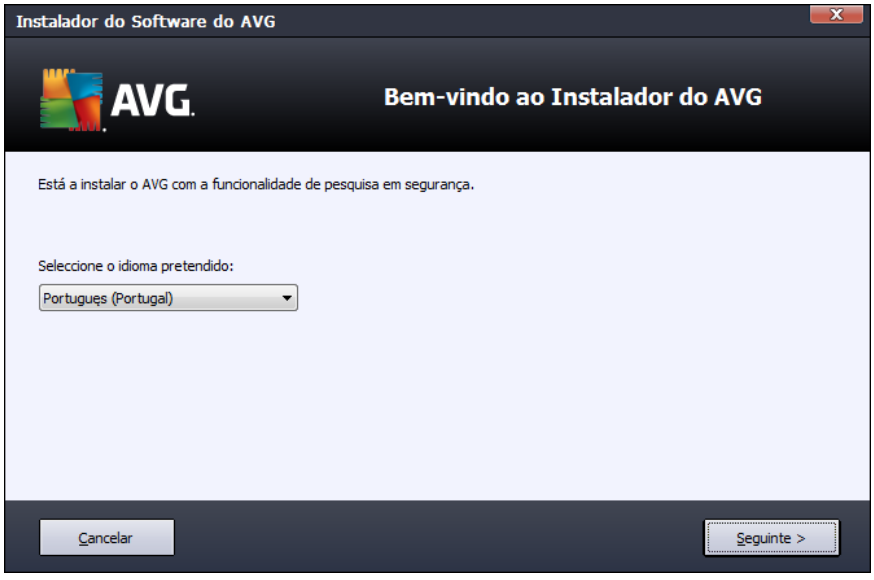
Se não tiver a certeza de quais os ficheiros que tem de transferir e instalar, pode querer usar o serviço ***Seleccione o produto*** na parte inferior da página. Depois de responder a três simples perguntas, este serviço define os ficheiros de que precisa. Clique no botão ***Continuar*** para ser redireccionado para uma lista completa de ficheiro para transferência de acordo com as suas necessidades.

Como é o processo de instalação?

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 simples e fáceis de interpretar. Cada janela descreve sucintamente o que fazer em cada passo do processo de instalação. A seguir, apresentamos uma explicação detalhada de cada janela:

3.1. Bem-vindo: Selecção do Idioma

O processo de instalação inicia com a janela ***Bem-vindo ao Instalador do AVG***:

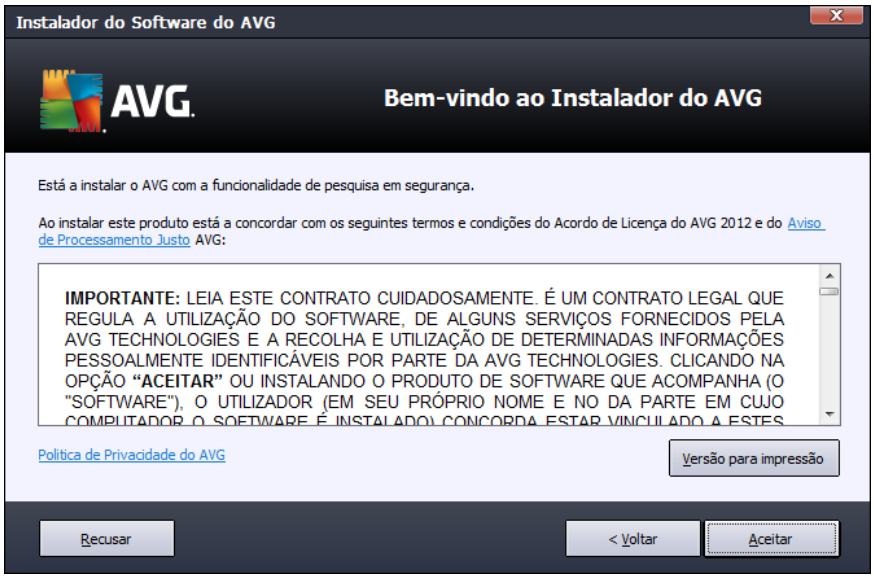


Nesta janela pode seleccionar o idioma usado para o processo de instalação. No canto superior direito da janela, clique na caixa para abrir o menu de idiomas. Seleccione o idioma pretendido e o processo de instalação continuará no idioma seleccionado.

Atenção: Está apenas a seleccionar o idioma do processo de instalação. O AVG Internet Security 2012 será instalado o idioma seleccionado e em Inglês, que é sempre instalado automaticamente. Contudo, é possível ter mais idiomas instalados e trabalhar com o AVG Internet Security 2012 num destes. Será instado a confirmar a selecção de idiomas alternativos numa das seguintes janelas de configuração com nome Opções Personalizadas.

3.2. Bem-vindo: Contrato de Licença

No passo seguinte, a janela ***Bem-vindo ao Instalador do AVG*** disponibiliza o texto integral do contrato de licença do AVG:



Leia atentamente todo o texto. Para confirmar que leu, compreendeu e aceita o acordo, clique no botão ***Aceito***. Se não concordar com o acordo de licença, clique no botão ***Não aceito*** e o processo de instalação será abortado imediatamente.

Política de Privacidade da AVG

Para além do acordo de licença, esta janela de configuração também lhe apresenta a opção de saber mais sobre a política de privacidade da AVG. No canto superior esquerdo da janela, pode ver a hiperligação da ***Política de Privacidade da AVG***. Clique na mesma para ser redireccionado para o Website da AVG (http://www.avg.com/) onde pode aceder à totalidade dos princípios da política de privacidade da AVG Technologies.

Botões de controlo

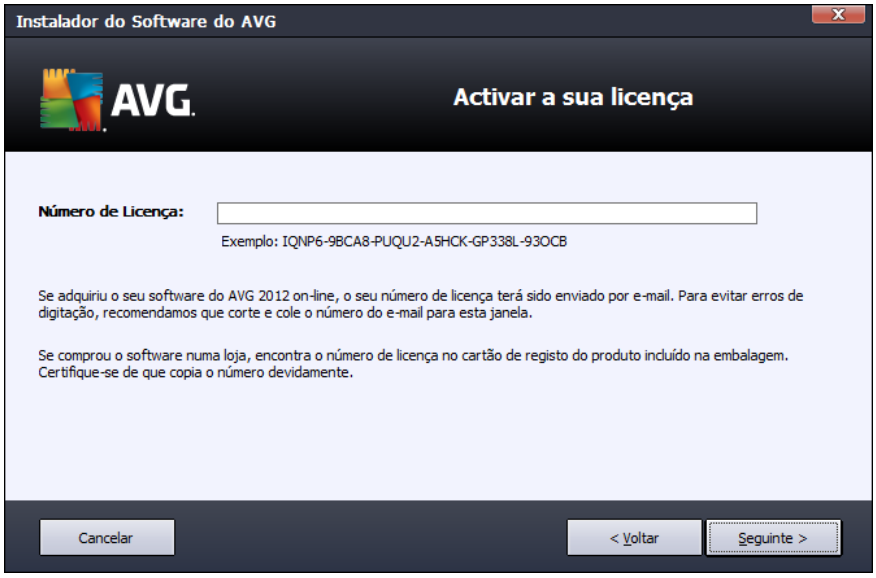
Na primeira janela de configuração, só há dois botões de controlo disponíveis:

- ***Versão para impressão*** – Clique para imprimir o texto integral do contrato de licença do AVG.

- ***Não aceito*** - Clique para recusar o acordo de licença. O processo de configuração será abortado imediatamente. O **AVG Internet Security 2012** não será instalado!
- ***Retroceder*** – Clique para retroceder um passo, para a janela de configuração anterior.
- ***Aceito*** - Clique para confirmar que leu, compreendeu e aceita o acordo de licença. A instalação continuará e passará ao passo seguinte da configuração.

3.3. Activar a sua licença

Na janela ***Activar a Sua Licença*** é convidado a introduzir o seu número de licença no campo de texto disponibilizado:



Onde encontrar o número de licença

O número de venda pode ser encontrado na caixa do CD do seu **AVG Internet Security 2012**. O número de licença estará na mensagem de e-mail de confirmação que recebeu após comprar o seu **AVG Internet Security 2012** on-line. Tem de digitar o número exactamente conforme apresentado. Se o formato o digital do número de licença estiver disponível (*no e-mail*), é aconselhável que utilize o método copiar e colar para o inserir.

Como usar o método Copiar/Colar

Usar o método ***Copiar/Colar*** para introduzir o número de licença do seu **AVG Internet Security 2012** no programa assegura que o número é devidamente introduzido. Proceda do seguinte modo:

- Abra o e-mail que contém o número de licença.
- Clique com o botão esquerdo do rato no início do número de licença, mantenha premindo e

arraste o rato até ao final do número, depois liberte o botão. O número deverá ficar em realce.

- Prima e mantenha a tecla ***Ctrl***, e depois prima a tecla ***C***. Esta acção copia o número.
- Aponte e clique na posição onde pretende colar o número copiado.
- Prima e mantenha a tecla ***Ctrl***, e depois prima a tecla ***V***. Esta acção cola o número na localização que seleccionou.

Botões de controlo

Como na maioria das janelas de configuração, há três botões de controlo disponíveis:

- ***Cancelar*** – Clique para sair imediatamente do processo de configuração: o **AVG Internet Security 2012** não será instalado!
- ***Retroceder*** – Clique para retroceder um passo, para a janela de configuração anterior.
- ***Seguinte*** – Clique para continuar a instalação e passar ao passo seguinte.

3.4. Seleccione o tipo de instalação

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

Instalação Rápida

Para a maioria dos utilizadores, é recomendável a opção ***Instalação Rápida***, que instala o **AVG Internet Security 2012** em modo totalmente automático com as predefinições do fornecedor do programa, incluindo o Gadget do AVG. Esta configuração proporciona a máxima segurança combinada com uma utilização de recursos optimizada. Futuramente, se houver necessidade de alterar a configuração, tem sempre a possibilidade de o fazer directamente no **AVG Internet Security 2012**.

Nesta opção é possível ver duas caixas de verificação pré-seleccionadas e é recomendável manter as duas opções assinaladas:

- ***Pretendo definir o AVG Secure Search como o meu motor de busca predefinido*** – mantenha esta opção assinalada para confirmar que pretende utilizar o motor de busca AVG Secure Search, que colabora de perto com o componente Link Scanner para obter segurança máxima online.

- ***Quero instalar a Barra de Ferramentas de Segurança AVG*** – mantenha esta opção assinalada para instalar a Barra de Ferramentas de Segurança AVG, que garante segurança máxima durante a navegação na Internet.

Clique no botão ***Seguinte*** para avançar para a janela Instalar a Barra de Ferramentas de Segurança AVG.

Instalação Personalizada

A ***Instalação Personalizada*** só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o **AVG Internet Security 2012** com definições que não as padrão; ex. para corresponder a requisitos do sistema específicos.

Se seleccionar esta opção, aparece uma nova secção chamada ***Pasta de Destino*** na janela. Nessa secção, deve especificar a localização na qual pretende instalar o **AVG Internet Security 2012**. Por predefinição, o **AVG Internet Security 2012** será instalado na pasta de ficheiros de programas localizada na unidade C:, conforme indicado no campo de texto da janela. Se quiser alterar esta localização, utilize o botão ***Procurar*** para visualizar a estrutura da unidade e seleccione a respectiva pasta. Para reverter para o destino predefinido pelo fornecedor do software, utilize o botão ***Predefinição***.

Em seguida, clique no botão ***Seguinte*** para avançar para a janela Opções Personalizadas.

Botões de controlo

Como na maioria das janelas de configuração, há três botões de controlo disponíveis:

- ***Cancelar*** – Clique para sair imediatamente do processo de configuração: o **AVG Internet Security 2012** não será instalado!

- ***Retroceder*** – Clique para retroceder um passo, para a janela de configuração anterior.

- ***Seguinte*** – Clique para continuar a instalação e passar ao passo seguinte.

3.5. Opções Personalizadas

A janela ***Opções Personalizadas*** permite-lhe configurar parâmetros detalhados da instalação:

A secção ***Selecção de Componentes*** apresenta uma síntese de todos os componentes do **AVG Internet Security 2012** 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!

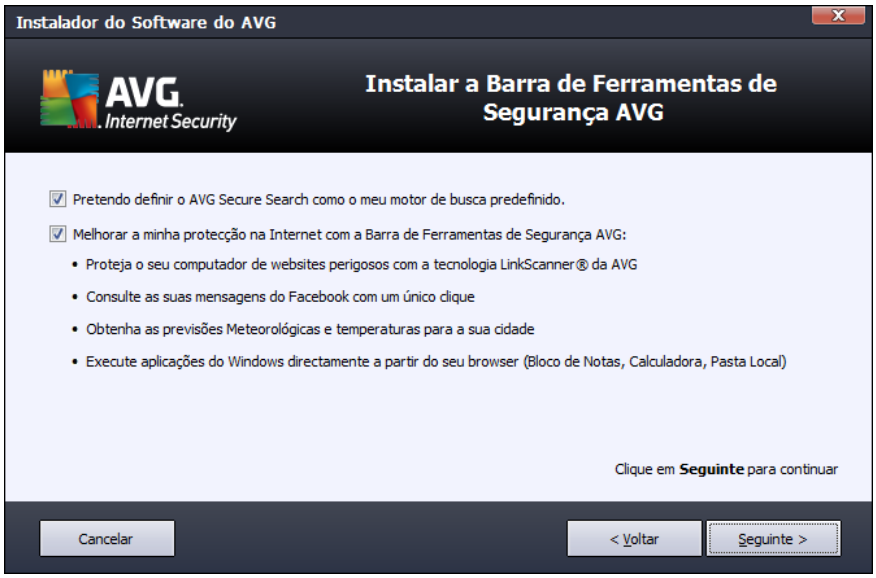
Realce qualquer um dos itens na lista ***Selecção de Componentes*** e será apresentada uma breve descrição do respectivo componente do lado direito desta secção. Para informações detalhadas sobre as funcionalidades de cada componente, queira consultar o capítulo Síntese de Componentes neste documento. Para reverter para a configuração predefinida pelo fornecedor do software, use o botão ***Predefinição***.

Botões de controlo

Como na maioria das janelas de configuração, há três botões de controlo disponíveis:

- ***Cancelar*** – Clique para sair imediatamente do processo de configuração: o **AVG Internet Security 2012** não será instalado!
- ***Retroceder*** – Clique para retroceder um passo, para a janela de configuração anterior.
- ***Seguinte*** – Clique para continuar a instalação e passar ao passo seguinte.

3.6. Instalar a Barra de Ferramentas de Segurança AVG



Na janela ***Instalar a Barra de Ferramentas de Segurança AVG*** decida se quer instalar a funcionalidade Barra de Ferramentas de Segurança AVG. Se não alterar as predefinições, este componente será instalado automaticamente no seu browser (*os browsers actualmente suportados são o Microsoft Internet Explorer v. 6.0 ou superior e o Mozilla Firefox v. 3.0 ou superior*) para lhe proporcionar protecção compreensiva on-line enquanto navega na Internet.

Além disso, tem a opção de decidir se pretende definir o *AVG Secure Search (powered by Google)* como o seu motor de busca predefinido. Se assim for, deixe a caixa respectiva marcada.

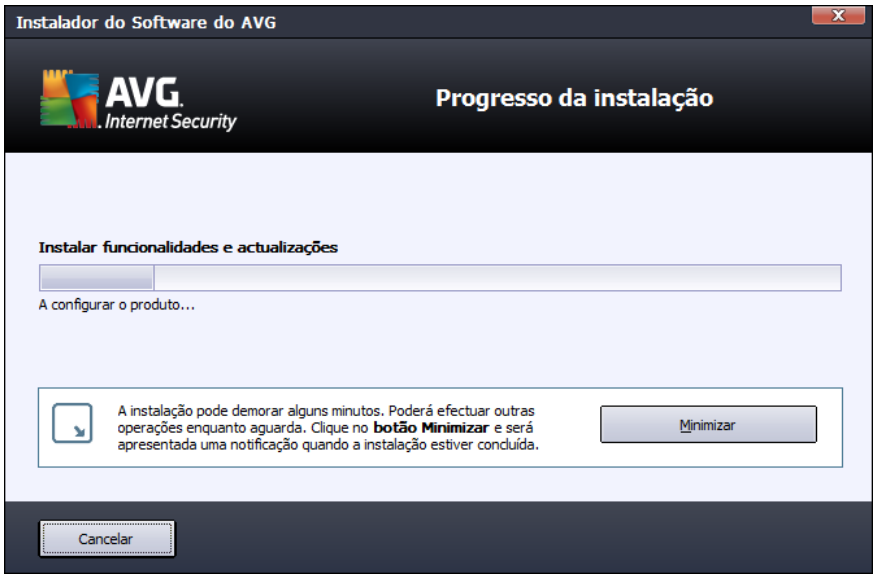
Botões de controlo

Como na maioria das janelas de configuração, há três botões de controlo disponíveis:

- ***Cancelar*** – Clique para sair imediatamente do processo de configuração: o **AVG Internet Security 2012** não será instalado!
- ***Retroceder*** – Clique para retroceder um passo, para a janela de configuração anterior.
- ***Seguinte*** – Clique para continuar a instalação e passar ao passo seguinte.

3.7. Progresso da instalação

A janela ***Progresso da Instalação*** apresenta o progresso do processo de instalação e não necessita de qualquer intervenção:



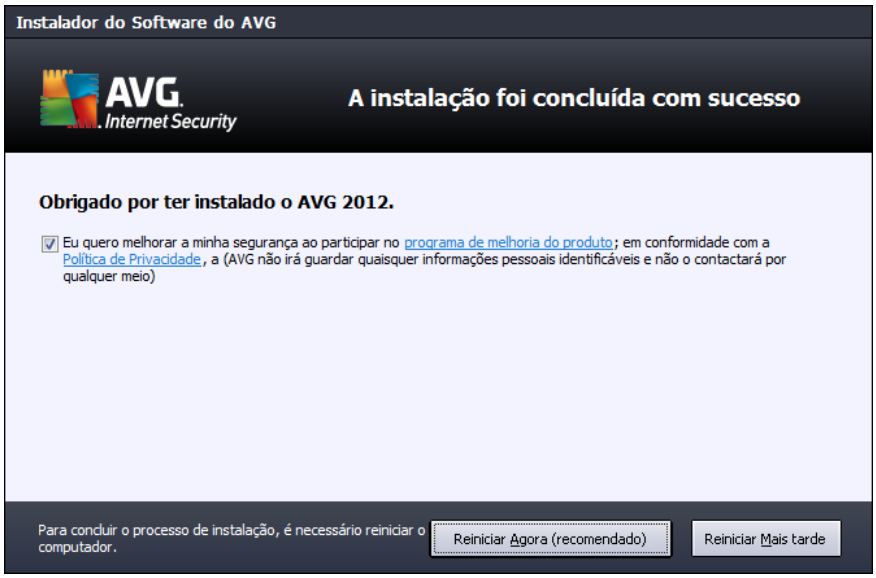
Após a conclusão do processo de instalação, será redireccionado para a janela seguinte.

Botões de controlo

Nesta janela, só há um botão de controlo disponível – ***Cancelar***. Este botão só deve ser usado se quiser parar o processo de instalação em decurso. Tenha em conta que, nesse caso, o **AVG Internet Security 2012** não será instalado!

3.8. A instalação foi concluída com sucesso

A janela ***A instalação foi concluída com sucesso*** confirma que o seu **AVG Internet Security 2012** foi totalmente instalado e configurado:



Programa de Melhoria do Produto

Aqui pode decidir se pretende participar no Programa de Melhoria do Produto (*para mais informações, consulte o capítulo Definições Avançadas do AVG / Programa de Melhoria do Produto*) que recolhe informações anónimas sobre as ameaças detectadas para aumentar o nível de segurança geral da Internet. Se concordar com esta declaração, mantenha a opção ***Programa de Melhoria do Produto e Segurança na Internet do AVG 2012...*** marcada *(a opção está confirmada por predefinição)*.

Reinicialização do computador

Para finalizar o processo de instalação, é preciso reiniciar o seu computador: seleccione se pretende ***Reiniciar agora***, ou se pretende adiar esta acção – ***Reiniciar mais tarde***.

4. Após a Instalação

4.1. Registo do produto

Uma vez concluída a instalação do **AVG Internet Security 2012**, queira registar o seu produto online no Website da AVG (http://www.avg.com/). Após o registo terá acesso total à sua conta de utilizador AVG, o boletim informativo de Actualização da AVG, e outros serviços fornecidos exclusivamente para os utilizadores registados.

A forma mais fácil de registar é directamente a partir da interface do utilizador do **AVG Internet Security 2012**. No menu principal, seleccione o item Ajuda/Registar agora. Será redireccionado para a página de ***Registo*** no website da AVG (http://www.avg.com/). Siga as instruções apresentadas na página.

4.2. Aceder à Interface do Utilizador

A janela principal do AVG pode ser acedida de muitas formas:

- fazendo duplo clique sobre o ícone do AVG na barra de tarefas
- fazendo duplo clique sobre o ícone do AVG no ambiente de trabalho
- a partir do menu ***Iniciar / Todos os Programas / AVG 2012***

4.3. Análise de todo o computador

Existe um risco potencial de que um vírus informático tenha sido transmitido ao seu computador antes da instalação do **AVG Internet Security 2012**. Por este motivo deve executar uma análise Analisar todo o computador para se certificar de que não existem infecções no seu PC. A primeira análise poderá demorar algum tempo *(cerca de uma hora)*, mas é aconselhável executar a análise para se certificar de que o seu computador não foi infectado por uma ameaça. Para instruções relativas à execução de Analisar todo o computador, consulte o capítulo Análise do AVG.

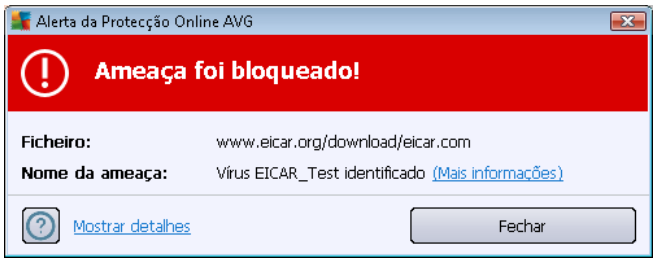
4.4. Teste Eicar

Para confirmar que o **AVG Internet Security 2012** foi devidamente instalado, pode executar o teste EICAR.

O teste Eicar é um método padrão e absolutamente seguro concebido para testar o funcionamento de sistemas antivírus. Pode ser transmitido com segurança, uma vez que não é um vírus verdadeiro e não contém fragmentos de código de vírus. A maioria dos produtos reage como se tratasse de um vírus (*embora o refiram normalmente com um nome óbvio, tal como "EICAR-AV-Test"*). Pode transferir o vírus EICAR a partir do website da Eicar em www.eicar.com, onde poderá encontrar igualmente todas as informações necessárias sobre o teste.

Tente transferir o ficheiro ***eicar.com*** e guardá-lo no disco local. Imediatamente após a confirmação da transferência do ficheiro de teste, a Protecção Online (*uma parte do componente Link Scanner*) reagirá com um aviso. Este aviso demonstra que o AVG está correctamente instalado no seu

computador.



A partir do website http://www.eicar.com também pode transferir a versão comprimida do 'virus' EICAR (*ex. no formato eicar_com.zip*). A Protecção Online permite-lhe transferir este ficheiro e guardá-lo no seu disco local, mas a Protecção Residente (*parte do componente Anti-Vírus*) detecta o 'vírus' quando o tentar descomprimir.

Se o AVG não identificar o ficheiro de teste EICAR como um vírus, verifique novamente a configuração do programa!

4.5. Configuração predefinida do AVG

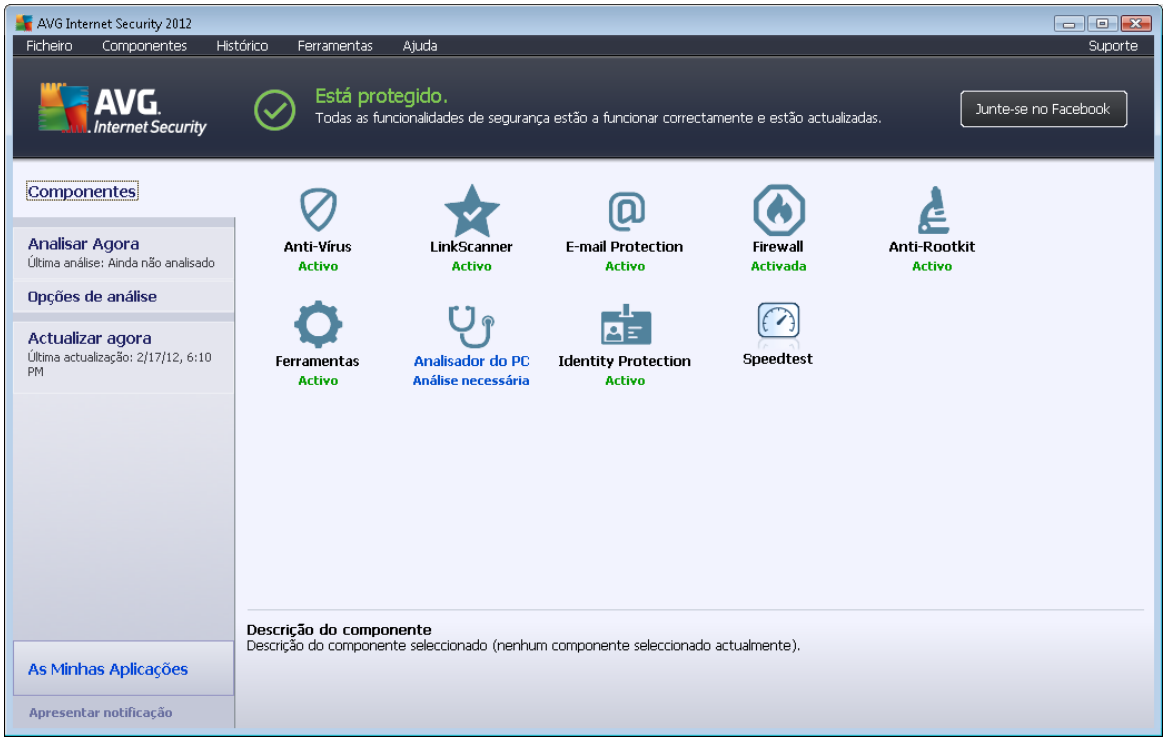
A configuração predefinida (*ou seja, a forma como a aplicação está configurada imediatamente após a instalação*) do **AVG Internet Security 2012** está configurada pelo fornecedor do software de forma a que todos os componentes e funções estejam afinados para proporcionarem um desempenho excelente.

Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente por um utilizador avançado.

Algumas pequenas opções de edição das definições dos componentes do AVG podem ser acedidas directamente a partir da interface do utilizador do componente em questão. Se necessitar de alterar a configuração do AVG para esta corresponder melhor às suas necessidades, vá a Definições Avançadas do AVG: seleccione o item do menu de sistema ***Ferramentas/Definições avançadas*** e edite a configuração do AVG na janela Definições Avançadas do AVG apresentada.

5. Interface de Utilizador AVG

O **AVG Internet Security 2012** abre na janela principal:



A janela principal está dividida em várias secções:

- ***Menu de Sistema*** *(linha superior do sistema na janela)* é a navegação standard que lhe permite aceder a todos os componentes, serviços, e funcionalidades do **AVG Internet Security 2012** – detalhes >>
- ***Informação de Estado de Segurança*** *(secção superior da janela)* faculta-lhe informação relativa ao estado actual do seu **AVG Internet Security 2012** – detalhes >>
- O botão ***Junte-se a nós no Facebook*** *(canto superior direito da janela)* permite-lhe juntar-se à comunidade AVG no Facebook. Contudo, o botão aparece apenas se todos os componentes estiverem totalmente activados e a funcionar correctamente *(para mais informações sobre a verificação do estado dos componentes AVG, consulte o capítulo Informação de Estado de Segurança)*
- ***Links rápidos*** *(secção esquerda da janela)* permite-lhe aceder rapidamente às tarefas mais importantes e utilizadas mais frequentemente do **AVG Internet Security 2012** – detalhes >>
- ***As Minhas Aplicações*** *(secção inferior esquerda da janela)* abre uma síntese de aplicações adicionais disponíveis para o **AVG Internet Security 2012**: LiveKive, Family safety, e Optimizador de Performance do PC
- ***Síntese de Componentes*** *(secção central da janela)* faculta uma síntese de todos os

componentes instalados do **AVG Internet Security 2012** - detalhes >>

- ***Ícone da Barra de Tarefas do Sistema****(canto inferior direito do monitor, na barra de tarefas do sistema)* indica o estado actual do **AVG Internet Security 2012** detalhes >>

- ***Gadget do AVG*** *(barra lateral do Windows, suportado no Windows Vista/7)* permite-lhe aceder rapidamente às análises e actualizações do **AVG Internet Security 2012** – detalhes >>

5.1. Menu de Sistema

O***menu de sistema*** é a navegação padrão utilizada em todas as aplicações do Wndows. Está localizado na parte superior da janela principal do **AVG Internet Security 2012**. Utilize o menu de sistema para aceder a componentes, funcionalidades e serviços específicos do AVG.

O menu de sistema está dividido em cinco secções principais:

5.1.1. Ficheiro

- ***Sair*** - fecha a interface do utilizador do**AVG Internet Security 2012**. No entanto, a aplicação AVG continuará a ser executada em segundo plano e o seu computador continuará protegido!

5.1.2. Componentes

O item Componentes do menu de sistema inclui ligações para todos os componentes do AVG instalados, abrindo a página predefinida dos mesmos na interface do utilizador:

- ***Síntese do sistema*** – alternar para a janela da interface do utilizador predefinida com a síntese de todos os componentes instalados e o seu estado

- ***Anti-Vírus*** detecta vírus, spyware, worms, trojans, ficheiros executáveis ou bibliotecas indesejáveis presentes no seu sistema e protege-o contra adware malicioso - detalhes >>

- ***LinkScanner*** protege-o contra ataques com base na Internet enquanto procura e navega na Internet – detalhes >>

- ***Protecção de E-mail*** verifica as mensagens de correio de entrada pela existência de SPAM e bloqueia vírus, ataques de phishing, ou outras ameaças – detalhes >>

- ***Firewall*** controla todas as comunicações em todas as portas de rede, protegendo-o contra ataques maliciosos e bloqueando todas as tentativas de intrusão - detalhes >>

- ***Anti-Rootkit*** verifica a existência de rootkits ocultos em aplicações, controladores ou bibliotecas – detalhes >>

- ***Ferramentas do Sistema*** faculta um resumo detalhado do ambiente do AVG e informações relativas ao sistema operativo – – detalhes >>

- ***O Analisador do PC*** proporciona informações sobre o estado do seu computador – detalhes >>

- ***Protecção de Identidade*** protege constantemente os seus bens digitais contra ameaças novas e desconhecidas – detalhes>>

- ***Administração Remota*** só é apresentada nas edições AVG Business caso tenha especificado durante o processo de instalação a instalação deste componente

5.1.3. Histórico

- Resultados da análise- muda para a interface de teste do AVG, mais especificamente para a janela Síntese de Resultados de Análise

- Detecção da Protecção Residente – abre uma janela com a síntese das ameaças detectadas pela Protecção Residente

- Detecção do Verificador de E-mail – abre a janela com a síntese dos anexos das mensagens de e-mail identificados como perigosos pelo componente Protecção de E-mail

- Detecção da Protecção Online – abre uma janela com a síntese das ameaças detectadas pelo serviço Protecção Online, parte do componente LinkScanner

- Quarentena de Vírus – abre a interface do espaço de quarentena (Quarentena de Vírus) para onde o AVG remove todas as infecções detectadas que por alguma razão não podem ser recuperadas automaticamente. Nesta quarentena, os ficheiros infectados são isolados e a segurança do seu computador está assegurada, enquanto que os ficheiros infectados são armazenados para possíveis reparações futuras

- Registo do Histórico de Eventos – abre a interface de registo do histórico com uma síntese de todas as acções do **AVG Internet Security 2012** registadas

- Registo de Firewall – abre a interface das definições da Firewall no separador Registos com uma síntese detalhada de todas as acções da Firewall

5.1.4. Ferramentas

- Analisar o computador – Inicia uma análise de todo o computador.

- Análise de pasta seleccionada... – Muda para a interface de análise do AVG e permite-lhe definir na estrutura em árvore do seu computador quais os ficheiros e pastas que devem ser analisados.

- ***Analisar ficheiro...*** – Permite-lhe executar um teste manual de um ficheiro específico. Clique nesta opção para abrir uma nova janela com a estrutura em árvore do disco. Seleccione o ficheiro pretendido e confirme o início da análise.

- Actualizar – Inicia automaticamente o processo de actualização do **AVG Internet Security 2012**.

- ***Actualizar a partir de directório...*** – Executa o processo de actualização a partir dos ficheiros de actualização localizados numa pasta específica no seu disco local. No entanto, esta opção só é recomendada como emergência, ex. em situações em que não está disponível uma ligação à Internet (*por exemplo, o seu computador está infectado e desconectado da Internet; o seu computador está conectado a uma rede sem acesso à*

Internet, etc.). Na nova janela seleccione a pasta onde colocou anteriormente o ficheiro de actualização, e inicie o processo de actualização.

- Definições avançadas... – Abre a janela Definições avançadas do AVG onde pode editar a configuração do AVG Internet Security 2012. Regra geral, é recomendável que mantenha as definições da aplicação conforme definidas pelo vendedor do software.

- Definições da Firewall... – Abre uma janela independente para configuração avançada do componente Firewall.

5.1.5. Ajuda

- ***Conteúdos***- abre os ficheiros de ajuda do AVG

- ***Obter suporte*** – abre o website da AVG (http://www.avg.com/) na página do centro de apoio ao cliente

- ***A sua Internet AVG*** – abre o website da AVG (http://www.avg.com/)

- ***Acerca de Vírus e Ameaças*** – abre a Enciclopédia de Vírus online onde pode consultar informações detalhadas sobre o vírus identificado

- ***Reactivar*** – abre a janela ***Activar o AVG***com os dados que introduziu na janela Personalizar o AVG do processo de instalação. Nesta janela pode introduzir o seu número de licença para substituir o número de venda (*com o qual instalou o AVG*) ou para substituir o número de licença antigo (*ex. ao actualizar para um novo produto AVG*).

- ***Registar agora*** – conecta à página de registo do website da AVG (http://www.avg.com/). Por favor preencha os seus dados de registo; somente os clientes que registem o seu produto AVG podem receber suporte técnico gratuito.

Nota*: Se estiver a utilizar a versão de teste do* **AVG Internet Security 2012***, os dois últimos itens aparecem como* ***Comprar agora*** *e* ***Activar****, permitindo-lhe comprar a versão completa do programa imediatamente. Para produtos* **AVG Internet Security 2012** *instalados com um número de venda, os itens são apresentados como* ***Registar*** *e* ***Activar****.*

- ***Acerca do AVG*** – abre a janela ***Informação*** com seis separadores que facultam dados sobre o nome do programa, versão do programa e da base de dados de vírus, informação de sistema, contrato de licença e informações de contacto da ***AVG Technologies CZ***.

5.1.6. Suporte

O link ***Suporte*** abre uma nova janela de ***Informação*** com todos os tipos de informações que possa precisar ao procurar ajuda. A janela inclui dados básicos sobre o seu programa AVG (*programa / versão da base de dados*), informações da licença e uma lista de hiperligações de suporte rápido.

A janela ***Informação*** está dividida em seis separadores:

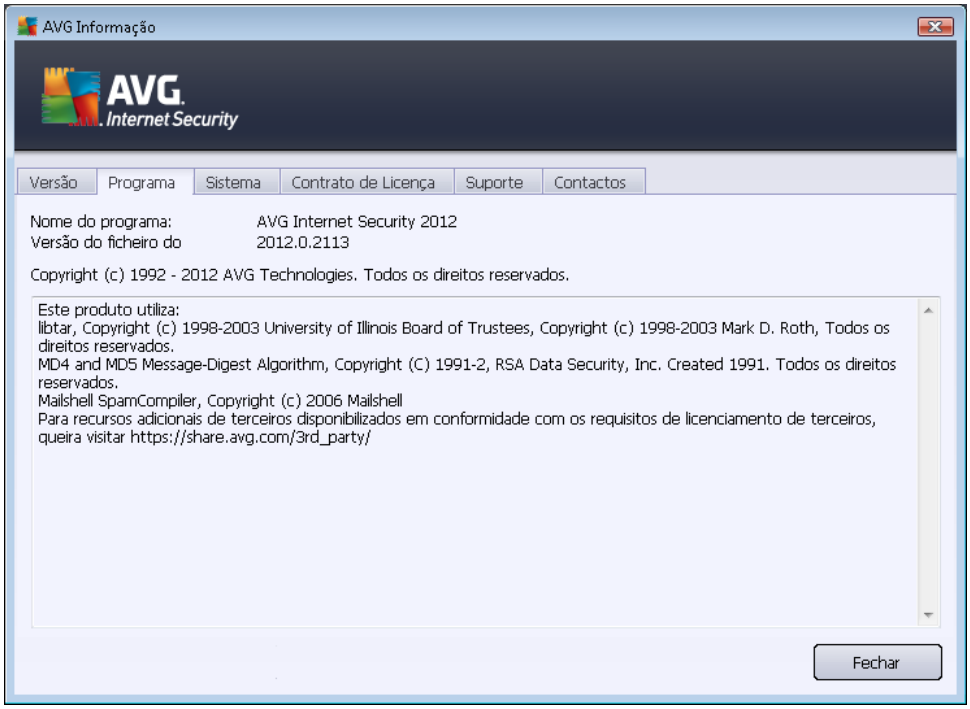
O separador ***Versão*** está dividido em três secções:

- ***Informações de Suporte*** - Proporciona informações sobre a versão do **AVG Internet Security 2012**, a versão da base de dados de vírus, a versão da base de dados do Anti-Spam e a versão do LinkScanner.

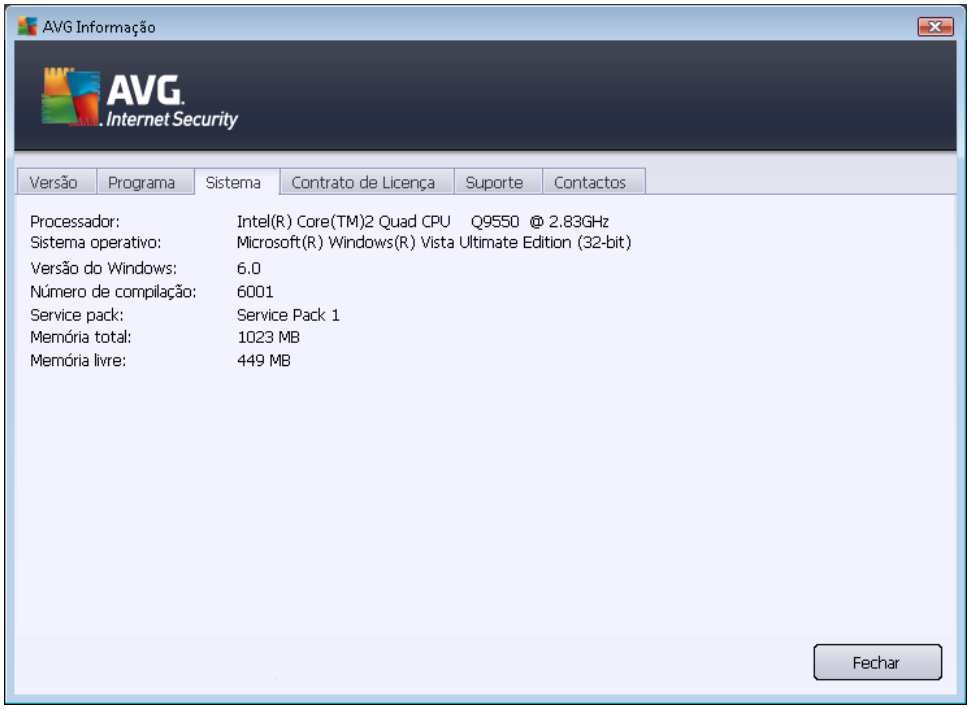
- ***Informações do Utilizador*** - Proporciona informações sobre o utilizador e a empresa licenciados.

- ***Detalhes da Licença*** - Proporciona informações sobre a sua licença *(nome do produto, tipo de licença, número de licença, data de expiração e número de postos*). Nesta secção, também pode usar o link ***Registar*** para registar o seu **AVG Internet Security 2012** online; isto permite-lhe usar o suporte técnico AVG por completo. Além disso, use o link ***Reactivar*** para abrir a janela ***Activar o AVG***: preencha o seu número de licença no campo respectivo para substituir o número de venda *(que usou durante a instalação do AVG Internet Security 2012)*, ou para alterar o seu número de licença actual para outro *(ex. ao actualizar para um produto AVG superior).*

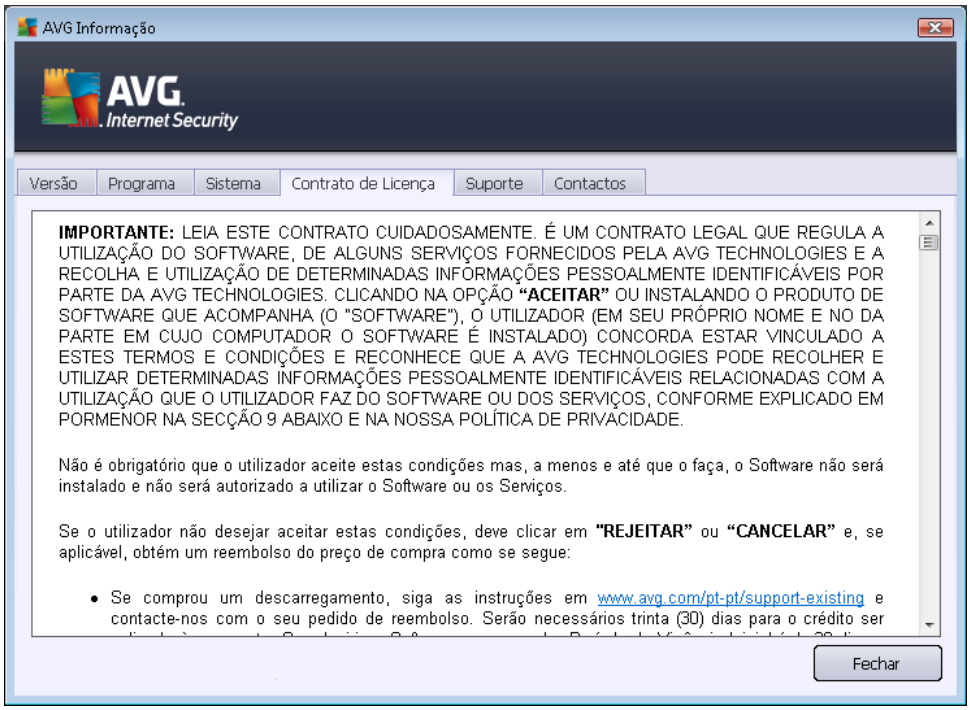
No separador ***Programa*** encontra informações sobre a versão do ficheiro do programa **AVG Internet Security 2012** e sobre o código de terceiros usado no produto:



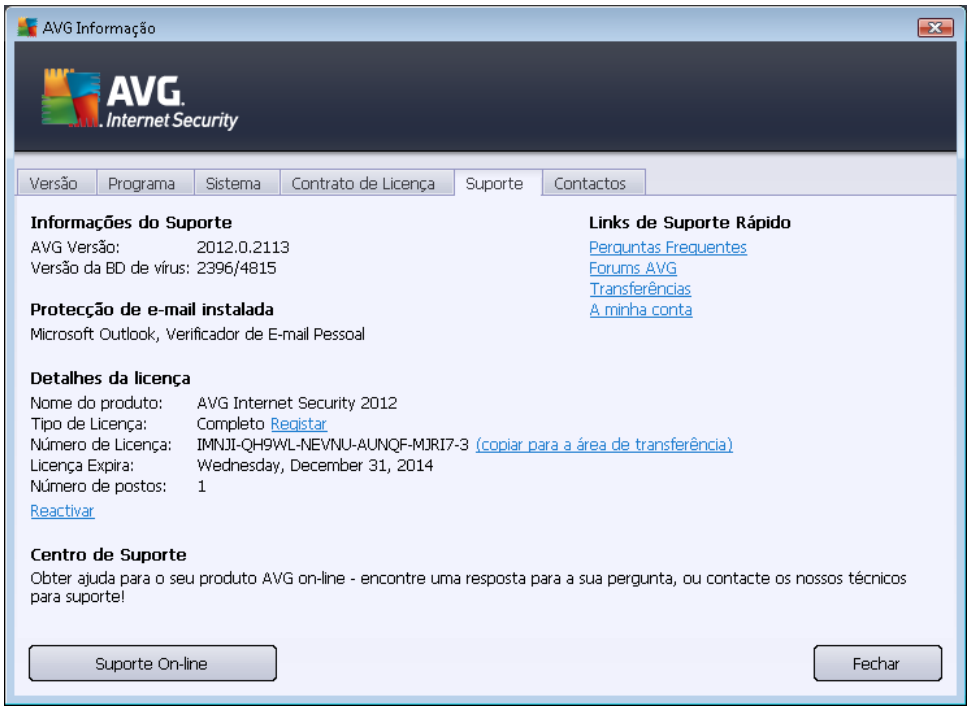
O separador ***Sistema*** apresenta uma lista de parâmetros do seu sistema operativo *(tipo de processador e respectiva versão, número de compilação, service packs usados, tamanho total da memória e tamanho da memória livre)*:



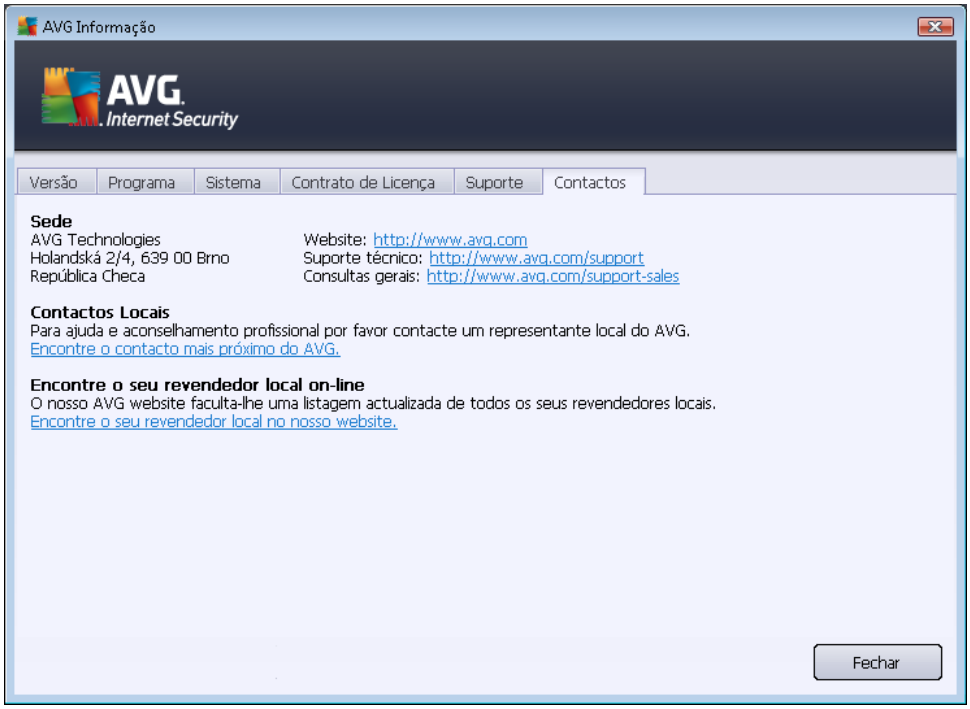
No separador ***Acordo de Licença*** pode ler o texto integral do acordo de licença entre o utilizador e a AVG Technologies:



O separador ***Suporte*** oferece uma lista de formas de contactar o apoio ao cliente. Além disso, disponibiliza links para o website da AVG (http://www.avg.com/), fóruns AVG, Perguntas Frequentes (FAQ), ... Podendo ainda encontrar informações que poderá usar aquando do contacto com o apoio ao cliente:



O separador ***Contactos*** providencia uma lista de todos os contactos da AVG Technologies, assim como contactos de representantes e revendedores locais do AVG:



5.2. Informação de Estado de Segurança

A secção ***Informação de Estado de Segurança*** está localizada na parte superior da janela principal do **AVG Internet Security 2012**. Nesta secção encontra sempre informações relativas ao estado de segurança actual do seu **AVG Internet Security 2012**. Por favor veja uma síntese dos ícones possivelmente apresentados, e a respectiva descrição:

 – O ícone verde indica que o seu ***AVG Internet Security 2012 está completamente funcional.*** O computador está totalmente protegido, actualizado e todos os componentes instalados estão a funcionar correctamente.

 – O ícone amarelo avisa que ***um ou mais componentes não estão configurados correctamente***, devendo o utilizador prestar atenção às respectivas propriedades/definições. Não existem problemas críticos com o **AVG Internet Security 2012** e provavelmente decidiu desactivar algum componente por alguma razão. Ainda continua protegido! No entanto, por favor preste atenção às definições do componente problemático! O nome do mesmo será facultado na secção ***Informação de Estado de Segurança***.

O ícone amarelo também é apresentado se, por alguma razão, tiver decidido ignorar o estado de erro de um componente. A opção ***Ignorar estado do componente*** está disponível no

menu de contexto (*acessível por meio de clique do botão direito do rato*) sobre o ícone do componente respectivo na síntese de componentes da janela principal do **AVG Internet Security 2012**. Seleccione esta opção para exprimir que está consciente do estado de erro do componente mas que por alguma razão pretende manter o **AVG Internet Security 2012** neste estado e não pretende ser avisado através do ícone da Barra de Tarefas. Pode ter de usar esta opção numa situação específica mas é especialmente recomendado desactivar a opção ***Ignorar estado do componente*** assim que possível.

Em alternativa, o icone amarelo também é apresentado se o **AVG Internet Security 2012** necessitar do reinício do computador (***Reinício necessário***). Preste atenção a este aviso e reinicie o PC utilizando o botão ***Reiniciar agora***.

 – O ícone cor-de-laranja indica que o ***AVG Internet Security 2012 está em estado crítico***! Um ou mais componentes não funcionam devidamente e o **AVG Internet Security 2012** não consegue proteger o computador. Preste atenção imediata à resolução do problema referenciado. Se não conseguir resolver o problema sozinho, contacte a equipa de suporte técnico da AVG.

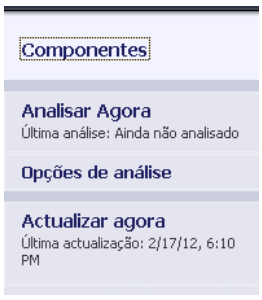
Na eventualidade de o AVG Internet Security 2012 não estar configurado para o melhor desempenho, há um novo botão Corrigir (em alternativa Corrigir todos, se o problema envolver mais de um componente) junto à informação do estado de segurança. Prima o botão para iniciar um processo automático de verificação e configuração do programa. Esta é uma forma fácil de configurar o AVG Internet Security 2012 para um desempenho optimizado e obter o nível máximo de segurança!

É recomendável que preste atenção à Informação de Estado de Segurança e que na eventualidade do relatório indicar algum problema, tente resolvê-lo imediatamente. Caso contrário, o seu computador está em risco!

Nota: *A informação de estado do AVG Internet Security 2012 também pode ser consultada a qualquer momento a partir do ícone da área de notificação.*

5.3. Links Rápidos

Os ***Links Rápidos*** estão localizados do lado esquerdo da interface do utilizador do **AVG Internet Security 2012**. Estes links permitem-lhe aceder imediatamente as funcionalidades mais importantes e mais frequentemente usados da aplicação, ou seja, as análises e as actualizações. Os links rápidos são acessíveis a partir de qualquer janela da interface do utilizador:



Os ***Links rápidos*** estão graficamente divididos em três secções:

- ***Analisar agora*** - Por predefinição, o botão disponibiliza informações relativas à última análise iniciada *(ou seja, tipo de análise e data da última execução)*. Clique no comando ***Analisar agora*** para iniciar a mesma análise novamente. Se quiser executar outra análise, clique no link ***Opções de Análise***. Desta forma, acede à Interface de Análise do AVG onde pode executar análises, agendar análises, ou editar os parâmetros das mesmas. *(Para pormenores, consulte o capítulo Análise do AVG)*

- ***Opções de análise*** - Utilize este link para alternar entre a interface do AVG actualmente aberta e a interface padrão com uma síntese de todos os componentes instalados. *(Para mais informações, consulte o capítulo Síntese de Componentes)*

- ***Actualizar agora*** – O link apresenta a data e a hora da última execução da actualização. Clique no botão para executar o processo de actualização imediatamente e acompanhar o progresso do mesmo. *(Para pormenores, consulte o capítulo Actualizações do AVG)*

Os ***Links rápidos*** são constantemente acessíveis a partir da Interface do Utilizador AVG. Quando utilizar um link específico para executar um processo específico, seja um actualização ou uma análise, a aplicação alternará para uma nova janela mas os links rápidos continuarão disponíveis. Além disso, o processo em execução é apresentado graficamente na navegação, para que tenha controlo absoluto de todos os processos em execução do **AVG Internet Security 2012**.

5.4. Síntese de Componentes

Secções da Síntese de Componentes

A secção ***Síntese de Componentes*** está localizada na parte central da Interface do Utilizador **AVG Internet Security 2012**. A secção está dividida em duas partes:

- ***A síntese de todos os componentes instalados*** que é composta por painéis gráficos de todos os componentes instalados. cada painel está identificado com o ícone do componente e apresenta informações sobre o estado do componente respectivo (activo ou inactivo).

- ***A descrição do componente*** está localizada na parte inferior desta janela. A descrição explica sucintamente a funcionalidade básica do componente. Além disso, providencia a informação do estado actual do componente seleccionado.

Lista de componentes instalados

No **AVG Internet Security 2012** , a secção ***Síntese de Componentes*** contém informações sobre os seguintes componentes:

- ***Anti-Vírus*** detecta vírus, spyware, worms, trojans, ficheiros executáveis ou bibliotecas indesejáveis presentes no seu sistema e protege-o contra adware malicioso - detalhes >>

- ***LinkScanner*** protege-o contra ataques com base na Internet enquanto procura e navega

na Internet – detalhes >>

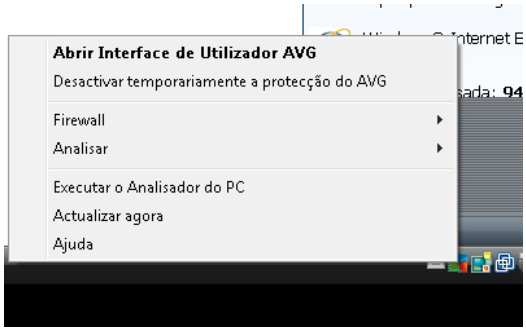
- ***Protecção de E-mail*** verifica as mensagens de correio de entrada pela existência de SPAM e bloqueia vírus, ataques de phishing, ou outras ameaças – detalhes >>
- ***Firewall*** controla todas as comunicações em todas as portas de rede, protegendo-o contra ataques maliciosos e bloqueando todas as tentativas de intrusão - detalhes >>
- ***Anti-Rootkit*** verifica a existência de rootkits ocultos em aplicações, controladores ou bibliotecas – detalhes >>
- ***Ferramentas do Sistema*** faculta um resumo detalhado do ambiente do AVG e informações relativas ao sistema operativo – – detalhes >>
- ***Analisador do PC*** proporciona informações sobre o estado do seu computador – detalhes >>
- ***Protecção de Identidade*** protege constantemente os seus bens digitais contra ameaças novas e desconhecidas – detalhes >>
- ***Administração Remota*** só é apresentada nas edições AVG Business caso tenha especificado durante o processo de instalação a instalação deste componente

Acções acessíveis

- ***Coloque o rato sobre o ícone de qualquer componente*** para o realçar na síntese de componentes. Simultaneamente é apresentada uma descrição da funcionalidade básica do componente na parte inferior da interface do utilizador.
- ***Clique uma vez sobre o ícone de qualquer componente*** para abrir a interface do componente propriamente dito com uma lista de dados estatísticos básicos.
- ***Clique com o botão direito do rato sobre o ícone de um componente*** para expandir um menu de contexto com várias opções:
  - ***Abrir*** – Clique nesta opção para abrir a janela do componente *(à semelhança do clique único sobre o ícone do componente)*.
  - ***Ignorar estado do componente*** – Seleccione esta opção para exprimir que está consciente do estado de erro do componente mas que por alguma razão pretende manter o AVG neste estado e não pretende ser avisado através do ícone da barra de tarefas.
  - ***Abrir nas Definições avançadas...*** - Esta opção só está disponível para alguns componentes; ou seja, os que dispõem de definições avançadas.

5.5. Ícone da barra de tarefas

O ***Ícone AVG da Barra de Tarefas*** *(na barra de tarefas do Windows, canto inferior direito do ecrã)* indica o estado actual do seu **AVG Internet Security 2012**. Está constantemente visível na sua Barra de Tarefas, independentemente de a interface do utilizador do seu **AVG Internet Security 2012** estar aberta ou fechada:



Apresentação do Ícone do AVG da Barra de Tarefas

- Com cor cheia, sem elementos adicionais, o ícone indica que todos os componentes do **AVG Internet Security 2012** estão activos e perfeitamente funcionais. No entanto, o ícone também pode ser apresentado desta forma numa situação em que um dos componentes não esteja completamente funcional, mas o utilizador tenha decidido ignorar p estado do componente. *(Tendo confirmado a opção de ignorar o estado do componente, exprime que está consciente do estado de erro do componente, mas que, por alguma razão, pretende mantê-lo assim e não quer ser notificado sobre esta situação).*

- O ícone com um ponto de exclamação indica que o componente *(ou vários componentes)* está em estado de erro. Preste sempre atenção a este aviso e tente corrigir a situação. Para poder efectuar as alterações necessárias à configuração de um componente, clique duas vezes sobre o ícone da barra de tarefas para abrir a interface do utilizador da aplicação. Para informações detalhadas sobre os componentes que estão em estado de erro, queira consultar a secção informação do estado de segurança.

- O ícone da barra de tarefas pode ainda ser apresentado com cor cheia e com uma raio de luz rotativo e intermitente. Esta versão gráfica sinaliza um processo de actualização em decurso.

- A apresentação alternativa de um ícone com cor cheia e uma seta indica que as análises do **AVG Internet Security 2012** estão em execução.

Informações do Ícone do AVG na Barra de Tarefas

O Ícone do AVG na Barra de Tarefas informa ainda sobre as actividades em decurso no seu **AVG Internet Security 2012** e potenciais alterações de estado no programa (*ex. execução automática de uma actualização ou análise agendada, mudança de perfil da Firewall, uma alteração de estado*

de um componente, uma ocorrência de um estado de erro, ...) por meio de uma janela pop-up aberta a partir do ícone da barra de tarefas:

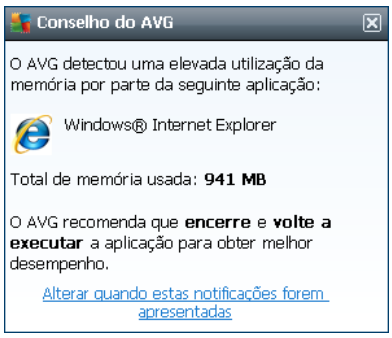
Acções acessíveis a partir do Ícone da Barra de Tarefas

O Ícone da Barra de Tarefas também pode ser usado como link rápido para aceder à interface do utilizador do **AVG Internet Security 2012**, bastando clicar duas vezes sobre o mesmo. Ao clicar com o botão direito do rato sobre o Ícone da Barra de Tarefas abre um pequeno menu de contexto com as seguintes opções:

- ***Abrir a Interface do Utilizador do AVG*** – Clique para abrir a Interface do Utilizador do **AVG Internet Security 2012**.
- ***Desactivar temporariamente a protecção do AVG*** – Esta opção permite-lhe desactivar toda a protecção assegurada pelo **AVG Internet Security 2012** de uma só vez. Tenha em atenção que não deverá usar esta opção a menos que seja absolutamente necessário! Na maioria dos casos, não é necessário desactivar o **AVG Internet Security 2012** antes de instalar novo software ou controladores, mesmo que o instalador ou o assistente do software sugiram que os programas e aplicações em execução devam ser encerrados primeiro para garantir que não ocorrem interrupções durante o processo de instalação. Se tiver de desactivar o **AVG Internet Security 2012** temporariamente, deverá voltar a activá-lo assim que terminar. Se estiver conectado à Internet ou a uma rede durante o período de desactivação do software antivírus, o seu computador estará vulnerável a ataques.
- ***Firewall*** – Clique para abrir o menu de contexto das opções de configuração da Firewall, onde pode editar os parâmetros principais: Estado da Firewall (*Firewall activada/Firewall desactivada/Modo de emergência*), alternância para o modo de jogo e Perfis da Firewall.
- ***Análises*** – Clique para abrir o menu de contexto das análises predefinidas (*Análise de todo o computador* e *Analisar pastas ou ficheiros específicos*) e seleccione a análise pretendida, que será iniciada imediatamente.
- ***Análises em execução...*** - Este item só é apresentado se houver uma análise em execução no computador. É possível definir a prioridade desta análise, parar ou pausar a análise. Além disso, estão acessíveis as seguintes acções: *Definir prioridade para todas as análises, Pausar todas as análises* ou *Parar todas as análises*.
- ***Executar a Optimização Rápida do*** – Clique para executar o componente Optimização Rápida do.
- ***Actualizar agora*** – Inicia imediatamente uma actualização.
- ***Ajuda*** – Abre o ficheiro de ajuda na página inicial.

5.6. AVG Advisor

O ***AVG Advisor*** é uma funcionalidade de desempenho que monitoriza continuamente todos os processos em execução no computador em busca de possíveis problemas, apresentando dicas para evitar esses problemas. O ***AVG Advisor*** aparece sob a forma de uma janela pop-up por cima da barra de tarefas.



O ***AVG Advisor*** poderá aparecer nas seguintes situações:

- O browser da Internet que está a utilizar está a ficar sem memória, o que poderá tornar o seu trabalho mais lento *(o AVG Advisor é compatível apenas com os seguintes browsers: Internet Explorer, Chrome, Firefox, Opera e Safari);*
- Um dos processos em execução no computador está a consumir uma quantidade demasiado grande de memória e a tornar o desempenho do computador mais lento;
- O computador está prestes a estabelecer uma ligação automaticamente a uma rede Wi-Fi desconhecida.

Em cada uma dessas situações, o ***AVG Advisor*** avisa o utilizador relativamente ao problema que pode ocorrer e apresenta o nome e o ícone do processo ou da aplicação em conflito. O ***AVG Advisor*** sugere também os passos que devem ser efectuados para evitar o problema.

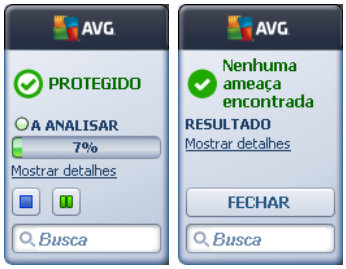
5.7. Gadget do AVG

O ***Gadget do AVG*** é apresentado na ambiente de trabalho do Windows (*Barra Lateral do Windows*). Esta aplicação só é suportada pelos sistemas operativos Windows Vista e Windows 7. O ***Gadget do AVG*** proporciona acesso imediato às mais importantes funcionalidades do **AVG Internet Security 2012**, ou seja, análises e actualizações:

Acesso rápido a análises e actualizações

Se necessário, o ***Gadget AVG*** permite-lhe iniciar uma análise ou actualização imediatamente:

- ***Analisar agora*** – Clique no link ***Analisar agora*** para iniciar a análise de todo o computador directamente. Pode consultar o progresso do processo de análise na interface alternada do utilizador no gadget. Um breve resumo das estatísticas apresenta informações sobre o número de objectos analisados, as ameaças detectadas e as ameaças restauradas. Durante a análise, pode sempre pausar  , ou parar  o processo de análise. Para informações pormenorizadas sobre os resultados da análise, queira consultar a janela Síntese dos resultados de análise que pode ser aberta directamente através do gadget via a opção ***Mostrar detalhes*** *(os resultados de análise respectivos serão listados na Análise da aplicação da barra lateral).*

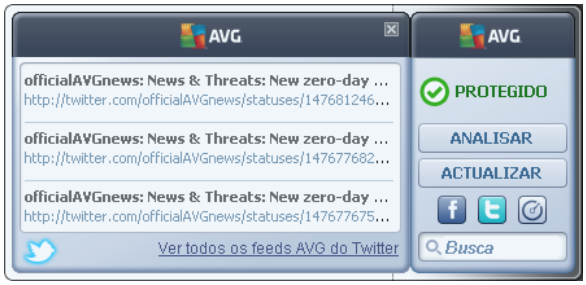


- ***Actualizar agora*** – Clique no link ***Actualizar agora*** para iniciar a actualização do **AVG Internet Security 2012** directamente a partir do gadget:

Acesso às redes sociais

O ***Gadget AVG*** também disponibiliza um link de acesso rápido às principais redes sociais. Use o botão respectivo para se conectar às comunidades AVG no Twitter, Facebook ou LinkedIn:

- ***Link do Twitter***  – Abre uma nova interface do ***gadget do AVG*** com uma síntese dos últimos feeds do AVG publicados no Twitter. Siga o link ***Ver todos os feeds AVG do Twitter*** para abrir o seu browser numa nova janela e será redireccionado directamente para o website do Twitter, especificamente na página dedicada às notícias do AVG:



- ***Link do Facebook*** - Abre o seu browser no website do Facebook, especificamente na página da ***comunidade AVG***.

- ***LinkedIn*** - Esta opção só está disponível na instalação de rede (*ou seja, desde que tenha instalado o AVG com recurso a uma das licenças da edição AVG Business Editions*) e abre o browser no website da ***AVG SMB Community*** na rede social LinkedIn.

Outras funcionalidades acessíveis através da aplicação

- ***Analisador do PC*** - Abre a interface do utilizador no componente Analisador do PC e inicia a análise de imediato.

- ***Caixa de pesquisa*** - Digite uma palavra-chave e obtenha os resultados imediatamente numa nova janela do seu browser predefinido.

6. Componentes do AVG

6.1. Anti-Vírus

O componente ***Anti-vírus*** é um marco do seu **AVG Internet Security 2012** e combina várias funcionalidades fundamentais de um programa de segurança:

- Componente de Análise
- Protecção Residente
- Protecção Anti-Spyware

6.1.1. Componente de Análise

O componente de análise que é a base do componente ***Anti-vírus*** analisa todos os ficheiros e actividades de ficheiros *(abertura/fecho de ficheiros, etc.)* pela existência de vírus conhecidos. Quaisquer vírus detectados serão impedidos de tomarem qualquer acção e serão eliminados ou colocados Quarentena de Vírus.

A funcionalidade importante da protecção do AVG Internet Security 2012 é que nenhum vírus conhecido poderá ser executado no computador!

Métodos de detecção

A maioria do software anti-vírus utiliza igualmente a análise heurística, em que os ficheiros são analisados pela existência de características inerentes aos vírus, apelidadas de assinaturas virais. Isto significa que o verificador anti-vírus consegue detectar um novo vírus, desconhecido, se o vírus tiver algumas das características habituais dos vírus existentes. O

- Análise – procura de cadeias de caracteres que são características de um determinado vírus
- *Análise heurística* – emulação dinâmica das instruções do objecto pesquisado num ambiente de computador virtual
- Detecção genérica – detecção de instruções características de um determinado vírus/grupo de vírus

Nos casos em que uma única tecnologia pode não ser suficiente para detectar ou identificar um vírus, o ***Anti-Vírus*** combina várias tecnologias para assegurar que o seu computador está protegido contra vírus. O **AVG Internet Security 2012** também possui a capacidade de analisar e detectar aplicações executáveis ou bibliotecas DLL que poderão ser potencialmente indesejadas no sistema. Tais ameaças são apelidadas de Programas Potencialmente Indesejados *(vários tipos de Spyware, adware, etc.)*.. Para além disso, o **AVG Internet Security 2012** analisa o registo do sistema para verificar a existência de entradas suspeitas, ficheiros temporários da Internet e cookies de rastreio, permitindo tratar todos os itens potencialmente prejudiciais da mesma forma que qualquer outra infecção.

O AVG Internet Security 2012 proporciona protecção ininterrupta ao seu computador!

6.1.2. Protecção Residente

O* AVG Internet Security 2012** proporciona protecção contínua na forma da protecção residente. O componente ***Anti-vírus analisa todos os ficheiros *(com extensões específicas, ou sem extensão)* que são abertos, guardados ou copiados. Guarda as áreas de sistema do computador e suportes amovíveis (*unidades flash, etc.*). Na eventualidade de a Protecção Residente detectar um vírus num ficheiro acedido, interrompe a operação em curso, não permitindo a activação do vírus. Normalmente, nem se apercebe do processo, uma vez que a protecção residente trabalha em segundo plano. Só recebe a notificação quando são detectadas ameaças; simultaneamente, o ***Anti-vírus*** bloqueia a activação da ameaça e remove-a.

A Protecção Residente é carregada para a memória do seu computador durante o arranque do sistema e é vital que a mantenha constantemente activada.

6.1.3. Protecção Anti-Spyware

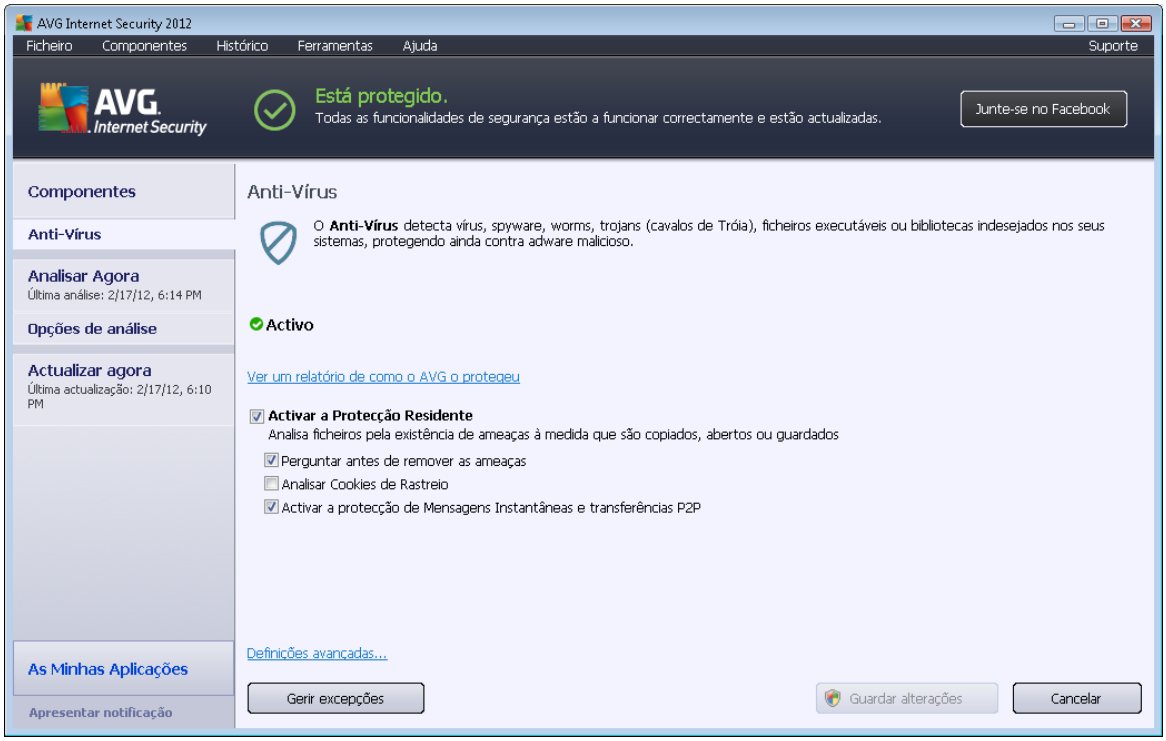
Anti-Spyware consiste numa base de dados de spyware usada para identificar tipos conhecidos de definições de spyware. Os especialistas em spyware da AVG trabalham afincadamente para identificar e descrever os mais recentes padrões de spyware assim que estes surgem, e depois adicionam as definições à base de dados. Estas novas definições são descarregadas para o seu computador através do processo de actualização, para que esteja constantemente e de forma fiável protegido mesmo contra os mais recentes tipos de spyware. O ***Anti-Spyware*** permite-lhe analisar todo o seu computador pela existência de malware/spyware. Detecta também malware latente e inactivo, isto é, malware que foi transferido mas ainda não foi activado.

O que é spyware?

Spyware é normalmente definido como um tipo de malware, isto é, software que recolhe informações do computador do utilizador sem o seu conhecimento ou consentimento. Algumas aplicações de spyware podem ser instaladas propositadamente e, na maior parte dos casos, incluem anúncios, janelas de pop-ups ou outros tipos de software desagradável. Actualmente, a maior fonte de infecções são os websites com conteúdos potencialmente perigosos. Outros métodos de transmissão como, por exemplo, através de e-mail ou de worms e vírus, são igualmente predominantes. A protecção mais importante consiste na utilização de um analisador permanente em segundo plano, ***Anti-Spyware***, que funciona como uma protecção residente e analisa as aplicações em segundo plano à medida que estas são executadas.

6.1.4. Interface do Anti-vírus

A interface do componente ***Anti-vírus*** providencia informações sucintas sobre a funcionalidade do componente, informações sobre o estado actual do computador *(Activo)* e opções básicas de configuração do componente:



Opções de configuração

A janela providencia algumas opções de configuração básicas para funcionalidades disponíveis no componente ***Anti-vírus***. Encontra, de seguida, uma breve descrição das mesmas:

- ***Ver um relatório online de como o AVG o protegeu*** – A hiperligação redirecciona-o para uma página específica no website da AVG (http://www.avg.com/). Na página, são disponibilizadas informações estatísticas pormenorizadas de todas as actividades do **AVG Internet Security 2012** executadas no seu computador durante um período de tempo específico e no total.

- ***Activar a Protecção Residente*** – Esta opção permite-lhe activar/desactivar facilmente a protecção residente. A Protecção Residente analisa ficheiros quando estes são copiados, abertos ou guardados. Quando um vírus ou qualquer tipo de ameaça for detectado, o utilizador será imediatamente notificado. Esta função está activada por predefinição e é recomendável mantê-la activada! Com a protecção residente pode ainda decidir como deverão ser tratadas as infecções possivelmente detectadas:

    - ***Perguntar antes de remover as ameaças*** – Mantenha a opção marcada para confirmar que pretende ser interpelado sempre que for detectada uma ameaça, antes de esta ser removida para a Quarentena de Vírus. Esta opção não tem impacto no nível de segurança e só reflecte as suas preferências.

    - ***Analisar Cookies de Rastreio*** – Independentemente das opções anteriores, pode decidir se quer verificar a existência de cookies de rastreio. *(Cookies são parcelas de texto enviadas por um servidor para um browser Web e depois enviadas de volta*

inalteradas pelo browser de cada vez que este acede ao servidor. As cookies HTTP são utilizadas para autenticar, rastrear e manter informações específicas acerca dos utilizadores, tais como preferências de sítios ou os conteúdos dos seus carrinhos de compras electrónicos.) Em casos específicos pode activar esta opção para obter níveis de segurança máximos, no entanto, está desactivada por predefinição.

- ***Activar a protecção de Mensagens Instantâneas e transferências P2P*** - Marque este item se pretender confirmar que a comunicação através de mensagens instantâneas (*ex., ICQ, MSN Messenger, etc.*) não tem vírus.

- ***Definições avançadas***... – Clique na hiperligação para ser redireccionado para a janela correspondente nas Definições avançadas do **AVG Internet Security 2012**. Aí, pode editar a configuração do componente em pormenor. No entanto, tenha em atenção que a configuração predefinida de todos os componentes está definida de forma que o **AVG Internet Security 2012** providencie um desempenho optimizado e máxima segurança. A menos que tenha uma razão válida para o fazer, recomendamos que mantenha a configuração predefinida!

Botões de controlo

Na janela, pode usar os seguintes botões de controlo:

- ***Gerir excepções*** – Abre uma nova janela com o nome ***Protecção Residente – Excepções***. A configuração de excepções na análise da Protecção Residente também é acessível a partir do menu principal, seguindo a sequência Definições Avançadas / Anti-Vírus / Protecção Residente / Excepções *(consulte o capítulo respectivo para uma descrição detalhada)*. Na janela pode especificar os ficheiros e pastas que deverão ser excluídos da análise da Protecção Residente. Se não for estritamente necessário, recomenda-se vivamente que não exclua quaisquer itens! A janela inclui os seguintes botões de controlo:

  - *Adicionar localização* – Especifique um directório *(ou directórios)* a excluir da análise, seleccionando-os individualmente a partir da árvore de navegação do disco local.

  - *Adicionar Ficheiro* – Permite especificar ficheiros a excluir da análise, seleccionando-os individualmente a partir da árvore de navegação do disco local.

  - *Editar Item* – Permite editar o caminho especificado para um ficheiro ou pasta seleccionado.

  - *Remover Item* – Permite eliminar o caminho para um item seleccionado na lista.

  - *Editar Lista* - Permite editar toda a lista de excepções definidas numa nova janela que se assemelha a um editor de texto tradicional.

- ***Aplicar*** - Guardar todas as alterações efectuadas às definições do componente nesta janela e regressar à interface do utilizador do **AVG Internet Security 2012** (*síntese de componentes*).

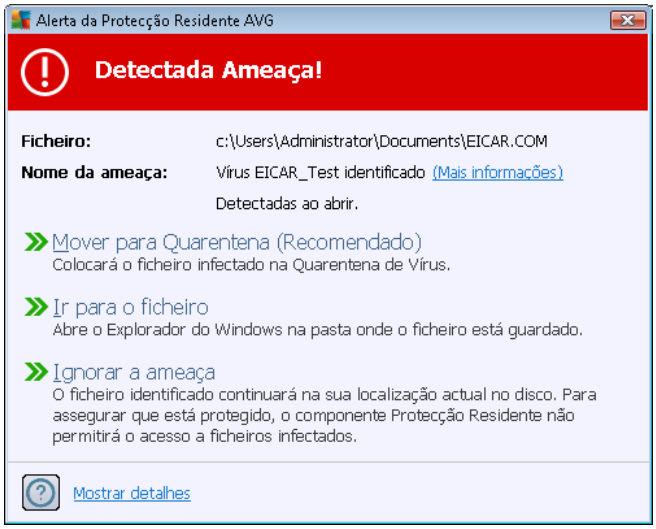
- ***Cancelar*** – Anular todas as alterações efectuadas às definições do componente nesta

janela. Não serão guardadas quaisquer alterações. Regressará à interface do utilizador **AVG Internet Security 2012** (*síntese de componentes*).

6.1.5. Detecções da Protecção Residente

Ameaça detectada!

A Protecção Residenteanalisa ficheiros quando estes são copiados, abertos ou guardados. Quando um vírus ou qualquer tipo de ameaça for detectado, o utilizador será imediatamente notificado através da seguinte janela:



Nesta janela de aviso encontra dados sobre o ficheiro que foi detectado e considerado infectado (*Nome do ficheiro*), o nome da infecção detectada (*Nome da ameaça*) e um link para a Enciclopédia de vírus onde pode aceder a informações detalhadas sobre a infecção detectada, se esta for conhecida (*Mais informações*).

Além disso, tem de decidir a acção a tomar. Há várias opções disponíveis. ***Tenha em atenção que em determinadas condições (que tipo de ficheiro está infectado e onde está localizado), nem todas as opções estarão sempre disponíveis!***

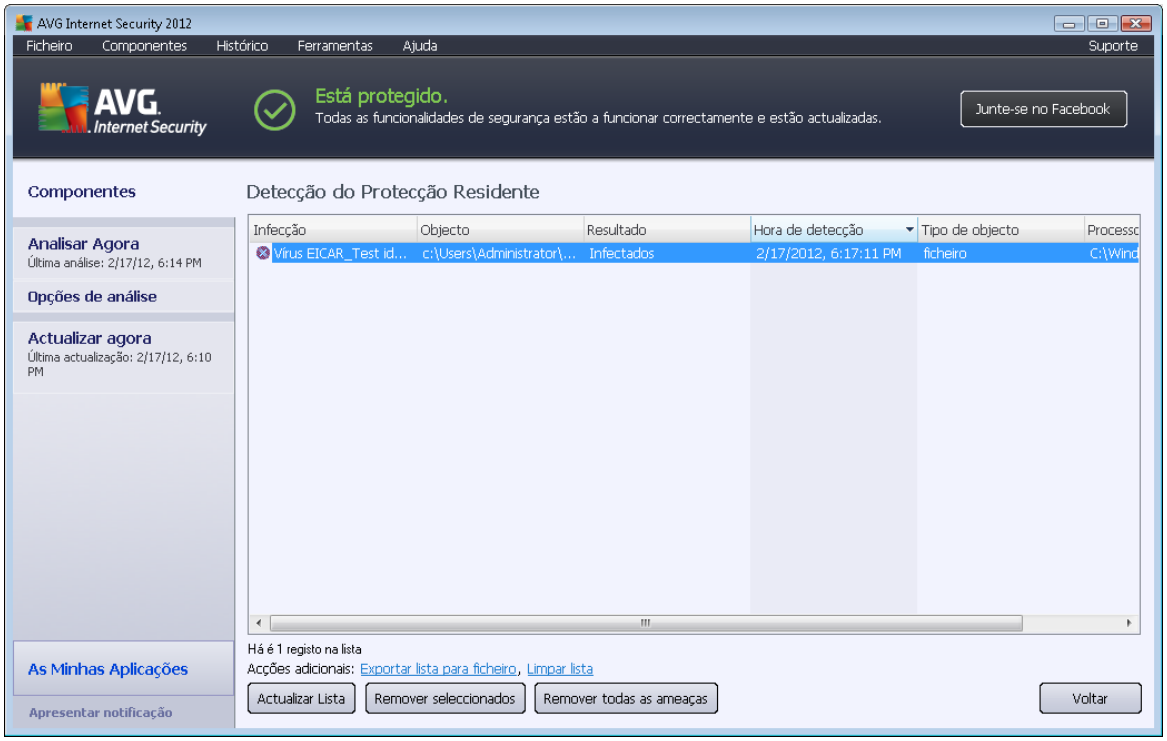
- ***Recuperar*** – este botão só é apresentado se a infecção detectada puder ser recuperada. Depois, remove-a do ficheiro e restaura o ficheiro para o estado original. Se o ficheiro em si for um vírus, use esta função para o eliminar (*ou seja, removê-lo para a Quarentena de Vírus*)
- ***Mover para Quarentena (Recomendado)*** – o vírus será movido para a Quarentena de Vírus
- ***Ir para o ficheiro*** - esta opção redirecciona-o para a localização exacta do objecto suspeito (*abre uma nova janela do Explorador do Windows*)
- ***Ignorar a ameaça*** – recomendamos vivamente que NÃO utilize esta opção a menos que tenha uma razão verdadeiramente válida para isso!

Nota: *Pode ocorrer que o tamanho do objecto detectado exceda o limite de espaço livre na Quarentena de Vírus. Se isso acontecer, será informado por meio de um pop-up sobre a questão quando tentar mover o objecto infectado para a Quarentena de Vírus. Contudo, o tamanho da Quarentena de Vírus pode ser editado. É definido como percentagem ajustável do tamanho real do seu disco rígido. Para aumentar o tamanho da Quarentena de Vírus, aceda à janela Quarentena de Vírus nas Definições Avançados do AVG, e defina-o na opção 'Tamanho limite da Quarentena de Vírus'.*

Na secção inferior da janela encontra o link ***Apresentar detalhes*** - clique sobre o mesmo para abrir uma janela de pop-up com informações detalhadas sobre o processo em execução, quando a infecção foi detectada e a identificação do processo.

Síntese das detecções da Protecção Residente

A síntese integral de todas as ameaças detectadas pela Protecção Residente pode ser encontrada na janela ***Detecção da Protecção Residente*** acessível a partir da opção do menu do sistema Histórico / detecções da Protecção Residente:



A ***Detecção da Protecção Residente*** faculta uma síntese de objectos que foram detectados pela Protecção Residente, avaliados como perigosos e recuperados ou movidos para a Quarentena de Vírus. É facultada a seguinte informação para cada objecto detectado:

- ***Infecção***- descrição (possivelmente até o nome) do objecto detectado
- ***Objecto***- localização do objecto

- ***Resultado***- acção efectuada com o objecto detectado
- ***Hora de detecção*** – data e hora em que o objecto foi detectado
- ***Tipo de objecto***- tipo do objecto detectado
- ***Processo*** – que acção foi efectuada para atrair o objecto potencialmente perigoso de forma a este poder ser detectado

Na parte inferior da janela, abaixo da lista, encontrará informações sobre o número total de objectos detectados listados acima. Pode ainda exportar toda a lista dos objectos detectados num ficheiro (***Exportar lista para ficheiro***) e eliminar todas as entradas sobre objectos detectados (***Lista vazia***). O botão ***Actualizar lista*** procederá à actualização da lista de detecções da ***Protecção Residente***. O botão ***Retroceder*** leva-o de volta à Interface do utilizador do AVG padrão (*síntese de componentes*).

6.2. Link Scanner

O LinkScanner protege-o contra o crescente número de ameaças 'transitórias' que populam a Internet. Estas ameaças podem estar ocultas em qualquer tipo de website, desde websites governamentais a websites de grandes multinacionais ou de pequenas empresas, e raramente permanecem nesses sites por mais de 24 horas. ***O LinkScanner*** protege-o ao analisar as páginas Web associadas a todos os links em qualquer página que esteja a visualizar e ao assegurar que estas são seguras no único momento em que importa – quando o utilizador está prestes a clicar no link.

O LinkScanner não se destina à protecção de plataformas de servidores!

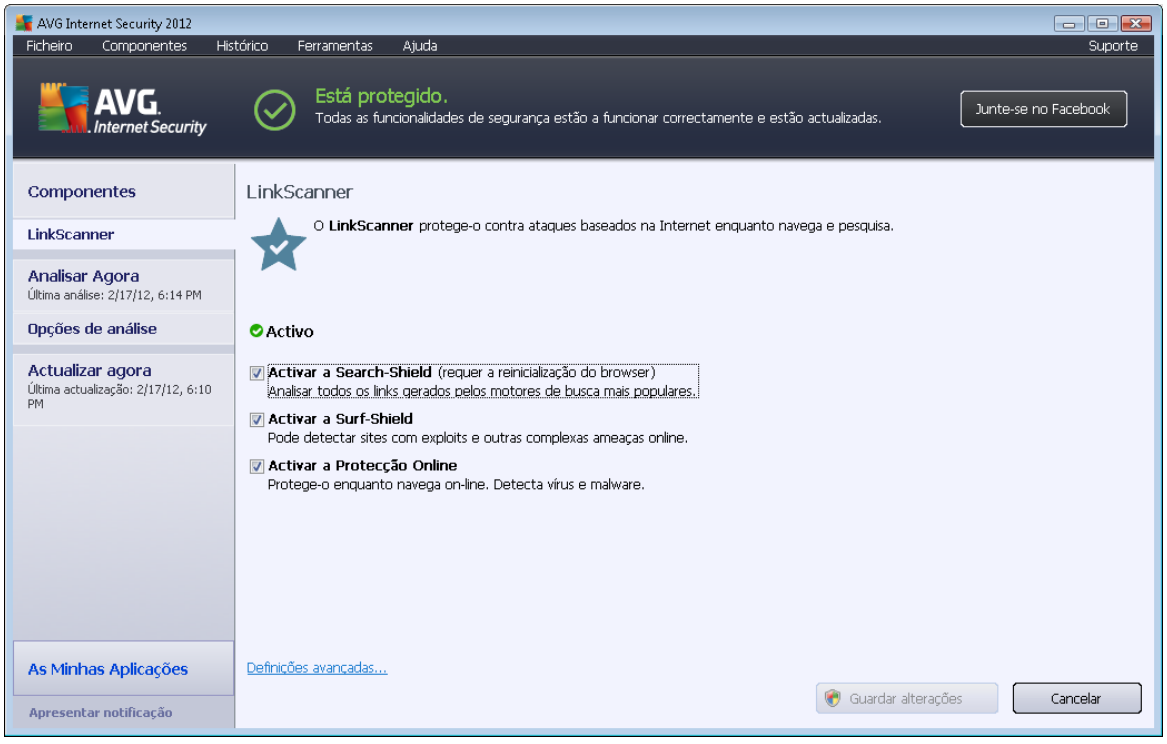
A tecnologia ***LinkScanner*** consiste nas seguintes funcionalidades principais:

- O Search-Shield contém uma lista de websites *(endereços URL)* que são conhecidos como sendo perigosos. Ao pesquisar com o Google, Yahoo!, JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask e Seznam, todos os resultados da pesquisa são verificados contra esta lista e é apresentado um ícone de veredicto *(para o Yahoo! só é apresentado o ícone de "Website com exploits" nos resultados de busca)*.
- O Surf-Shield analisa o conteúdo dos websites que visita, independentemente do endereço do website. Mesmo que um website não seja detectado pelo Search Shield *(ex. quando um novo website malicioso é criado, ou quando um website anteriormente seguro passa a conter malware*), será detectado e bloqueado pelo Surf-Shield assim que tentar visitar o website.
- A Protecção Online funciona como uma protecção em tempo real quando navega na Internet. Analisa o conteúdo de páginas web visitadas e de possíveis ficheiros incluídos nas mesmas antes destas serem apresentadas no seu browser ou serem transferidas para o seu computador. A Protecção Online detecta vírus e spyware contido na página que está prestes a visitar e pára a transferência imediatamente para que nenhuma ameaça consiga aceder ao seu computador.
- O ***Acelerador AVG*** permite umareprodução de vídeos online mais fluida e facilita as

transferências. Quando o processo de aceleração do vídeo estiver em decurso, será notificado via uma janela de notificação na barra de tarefas.

6.2.1. Interface do Link Scanner

A interface do componente LinkScanner providencia uma breve descrição das funcionalidades do componente e informações relativas ao seu estado actual *(Activo)*:



Na parte inferior da janela, estão disponíveis algumas opções básicas de configuração do componente:

- ***Activar o Search-Shield*** – (*activado por predefinição*): Desmarque a caixa apenas se tiver uma boa razão para desactivar a funcionalidade Search Shield.
- ***Activar o Surf-Shield*** – (*activado por predefinição*): Protecção activa (*em tempo real*) contra websites maliciosos à medida que estes são acedidos. Ligações de websites maliciosos conhecidos são bloqueadas à medida que estes são acedidos pelo utilizador via um browser (*ou qualquer outra aplicação que utilize HTTP*).
- ***Activar a Protecção Online*** – (*activado por predefinição*): Análise em tempo real pela potencial existência de vírus ou spyware nas páginas que está prestes a visitar. Se forem detectadas ameaças, a transferência pára imediatamente para que nenhuma ameaça

consiga aceder ao seu computador.

6.2.2. Detecções do Search-Shield

Ao pesquisar na internet com o ***Search-Shield*** activado, todos os resultados de pesquisa devolvidos pelos motores de busca mais populares (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, e SlashDot*) são avaliados pela existência de links perigosos ou suspeitos. Ao verificar estes links e marcando os perigosos, o LinkScanner avisa-o antes de clicar em links perigosos ou suspeitos, para poder ter a certeza de que só visita websites seguros.

Enquanto um link está a ser analisado na página de resultados de busca, verá um sinal gráfico junto ao link a informar que a verificação do link está em curso. Quando a avaliação estiver terminada será apresentado o respectivo ícone informativo:

 A página de destino é segura.

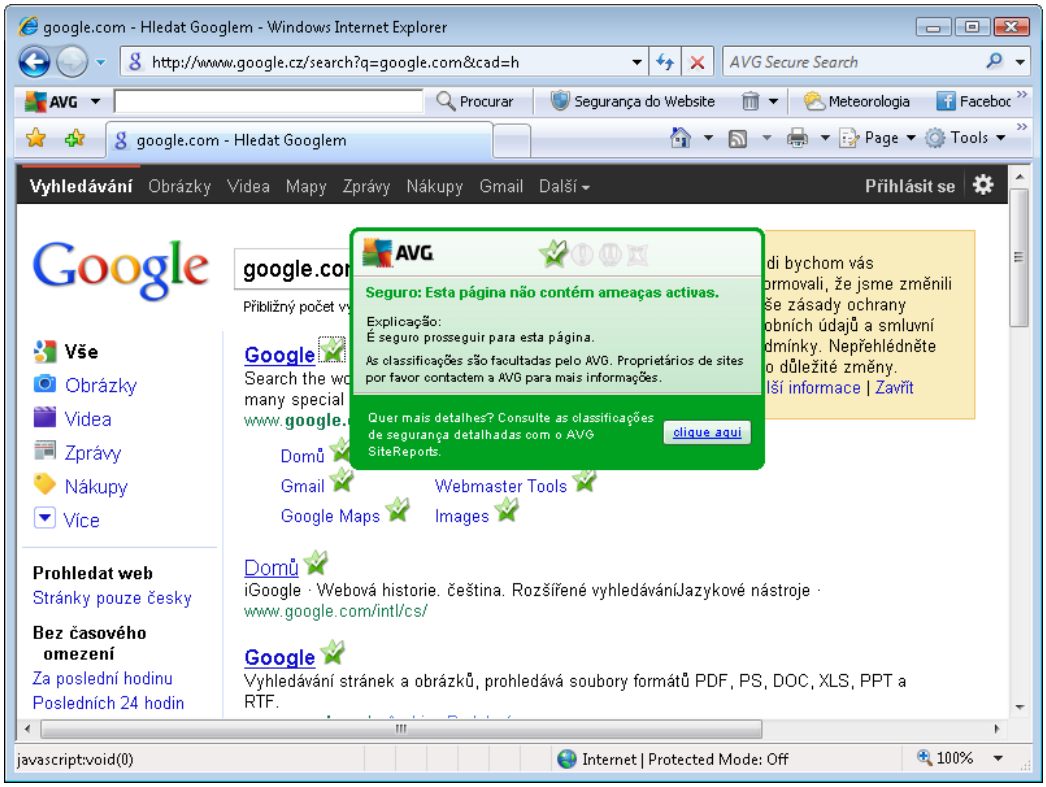
 A página de destino não contém ameaças mas é algo suspeita (*questionável em termos de origem ou motivo, como tal, não é recomendável para compras on-line, etc.*).

 A página destino pode ser segura em si, mas contém ligações adicionais a páginas assumidamente perigosas, ou com códigos suspeitos, embora não utilizando quaisquer ameaças de momento.

 A página de destino contém ameaças activas! Para sua segurança, não lhe será permitido visitar esta página.

 A página de destino não está acessível, e, como tal, não pôde ser analisada.

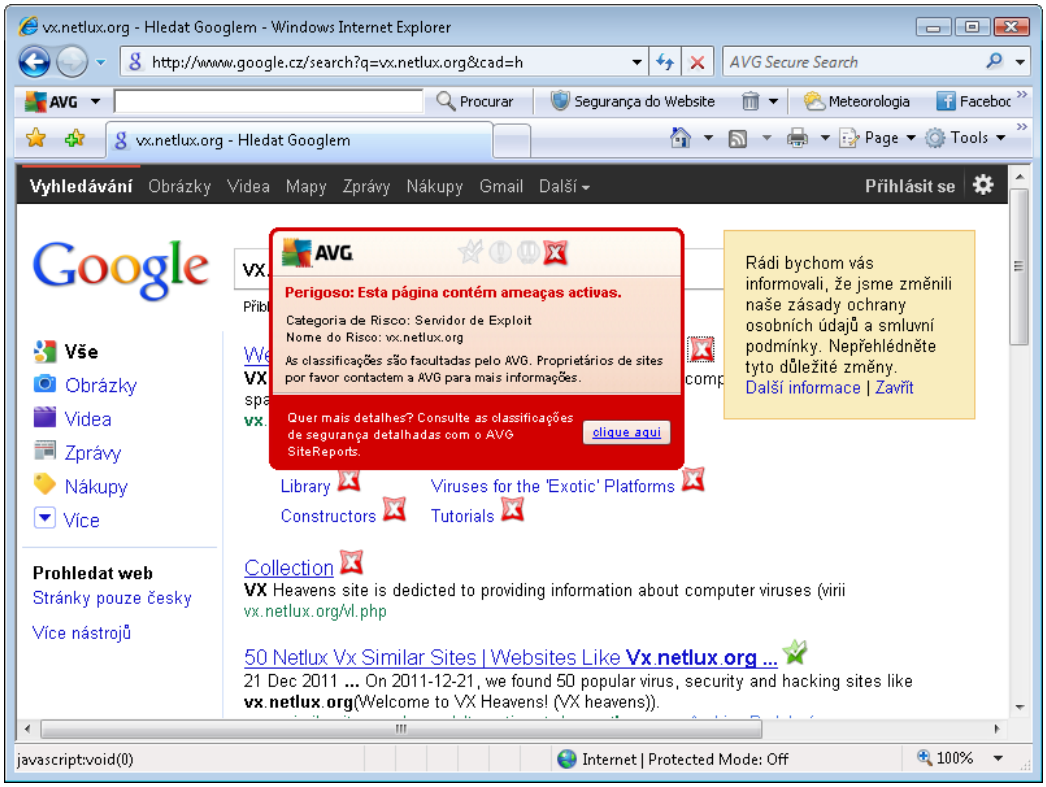
Colocar o cursor sobre um ícone de classificação individual apresentará detalhes acerca do link em questão. As informações incluem detalhes adicionais sobre a ameaça (*se for o caso*):



6.2.3. Detecções do Surf-Shield

Esta poderosa protecção bloqueará o conteúdo malicioso de qualquer página Web que tentar abrir, e evita que o mesmo seja transferido para o seu computador. Com esta funcionalidade activada, clicar num link ou digitar um URL de um sítio perigoso bloqueará automaticamente a abertura da página Web, protegendo-o de ser inadvertidamente infectado. É importante que tenha em mente que as páginas Web com exploits podem infectar o seu computador simplesmente por as visitar; como tal, ao solicitar a abertura de uma página Web que contenha exploits ou outras ameaças sérias, o LinkScanner não permitirá que o seu browser a apresente.

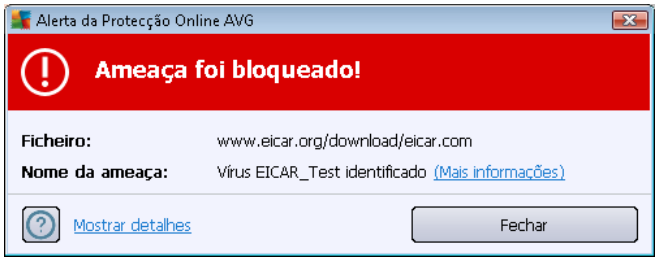
Se se deparar com um website malicioso, o LinkScanner avisa-o no seu browser por meio de uma janela semelhante a:



Aceder a esse website é extremamente perigoso e completamente desaconselhável!

6.2.4. Detecções da Protecção Online

A Protecção Online analisa o conteúdo de páginas Web visitadas e de possíveis ficheiros incluídos nas mesmas antes destas serem apresentadas no seu browser ou serem transferidas para o seu computador. Se for detectada uma ameaça, será imediatamente avisado por meio da seguinte janela:

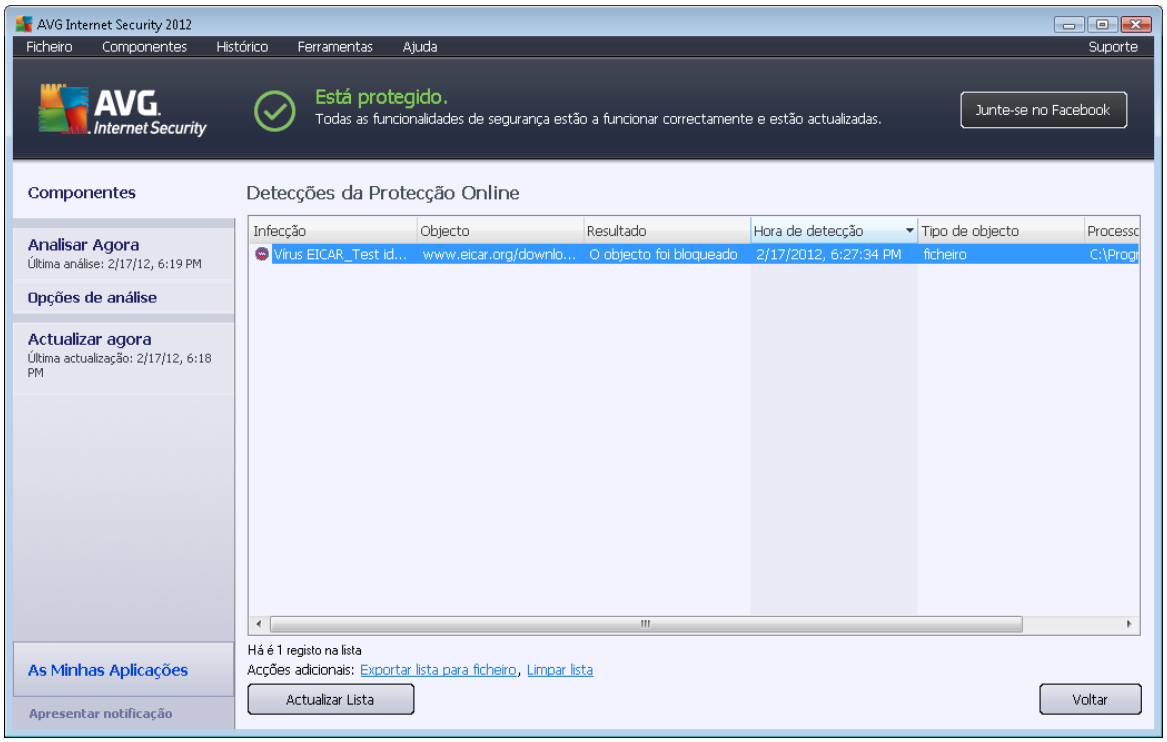


Nesta janela de aviso encontra dados sobre o ficheiro que foi detectado e considerado infectado (*Nome do ficheiro*), o nome da infecção detectada (*Nome da ameaça*) e um link para a Enciclopédia de vírus onde pode aceder a informações detalhadas sobre a infecção detectada (*se esta for conhecida*). A janela inclui os seguintes botões:

- ***Apresentar detalhes*** - clique no botão ***Apresentar detalhes*** para abrir uma nova janela pop-up onde pode encontrar informações sobre o processo em execução quando a infecção foi detectada e a identificação do processo.

- ***Fechar*** – clique no botão para fechar a janela de aviso.

A página Web suspeita não será aberta e a detecção da ameaça será registada na lista de ***Detecções da Protecção Online*** – esta síntese de ameaças detectadas é acessível via o menu de sistema Histórico / Detecções da Protecção Online.



É facultada a seguinte informação para cada objecto detectado:

- ***Infecção***- descrição (*possivelmente até o nome*) do objecto detectado
- ***Objecto*** – fonte do objecto (*página Web*)
- ***Resultado***- acção efectuada com o objecto detectado
- ***Hora de detecção*** – data e hora em que a ameaça foi detectada e bloqueada
- ***Tipo de objecto***- tipo do objecto detectado
- ***Processo*** – que acção foi efectuada para atrair o objecto potencialmente perigoso de forma a este poder ser detectado

Na parte inferior da janela, abaixo da lista, encontrará informações sobre o número total de objectos detectados listados acima. Pode ainda exportar toda a lista dos objectos detectados num ficheiro (***Exportar lista para ficheiro***) e eliminar todas as entradas sobre objectos detectados (***Lista vazia***).

Botões de controlo

- ***Actualizar lista*** – procederá à actualização da lista de detecções da ***Protecção Online***
- ***Retroceder*** – leva-o de volta à Interface do utilizador do AVG *padrão (síntese de componentes).*

6.3. Protecção de E-mail

Uma das origens mais comum de vírus e trojans é via e-mail. O phishing e o spam fazem dos e-mails uma fonte ainda maior de riscos. As contas de e-mail gratuitas têm maiores probabilidades de receber e-mails maliciosos (*uma vez que raramente utilizam tecnologia anti-spam*), e os utilizadores domésticos dependem em grande parte de tais contas. Além disso, os utilizadores domésticos ao navegarem por websites desconhecidos e preenchendo formulários on-line com dados pessoais (*como o seu endereço de e-mail*) aumentam a exposição a ataques via e-mail. As empresas utilizam contas de e-mail empresariais e utilizam filtros anti-spam, etc., para reduzir o risco.

O componente ***Protecção de E-mail*** é responsável pela análise de todas as mensagens de e-mail, enviadas ou recebidas; sempre que for detectado um vírus num e-mail, é removido imediatamente para a Quarentena de Vírus. O componente também pode filtrar determinados tipos de anexos de e-mail e adicionar um texto de certificação às mensagens que não contenham infecções. ***A Protecção de E-mail*** é composta por duas funções principais:

- Verificador de E-mail
- Anti-Spam

6.3.1. Verificador de E-mail

O Verificador de E-mail Pessoal analisa os e-mails a receber e a enviar automaticamente. Pode usá-lo com clientes de e-mail que não tenham um plug-in dedicado no AVG (*mas também pode ser usado para analisar mensagens de e-mail em clientes suportados por um plug-in específico do AVG, ex. Microsoft Outlook, The Bat e Mozilla Thunderbird*). A sua função primária é a utilização com aplicações de e-mail como o Outlook Express, Incredimail, etc.

Durante a instalação do AVG são criados servidores automáticos para controlo das mensagens de e-mail: um para verificar e-mails a receber e um segundo para verificar e-mails a enviar. A utilização destes dois servidores é automaticamente associada às portas 110 e 25 (*portas padrão para o envio/recepção de e-mails*).

O Verificador de E-mail funciona como uma interface entre o cliente de e-mail e os servidores de e-mail na Internet.

- ***Correio a receber:*** Durante a recepção de uma mensagem do servidor, o componente ***Verificador de E-mail*** testa-a pela existência de vírus, remove os anexos infectados e adiciona a certificação. Ao serem detectados, os vírus são colocados na Quarentena de Vírus imediatamente. Depois, a mensagem é enviada para o cliente de e-mail.
- ***Correio a enviar:*** A mensagem é enviada do cliente de e-mail para o Verificador de E-mail; este último analisa a mensagem pela existência de vírus e depois envia a mensagem para

o servidor SMTP (*a análise de correio a enviar está desactivada por predefinição e pode ser configurada manualmente*).

O Verificador de E-mail não se destina a plataformas de servidores!

6.3.2. Anti-Spam

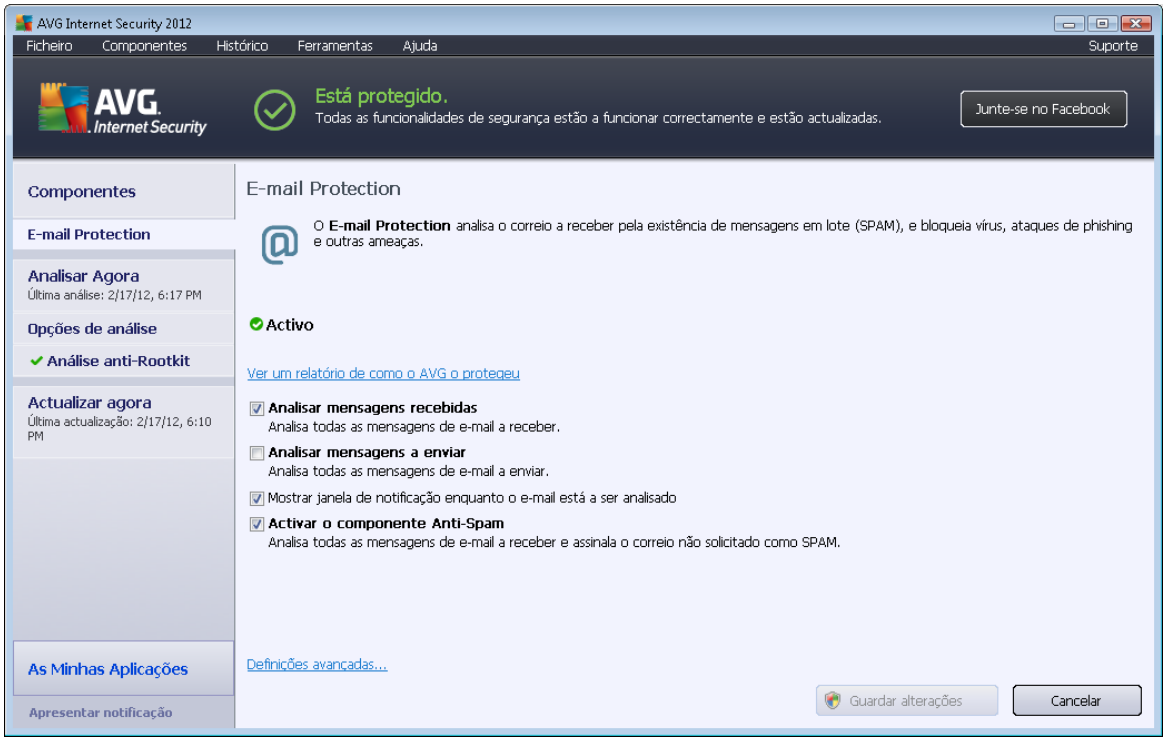
Como é que funciona o Anti-Spam?

O componente Anti-Spam verifica todo e-mail a receber e assinala o e-mail solicitado como spam. ***O Anti-Spam*** pode modificar o assunto do e-mail (*que foi identificado como sendo spam*) ao adicionar uma linha de texto especial. Poderá depois filtrar facilmente os e-mails no seu cliente de e-mail. ***O componente Anti-Spam*** utiliza vários métodos de análise para processar cada e-mail, oferecendo o máximo de protecção possível contra e-mails indesejados. O ***Anti-Spam*** utiliza uma base de dados que é actualizada regularmente para a detecção de spam. Também é possível utilizar os Servidores RBL ((*bases de dados públicas de endereços de e-mail de "spammers conhecidos"*) e adicionar manualmente endereços de e-mail à sua Lista Branca (*nunca marcar como spam*) e à Lista negra (*marcar sempre como spam*).

O que é spam?

Spam refere-se a correio electrónico não solicitado, que normalmente publicita um produto ou serviço e 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.

6.3.3. Interface da Protecção de E-mail



No janela do componente ***Protecção de E-mail*** pode encontrar um pequeno texto com a descrição da funcionalidade do componente e informações relativas ao seu estado actual *(Activo)*. Use a hiperligação ***Consulte um relatório online de como o AVG o protegeu*** para rever estatísticas detalhadas das actividades e detecções do **AVG Internet Security 2012** numa página dedicada do Website da AVG (http://www.avg.com/).

Definições Básicas da Protecção de E-mail

Na janela ***Protecção de E-mail*** pode ainda editar algumas funcionalidades básicas do componente:

- ***Analisar mensagens recebidas*** *(activado por predefinição)* - Assinale a caixa para especificar que todos os e-mails entregues na sua conta devem ser analisados para verificar se contêm vírus.
- ***Analisar mensagens a enviar*** *(desactivado por predefinição)* - Assinale a caixa para confirmar que todos os e-mails enviados a partir da sua conta devem ser analisados para verificar se contêm vírus.
- ***Mostrar janela de notificação enquanto o e-mail está a ser analisado*** *(activado por predefinição)* – marque este item para confirmar que pretende ser avisado através de uma janela de notificação acima do ícone do AVG na barra de tarefas durante a análise ao seu e-mail.
- ***Activar o componente Anti-Spam*** *(activado por predefinição)*- Marque este item para

especificar se pretende que o correio de entrada seja filtrado pela existência de correio não solicitado.

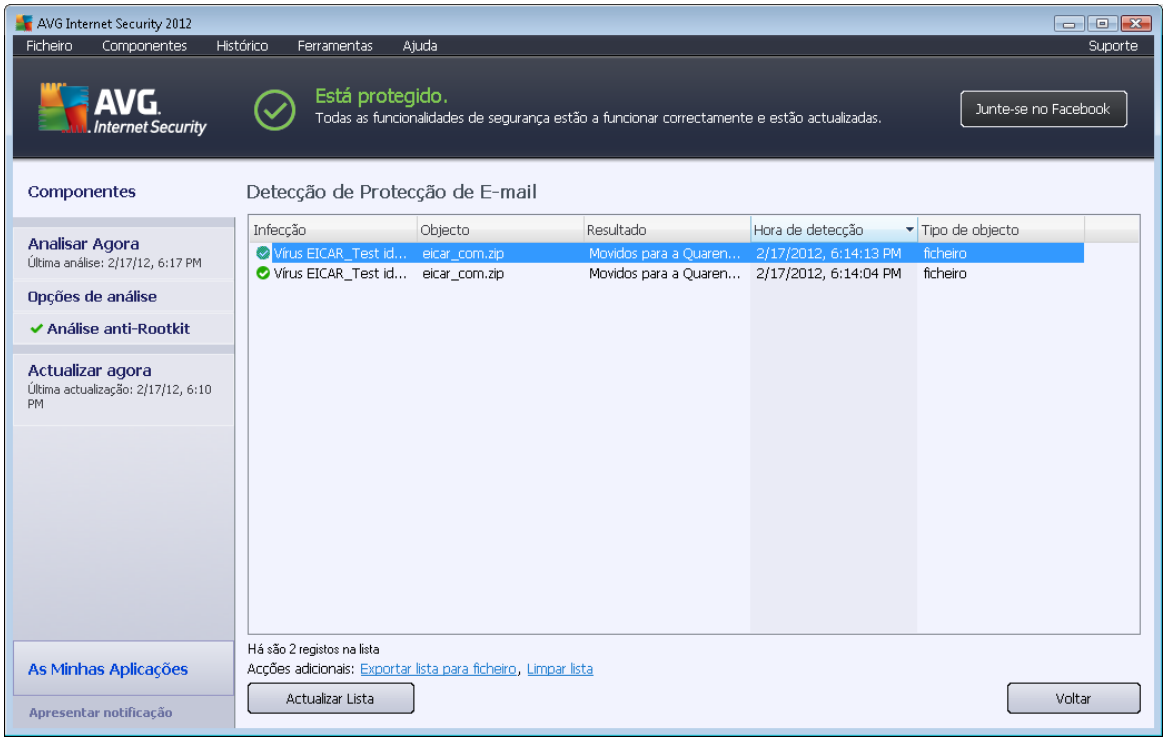
O fornecedor do software configurou todos os componentes do AVG de forma a estes proporcionarem um excelente desempenho. Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente por um utilizador avançado. Se necessitar de alterar a configuração do AVG, seleccione o item do menu de sistema Ferramentas / Definições avançadas e edite a configuração do AVG na janela Definições Avançadas do AVG que lhe é apresentada.

Botões de controlo

Os botões de controlo disponíveis na janela da ***Protecção de E-mail*** são os seguintes:

- ***Guardar alterações*** – clique neste botão para guardar e aplicar quaisquer alterações efectuadas nesta janela
- ***Cancelar*** – clique neste botão para retroceder para a janela principal do AVG (*síntese de componentes*)

6.3.4. Detecções de verificador de Correio Electrónico



Na janela ***Detecção da Protecção de E-mail*** (*acessível via a opção do menu de sistema Histórico / Detecção da Protecção de E-mail*) poderá ver uma lista de todas as infecções encontradas pelo componente Protecção de E-mail. É facultada a seguinte informação para cada

objecto detectado:

- ***Infecção***- descrição (possivelmente até o nome) do objecto detectado
- ***Objecto***- localização do objecto
- ***Resultado***- acção efectuada com o objecto detectado
- ***Hora de detecção*** – data e hora em que o objecto suspeito foi detectado
- ***Tipo de objecto***- tipo do objecto detectado

Na parte inferior da janela, abaixo da lista, encontrará informações sobre o número total de objectos detectados listados acima. Pode ainda exportar toda a lista dos objectos detectados num ficheiro (***Exportar lista para ficheiro***) e eliminar todas as entradas sobre objectos detectados (***Lista vazia***).

Botões de controlo

Os botões de controlo disponíveis na interface ***detecção do Verificador de E-mail***são os seguintes:

- ***Actualizar lista*** – Actualiza a lista de ameaças detectadas.
- ***Retroceder*** – Regressa à janela apresentada anteriormente.

6.4. Firewall

Uma Firewall é um sistema que implementa uma política de controlo de acesso entre duas ou mais redes, bloqueando/autorizando o tráfego. ***A Firewall*** contém um conjunto de regras que protege a rede interna de ataques provenientes do exterior *(normalmente da Internet)* e controla todas as comunicações em todas as portas de rede. A comunicação é avaliada de acordo com as regras definidas, sendo então permitida ou proibida. Se uma ***Firewall*** detectar alguma tentativa de intrusão, "bloqueia" a tentativa e não deixa o intruso aceder ao computador.

A Firewall está configurada para permitir ou negar comunicações internas/externas (ambos os sentidos, entrada ou saída) através das portas definidas, e para as aplicações de software definidas. Por exemplo, a firewall pode ser configurada para permitir apenas o fluxo de entrada ou saída de dados da Internet utilizando o Microsoft Explorer. Qualquer tentativa de transmissão de dados da Internet por qualquer outro browser será bloqueada.

A Firewall protege as suas informações de identificação pessoal de serem enviadas do seu computador sem a sua autorização. Controla a forma como é efectuada a comunicação de dados entre o seu computador e outros computadores da Internet ou da rede local. Dentro de uma organização, a ***Firewall*** também protege o computador individual de ataques desencadeados por utilizadores internos ou por outros computadores da rede.

Os computadores que não estiverem protegidos por uma Firewall tornam-se alvos fáceis para ataques de piratas informáticos e roubos de dados.

Recomendação: *Regra geral, não é recomendável utilizar mais de uma firewall num mesmo*

computador. A segurança do computador não é potenciada se instalar mais firewalls. É, na verdade, mais provável que ocorram alguns conflitos entre estas duas aplicações. Como tal, é recomendável que utilize apenas uma firewall no seu computador e desactive todas as outras, eliminando desta forma o risco de possíveis conflitos e quaisquer problemas associados.

6.4.1. Princípios da Firewall

No **AVG Internet Security 2012**, a ***Firewall*** controla todo o tráfego em todas as portas de rede do seu computador. Com base nas regras definidas, a ***Firewall*** avalia as aplicações que estão a funcionar no seu computador *(e que pretendem estabelecer ligação à rede local ou à Internet)*, ou as aplicações que tentam estabelecer ligação ao seu PC a partir do exterior. Para cada uma dessas aplicações, a ***Firewall*** permite ou proíbe as comunicações através das portas da rede. Por predefinição, se a aplicação for desconhecida *(ex. não tiver regras da Firewall definidas)*, a ***firewall*** solicitar-lhe-á se pretende permitir ou bloquear a tentativa de comunicação.

A Firewall do AVG não se destina a plataformas de servidores!

O que a Firewall do AVG pode fazer:

- Permitir ou bloquear automaticamente tentativas de comunicação de Aplicações conhecidas, ou solicitar a sua confirmação
- Usar Perfis completos com regras predefinidas, consoante as suas necessidades
- Mudar perfis automaticamente ao ligar a várias redes, ou usando vários adaptadores de rede

6.4.2. Perfis da Firewall

A Firewall permite-lhe definir regras de segurança específicas consoante o seu computador esteja localizado num domínio, ou seja um computador independente, ou mesmo um portátil. Cada uma destas opções requer um nível de protecção diferente, sendo os níveis abrangidos pelos respectivos perfis. Resumindo, um perfil da Firewall é uma configuração específica do componente Firewall, e pode usar uma variedade dessas configurações predefinidas.

Perfis disponíveis

- ***Permitir todos*** - um perfil de sistema da Firewall que foi predefinido pelo fabricante e que está sempre presente. Quando este perfil está activado, todas as comunicações de rede são permitidas e não são aplicadas quaisquer regras de politica de segurança, como se a protecção da Firewall estivesse desactivada (ex. são permitidas todas as aplicações mas os pacotes ainda são verificados – para desactivar por completo qualquer filtragem é necessário desactivar a Firewall). Este perfil de sistema não pode ser duplicado ou eliminado, e as suas definições não podem ser modificadas.
- ***Bloquear todos*** – um perfil de sistema da Firewall que foi predefinido pelo fabricante e que está sempre presente. Quando este perfil está activado, todas as comunicações de rede são bloqueadas, e o computador não é acessível a partir de redes externas, nem pode comunicar com o exterior. Este perfil de sistema não pode ser duplicado ou eliminado e as

suas definições não podem ser modificadas.

- ***Perfis definidos*** Os perfis definidos também lhe permitem tirar proveito da funcionalidade de mudança automática de perfil, o que pode ser especialmente prático se se conectar a várias redes com frequência *(ex. com um portátil).* Os perfis definidos são gerados automaticamente após a instalação do **AVG Internet Security 2012** e abrangem quaisquer necessidades individuais em termos de regras de política da Firewall. Estão disponíveis os seguintes perfis definidos:

    - ***Ligado directamente à Internet*** – adequado para a maioria dos computadores de secretária domésticos ou portáteis com ligação directa à Internet, sem qualquer protecção adicional. Esta opção também é recomendada para quando liga o seu portátil a várias redes desconhecidas, e provavelmente inseguras (*ex. num ciberespaço, hotel, etc.*).As regras de política da Firewall

    - ***Computador num domínio*** – adequado para computadores numa rede local, normalmente uma escola ou local de trabalho. Assume-se que a rede é administrada por profissionais e protegida com algumas medidas de segurança adicionais; como tal, o nível de segurança pode ser menor do que nos casos mencionados acima, permitindo o acesso a pastas partilhadas, unidades de disco, etc.

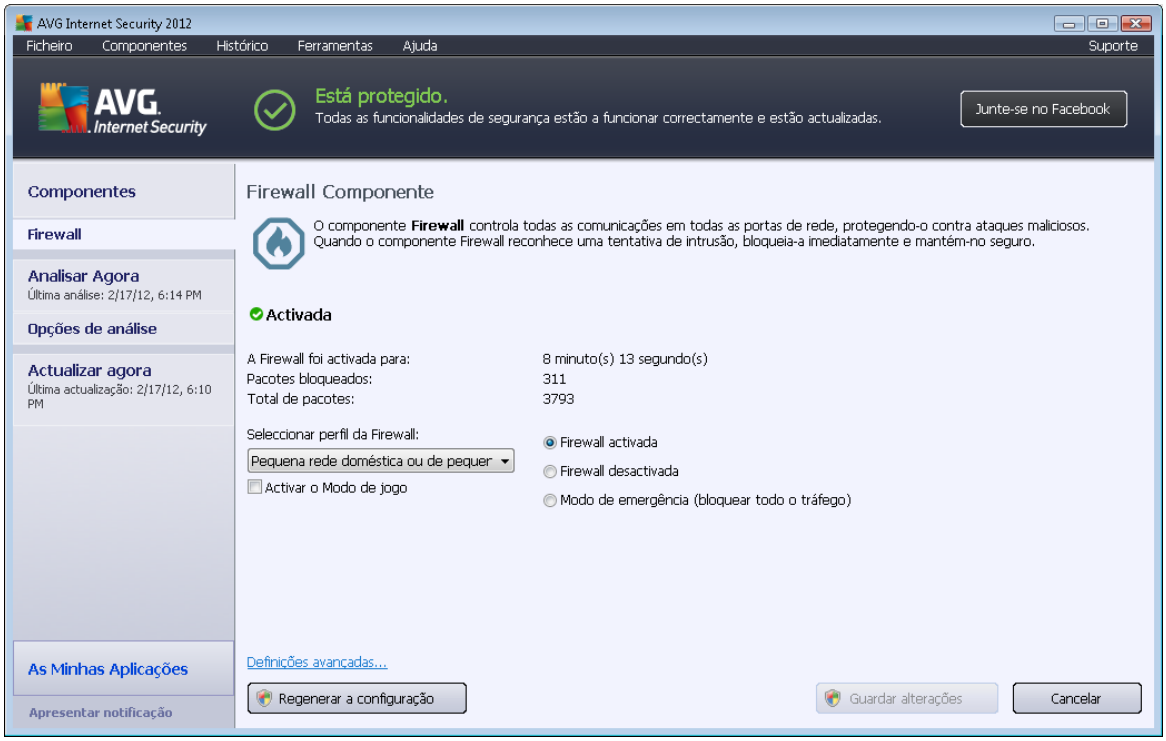
    - ***Pequena rede doméstica ou de pequena empresa*** – adequado para computadores numa pequena rede, normalmente em casa ou numa pequena empresa. Normalmente, este tipo de rede não possui um administrador "central" e é composta por vários computadores interligados, muitas vezes partilhando uma impressora, um scanner ou um dispositivo semelhante, que as regras da Firewall devem reflectir.

Mudança de perfil

A funcionalidade de mudança de perfil permite à Firewall mudar automaticamente para o Perfil definido durante a utilização de uma determinada placa de rede ou quando está ligado a um determinado tipo de rede. Se ainda não estiver atribuído nenhum perfil a uma área de rede, então aquando da próxima ligação a essa área, a Firewall irá apresentar uma janela a pedir-lhe que atribua um perfil. Pode atribuir perfis a todas as interfaces ou áreas de redes locais ou especificar mais definições na janela Perfis de Áreas e Adaptadores, onde também pode desactivar a funcionalidade se não a quiser utilizar (*então será utilizado o perfil predefinido para qualquer tipo de ligação*).

Regra geral, os utilizadores que possuem um portátil e usam vários tipos de ligação considerarão esta funcionalidade útil. Se tiver um computador de secretária, e usa sempre um tipo de ligação (*ex. ligação de cabo à Internet*), não tem de se preocupar com mudanças de perfil uma vez que nunca necessitará delas.

6.4.3. Interface da Firewall



A janela principal apelidada ***Componente Firewall*** providencia algumas informações básicas sobre a funcionalidade do componente, o seu estado *(Activo)* e uma breve síntese das estatísticas do componente:

- ***A Firewall está activada há*** – tempo decorrido desde a última vez que a Firewall foi iniciada
- ***Pacotes bloqueados*** - número de pacotes bloqueados da totalidade de pacotes verificados
- ***Total de pacotes*** – número de todos os pacotes verificados durante a execução da Firewall

Definições básicas da Firewall

- ***Selecção do perfil da Firewall*** – a partir do menu de opções, seleccione um dos perfis definidos (*para uma descrição detalhada de cada perfil e respectiva utilização recomendada, queira consultar o capítulo Perfis da Firewall*)
- ***Activar o Modo de Jogo*** – Marque esta opção para garantir que, durante a execução de aplicações de ecrã inteiro (*jogos, apresentações, filmes, etc.*), a Firewall não apresenta janelas a inquirir se pretende permitir ou bloquear a comunicação a aplicações desconhecidas. Na eventualidade de uma aplicação tentar comunicar através da rede em qualquer dado momento, a Firewall permitirá ou bloqueará a tentativa automaticamente consoante as definições do perfil actual. ***Nota:*** Com o modo de jogo activado, todas as

tarefas agendadas (análises, actualizações) são adiadas até ao encerramento da aplicação.

- Além disso, nesta secção de definições básicas, pode seleccionar entre três opções alternativas de definição do estado do componente Firewall:
    - ***Firewall activada*** *(predefinição)*- seleccione esta opção para permitir a comunicação para as aplicações que estão atribuídas como "permitidas" no conjunto de regras definidas no perfil da Firewall seleccionado.
    - ***Firewall desactivada*** – esta opção desactiva a Firewall por completo, todo o tráfego de rede é permitido mas não verificado!
    - ***Modo de emergência (bloquear todo o tráfego)*** – seleccione esta opção para bloquear todo o tráfego em todas as portas de rede; a Firewall ainda está em execução mas todo o tráfego de rede está parado.

Tenha em atenção: *O fornecedor do software configurou todos os componentes do AVG Internet Security 2012 para um desempenho optimizado. Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente por um utilizador avançado. Se necessitar de alterar a configuração da Firewall, seleccione o item do menu de sistema****Ferramentas/Definições da Firewall*** *e edite a configuração da Firewall na janela recentemente aberta das Definições da Firewall.*

Botões de controlo

- ***Regenerar a configuração*** – prima este botão para substituir a configuração actual da Firewall e reverter para a configuração predefinida baseada na detecção automática.
- ***Guardar alterações*** – clique neste botão para guardar e aplicar quaisquer alterações efectuadas nesta janela.
- ***Cancelar*** – clique neste botão para retroceder para a janela principal do AVG (*síntese de componentes*).

6.5. Anti-Rootkit

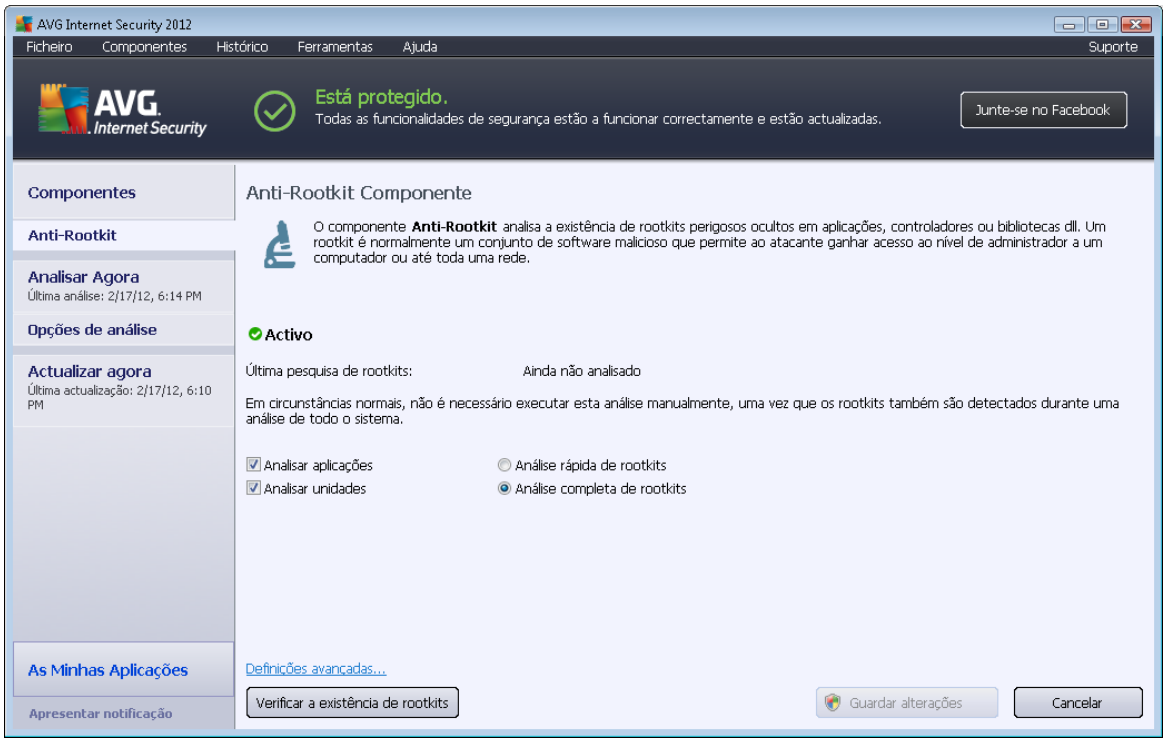
O componente Anti-Rootkit é uma ferramenta especializada na detecção e remoção efectiva de perigosos rootkits, ou seja, programas e tecnologias que podem camuflar a presença de software malicioso no seu computador. O ***Anti-Rootkit*** consegue detectar rootkits com base num conjunto de regras previamente definidas. Tenha em atenção que são detectados todos os rootkits *(não apenas os infectados)*. Na eventualidade de o ***Anti-Rootkit*** encontrar um rootkit, isso não significa necessariamente que o mesmo esteja infectado. Por vezes, os rootkits são usados como controladores ou como componentes de aplicações seguras.

O que é um rootkit?

Um rootkit é um programa concebido para assumir controlo do sistema do computador, sem a

autorização dos proprietários e gestores legítimos do mesmo. O acesso ao hardware é raramente necessário uma vez que um rootkit destina-se a assumir o controlo do sistema operativo em execução no hardware. Regra geral, os rootkits agem de forma a ocultar a sua presença no sistema através de subversões ou evasões dos mecanismos de segurança padrão dos sistemas operativos. Acontece que estes também são frequentemente Trojans; como tal, enganam os utilizadores para que estes pensem que os mesmos podem ser executados em segurança nos seus sistemas. As técnicas utilizadas para este efeito podem incluir ocultar processos em execução de programas de monitorização, ou esconder ficheiros ou dados de sistema do sistema operativo.

6.5.1. Interface do Anti-Rootkit



A janela ***Anti-Rootkit*** disponibiliza uma breve descrição da funcionalidade do componente, apresenta informação sobre o estado actual do componente *(Activo)* e disponibiliza informação sobre a última vez que o teste ***Anti-Rootkit*** foi executado (*Última pesquisa de rootkits; o teste de rootkits é um processo predefinido que é executado dentro da Análise de todo o computador*). A janela ***Anti-Rootkit*** apresenta ainda o link Ferramentas/Definições Avançadas. Use o link para aceder à configuração avançada do componente ***Anti-Rootkit***.

O fornecedor do software configurou todos os componentes do AVG de forma a estes proporcionarem um excelente desempenho. Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente por um utilizador avançado.

Definições básicas do Anti-Rootkit

Na parte inferior da janela pode configurar algumas funções elementares da análise pela presença

de rootkits. Primeiro, seleccione as caixas respectivas para especificar os objectos que devem ser analisados:

- ***Analisar aplicações***
- ***Analisar unidades***

Posteriormente, pode escolher o modo de análise de rootkits:

- ***Análise rápida de rootkits*** – Analisa todos os processos em execução, controladores carregados e a pasta de sistema (*normalmente c:\Windows*).
- ***Análise completa de rootkits*** – Analisa todos os processos em execução, controladores carregados, a pasta de sistema (*normalmente c:\Windows*), e todos os discos locais (*incluindo unidades flash mas excluindo unidades de disquete/CD*).

Botões de controlo

- ***Verificar a existência de rootkits*** – Uma vez que a análise de rootkits não é uma parte implícita da Análise de todo o computador, pode executar a análise de rootkits directamente a partir da interface do ***Anti-Rootkit*** utilizando, para o efeito, este botão.
- ***Guardar alterações*** – Clique neste botão para guardar todas as alterações efectuadas nesta interface e para regressar à janela principal do AVG (*síntese de componentes*)
- ***Cancelar*** – Clique neste botão para regressar à Janela principal do AVG (*síntese de componentes*) sem ter guardado quaisquer alterações efectuadas

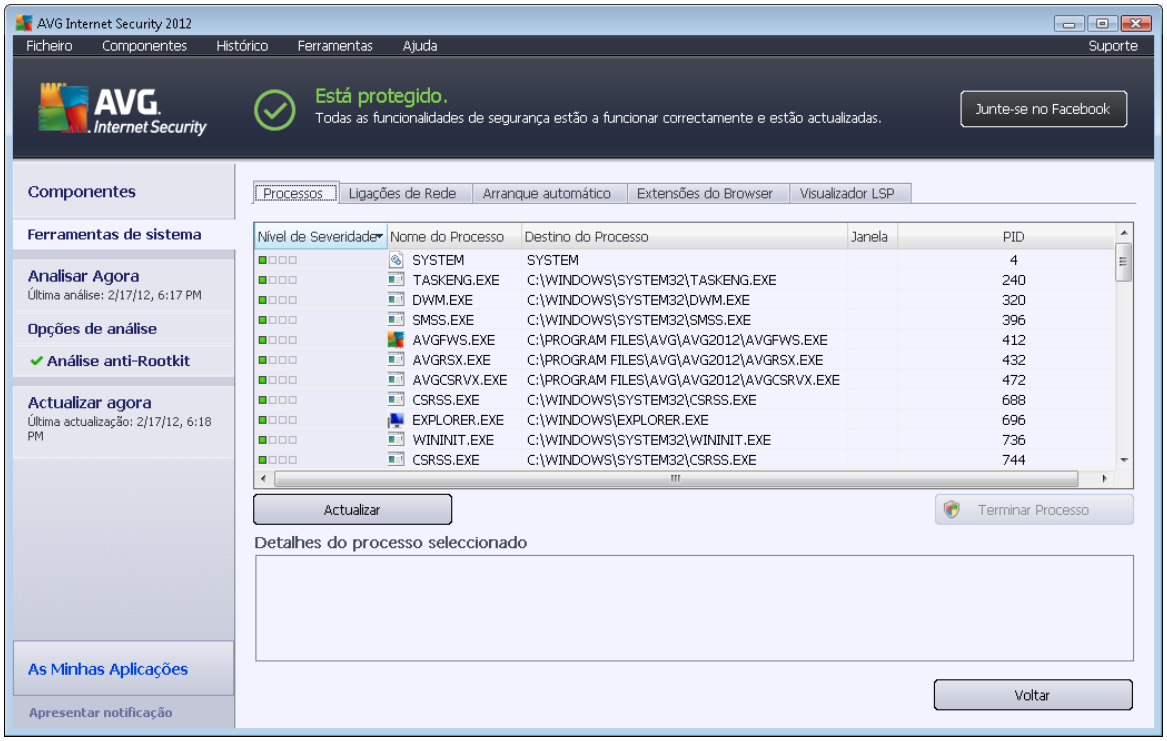
6.6. Ferramentas

As ***Ferramentas de sistema*** são referentes a ferramentas que disponibilizam um resumo detalhado do ambiente e sistema operativo do **AVG Internet Security 2012** . O componente apresenta uma síntese de:

- Processos – lista de processos (*ou seja, aplicações em execução*) que estão actualmente activos no seu computador
- Ligações de rede – lista de ligações actualmente activas
- Arranque automático – lista de todas as aplicações que são executadas durante o arranque do sistema do Windows
- Extensões do Browser – lista de plug-ins (*ou seja, aplicações*) que estão instaladas no seu browser
- Visualizador LSP – lista de LSPs (*Layered Service Providers*)

Também podem ser editadas sínteses específicas mas isto só é recomendado para utilizadores muito experientes!

6.6.1. Processos



A janela ***Processos***contém uma lista de processos (*ou seja, aplicações em execução*) que estão actualmente activas no seu computador. A lista está dividida em várias colunas:

- ***Nível de Gravidade*** -identificação gráfica da gravidade do processo respectivo numa escala de quatro níveis, do menos grave ( ) até ao crítico (■□□□■■■■)
- ***Nome do processo*** – nome do processo em execução.
- ***Destino do processo*** – caminho físico para o processo em execução
- ***Janela*** – se aplicável, indica o nome da Janela da aplicação
- ***PID***- número de identificação do processo é um identificador de processo interno do Windows

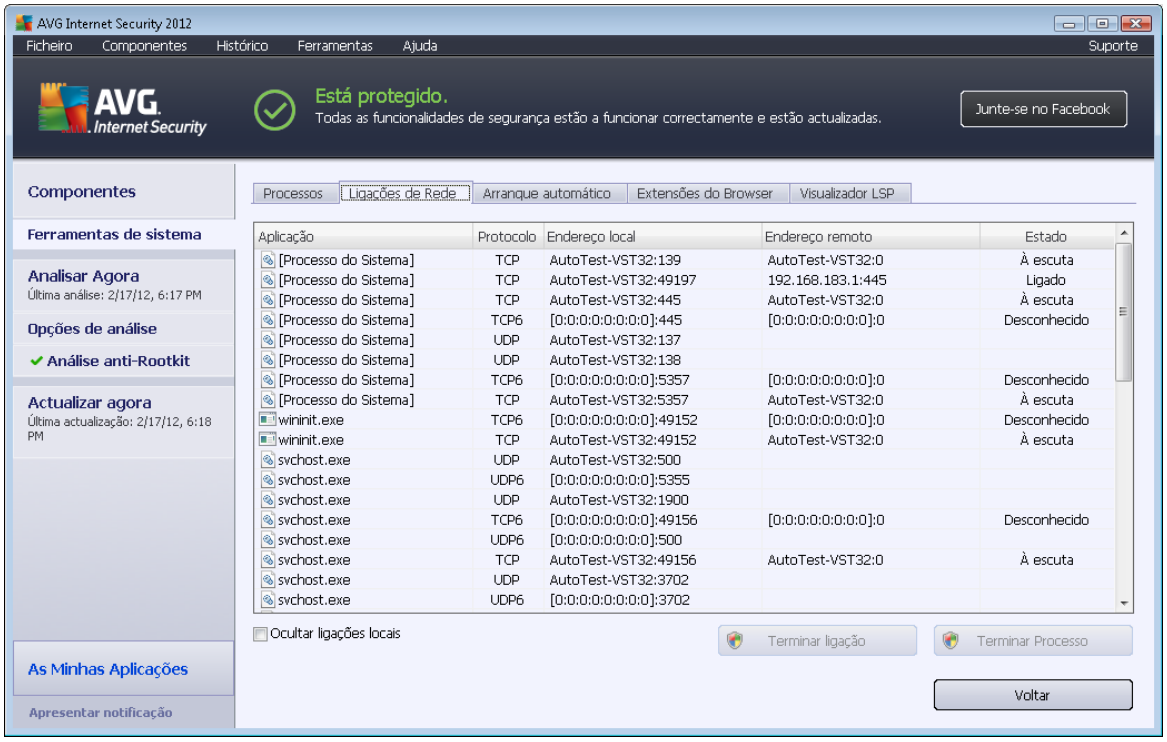
Botões de controlo

Os botões de controlo disponíveis no separador ***Processos*** são os seguintes:

- ***Actualizar*** – actualiza a lista de processos em conformidade com o estado actual
- ***Terminar Processo*** - pode seleccionar uma ou mais aplicações e depois terminá-las premindo este botão. ***Recomenda-se vivamente que não termine nenhuma aplicação, a menos que tenha a certeza absoluta de que representa uma ameaça real!***

- ***Retroceder*** – leva-o de volta à janela principal do AVG (*síntese de componentes*)

6.6.2. Ligações de Rede



A janela ***Ligações de Rede*** apresenta uma lista das ligações actualmente activas. A lista está dividida nas seguintes colunas:

- ***Aplicação*** – nome da aplicação associada à ligação (*excepto Windows 2000 em que a informação não está disponível*)
- ***Protocolo*** – tipo de protocolo de transmissão usada para a ligação:
  - TCP – protocolo utilizado em conjunto com o Protocolo de Internet (IP) para transmitir informações através da Internet
  - UDP – alternativa ao protocolo TCP
- ***Endereço local*** – endereço IP do computador local e o número da porta usada
- ***Endereço remoto*** – endereço IP do computador remoto e o número da porta a que está conectado. Se possível, indica também o nome de anfitrião do computador remoto.
- ***Estado*** – indica o estado actual mais provável (*Conectado, Servidor devia Fechar, Escuta, Fecho activo concluído, Fecho passivo, Fecho activo*)

Para listar apenas ligações externas, seleccione a caixa ***Ocultar ligações locais*** na secção inferior da janela abaixo da lista.

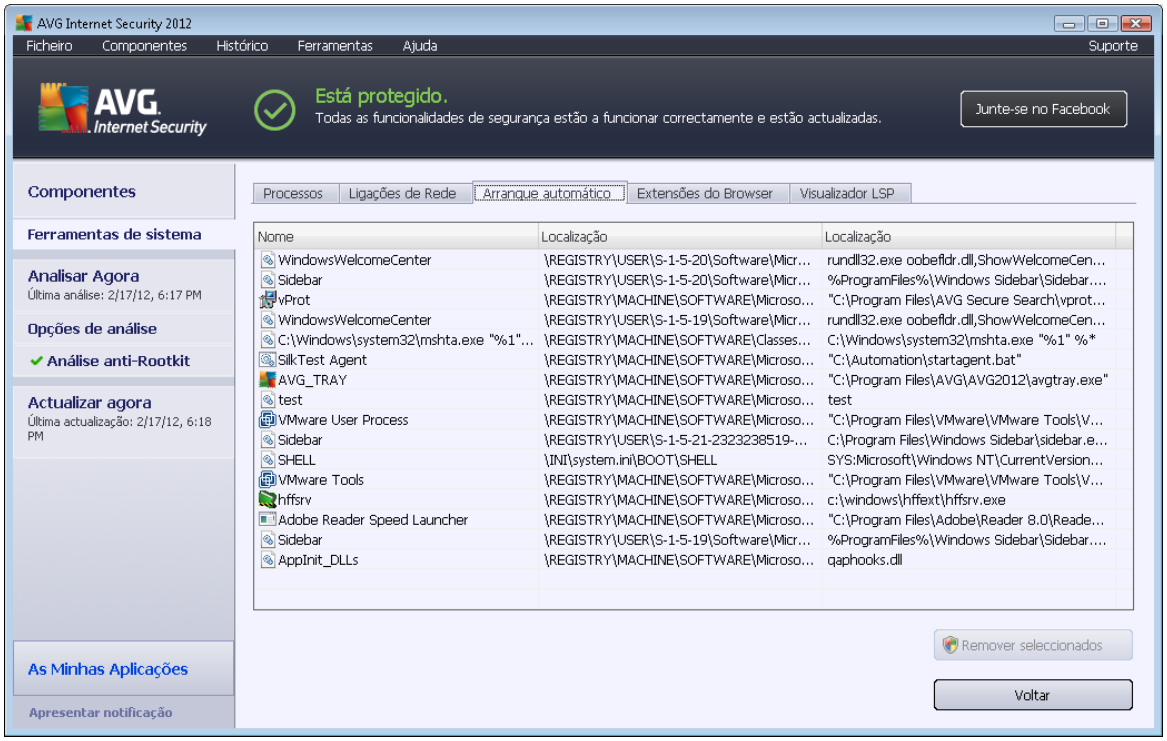
Botões de controlo

Os botões de controlo disponíveis no separador ***Ligações de Rede*** são os seguintes:

- ***Terminar ligação***- fecha uma ou mais ligações seleccionadas na lista
- ***Terminar Processo*** – fecha uma ou mais aplicações associadas às ligações seleccionadas na lista
- ***Retroceder*** – leva-o de volta à Interface do utilizador do AVG padrão (síntese de componentes).

por vezes é possível terminar apenas aplicações que estejam no estado ligado. Recomenda-se vivamente que não termine nenhuma ligação, a menos que tenha a certeza absoluta de que representa uma ameaça real!

6.6.3. Arranque automático



A janela ***Arranque automático*** apresenta uma lista de todas as aplicações que são executadas durante o arranque do sistema Windows. Com frequência, várias aplicações de malware adicionam-se automaticamente à entrada de arranque do registo.

Botões de controlo

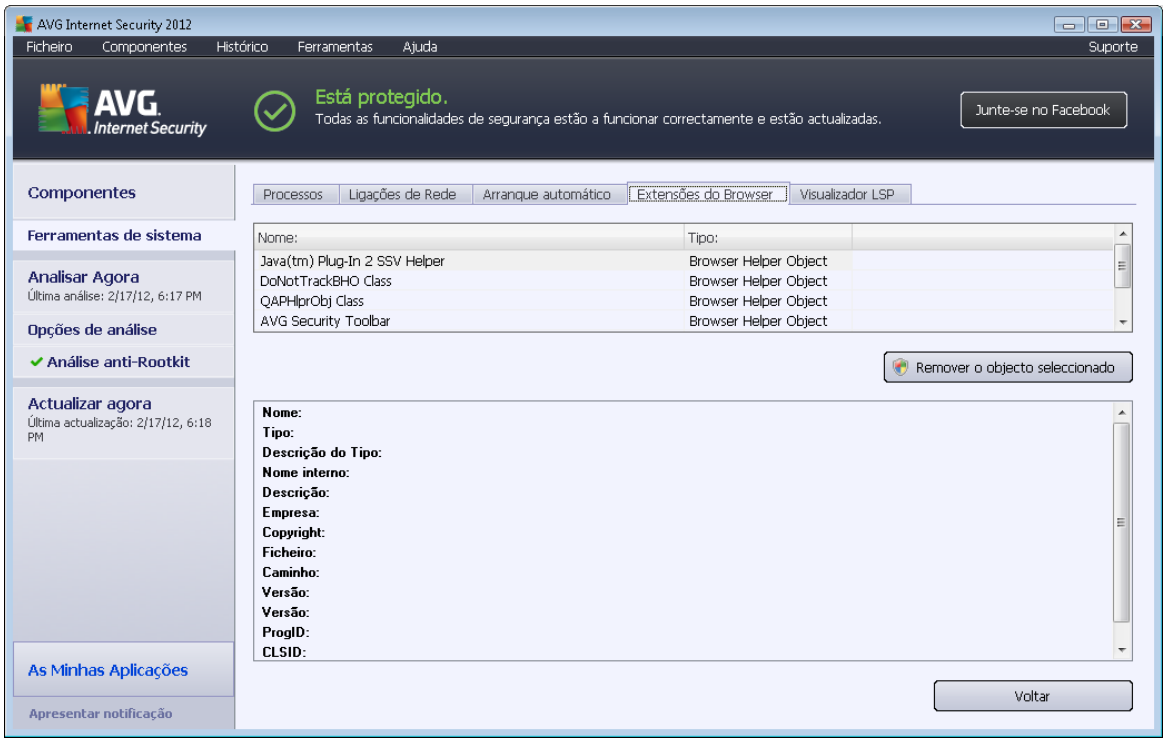
Os botões de controlo disponíveis no separador ***Arranque automático*** são os seguintes:

- ***Remover seleccionados*** – Clique no botão para eliminar uma ou mais entradas seleccionadas.

- ***Retroceder*** – leva-o de volta à janela principal do AVG *(síntese de componentes).*

Recomenda-se vivamente que não elimine nenhuma aplicação da lista, a menos que tenha a certeza absoluta de que representa uma ameaça real!

6.6.4. Extensões do Browser



A janela ***Extensões do Browser*** contém uma lista de plug-ins (*ou seja, aplicações*) que estão instaladas no seu browser da Internet. Esta lista pode conter plug-ins de aplicações normais e programas potenciais de malware. Clique num objecto na lista para obter informações detalhadas sobre o plug-in seleccionado que serão apresentadas na parte inferior da janela.

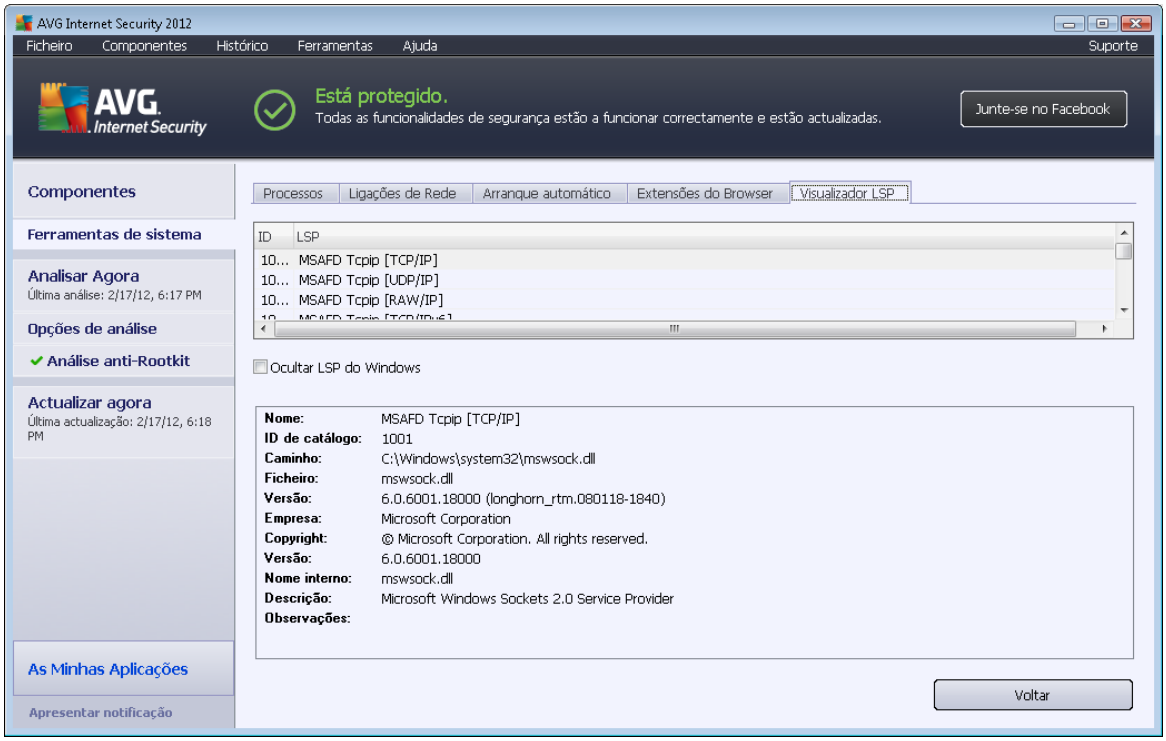
Botões de controlo

Os botões de controlo disponíveis no separador ***Extensões do Browser*** são os seguintes:

- ***Remover objecto seleccionado*** – remove o plug-in que está actualmente em realce na lista. ***Recomenda-se vivamente que não elimine nenhum plug-in da lista, a menos que tenha a certeza absoluta de que representa uma ameaça real!***

- ***Retroceder*** – leva-o de volta à janela principal do AVG *(síntese de componentes).*

6.6.5. Visualizador LSP



A janela ***Visualizador de LSP*** apresenta uma lista de Layered Service Providers (LSP).

Um ***Layered Service Provider*** (LSP) é um controlador do sistema ligado aos serviços de rede do sistema operativo Windows. Tem acesso a todos os dados que entram e saem do computador, incluindo a capacidade de os modificar. Alguns LSPs são necessários para permitir que o Windows estabeleça ligação a outros computadores, incluindo a Internet. No entanto, algumas aplicações de malware podem também instalar-se como um LSP, acedendo assim a todos os dados transmitidos pelo computador. Por conseguinte, esta análise pode ajudá-lo a verificar todas as possíveis ameaças LSP.

Em algumas situações é possível reparar LSPs danificados (*por exemplo, quando o ficheiro tiver sido removido mas as entradas de registo permanecerem intactas*). É apresentado um novo botão para corrigir o problema sempre que é encontrado um LSP reparável.

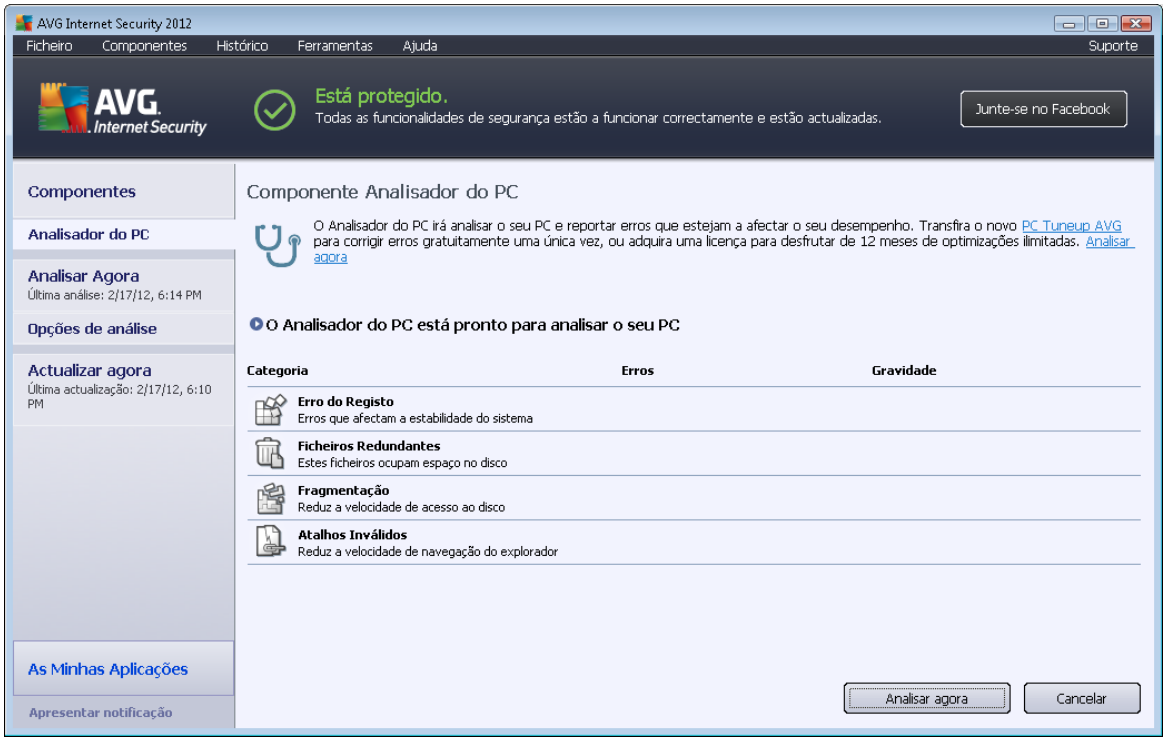
Botões de controlo

Os botões de controlo disponíveis no separador ***Visualizador de LSP***são os seguintes:

- ***Ocultar LSP do Windows*** – para incluir os LSP do Windows na lista, desmarque este item.
- ***Retroceder*** – leva-o de volta à janela principal do AVG (*síntese de componentes*).

6.7. Analisador do PC

O componente ***Analisador do PC*** pode analisar o seu computador pela existência de problemas no sistema e apresenta uma síntese transparente do que pode estar a perturbar o desempenho geral do computador. Na interface do utilizador do componente, pode consultar uma tabela dividida em quatro linhas referentes às categorias respectivas: erros do registo, ficheiros redundantes, fragmentação e atalhos inválidos:



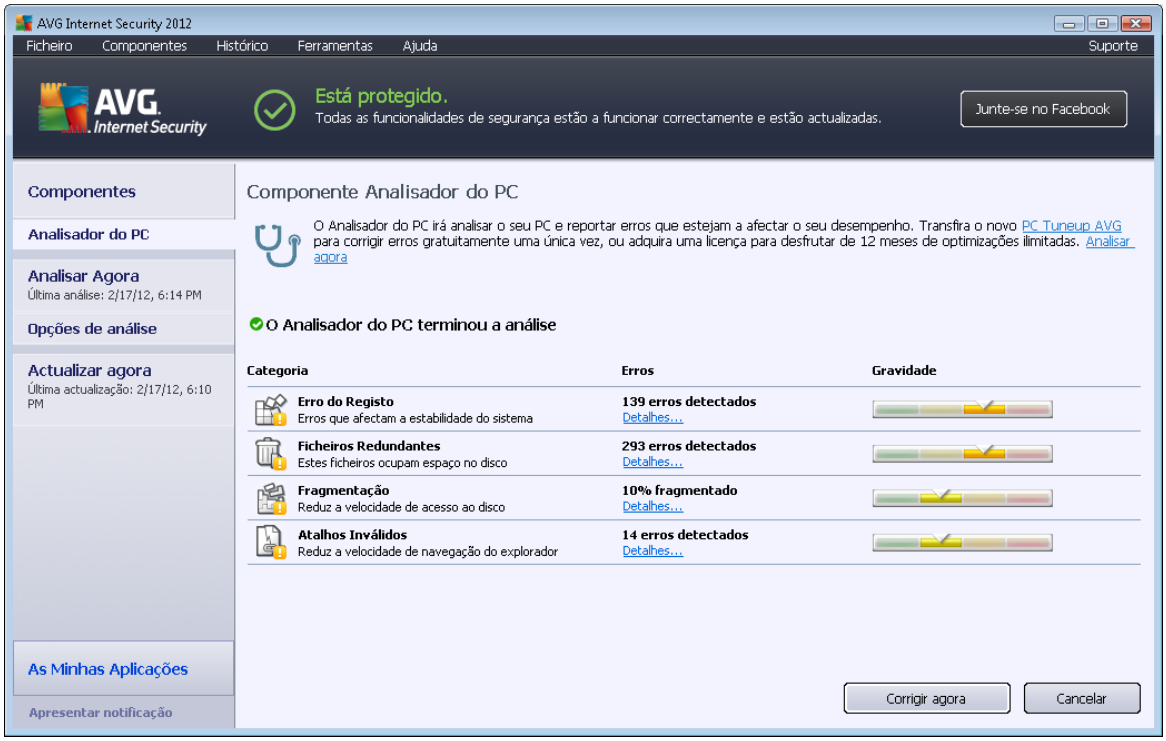
- ***Erros do Registo*** apresenta o número de erros no Registo do Windows. Uma vez que a correcção do Registo requer conhecimentos muito avançados, recomendamos que não o tente reparar autonomamente.

- ***Ficheiros Redundantes*** apresenta o número de ficheiros que provavelmente não estão a fazer nada no sistema. Normalmente, estes ficheiros são vários tipos de ficheiros temporários e ficheiros da Reciclagem.

- ***Fragmentação*** calcula a percentagem do seu disco rígido que está fragmentada, ou seja, usada prolongadamente, de tal forma que a maioria dos ficheiros está espalhada por várias secções do disco físico. Pode usar uma ferramenta de desfragmentação para corrigir esta situação.

- ***Atalhos Inválidos*** notifica-o de atalhos que já não funcionam, conduzem a localizações não existentes, etc.

Para iniciar a análise ao seu sistema, prima o botão ***Analisar agora***. Poderá, então, visualizar o progresso da análise e os resultados da mesma directamente na tabela:



A síntese dos resultados apresenta o número de problemas detectados no sistema (***Erros***) divididos consoante as categorias de teste respectivas. Os resultados da análise também serão apresentados graficamente num eixo, na coluna ***Gravidade***.

Botões de controlo

- ***Analisar agora*** (*apresentado antes do início da análise*) - prima este botão para iniciar imediatamente a análise do seu computador
- ***Corrigir agora*** (*apresentado quando a análise concluir*) - prima este botão para aceder ao website da AVG (http://www.avg.com/) numa página com informações detalhadas e actualizadas relativas ao componente ***Analisador do PC***
- ***Cancelar*** – prima este botão para parar a análise em execução, ou para regressar à interface do utilizador do AVG padrão (*síntese dos componentes*) quando a análise concluir

6.8. Protecção de Identidade

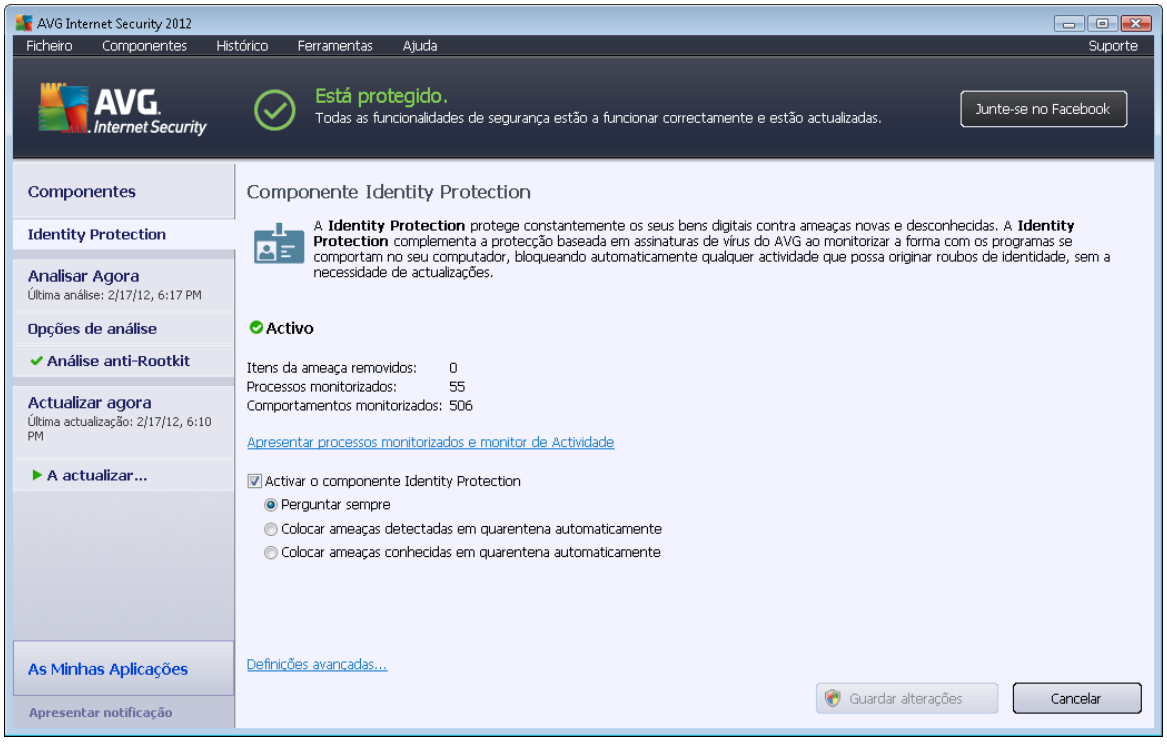
A Protecção de Identidade é um componente anti-malware que o protege de todos os tipos de malware (*spyware, bots, roubos de identidade, ...*) utilizando tecnologias comportamentais e proporciona protecção contra imediata contra novos vírus. ***A Protecção de Identidade*** destina-se a evitar que ladrões de identidade roubem as suas palavras-passe, detalhes de contas bancárias, números de cartões de crédito e outros valores digitais pessoais por meio de todos os tipos de software malicioso (*malware*) que atacam o seu PC. Assegura o funcionamento correcto de todos os programas em execução no seu computador ou na sua rede partilhada. ***A Protecção de Identidade*** identifica e bloqueia continuamente comportamentos suspeitos e protege o seu

computador contra todo o novo malware.

A Protecção de Identidade proporciona protecção em tempo real do seu computador contra ameaças novas e, inclusivamente, ameaças desconhecidas. Monitoriza todos os processos *(incluindo os ocultos)* e mais de 285 padrões de comportamento diferentes, podendo ainda determinar se algo malicioso está decurso no seu sistema. Desta forma, pode revelar ameaças ainda não descritas na base de dados de vírus. Sempre que um pedaço de código desconhecido chega um computador é imediatamente analisado em função de comportamento malicioso e rastreado. Se o ficheiro for considerado malicioso, a ***Protecção de Identidade*** remove o código para a Quarentena de Vírus e anula quaisquer alterações que tenham sido feitas ao sistema *(injecções de código, alterações ao registo, abertura de portas, etc.)*. Não é preciso iniciar uma análise para se manter protegido. A tecnologia é muito proactiva, raramente precisa de ser actualizada e está sempre de vigia.

A Protecção de Identidade é uma protecção complementar do Anti-Vírus. Recomendamos vivamente que mantenha ambos os componentes instalados para usufruir de uma protecção completa para o seu PC!

6.8.1. Interface da Protecção de Identidade



A interface da Protecção de Identidade disponibiliza uma breve descrição da funcionalidade básica do componente, o estado*(Activo)* e alguns dados estatísticos:

- ***Itens da ameaça removidos*** - apresenta o número de aplicações detectadas como sendo malware e removidas
- ***Processos monitorizados*** – número de aplicações actualmente em execução que estão a ser monitorizadas pela Protecção de Identidade

- ***Comportamentos monitorizados*** – número de acções específicas em execução nas aplicações monitorizadas

Abaixo encontra o link Apresentar processos monitorizados e monitor de actividade que o redirecciona para a interface do utilizador do componente Ferramentas do Sistema onde pode encontrar uma síntese detalhada de todos os processos monitorizados.

Definições básicas da Protecção de Identidade

Na parte inferior da janela, pode editar algumas funcionalidades básicas do componente:

- ***Activar a Protecção de Identidade*** - (*activado por predefinição*): marque para activar o componente Protecção de Identidade e para aceder a mais opções editáveis.

  Em alguns casos, a ***Protecção de Identidade*** pode reportar que um ficheiro legítimo é suspeito ou perigoso. Uma vez que a ***Protecção de Identidade*** detecta as ameaças com base no seu comportamento, isto pode acontecer se algum programa tentar monitorizar o clicar de teclas, instalar outros programas ou for instalado um novo controlador no computador. Como tal, queira seleccionar uma das seguintes opções para especificar o comportamento do componente ***Protecção de Identidade*** em situações de detecção de actividade suspeita:

  - ***Perguntar sempre*** - se uma aplicação for detectada como malware, ser-lhe-á perguntado se esta deve ser bloqueada (*esta opção está activada por predefinição e é recomendável que não a altere a menos que tenha uma razão válida para o fazer*)
  - ***Colocar ameaças detectadas em quarentena automaticamente*** - todas as aplicações detectadas como sendo malware serão bloqueadas automaticamente
  - ***Colocar ameaças conhecidas em quarentena automaticamente*** - só as aplicações que são indubitavelmente reconhecidas como malware serão bloqueadas

- ***Definições avançadas...*** – Clique na hiperligação para ser redireccionado para a janela correspondente nas Definições avançadas do **AVG Internet Security 2012**. Aí, pode editar a configuração do componente em pormenor. No entanto, tenha em atenção que a configuração predefinida de todos os componentes está definida de forma a que o **AVG Internet Security 2012** providencie um desempenho optimizado e máxima segurança. A menos que tenha uma razão válida para o fazer, recomendamos que mantenha a configuração predefinida!

Botões de controlo

Os botões de controlo disponíveis na interface da ***Protecção de Identidade*** são os seguintes:

- ***Guardar alterações*** – clique neste botão para guardar e aplicar quaisquer alterações efectuadas nesta janela
- ***Cancelar*** – clique neste botão para retroceder para a janela principal do AVG (*síntese de*

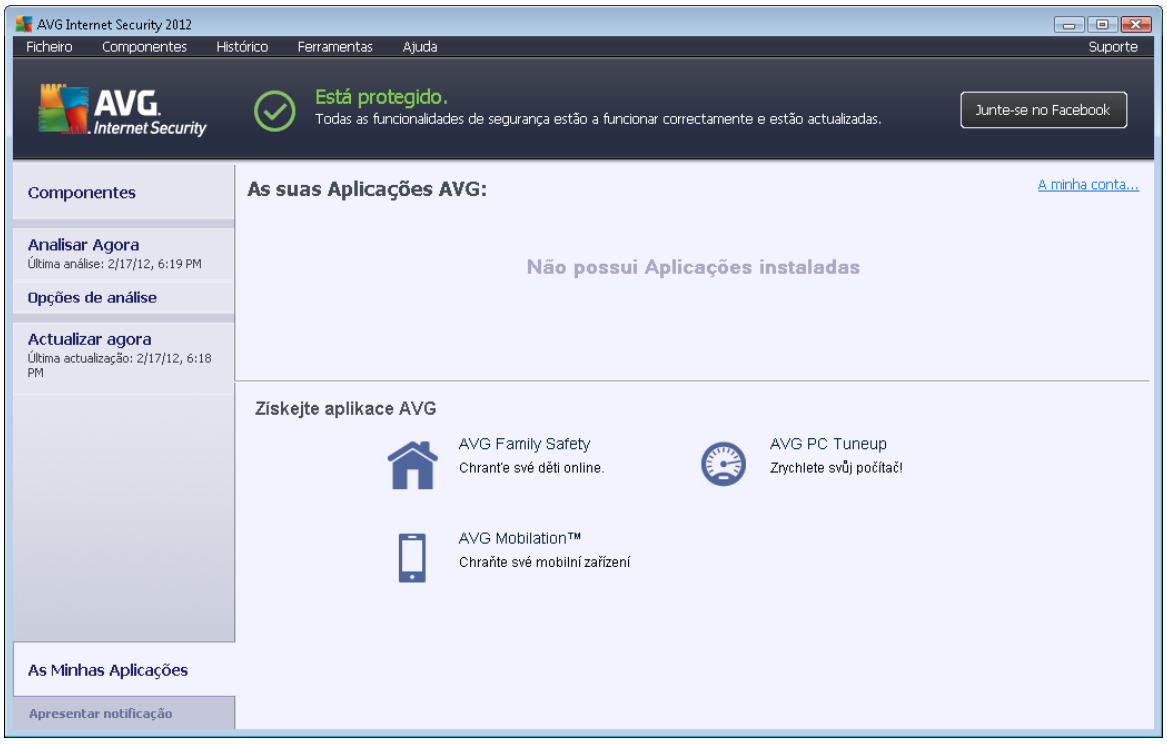
componentes)

6.9. Administração Remota

O componente ***Administração Remota*** só é apresentado na interface do utilizador do **AVG Internet Security 2012** se tiver instalado a versão Business Edition do seu produto *(para obter informações sobre a licença usada para a instalação, consulte o separador Versão da janela Informação que pode ser acedida através do item Suporte do menu)*. Para uma descrição detalhada das opções do componente e funcionalidade no sistema de Administração Remota AVG, queira consultar a documentação específica dedicada exclusivamente a este tópico. Esta documentação está disponível para transferência no website da AVG (http://www.avg.com/), na secção ***Centro de Suporte / Transferências / Documentação***.

7. As Minhas Aplicações

A janela ***As Minhas Aplicações*** *(acessível através do botão As Minhas Aplicações directamente na janela principal do AVG)* apresenta uma síntese de aplicações autónomas do AVG, tanto as que já estão instaladas no computador, como as que estão prontas para instalação opcional:



A janela de diálogo está dividida em duas secções:

- ***As suas Aplicações AVG*** – apresenta uma síntese de todas as aplicações autónomas do AVG que já estão instaladas no computador;
- ***Obter Aplicações do AVG*** – apresenta uma síntese de aplicações autónomas do AVG nas quais poderá ter algum interesse. Essas aplicações estão prontas para instalação. A oferta disponível varia dinamicamente consoante a sua licença, localização e outros critérios. Para obter informações detalhadas sobre estas aplicações, consulte o website do AVG (http://www.avg.com/).

Pode encontrar abaixo uma síntese de todas as aplicações disponíveis e uma breve explicação da funcionalidade de cada uma:

7.1. AVG Family Safety

A aplicação ***AVG Family Safety*** ajuda-o a proteger os seus filhos de websites, conteúdos multimédia e pesquisas online inapropriados, proporcionando-lhe relatórios relativos à actividade deles online. A ***AVG Family Safety*** utiliza tecnologia de pressão de teclas para monitorizar as actividades do seu filho em salas de chat e em sites de redes sociais. Se a aplicação detectar palavras, expressões ou linguagem conhecidas por serem utilizadas para vitimizar crianças online,

receberá de imediato uma notificação através de SMS ou e-mail. A aplicação permite-lhe definir o nível de protecção adequado para cada um dos seus filhos e monitorizá-los separadamente por meio de credenciais de início de sessão individuais.

Para informações detalhadas, queira visitar a página dedicada da AVG, onde também pode transferir o componente imediatamente. Para o efeito, pode usar a hiperligação AVG Family Safety na janela As Minhas Aplicações.

7.2. AVG LiveKive

O componente ***AVG LiveKive*** destina-se à cópia de segurança on-line de dados em servidores seguros. ***O AVG LiveKive*** faz cópias de segurança automáticas de todos os seus ficheiros, fotografias e músicas para um local seguro, permitindo que os partilhe com os seus familiares e amigos e aceda aos mesmos a partir de qualquer dispositivo com ligação à Internet, incluindo dispositivos iPhone e Android. O ***AVG LiveKive*** inclui as seguintes funcionalidades:

- Medidas de segurança caso o computador e/ou disco rígido sejam corrompidos
- Acesso aos seus dados a partir de qualquer dispositivo ligado à Internet
- Facilidade de organização
- Partilha com qualquer pessoa autorizada pelo utilizador

Para informações detalhadas queira visitar a página dedicada da AVG, onde também pode transferir o componente imediatamente. Para o efeito, pode usar a hiperligação AVG LiveKive na janela As Minhas Aplicações.

7.3. AVG Mobilation

O ***AVG Mobilation*** protege o seu telemóvel contra vírus e malware e proporciona também a capacidade de procurar o seu smartphone remotamente caso se separe do mesmo. O ***AVG Mobilation*** inclui as seguintes funcionalidades:

- A funcionalidade *Analisador de ficheiros* possibilita uma análise de segurança de ficheiros guardados em diferentes localizações;
- A funcionalidade *Eliminação de tarefas* permite parar uma aplicação no caso de o dispositivo ficar mais lento ou bloquear;
- A funcionalidade *Bloqueio de aplicações* permite bloquear e proteger uma ou mais aplicações contra utilização incorrecta, através de uma palavra-passe;
- A funcionalidade *Tuneup* recolhe vários parâmetros de sistema *(contador da bateria, capacidade de armazenamento, tamanho e localização da instalação de aplicações, etc.)* e junta-os numa única vista centralizada, para o ajudar o controlar o desempenho do sistema;
- A funcionalidade *Cópias de segurança de aplicações* permite fazer uma cópia de segurança das aplicações no cartão SD e restaurar as cópias mais tarde;

- A funcionalidade *Spam e Scam* permite assinalar mensagens SMS como spam e reportar websites fraudulentos;
- A *Limpeza de dados pessoais* permite apagar dados remotamente no caso de o telemóvel ser roubado;

- A funcionalidade *Navegação segura na Web* fornece monitorização em tempo real das páginas Web visitadas.

Para informações detalhadas queira visitar a página dedicada da AVG, onde também pode transferir o componente imediatamente. Para o efeito, pode usar a hiperligação AVG Mobilation na janela As Minhas Aplicações.

7.4. AVG PC Tuneup

A aplicação ***AVG PC Tuneup*** é uma avançada ferramenta para a análise e correcção minuciosas do sistema em termos de melhoria geral e maior velocidade do seu computador. O ***AVG PC Tuneup*** inclui as seguintes funcionalidades:

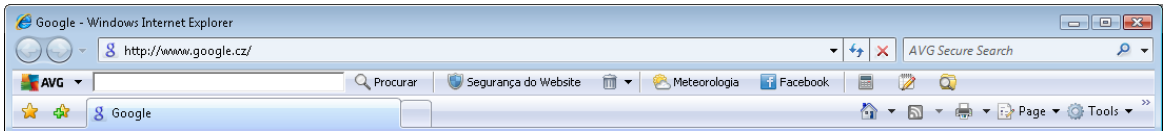
- *Limpeza do Disco* – Remoção de ficheiros inúteis que abrandam o computador.
- *Desfragmentação do Disco* – Desfragmentação das unidades de disco rígido e optimização do posicionamento dos ficheiros do sistema.
- *Limpeza do Registo* – Reparação dos erros do registo para aumentar a estabilidade do PC.
- *Desfragmentação do Registo* – Compactação do registo eliminando espaços vazios consumidores de memória.
- *Médico do Disco* – Detecção de sectores corrompidos, clusters perdidos e erros de directórios e respectiva correcção.
- *Optimização da Internet* – Adequação das definições gerais especificamente à sua ligação à Internet.
- *Eliminação de Rasto* – Remoção do histórico de utilização do computador e da Internet.
- *Limpeza Aprofundada do Disco* – Limpeza do espaço livre no disco para evitar a recuperação de dados sensíveis.
- *Destruição de Ficheiros* – Eliminação dos ficheiros seleccionados de forma a não poderem ser recuperados, num disco ou unidade USB.
- *Recuperação de Ficheiros* – Recuperação de ficheiros eliminados acidentalmente de discos, unidades USB ou câmaras.
- *Identificação de Ficheiros Duplicados* – Ajuda a encontrar e remover ficheiros duplicados para libertar espaço no disco.

- *Gestor de Serviços* – Desactivação de serviços desnecessários que abrandam o computador.
- *Gestor de Arranque* – Gestão dos programas que iniciam automaticamente aquando do arranque do Windows.
- *Gestor de Desinstalação* – Desinstalação completa de programas que já não são necessários.
- *Gestor de Optimizações* – Optimização de centenas de definições ocultas do Windows.
- *Gestor de Tarefas* – Listagem de todos os processos em execução, serviços e ficheiros bloqueados.
- *Explorador do Disco* – Apresentação dos ficheiros que ocupam mais espaço no computador.
- *Informações do Sistema* – Informações detalhadas sobre o hardware e software instalado.

Para informações detalhadas queira visitar a página dedicada da AVG, onde também pode transferir o componente imediatamente. Para o efeito, pode usar a hiperligação AVG PC Tuneup na janela As Minhas Aplicações.

8. Barra de Ferramentas de Segurança do AVG

A ***Barra de Ferramentas de Segurança AVG*** é uma ferramenta que coopera proximamente com o componente LinkScanner e o protege ao máximo enquanto navega na Internet. No **AVG Internet Security 2012**, a instalação da ***Barra de Ferramentas de Segurança AVG*** é opcional; durante o processo de instalação foi convidado a decidir a instalação do componente. A ***Barra de Ferramentas de Segurança AVG*** está disponível directamente no seu Browser. Presentemente, os browsers suportados são o Internet Explorer (*versão 6.0 e superiores*) e/ou Mozilla Firefox (*versão 3.0 e superiores*). Não são suportados outros browsers *(na eventualidade de utilizar um browser alternativo, ex. Avant Browser, pode ocorrer um comportamento inesperado)*.



A ***Barra de Ferramentas de Segurança AVG*** integra os seguintes itens:

- ***Logótipo AVG*** com o menu de opções:
  - ***Use o AVG Secure Search*** - Permite-lhe procurar directamente a partir da ***Barra de Ferramentas de Segurança AVG*** usando o componente ***AVG Secure Search***. Todos os resultados de procura são continuamente verificados pelo serviço Search-Shield e pode navegar em plena segurança.
  - ***Nível de Ameaça Actual*** - Abre a página do laboratório de vírus com uma apresentação gráfica do nível de ameaças actual na Internet.
  - ***AVG Threat Labs*** – Abre um website ***AVG Threat Lab*** específico *(em http://www.avgthreatlabs.com)*, no qual pode encontrar informações sobre a segurança e o nível actual de perigo de vários websites.
  - ***Ajuda da Barra de Ferramentas*** - Abre a ajuda online que abrange todas as funcionalidades da ***Barra de Ferramentas de Segurança AVG***.
  - ***Enviar um Comentário sobre o Produto*** - Abre uma página da Internet com um formulário que pode preencher para dar a sua opinião sobre a ***Barra de Ferramentas de Segurança AVG***.
  - ***Acerca de...*** - Abre uma nova janela com as informações sobre a versão da ***Barra de Ferramentas de Segurança AVG*** instalada.
- ***Campo de procura*** - Procure na Internet com a ***Barra de Ferramentas de Segurança AVG*** para estar completamente seguro e descansado, uma vez que todos os resultados de procura apresentados são cem por cento seguros. Introduza a palavra-chave ou frase no campo de procura e clique no botão ***Procurar*** *(ou Enter)*. Todos os resultados de procura são continuamente verificados pelo serviço Search-Shield *(parte do componente LinkScanner)*.
- ***Segurança do Website*** – Este botão abre uma nova janela que disponibiliza informações sobre o nível de ameaça actual (*Actualmente seguro*) da página que está a consultar. Esse resumo pode ser alargado e apresentado com detalhes completos de todas as actividades de segurança

relacionadas com a página dentro da janela do browser (*Ver o relatório completo*):

- ***Eliminar*** – O ícone de "caixote de lixo" disponibiliza um menu pendente no qual pode seleccionar se pretende eliminar informações relacionadas com a navegação, transferências ou formulários online, ou se pretende eliminar todo o histórico de navegação de uma só vez.

- ***Meteorologia*** – O botão abre uma nova janela que apresenta informações sobre a situação meteorológica actual da sua localização e a previsão para os próximos dois dias. Estas informações são actualizadas regularmente, a cada 3-6 horas. Na janela, pode alterar a localização pretendida manualmente e decidir se quer visualizar a informação da temperatura em graus Celsius ou Fahrenheit.

- ***Facebook*** – Estes botões permitem-lhe conectar-se à rede social Facebook directamente a partir da ***Barra de Ferramentas de Segurança AVG***.

- Botões de atalho para acesso rápido às seguintes aplicações: ***Calculadora***, ***Bloco de notas***, ***Explorador do Windows***.

9. AVG Do Not Track

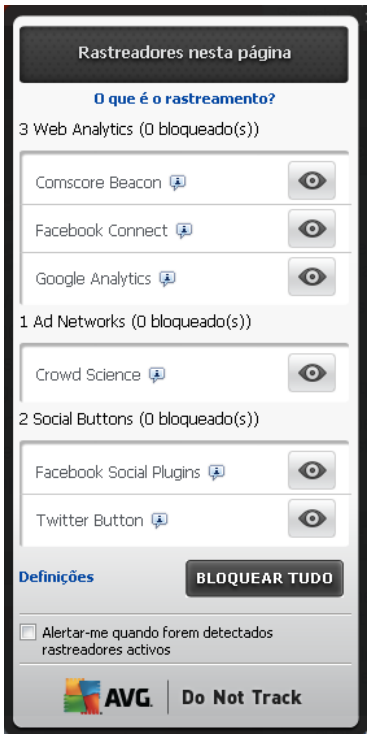
O AVG Do Not Track ajuda-o a identificar os websites que estão a recolher dados relativos às suas actividades online. Um ícone no browser mostra os websites ou os anunciantes que estão a recolher dados relativos à sua actividade e permite-lhe optar por permitir ou não permitir os serviços.

- ***O AVG Do Not Track*** fornece-lhe informações adicionais relativamente à política de privacidade de cada serviço, assim como uma ligação directa para optar por não ser incluído no serviço, se tal estiver disponível.
- Além disso, o ***AVG Do Not Track*** é compatível com o protocolo DNT do consórcio W3C, destinado a notificar automaticamente os sites de que não pretende ser rastreado. Essa notificação está activada por predefinição, mas pode ser alterada a qualquer altura.
- ***O AVG Do Not Track*** é disponibilizado de acordo com os seguintes termos e condições.
- ***O AVG Do Not Track*** encontra-se activado por predefinição, mas pode ser facilmente desactivado a qualquer altura. Pode encontrar instruções no artigo Desactivar a funcionalidade AVG Do Not Track da secção Perguntas Frequentes.
- Para obter mais informações sobre o ***AVG Do Not Track***, consulte o nosso website.

Actualmente, a funcionalidade ***AVG Do Not Track*** é compatível apenas com os browsers Mozilla Firefox, Chrome e Internet Explorer. *(No Internet Explorer, o ícone do AVG Do Not Track encontra-se no lado direito da barra de comandos. Se não conseguir visualizar o ícone do AVG Do Not Track com as predefinições do browser, certifique-se de que a barra de comandos está activada. Se mesmo assim não conseguir visualizar o ícone, arraste a barra de comandos para a esquerda para ver todos os ícones e botões disponíveis nessa barra de ferramentas.)*

9.1. Interface do AVG Do Not Track

Enquanto estiver online, o componente ***AVG Do Not Track*** avisa-o assim que for detectado qualquer tipo de actividade de recolha de dados. Será apresentada a seguinte janela:



Todos os serviços de recolha de dados detectados são apresentados por nome na síntese ***Rastreadores nesta página***. Existem três tipos de actividades de recolha de dados reconhecidas pelo ***AVG Do Not Track***:

- ***Web Analytics*** *(permitido por predefinição):* Serviços utilizados para melhorar o desempenho e a utilização do website respectivo. Nesta categoria incluem-se serviços como Google Analytics, Omniture ou Yahoo Analytics. É aconselhável não bloquear os serviços de estatísticas da Web, uma vez que o website pode não funcionar correctamente se esses serviços forem bloqueados.

- ***Social Buttons*** *(permitido por predefinição):* Elementos que se destinam a melhorar a experiência das redes sociais. Os botões de redes sociais são disponibilizados pelas redes sociais e incluídos no site visitado. Podem recolher dados relativos à actividade online do utilizador quando este tem sessão iniciada. Exemplos de botões de redes sociais: plug-ins sociais do Facebook, botão do Twitter, Google +1.

- ***Ad Networks*** *(alguns serviços são bloqueados por predefinição):* Serviços que recolhem ou partilham dados relativos à actividade online do utilizador em vários sites, directa ou indirectamente, para fornecer anúncios publicitários personalizados, ao contrário de anúncios baseados em conteúdos. O processo é determinado com base na política de privacidade de cada rede de anúncios, conforme disponível no respectivo website. Algumas redes de anúncios são bloqueadas por predefinição.

***Nota:** dependendo dos serviços em execução no website em segundo plano, algumas das três secções descritas acima podem não aparecer na janela AVG Do Not Track.*

A janela contém também duas hiperligações:

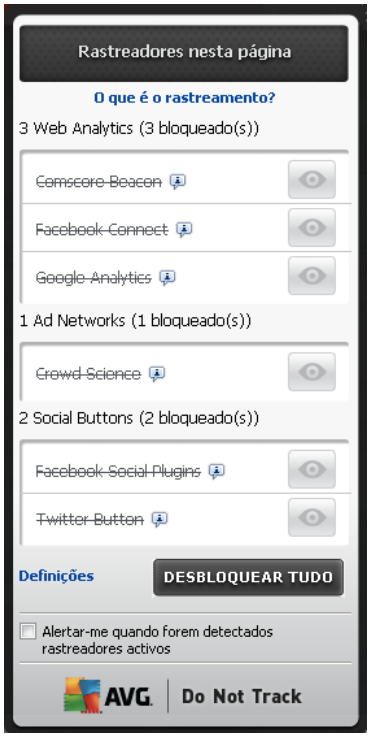
- ***O que é o rastreamento?*** - clique nesta ligação na parte superior da janela para ser reencaminhado para uma página Web dedicada que disponibiliza uma explicação detalhada dos princípios de rastreamento e uma descrição de tipos específicos de rastreamento.

- ***Definições*** - clique nesta ligação na parte inferior da janela para ser reencaminhado para uma página Web dedicada, na qual pode definir a configuração específica de vários parâmetros do ***AVG Do Not Track*** *(consulte o capítulo Definições do AVG Do Not Track para obter informações detalhadas)*

9.2. Informação relativa a processos de rastreamento

A lista de serviços de recolha de dados detectados apresenta apenas o nome do serviço específico. Para tomar uma decisão informada relativamente ao bloqueio ou permissão do serviço em questão, poderá ser necessário obter mais informações. Passe o cursor do rato por cima do respectivo item da lista. Aparece um balão informativo com dados detalhados sobre o serviço. Ficará a saber se o serviço recolhe dados pessoais ou outros dados disponíveis, se os seus dados estão a ser partilhados com terceiros e se os dados recolhidos estão a ser arquivados para outros usos possíveis.

Na parte inferior do balão informativo encontra-se a hiperligação ***Política de Privacidade***, que o reencaminha para o website que disponibiliza a política de privacidade do serviço detectado.

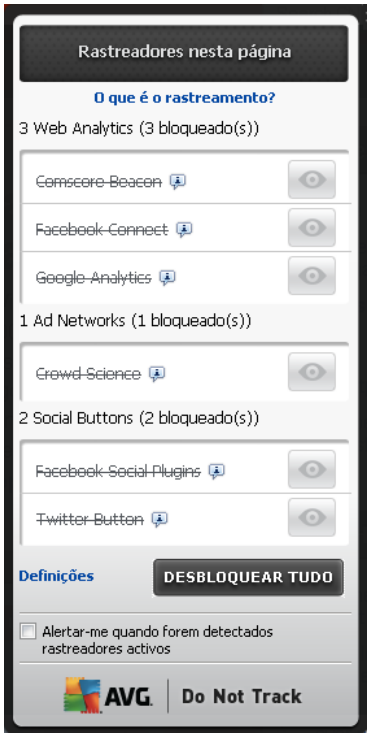


9.3. Bloquear processos de rastreamento

Com as listas de todos os serviços Ad Networks / Social Buttons / Web Analytics, passa a dispor da possibilidade de controlar os serviços que devem ser bloqueados. Dispõe de duas opções:

- ***Bloquear tudo*** - Clique neste botão, localizado na parte inferior da janela, para informar o componente de que não pretende qualquer tipo de actividade de recolha de dados. *(No entanto, tenha em atenção que essa acção pode prejudicar a funcionalidade da página Web que tem o serviço em execução!)*

-  - Se não quiser bloquear todos os serviços detectados de uma só vez, pode especificar a permissão ou o bloqueio de um serviço individualmente. Pode permitir a execução de alguns dos sistemas detectados *(por exemplo, Web Analytics):* esses sistemas utilizam os dados recolhidos para optimização do respectivo website, o que poderá ajudar a melhorar o ambiente de Internet comum a todos os utilizadores. No entanto, poderá também bloquear as actividades de recolha de dados de todos os processos classificados como Ad Networks. Basta clicar no ícone  junto ao respectivo serviço para bloquear a recolha de dados *(o nome do processo fica riscado)* ou para voltar a permitir a recolha de dados.

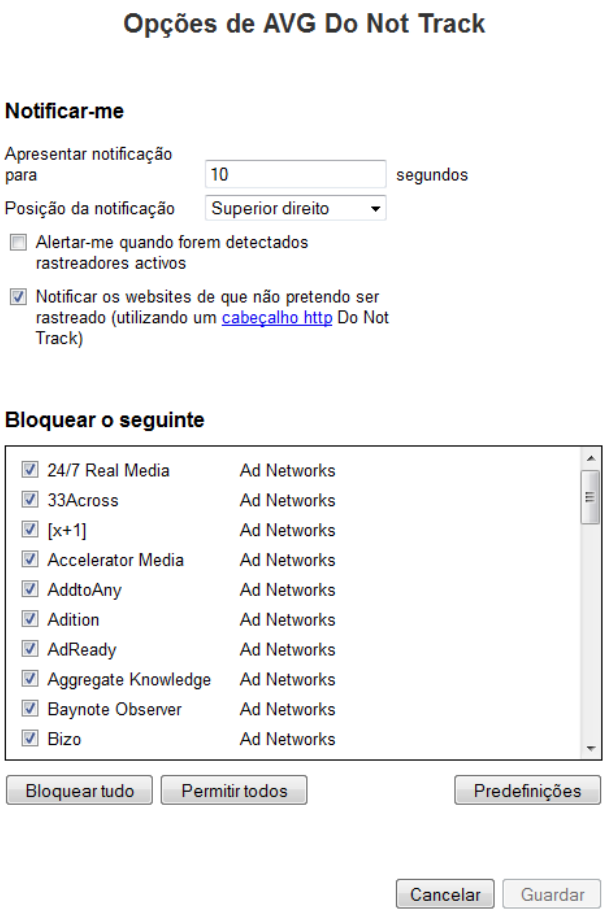


9.4. Definições do AVG Do Not Track

Na janela ***AVG Do Not Track***, existe apenas uma opção de configuração: na parte inferior da janela encontra-se a caixa de verificação ***Alertar-me quando forem detectados rastreadores activos***. Por predefinição, este item não se encontra seleccionado. Assinale a caixa de verificação para confirmar que pretende ser avisado sempre que aceder a uma página Web que contenha um novo serviço de

recolha de dados que ainda não foi bloqueado. Se a caixa estiver assinalada, a janela de notificação aparece no ecrã quando o ***AVG Do Not Track*** detectar um novo serviço de recolha de dados na página que está a consultar. Caso contrário, só notará que um serviço foi detectado quando o ícone do ***AVG Do Not Track*** *(localizado na barra de comandos do browser)* mudar de cor, de verde para amarelo.

No entanto, na parte inferior da janela ***AVG Do Not Track***, pode encontrar a ligação ***Definições***. Clique na ligação para ser reencaminhado para uma página Web dedicada, na qual pode especificar ***Opções de AVG Do Not Track*** detalhadas:



- ***Posição da notificação*** *(por predefinição, Superior direito)* - Abra o menu pendente para especificar a posição na qual pretende que a janela ***AVG Do Not Track*** apareça no monitor.

- ***Apresentar notificação para*** *(por predefinição, 10)* - Neste campo deve escolher o período de tempo *(em segundos)* durante o qual pretende ver a notificação do ***AVG Do Not Track*** no ecrã. Pode especificar um número entre 0 e 60 segundos *(se escolher 0, a notificação não aparece no ecrã)*.

- ***Alertar-me quando forem detectados rastreadores activos*** *(desactivado por*

predefinição) - Assinale a caixa de verificação para confirmar que pretende ser avisado sempre que aceder a uma página Web que contenha um serviço de recolha de dados que ainda não foi bloqueado. Se a caixa estiver assinalada, a janela de notificação aparece no ecrã quando o ***AVG Do Not Track*** detectar um novo serviço de recolha de dados na página que está a consultar. Caso contrário, só notará que um serviço foi detectado quando o ícone do ***AVG Do Not Track*** *(localizado na barra de comandos do browser)* mudar de cor, de verde para amarelo.

- ***Notificar os websites de que não pretendo ser rastreado*** *(activado por predefinição)* - Mantenha esta opção assinalada para confirmar que pretende que o ***AVG Do Not Track*** informe o fornecedor de um serviço de recolha de dados detectado de que não pretende ser rastreado.

- ***Bloquear o seguinte*** *(todos os serviços de recolha de dados listados são permitidos por predefinição)* - Nesta secção pode encontrar uma caixa com uma lista de serviços de recolha de dados conhecidos, que podem ser classificados como Ad Networks. Por predefinição, o ***AVG Do Not Track*** bloqueia determinados serviços Ad Networks automaticamente, ficando depois ao critério do utilizador bloquear ou manter a permissão dos restantes. Para tal, basta clicar no botão ***Bloquear tudo*** que se encontra por baixo da lista.

Os botões de controlo disponíveis na página ***Opções de AVG Do Not Track*** são os seguintes:

- ***Bloquear tudo*** – clique neste botão para bloquear de uma só vez todos os serviços listados na caixa acima que sejam classificados como Ad Networks;

- ***Permitir todos*** – clique neste botão para desbloquear de uma só vez todos os serviços listados na caixa acima que foram bloqueados anteriormente e classificados como Ad Networks;

- ***Predefinições*** – clique neste botão para anular todas as definições personalizadas e voltar à configuração predefinida;

- ***Guardar*** – clique neste botão para aplicar e guardar toda a configuração especificada;

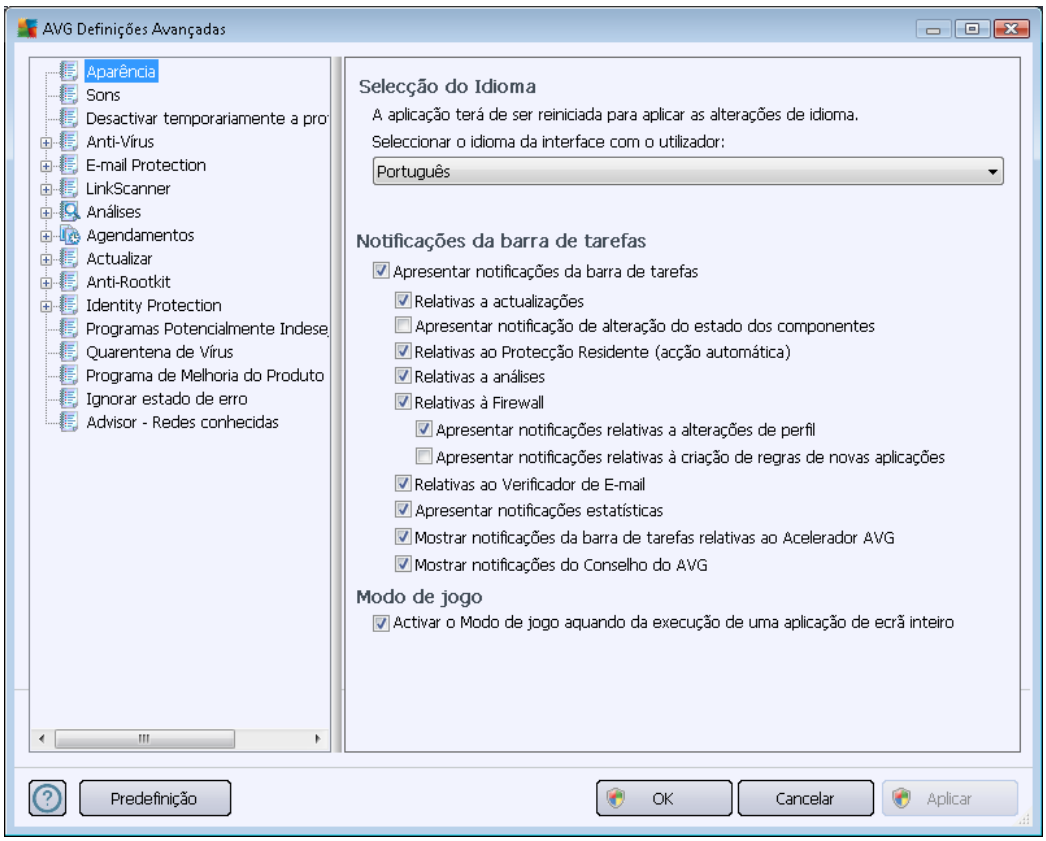
- ***Cancelar*** – clique neste botão para cancelar todas as definições especificadas anteriormente.

10. Definições Avançadas do AVG

A janela de configuração avançada do **AVG Internet Security 2012** abre numa nova janela com a identificação ***Definições Avançadas do AVG***. A janela está dividida em duas secções: a parte esquerda disponibiliza uma navegação esquematizada em árvore às opções de configuração do programa. Seleccione o componente ao qual pretende alterar a configuração (*ou a parte especifica deste*) para abrir a janela de edição na janela na secção do lado direito.

10.1. Aparência

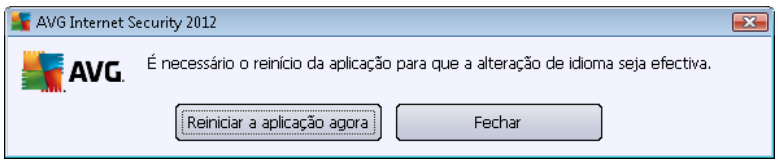
O primeiro item da árvore de navegação, ***Aparência***, refere-se às definições gerais da Interface do utilizador do **AVG Internet Security 2012** e disponibiliza algumas opções básicas do comportamento da aplicação:



Selecção do Idioma

Na secção ***Selecção do idioma*** pode escolher o idioma pretendido a partir do menu de opções. O idioma seleccionado será então usado para toda a interface do utilizador do **AVG Internet Security 2012**. O menu de opções só apresenta os idiomas que o utilizador tiver seleccionado previamente para instalação durante o processo de instalação (*consulte o capítulo Opções personalizadas*) e o idioma Inglês (*que é sempre instalado por predefinição*). Para concluir a alteração do idioma do **AVG Internet Security 2012** , é necessário reiniciar a aplicação. Proceda do seguinte modo:

- No menu de opções, seleccione o idioma pretendido para a aplicação
- Confirme a selecção clicando no botão ***Aplicar*** *(canto inferior direito da janela)*
- Clique no botão ***OK*** para confirmar
- É apresentada uma nova janela a informá-lo de que para alterar o idioma da aplicação, é necessário reiniciar o seu **AVG Internet Security 2012**
- Clique no botão ***Reiniciar a aplicação agora*** para concordar com a reinicialização do programa e aguarde uns momentos para que a alteração de idioma seja efectiva:



Notificações da barra de tarefas

Nesta secção pode suprimir a apresentação de notificações da barra de tarefas relativas ao estado do **AVG Internet Security 2012**. Por predefinição, as notificações do sistema estão definidas como permitidas. Recomendamos vivamente que mantenha esta configuração! As notificações do sistema informam-no, por exemplo, sobre a execução de análises ou do processo de actualização, ou alterações do estado de um componente do **AVG Internet Security 2012**. Estas informações são sempre importantes!

No entanto, se, por alguma razão, decidir que não quer que estas notificações sejam apresentadas, ou que só quer visualizar algumas notificações *(relacionadas com um componente específico do AVG Internet Security 2012*), pode definir e especificar as suas preferências marcando/ desmarcando as seguintes opções:

- ***Apresentar notificações na barra de tarefas*** *(activado por predefinição)* - Por predefinição, todas as notificações são apresentadas. Desmarque este item para desactivar por completo a apresentação das notificações do sistema. Quando activado, pode ainda especificar quais as notificações específicas que devem ser apresentadas.
    - ***Apresentar notificações da Barra de Tarefas relativas a actualizações*** *(activado por predefinição)* - Decida se as informações relativas ao início, progresso e conclusão da actualização do **AVG Internet Security 2012** deverão ser apresentadas.
    - ***Apresentar notificações relativas a alterações de estado dos componentes*** *(activado por predefinição)* – decida se as informações relativas à actividade/ inactividade dos componentes , ou os seus possíveis problemas deverão ser apresentadas. Ao notificar do estado de erro de um componente, esta opção é equivalente à função informativa do ícone da Barra de Tarefas do sistema que notifica de problemas em qualquer componente do **AVG Internet Security 2012**.
    - ***Apresentar notificações da Barra de Tarefas relativas à Protecção Residente***

(acção automática)*(activado por predefinição)* – Decida se as informações relativas aos processos de salvaguarda, cópia e abertura de ficheiros devem ser apresentadas ou ocultas (*esta configuração só é possível se a opção de Restauro automático da Protecção Residente estiver activada*).

- ***Apresentar notificações da Barra de Tarefas relativas a análises*** *(activado por predefinição)* – Decida se as informações relativas ao início automático da análise agendada, o seu progresso e resultados deverão ser apresentadas.

- ***Apresentar notificações da Barra de Tarefas relativas à Firewall*** *(activado por predefinição)* – Decida se as informações relativas ao estado e processos da Firewall, ex. avisos de activação/desactivação do componente, possível bloqueio de tráfego, etc., deverão ser apresentadas. Este item apresenta mais duas opções de selecção específicas *(para uma explicação detalhada de cada uma delas, queira consultar o capítulo Firewall deste documento*:

  - ***Apresentar notificações relativas a alterações de perfil*** *(activado por predefinição)* – Notifica-o sobre alterações automáticas dos perfis da Firewall.

  - ***Apresentar notificações relativas a regras de novas aplicações criadas*** *(desactivado por predefinição)* – Notifica-o sobre a criação automática de regras da Firewall para novas aplicações com base numa lista de aplicações seguras.

- ***Apresentar notificações da Barra de Tarefas relativas ao Verificador de E-mail*** *(activado por predefinição)* – Decida se as informações relativas à execução da análise de todas as mensagens de e-mail de entrada e a enviar deverão ser apresentadas.

- ***Apresentar notificações estatísticas*** *(activado por predefinição)* - Mantenha a opção marcada para permitir a apresentação de notificações estatísticas na barra de tarefas.

- ***Mostrar notificações da barra de tarefas relativas ao Acelerador AVG*** *(activado por predefinição)* – Decida se as informações relativas às actividades do ***Acelerador AVG*** deverão ser apresentadas. O ***Acelerador AVG*** é um serviço que permite uma reprodução de vídeos online mais fluida e facilita as transferências.

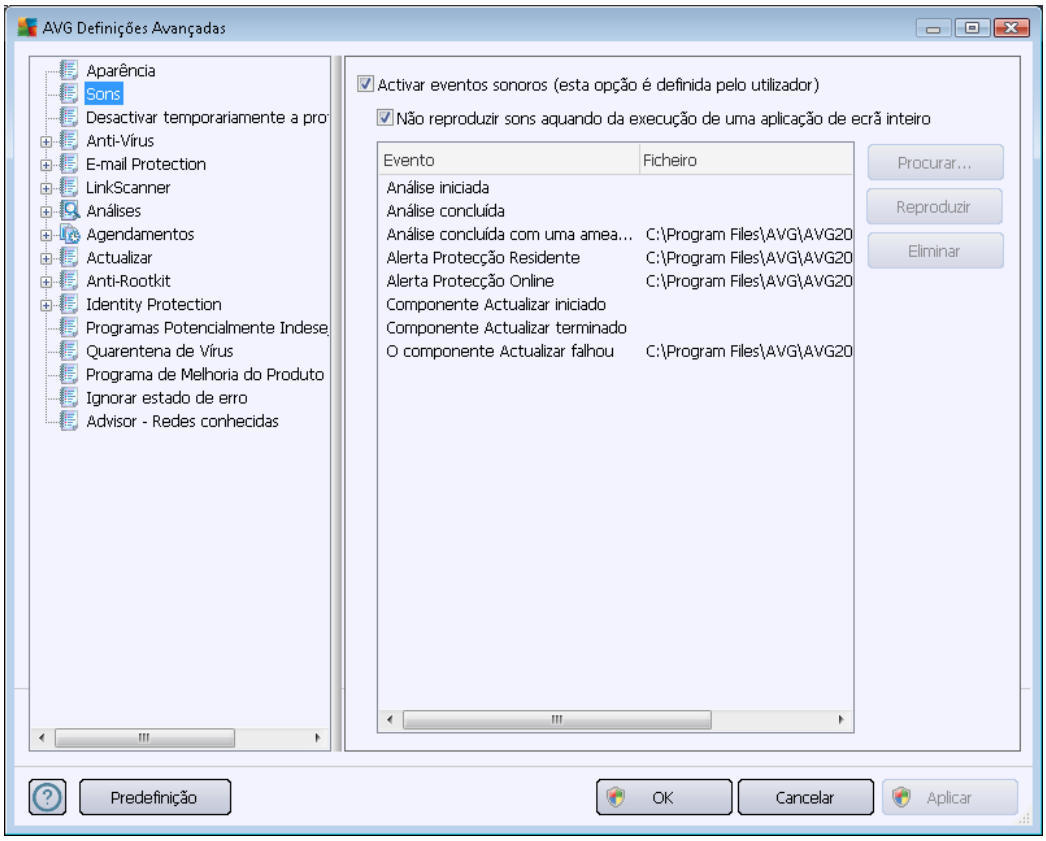
- ***Apresentar notificações de desempenho do AVG Advice*** *(activado por predefinição)* - O ***AVG Advice*** vigia o desempenho dos browsers suportados *(Internet Explorer, Chrome, Firefox, Opera e Safari)* e informa-o na eventualidade de o seu browser exceder a quantidade de memória recomendada. Se isso acontecer, o desempenho do seu computador pode diminuir significativamente e é aconselhável reiniciar o browser para acelerar os processos. Deixe o item ***Apresentar notificações de desempenho do AVG Advice*** activado para ser informado.

Modo de Jogo

Esta função destina-se a aplicações de ecrã inteiro em que a apresentação de janelas de informação do AVG (*apresentadas, por exemplo, quando uma análise agendada é iniciada*) seria incómoda (*poderiam minimizar a aplicação ou corromper os seus gráficos*). Para evitar esta situação, mantenha a caixa de verificação da opção ***Activar o modo de jogo aquando da execução de uma aplicação de ecrã inteiro*** marcada (*predefinição*).

10.2. Sons

Na janela ***Sons*** pode especificar se quer ser informado de acções específicas do **AVG Internet Security 2012** por meio de uma notificação sonora:



As definições só são válidas para a conta de utilizador actual; ou seja, cada utilizador do computador pode ter as suas próprias definições de sons. Se quiser permitir a notificação sonora, mantenha a opção ***Activar eventos sonoros*** marcada (*a opção está activada por predefinição*) para activar a lista de todas as acções relevantes. Além disso, pode querer marcar a opção ***Não reproduzir sons aquando da execução de uma aplicação de ecrã inteiro*** para suprimir a notificação sonora em situações em que o evento possa ser perturbador *(consulte também a secção Modo de Jogo no capítulo Definições avançadas/Aparência deste documento)*.

Botões de controlo

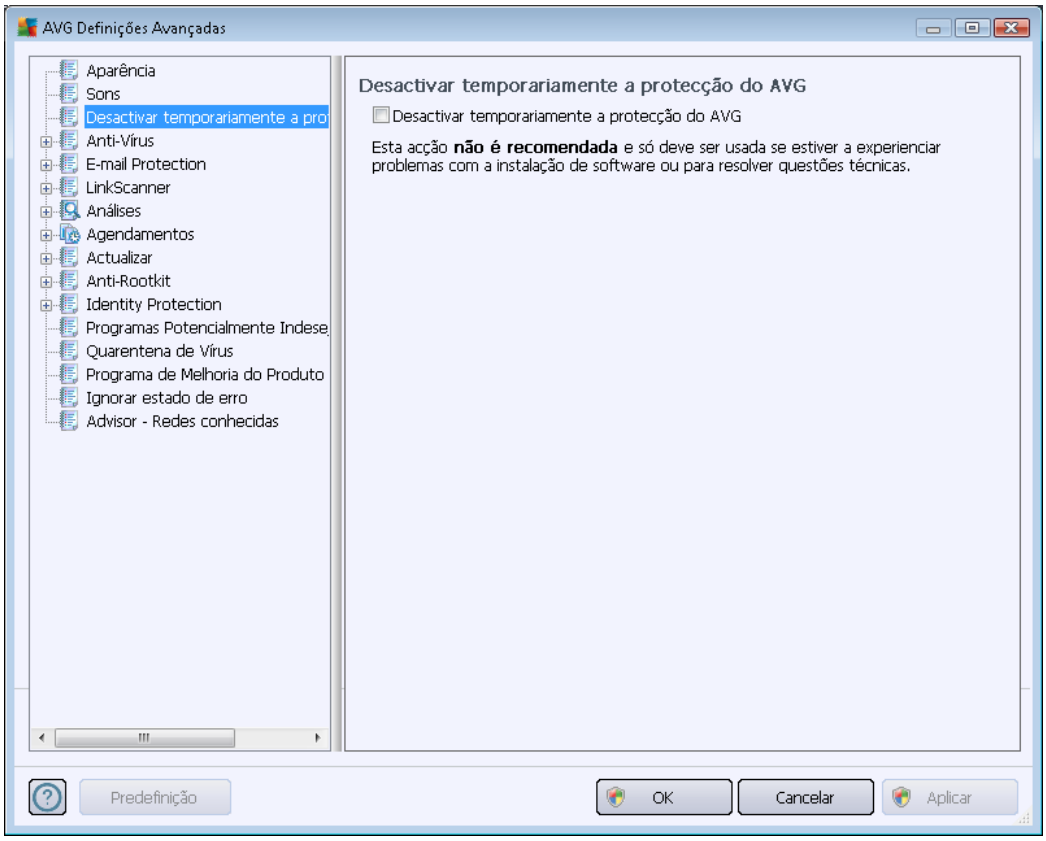
- ***Procurar*** – Tendo seleccionado o respectivo evento da lista, use o botão ***Procurar*** para procurar no seu disco o ficheiro de som que pretende atribuir ao evento. *(Tenha em atenção que só são suportados sons no formato *.wav!)*
- ***Reproduzir*** – Para ouvir o som seleccionado, realce o evento na lista e prima o botão ***Reproduzir***.
- ***Eliminar*** – Use o botão ***Eliminar para remover o som atribuído a um evento***

específico.

10.3. Desactivar temporariamente a protecção do AVG

Na janela ***Desactivar temporariamente a protecção do AVG*** existe a possibilidade de desactivar toda a protecção oferecida pelo **AVG Internet Security 2012** de uma só vez.

Tenha em atenção que não deverá usar esta opção a menos que seja absolutamente necessário!



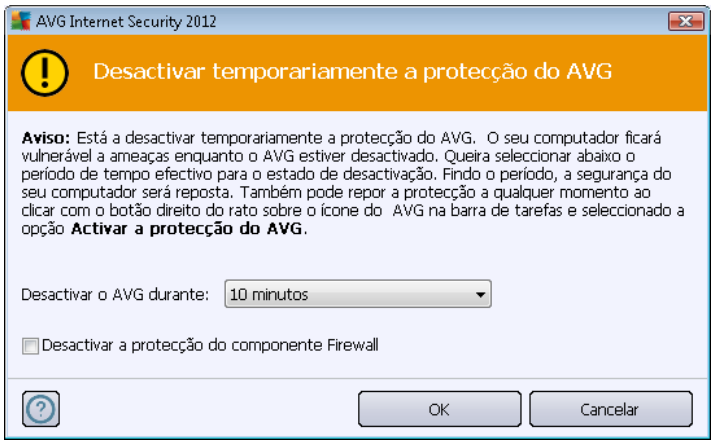
Na maioria dos casos, ***não é necessário*** desactivar o **AVG Internet Security 2012** antes de instalar novo software ou controladores, mesmo que o instalador ou o assistente do software sugiram que os programas e aplicações em execução devam ser encerrados primeiro para garantir que não ocorrem interrupções durante o processo de instalação. Caso se depare com problemas durante a instalação, experimente desactivar o componente Protecção Residente (*Activar a Protecção Residente*) primeiro. Se tiver de desactivar o **AVG Internet Security 2012** temporariamente, deverá voltar a activá-lo assim que terminar. Se estiver conectado à Internet ou a uma rede durante o período de desactivação do software antivírus, o seu computador estará vulnerável a ataques.

Como desactivar a protecção do AVG

- Marque a caixa ***Desactivar temporariamente a protecção do AVG*** e confirme a sua

opção clicando no botão ***Aplicar***

- Na janela ***Desactivar temporariamente a protecção do AVG*** especifique a duração da desactivação do **AVG Internet Security 2012**. Por predefinição, a protecção será desactivada durante 10 minutos, o que deve ser suficiente para qualquer tarefa comum como a instalação de novo software, etc. Tenha em atenção que o limite de tempo inicial pode ser definido para 15 minutos e não pode ser substituído por um valor personalizado pelo utilizador por razões de segurança. Após o período de tempo, todos os componentes desactivados serão automaticamente activados de novo.

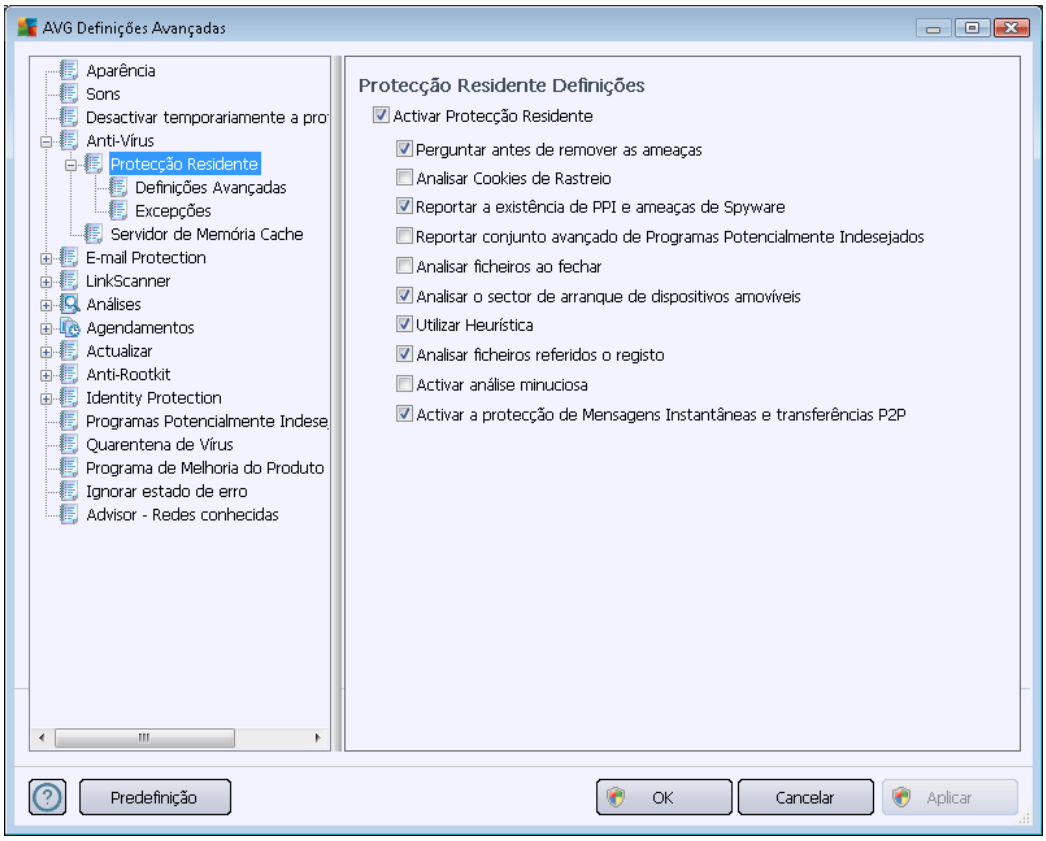


10.4. Anti-Vírus

O componente ***Anti-Vírus*** protege o seu computador continuamente contra todos os tipos de vírus e spyware conhecidos *(incluindo o chamado malware latente ou não-activo, ou seja, malware que foi transferido mas que ainda não está activado)*.

10.4.1. Protecção Residente

A Protecção Residente efectua a protecção activa dos ficheiros e pastas contra vírus, spyware e outro malware.



Na janela ***Definições da Protecção Residente*** pode activar ou desactivar a Protecção Residente completamente ao marcar/desmarcar o item ***Activar Protecção Residente*** (*esta opção está activada por predefinição*). Além disso, pode seleccionar as funcionalidades da protecção residente que deverão ser activadas:

- ***Perguntar antes de remover as ameaças*** (*activado por predefinição*) – Seleccione para garantir que a Protecção Residente não realiza qualquer acção automaticamente; em vez disso, apresenta uma janela com a descrição da ameaça detectada, permitindo-lhe decidir o que pretende fazer. Se deixar a caixa desmarcada, o **AVG Internet Security 2012** removerá automaticamente a infecção e, se tal não for possível, o objecto será movido para a Quarentena de Vírus.

- ***Analisar a Existência de Cookies de Rastreio*** (*desactivado por predefinição*) – Este parâmetro define que as cookies devem ser detectadas durante a análise. (*as cookies HTTP são utilizadas para autenticar, rastrear e manter informações específicas acerca dos utilizadores, tais como preferências de sítios ou os conteúdos dos seus carrinhos de compras electrónicos*).

- ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** (*activado por predefinição*) – Marque para activar o componente Anti-Spyware e analisar a existência de

spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado por predefinição*) – Marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

- ***Analisar ficheiros ao fechar*** (*desactivado por predefinição*) – Análise ao fechar os ficheiros que assegura que o AVG analisa objectos activos (ex. aplicações, documentos...) quando estes são abertos, e também quando estes são fechados; esta funcionalidade ajuda a proteger o seu computador contra alguns tipos de vírus sofisticados.

- ***Analisar o sector de arranque de discos amovíveis*** (*activado por predefinição*)

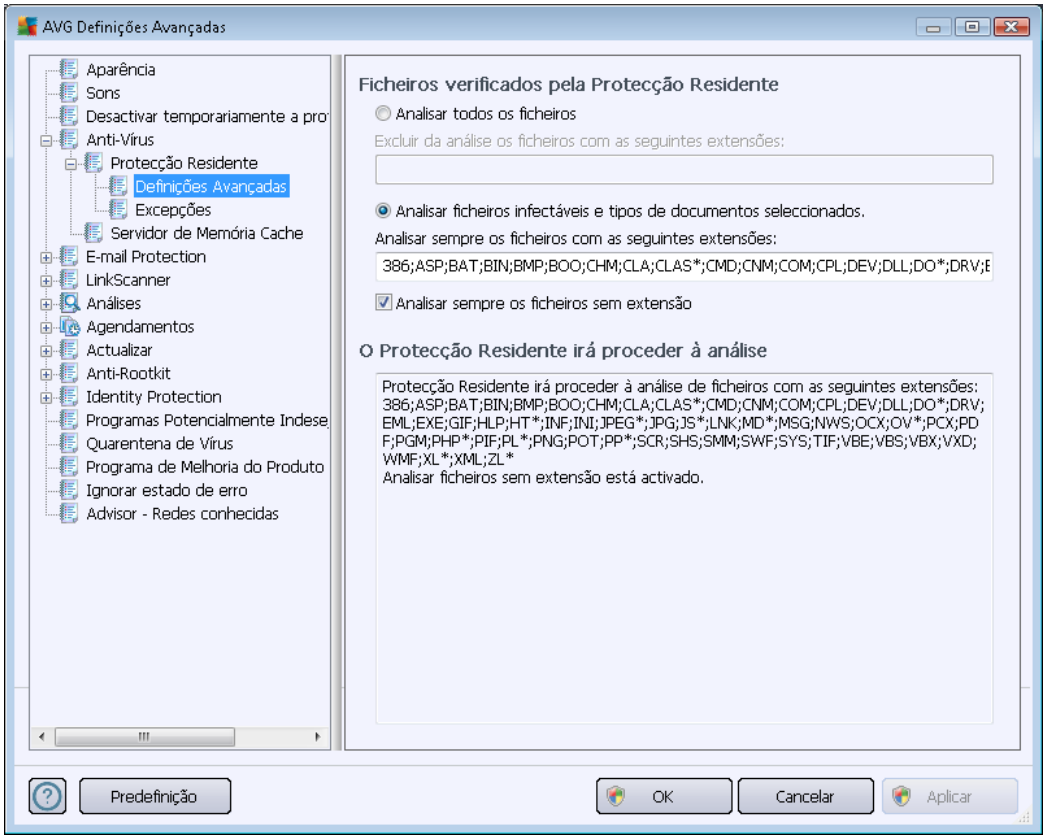
- ***Utilizar heurística*** - (*activado por predefinição*) – A análise heurística será utilizada para detecção (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*).

- ***Analisar ficheiros referidos no registo***(*activado por predefinição*) – Este parâmetro define que o AVG irá analisar todos os ficheiros executáveis adicionados ao registo de arranque para evitar a execução de infecções conhecidas aquando do próximo arranque do computador.

- ***Activar análise minuciosa*** (*desactivado por predefinição*) -Em situações específicas (*num estado extremo de emergência*) pode marcar esta opção para activar os mais rigorosos algoritmos que irão verificar aprofundadamente a existência de objectos perigosos. Tenha em consideração que este método é bastante demorado.

- ***Activar a protecção de Mensagens Instantâneas e transferências P2P*** (*activado por predefinição*) - Marque este item se quiser que as comunicações das mensagens instantâneas (*ex. ICQ, MSN Messenger, ...*) e as transferências P2P sejam analisadas pela existência de vírus.

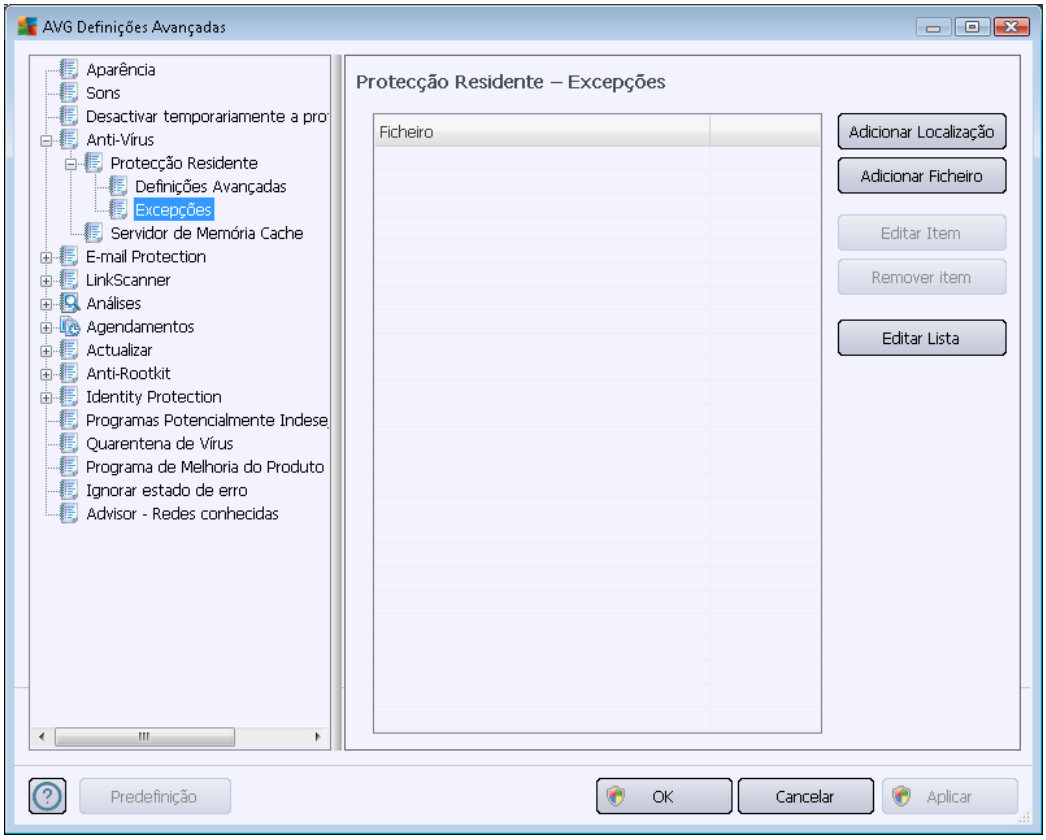
Na janela ***Ficheiros verificados pela Protecção Residente*** é possível configurar os ficheiros a analisar (*por extensões específicas*):



Marque a caixa respectiva para decidir se pretende ***Analisar todos os ficheiros*** ou apenas ***Analisar ficheiros infectáveis e os tipos de documentos seleccionados***. Se tiver optado pela última opção, pode ainda especificar uma lista de extensões definidora dos ficheiros que devem ser excluídos da análise, e também uma lista de extensões de ficheiros definidora de ficheiros que devem ser analisados em qualquer situação.

Marque a caixa ***Analisar sempre os ficheiros sem extensão*** (*activado por predefinição*) para assegurar a análise de ficheiros sem extensão e formato desconhecido pela Protecção Residente. Recomendamos que mantenha esta funcionalidade activada, uma vez que os ficheiros sem extensão são suspeitos.

A secção abaixo, com o nome ***A Protecção Residente analisará***, resume as definições actuais ao apresentar uma síntese detalhada dos ficheiros que a ***Protecção Residente*** efectivamente analisará.



A janela ***Protecção Residente – Excepções*** oferece a possibilidade de definir ficheiros e/ou pastas que devem ser excluídos da análise da ***Protecção Residente*** .

Se não for estritamente necessário, recomenda-se vivamente que não exclua quaisquer itens!

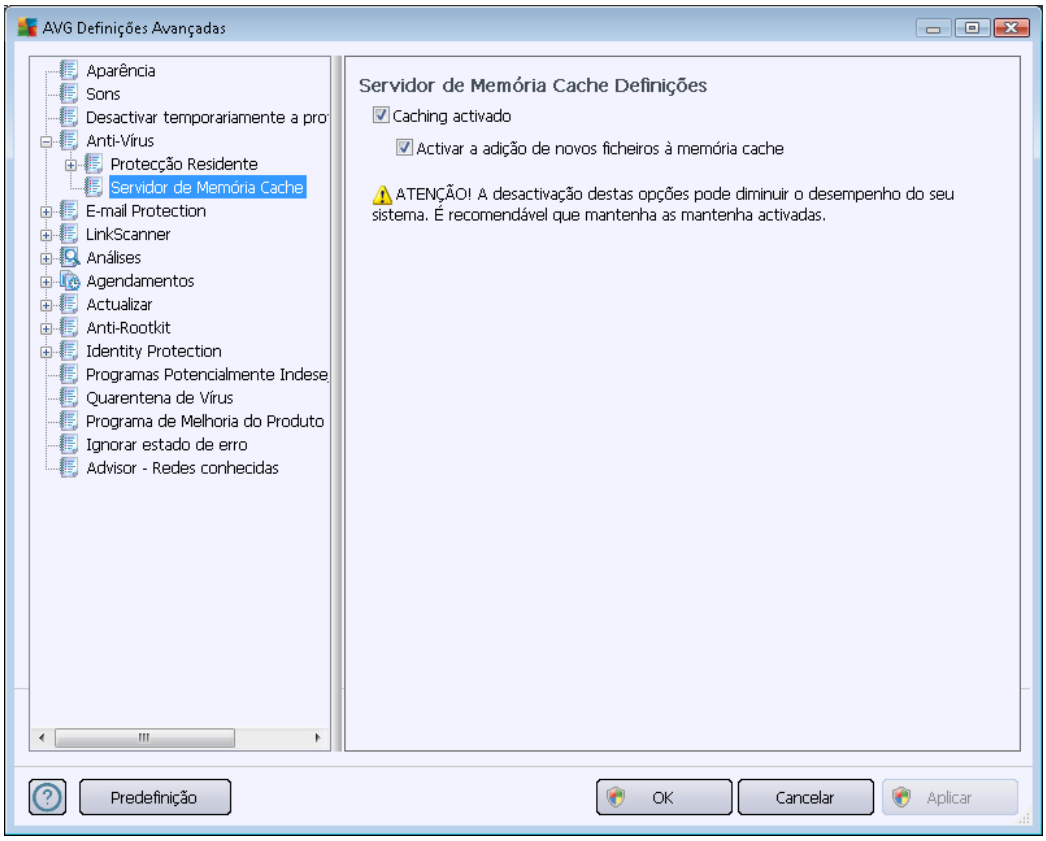
Botões de controlo

A janela inclui os seguintes botões de controlo:

- ***Adicionar localização*** – permite especificar directórios a excluir da análise, seleccionando-os individualmente a partir da árvore de navegação do disco local
- ***Adicionar Ficheiro*** – permite especificar ficheiros a excluir da análise, seleccionando-os individualmente a partir da árvore de navegação do disco local
- ***Editar Item*** – permite editar o caminho especificado para um ficheiro ou pasta seleccionado
- ***Remover Item*** – permite eliminar o caminho para um item seleccionado na lista
- ***Editar lista*** – permite-lhe editar toda a lista de excepções definidas numa nova janela que se assemelha a um editor de texto tradicional

10.4.2. Servidor de Memória Cache

A janela das ***Definições do Servidor de Memória Cache*** é referente ao processo do servidor de memória cache destinado a acelerar todos os tipos de análises do **AVG Internet Security 2012**:



O servidor de memória cache recolhe e guarda as informações relativas a ficheiros fiáveis (*um ficheiro é considerado fiável se estiver assinado com uma assinatura digital emitida por uma fonte fiável*). Estes ficheiros são então automaticamente considerados seguros e não precisam de voltar a ser analisados; como tal, estes ficheiros são ignorados durante a análise.

A janela das ***Definições do Servidor de Memória Cache*** apresenta as seguintes opções de configuração:

- ***Caching activado*** (*activado por predefinição*) – desmarque a caixa para desactivar o ***Servidor de Memória Cache*** e limpar a memória cache. Tenha em atenção que a análise pode ficar mais morosa, assim como o desempenho do computador, uma vez que todos os ficheiros em utilização serão analisados pela existência de vírus e spyware.

- ***Activar a adição de novos ficheiros à memória cache*** (*activada por predefinição*) – desmarque a caixa para parar a adição de mais ficheiros à memória cache. Quaisquer ficheiros já colocados na memória cache serão aí mantidos e utilizados até a acção de caching ser desactivada por completo, ou até à próxima actualização da base de dados de vírus.

A menos que tenha uma boa razão para desactivar o servidor de memória cache,

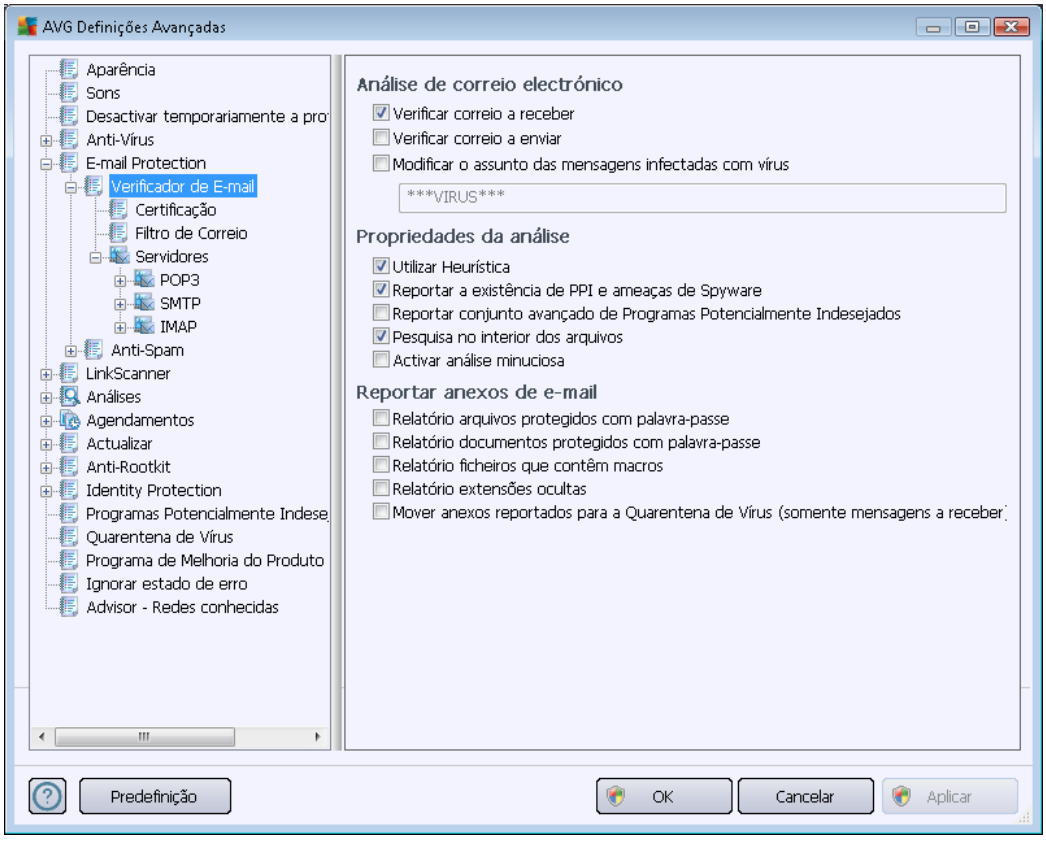
recomendamos vivamente que mantenha as predefinições e deixe a opção activada! Caso contrário, poderá ocorrer uma diminuição significativa da velocidade e desempenho do seu sistema.

10.5. Protecção de E-mail

Na secção ***Protecção de E-mail*** pode editar detalhadamente a configuração do Verificador de E-mail e Anti-Spam:

10.5.1. Verificador de E-mail

A janela ***Verificador de E-mail*** está dividida em três secções:



Análise de e-mail

Nesta secção, pode configurar estas definições básicas para as mensagens de e-mail a receber e/ou a enviar:

- ***Verificar correio a receber*** (*activado por predefinição*) – marque para activar/desactivar a opção de análise de todas as mensagens de e-mail entregues no seu cliente de e-mail
- ***Verificar correio a enviar*** (*desactivado por predefinição*) – marque para activar/desactivar a opção de análise de todas as mensagens de e-mail enviadas a partir da sua conta
- ***Modificar o assunto das mensagens infectadas com vírus*** (*desactivado por predefinição*)

– se quiser ser informado quando uma mensagem for detectada como infectada, marque este item e preencha o texto pretendido no campo de texto. Este texto será então adicionado ao campo "Assunto" de cada e-mail infectado para uma identificação e filtragem mais fáceis. O valor predefinido é ***VIRUS***, que recomendamos que mantenha.

Propriedades da análise

Nesta secção, pode especificar como as mensagens de e-mail serão analisadas:

- ***Utilizar a heurística*** (*activado por predefinição*) – marque para usar o método de detecção da análise heurística durante a análise de mensagens de e-mail. Quando esta opção está activada, pode filtrar anexos de e-mail não só por extensão mas também serão considerados os conteúdos do anexo. O filtro pode ser definido na janela Filtro de Correio.

- ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** (*activado por predefinição*) – marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado por predefinição*) – marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

- ***Analisar no interior de arquivos*** (*activado por predefinição*) – seleccione para analisar os conteúdos de arquivos anexados a mensagens de e-mail.

- ***Activar análise minuciosa*** (*desactivado por predefinição*) – em situações específicas (*ex. suspeita de infecção do computador por um vírus ou exploit*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.

Reportar anexos de e-mail

Nesta secção, pode configurar relatórios adicionais acerca de ficheiros potencialmente perigosos ou suspeitos. Por favor tenha em atenção que não será apresentada qualquer janela de aviso, só será adicionado um texto de certificação no final do e-mail, e todos esses relatórios serão listados na janela Detecção de Verificador de E-mail:

- ***Reportar arquivos protegidos por palavra-passe*** – arquivos (*ZIP, RAR, etc.*) que estão protegidos por palavra-passe e que não podem ser analisados pela existência de vírus; seleccione a caixa para os reportar como potencialmente perigosos.

- ***Reportar documentos protegidos por palavra-passe*** – documentos que estão protegidos

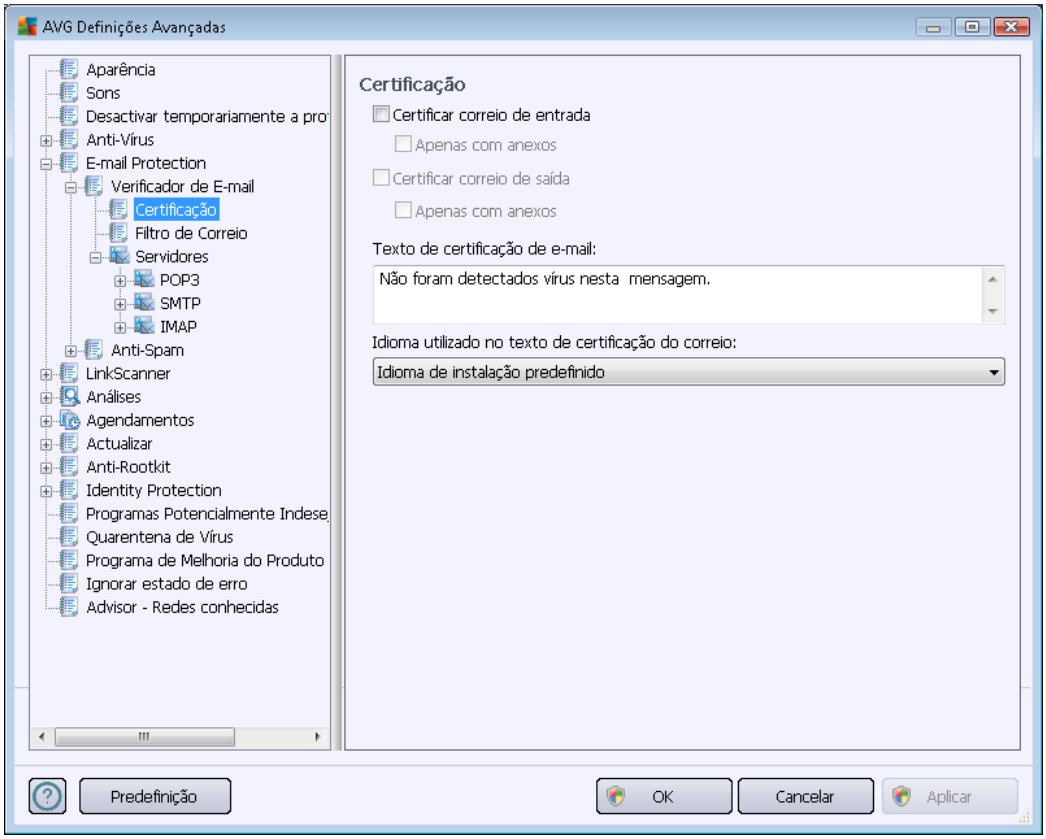
por palavra-passe e que não podem ser analisados pela existência de vírus; seleccione a caixa para os reportar como potencialmente perigosos.

- ***Reportar ficheiros que contenham macros*** – uma macro é uma sequência predefinida de passos destinada a facilitar determinadas tarefas ao utilizador (*as macros do MS Word são amplamente conhecidas*). Como tal, uma macro pode conter instruções potencialmente perigosas e pode querer seleccionar a caixa para se certificar de que os ficheiros com macros serão reportados como suspeitos.

- ***Reportar extensões ocultas*** – extensões ocultas podem fazer, por exemplo, com que um ficheiro executável suspeito "qualquercoisa.txt.exe" pareça um inofensivo ficheiro de texto "qualquercoisa.txt"; seleccione a caixa para reportá-los como potencialmente perigosos.

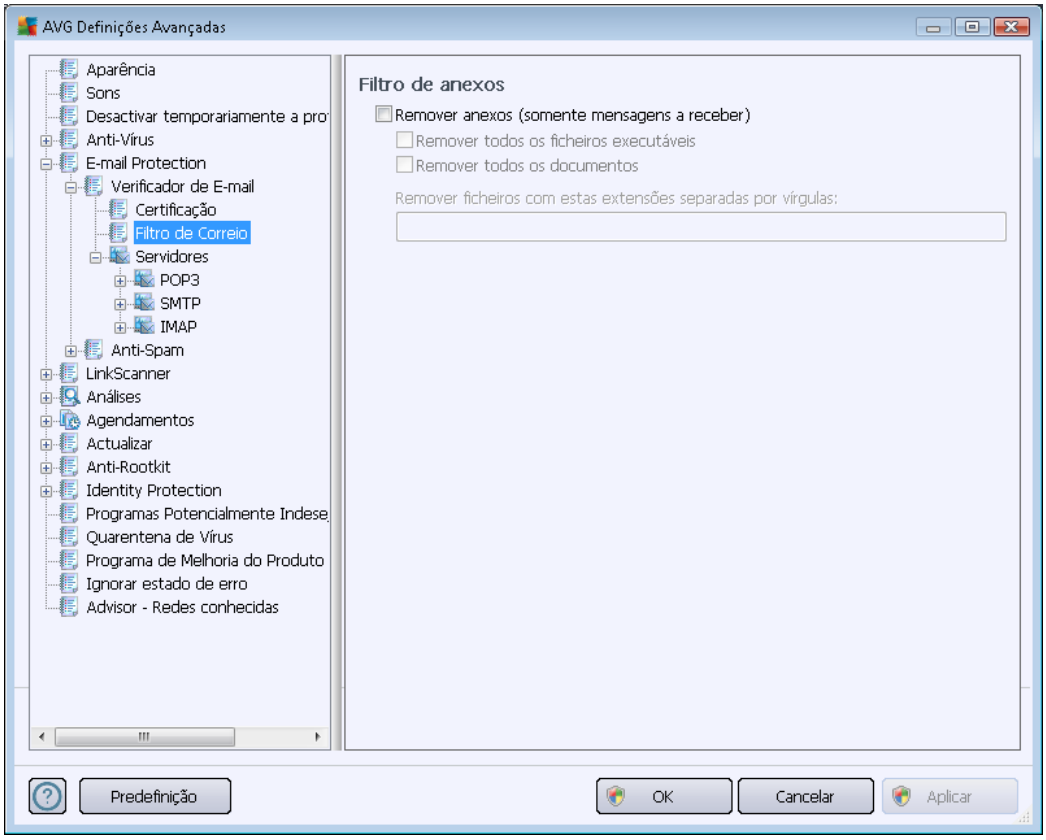
- ***Mover anexos reportados para a Quarentena de Vírus*** – especifique se pretende ser notificado via e-mail acerca de arquivos protegidos com palavra-passe, documentos protegidos com palavra-passe, ficheiros que contenham macros e/ou ficheiros com extensões ocultas detectadas como anexos das mensagens de e-mail analisadas. Se for identificada uma mensagem destas durante a análise, defina se os objectos infecciosos detectados devem ser removidos para a Quarentena de Vírus.

Na janela ***Certificação*** pode marcar as caixas específicas para decidir se pretende certificar o correio a receber (***Certificar correio de entrada***) e/ou o correio o enviar (***Certificar correio de saída***). Pode ainda especificar, para cada uma destas opções, o parâmetro ***Apenas com anexos*** para que a certificação só seja adicionada a mensagens de e-mail que contenham anexos:



Por predefinição, o texto de certificação é composto por uma mera informação básica que declara que *Não foram detectados vírus nesta mensagem.* No entanto, esta informação pode ser alterada conforme as suas necessidades: escreva o texto de certificação pretendido no campo ***Texto de certificação de e-mail***. Na secção ***Idioma utilizado no texto de certificação do correio*** pode ainda definir em que idioma deverá ser apresentada a informação da certificação gerada automaticamente (*Não foram detectados vírus nesta mensagem*).

Nota: *Tenha em consideração que só o texto predefinido será apresentado no idioma seleccionado e que texto personalizado não será traduzido automaticamente!*



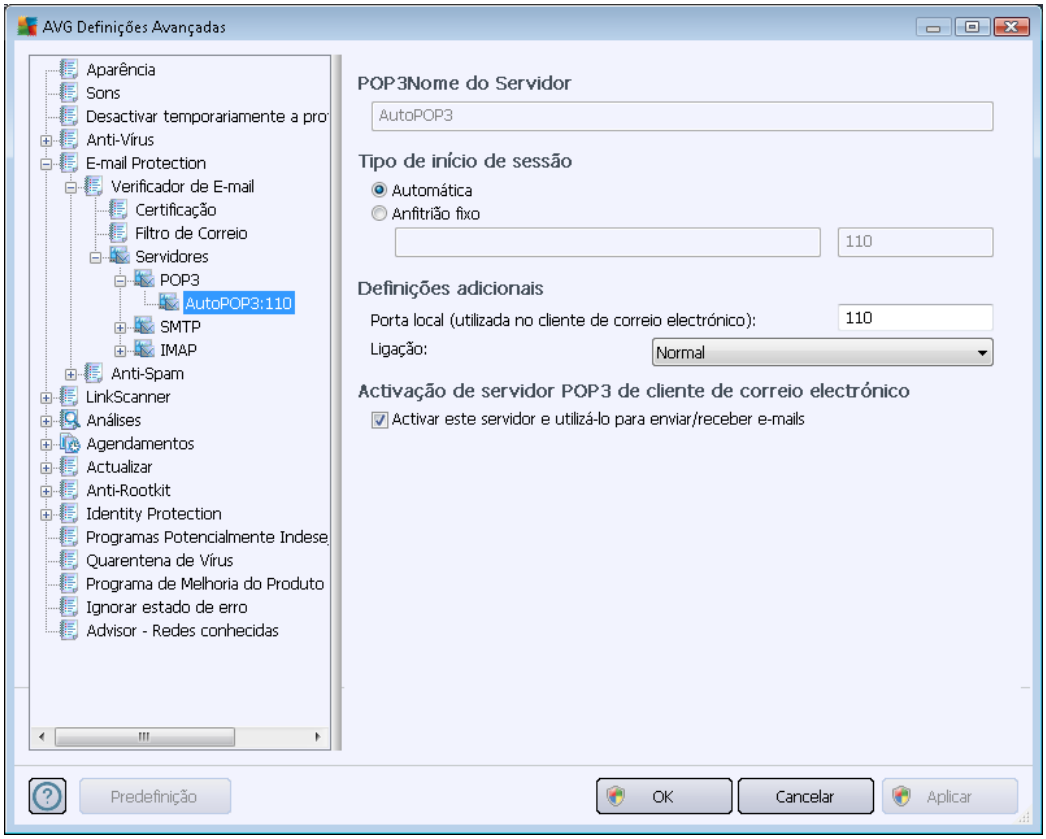
A janela ***Filtro de anexos*** permite-lhe configurar parâmetros para a análise de anexos do e-mail.A opção ***Remover anexos*** está desactivada por predefinição. Se decidir activá-la, todos os anexos do e-mail detectados como infecciosos ou potencialmente perigosos serão removidos automaticamente. Se quiser definir tipos específicos de anexos que podem ser removidos, seleccione a opção respectiva:

- ***Remover todos os ficheiros executáveis*** – todos os ficheiros *.exe serão eliminados
- ***Remover todos os documentos*** – todos os ficheiros *.doc, *.docx, *.xls, *.xlsx serão eliminados
- ***Remover ficheiros com estas extensões separadas por vírgula*** – removerá todos os ficheiros com as extensões definidas

Na secção ***Servidores*** pode editar os parâmetros dos servidores do Verificador de E-mail:

- Servidor POP3
- Servidor SMTP
- Servidor IMAP

Além disso, pode definir um novo servidor para o correio de entrada e de saída, usando o botão ***Adicionar novo servidor***.



Nesta janela (*acessível via **Servidores / POP3***) pode configurar um novo servidor do Verificador de E-mail utilizando o protocolo POP3 para e-mail a receber:

- ***Nome do Servidor POP3*** – neste campo pode especificar o nome de servidores adicionados recentemente (*para adicionar um servidor POP3, clique com o botão direito do rato sobre o item POP3 do menu de navegação à esquerda*). Este campo estará desactivado para servidores "AutoPOP3" criados automaticamente.

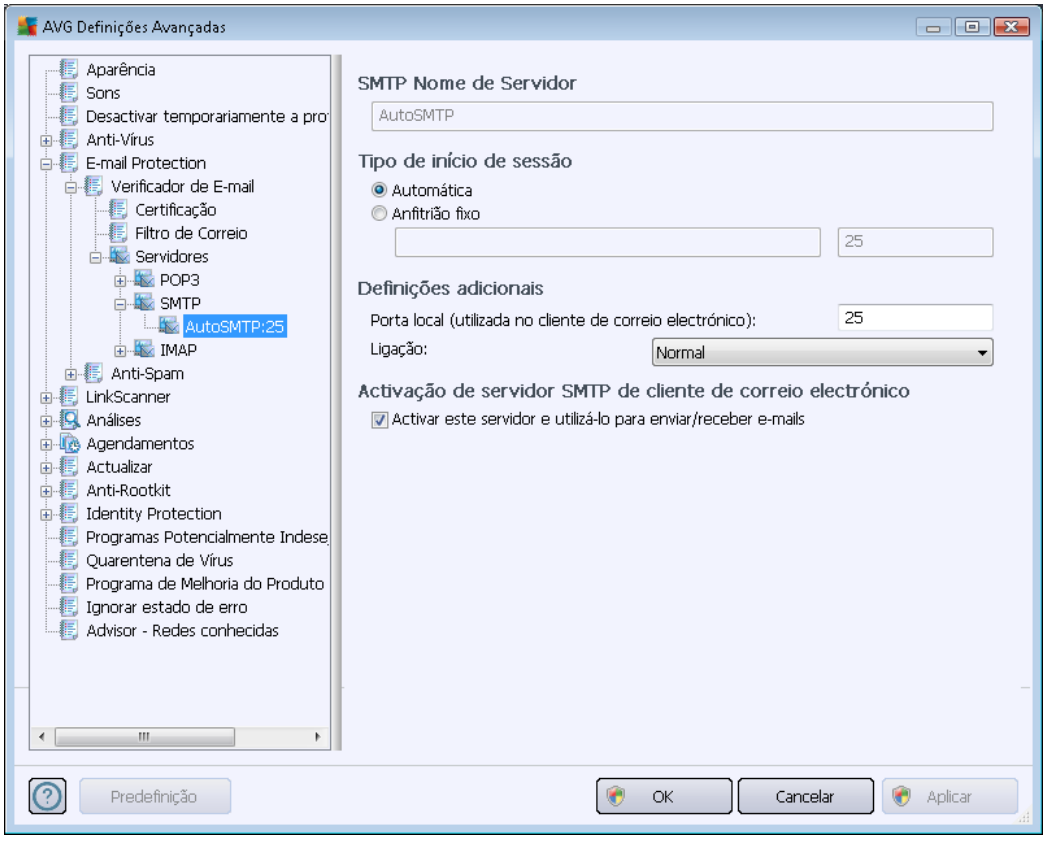
- ***Tipo de inicio de sessão***- define o método para determinar o servidor de e-mail utilizado para e-mail a receber:

    - ***Automático*** - O início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de correio electrónico.

    - ***Anfitrião fixo*** – Neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. O nome de início de sessão permanece inalterado. Para um nome, pode utilizar um nome de domínio (*por exemplo, pop.acme.com*) e um endereço IP (*por exemplo, 123.45.67.89*). Se o servidor de e-mail utilizar uma porta não padrão, pode especificar esta porta a seguir ao nome do servidor, utilizando uma vírgula como delimitador (*por exemplo, pop.*

acme.com:8200). A porta padrão para comunicação POP3 é 110.

- ***Definições adicionais*** – especifica parâmetros mais detalhados:
  - ***Porta local*** – especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação POP3.
  - ***Ligação*** – no menu pendente pode especificar que tipo de ligação utilizar (*normal/ SSL/SSL predefinida*). Se seleccionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só estará disponível se o servidor de e-mail de destino a suportar.
- ***Activação do servidor POP3 do cliente de correio electrónico*** - marque/desmarque este item para activar ou desactivar o servidor POP3 especificado

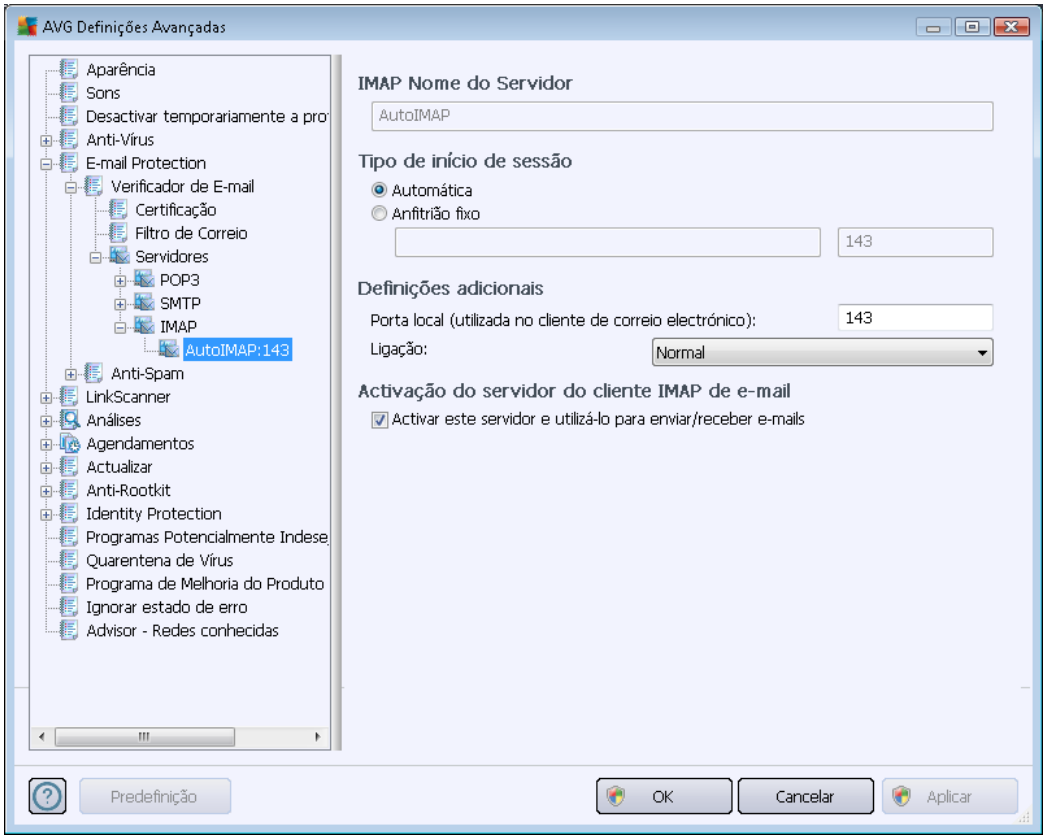


Nesta janela (*acessível via **Servidores / SMTP***) pode configurar um novo servidor do Verificador de E-mail utilizando o protocolo SMTP para e-mail a enviar:

- ***Nome do Servidor SMTP*** – neste campo pode especificar o nome de servidores adicionados recentemente (*para adicionar um servidor SMTP, clique com o botão direito do rato sobre o item SMTP do menu de navegação à esquerda*). Este campo estará

desactivado para servidores "AutoSMTP" criados automaticamente.

- ***Tipo de inicio de sessão*** - define o método para determinar o servidor de e-mail utilizado para e-mail a enviar:
    - ***Automático*** – o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
    - ***Anfitrião Fixo*** – i- Neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. Pode utilizar um nome de domínio (*por exemplo, smtp.acme.com)*) e um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de correio utilizar uma porta não padrão, pode escrever esta porta atrás do nome do servidor, utilizando uma vírgula como delimitador (*por exemplo, smtp.acme.com:8200*). A porta padrão para comunicação SMTP é 25.
- ***Definições adicionais*** – especifica parâmetros mais detalhados:
    - ***Porta local*** – especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação SMTP.
    - ***Ligação*** – na lista de opções pode especificar que tipo de ligação utilizar (*normal/ SSL/SSL predefinida*). Se seleccionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só está disponível se o servidor de e-mail de destino a suportar.
- ***Activação do servidor SMTP do cliente de e-mail*** – marque/desmarque esta caixa para activar/desactivar o servidor SMTP especificado acima



Nesta janela (acessível via ***Servidores / IMAP***) pode configurar um novo servidor do Verificador de E-mail utilizando o protocolo IMAP para e-mail a enviar:

- ***Nome do Servidor IMAP*** – neste campo pode especificar o nome de servidores adicionados recentemente (*para adicionar um servidor IMAP, clique com o botão direito do rato sobre o item IMAP do menu de navegação à esquerda*). Este campo estará desactivado para servidores "AutoIMAP" criados automaticamente.

- ***Tipo de inicio de sessão*** - define o método para determinar o servidor de e-mail utilizado para e-mail a enviar:

    - ***Automático*** – o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.

    - ***Anfitrião Fixo*** – i- Neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. Pode utilizar um nome de domínio (*por exemplo, smtp.acme.com*)) e um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de correio utilizar uma porta não padrão, pode escrever esta porta atrás do nome do servidor, utilizando uma vírgula como delimitador (*por exemplo, imap.acme.com:8200*). A porta padrão para comunicação IMAP é a 143.

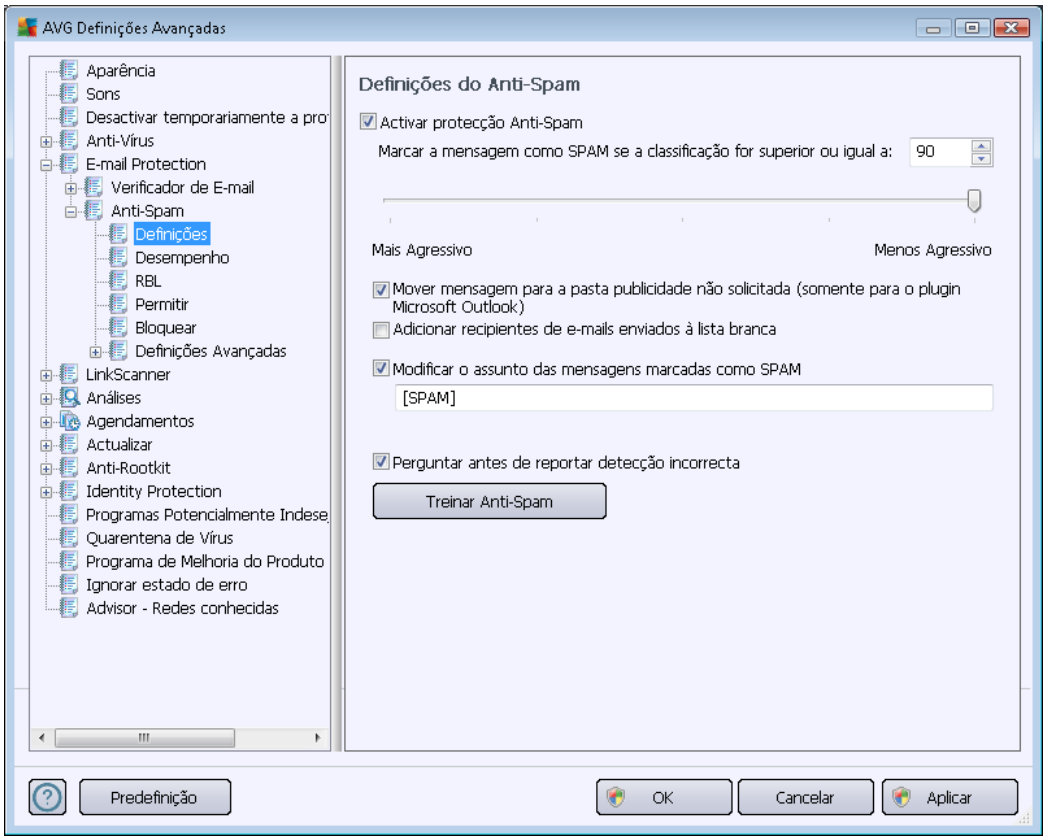
- ***Definições adicionais*** – especifica parâmetros mais detalhados:

- ***Porta local*** – especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação IMAP.

- ***Ligação*** – na lista de opções pode especificar que tipo de ligação utilizar (*normal/ SSL/SSL predefinida*). Se seleccionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só está disponível se o servidor de e-mail de destino a suportar.

- ***Activação do servidor IMAP do cliente de e-mail*** – marque/desmarque esta caixa para activar/desactivar o servidor IMAP especificado acima

10.5.2. Anti-Spam



Na janela ***Definições do componente Anti-Spam*** pode marcar/desmarcar a caixa ***Activar protecção Anti-Spam*** para permitir/interditar a análise anti-spam de comunicações de e-mail. Esta opção está activada por predefinição e, como sempre, é recomendável que mantenha esta configuração a menos que tenha uma razão válida para a alterar.

A seguir, 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 classificação for superior a*** digitando o valor, ou

deslocando o cursor para a esquerda ou para a direita (*o intervalo de valores está limitado a 50-90*).

Regra geral, recomendamos que defina o limiar entre 50-90, ou, se não tiver a certeza, para 90. Veja aqui uma revisão geral do limiar de classificação:

- ***Valor 80-90*** – As mensagens de e-mail passíveis de serem spam serão 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 spam serão 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.

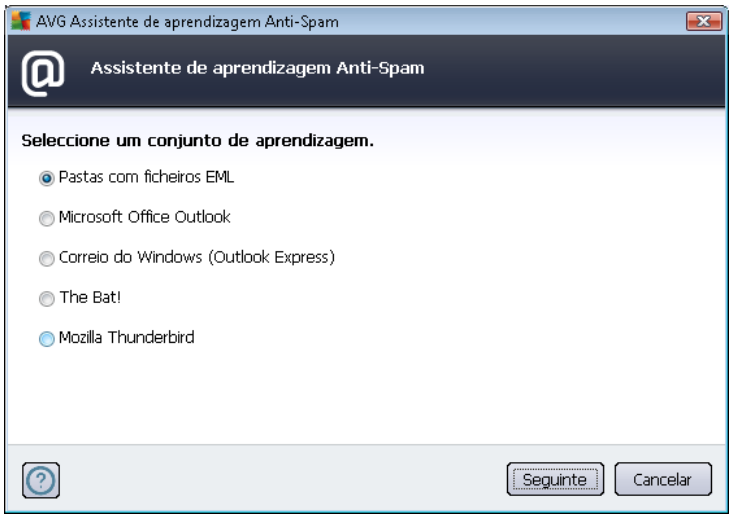
Na janela ***Definições do componente Anti-Spam*** pode definir a forma como os e-mails detectados comospamdeverão ser tratados:

- ***Mover mensagem para a pasta publicidade não solicitada*** *(somente para o plugin Microsoft Outlook)* - Seleccione esta caixa para especificar que cada mensagem de spam detectada deverá ser movida automaticamente para a pasta publicidade não solicitada especificada no seu cliente de e-mail MS Outlook. De momento, esta funcionalidade não é suportada noutros clientes de correio electrónico.
- ***Adicionar destinatários de e-mails enviados à lista branca*** - Assinale esta caixa para confirmar que todos os destinatários de e-mails enviados são de confiança e que todos os e-mails enviados das suas contas de e-mail podem ser entregues.
- ***Modificar o assunto das mensagens marcadas como SPAM*** - Assinale esta caixa 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*** – Desde que, durante o processo de instalação, tenha aceitado participar no Programa de Melhoria do Produto. Se for o caso, permitiu a reportação de 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.

Botões de controlo

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

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:

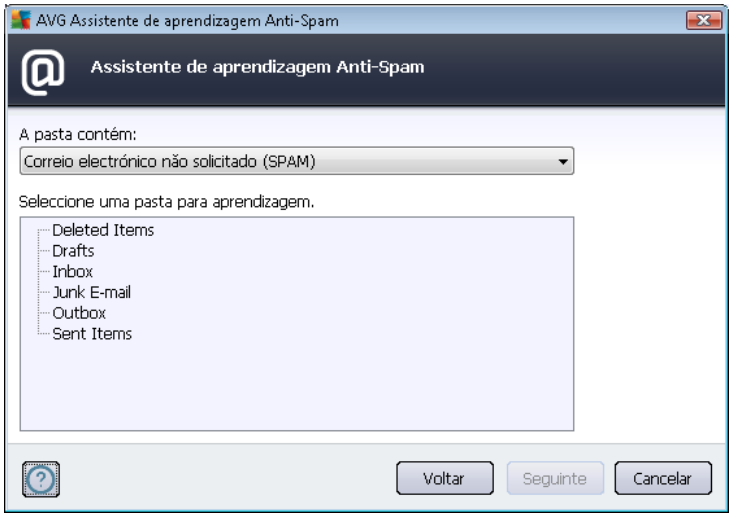
- ***Um cliente de e-mail específico*** – se usar um dos clientes de e-mail listados (*MS Outlook, Outlook Express, The Bat!*), basta seleccionar a opção respectiva
- ***Pasta com ficheiros EML***- Se utilizar outro programa de e-mail, deverá primeiro guardar as mensagens para uma pasta específica (no *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.

A janela apresentada neste passo depende da sua selecção anterior.

Pastas com ficheiros EML



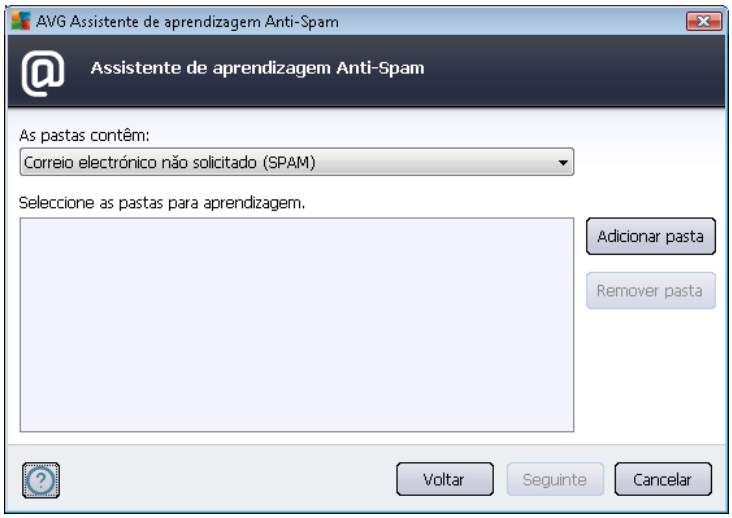
Nesta janela, por favor seleccione a pasta que contém as mensagens que pretende utilizar para a aprendizagem. Clique no botão ***Adicionar pasta*** para localizar a pasta com os ficheiros .eml (*mensagens de e-mail guardadas*). A pasta seleccionada será então apresentada na janela.

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.

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)***.

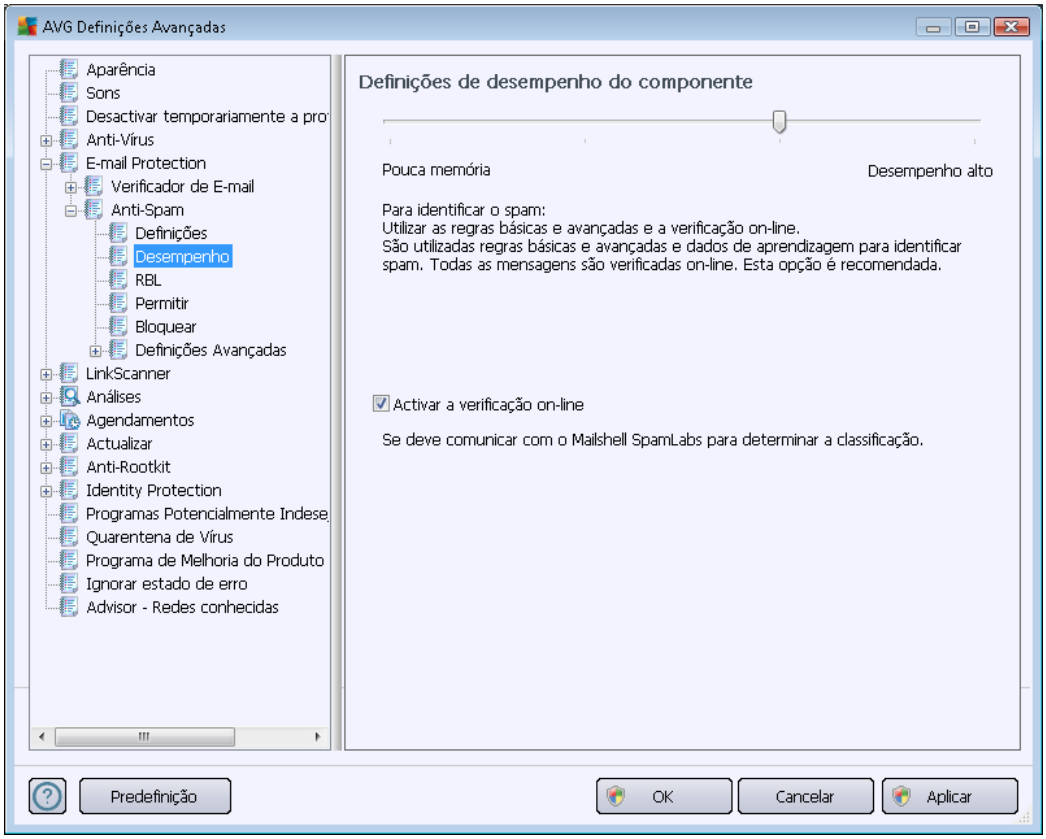
- ***Utilizar filtro*** - Para uma filtragem mais avançada, seleccione a opção ***Utilizar filtro***. Pode introduzir uma palavra (*nome*), parte de uma palavra, ou frase a ser procurada no campo assunto/e ou remetente do e-mail Todas as mensagens que correspondam ao critério com exactidão serão utilizadas 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.

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.

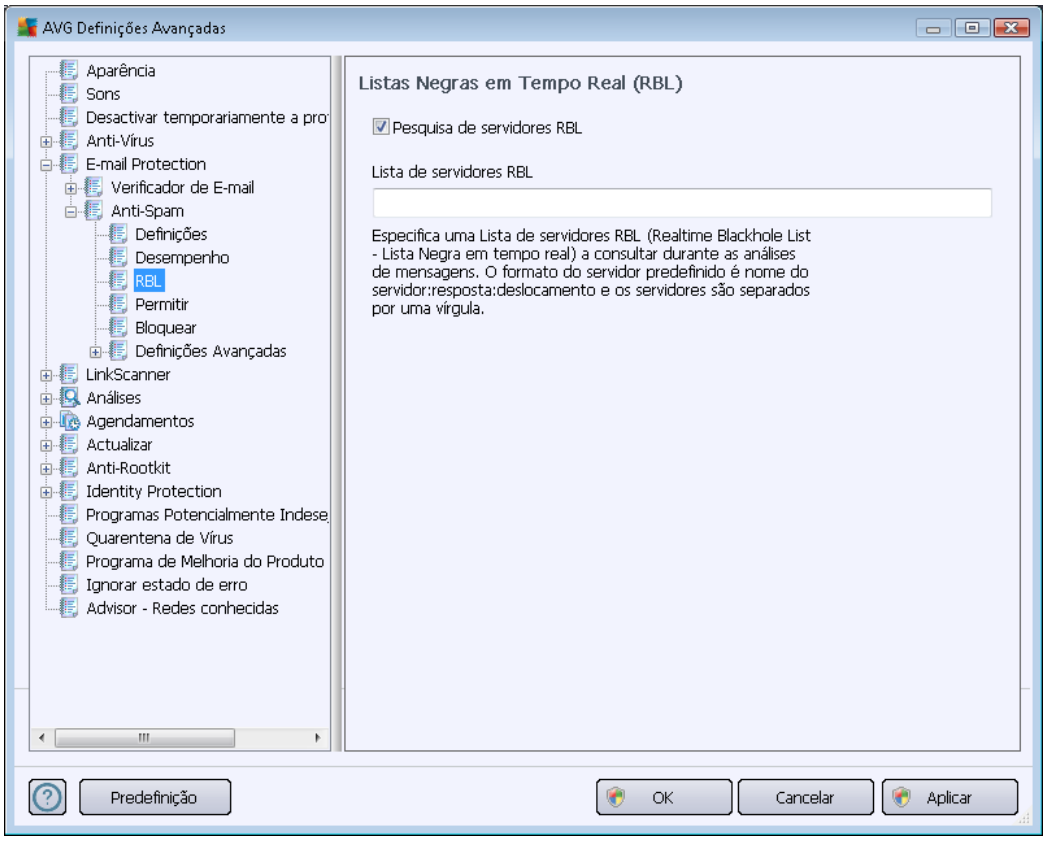
- ***Alto desempenho*** - este modo requer uma grande quantidade de memória. Durante o processo de análise para identificar spam, serão utilizadas as seguintes características: regras e cache de base de dados de spam, regras básicas e avançadas, endereços IP de remetentes de spam e bases de dados de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

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!

O item ***RBL*** abre uma janela de edição apelidada ***Listas Negras em Tempo Real*** onde pode activar/ desactivar a função ***Pesquisa de servidores RBL***:

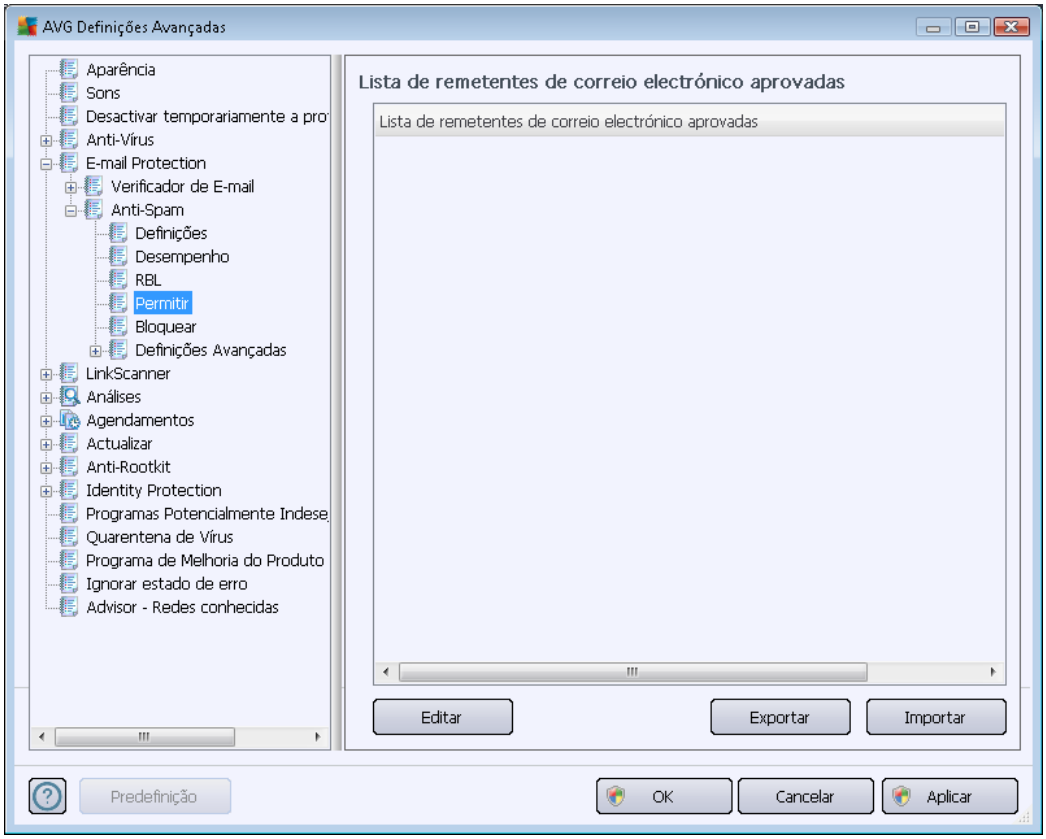


O servidor RBL (*Real-time Blackhole List)* é um servidor DNS com uma base de dados extensiva de remetentes de spam conhecidos. Quando esta funcionalidade está ligada, todas as mensagens de e-mail serão verificadas de acordo com a base de dados do servidor RBL e serão assinaladas como spam se forem idênticas a qualquer uma das entradas da base de dados. As bases de dados dos servidores RBL contêm vestígios de spam actualizados até ao último 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 de servidores RBL específicos (*tenha em conta que a activação desta funcionalidade, em alguns sistemas e configurações, pode abrandar o processo de recepção de e-mails, uma vez que todas as mensagens serão verificadas contra a base de dados do servidor RBL).*

Não são enviados dados pessoais para o servidor!

O item ***Lista Branca*** abre uma janela apelidada de ***Lista de remetentes de e-mail aprovados*** com uma listagem 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.

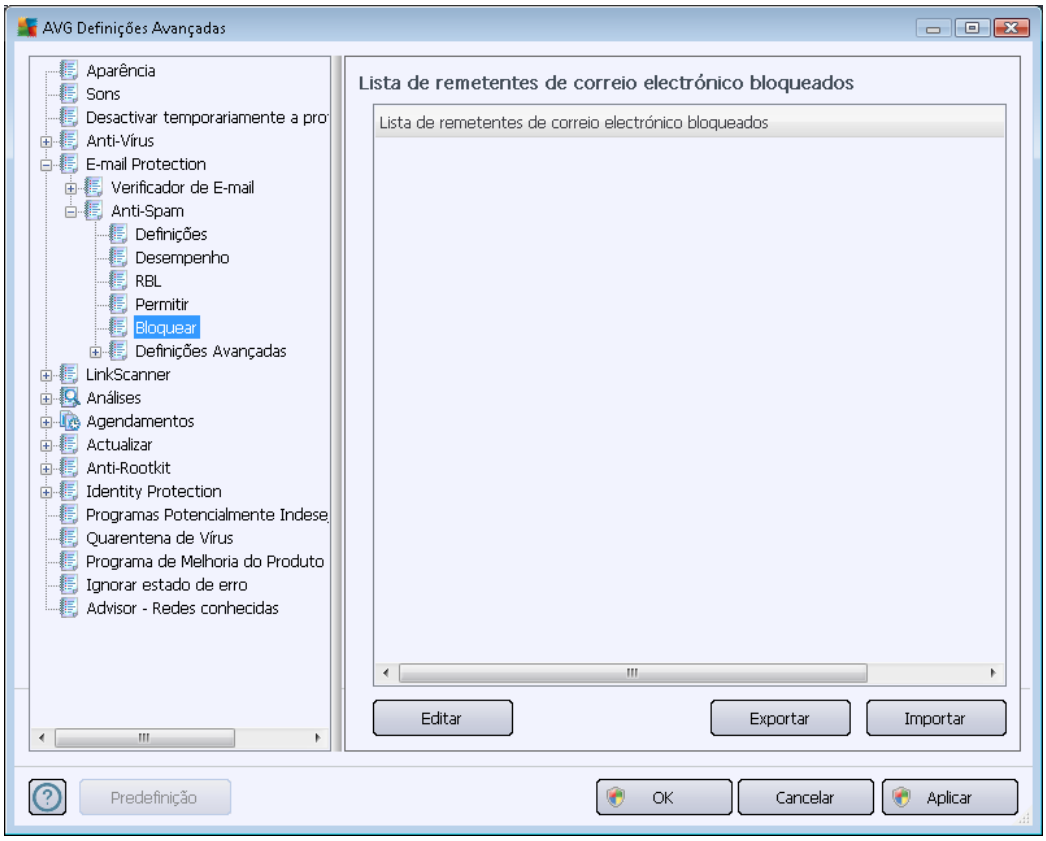
Botões de controlo

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.
- ***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.
- ***Importar*** – se já tiver um ficheiro de texto preparado com endereços de e-mail / nomes de

domínios, pode simplesmente importá-lo, seleccionando este botão. O conteúdo do ficheiro deve conter apenas um item (*endereço, nome de domínio*) por linha.

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 como spam.



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.

Botões de controlo

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.

- ***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.

- ***Importar*** – se já tiver um ficheiro de texto preparado com endereços de e-mail / nomes de domínios, pode simplesmente importá-lo, seleccionando este botão.

O separador Definições Avançadas contém opções de definições suplementares para o componente Anti-Spam. Estas definições destinam-se exclusivamente a utilizadores experientes, regra geral administradores de redes que precisem de configurar detalhadamente a protecção anti-spam para uma protecção superior dos servidores de e-mail. Como tal, não existe qualquer ajuda suplementar disponível para as janelas individuais; no entanto, está disponível uma pequena descrição de cada opção directamente na interface do utilizador.

Recomendamos vivamente que não altere quaisquer definições a menos que esteja perfeitamente familiarizado com todas as definições avançadas do Spamcatcher (MailShell Inc.) Quaisquer alterações inadequadas podem resultar numa diminuição de desempenho, ou num mau funcionamento do componente.

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

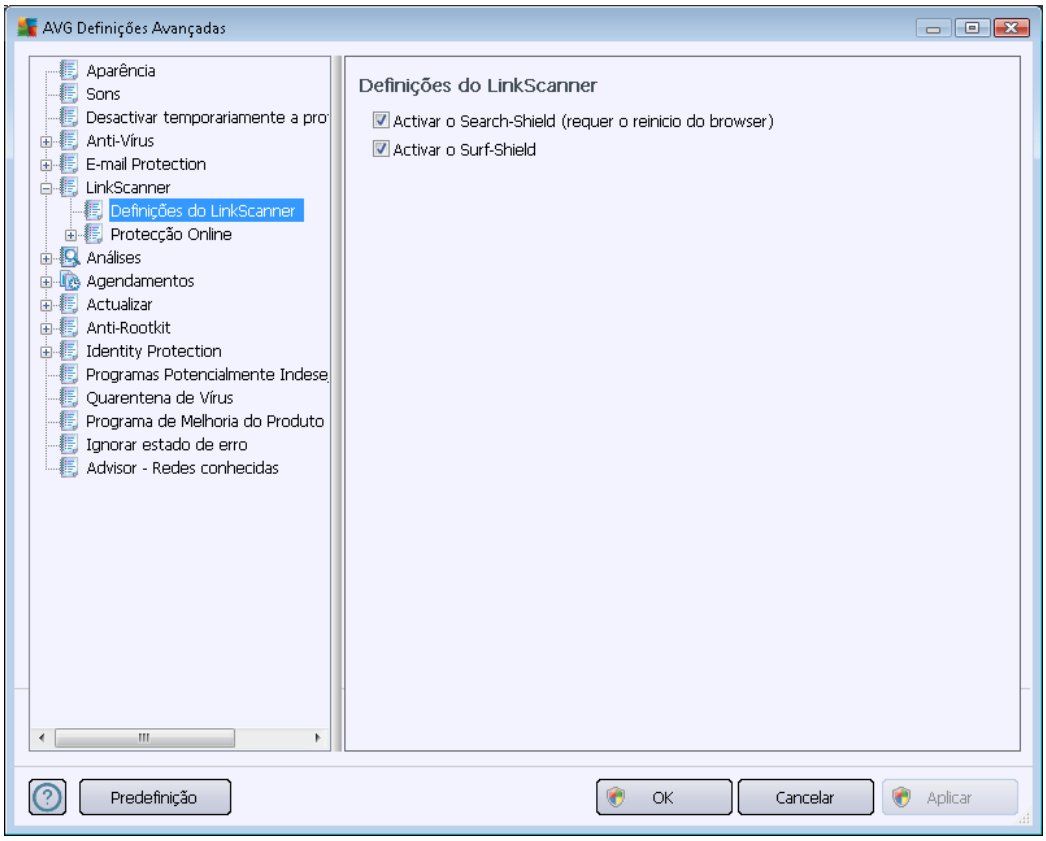
- ***RBL*** – Servidores RBL, multi-correspondências, limiar, temporização, máximo de IPs

- ***Ligação à Internet*** - temporização, servidor proxy, autenticação de servidor proxy

10.6. Link Scanner

10.6.1. Definições do Link Scanner

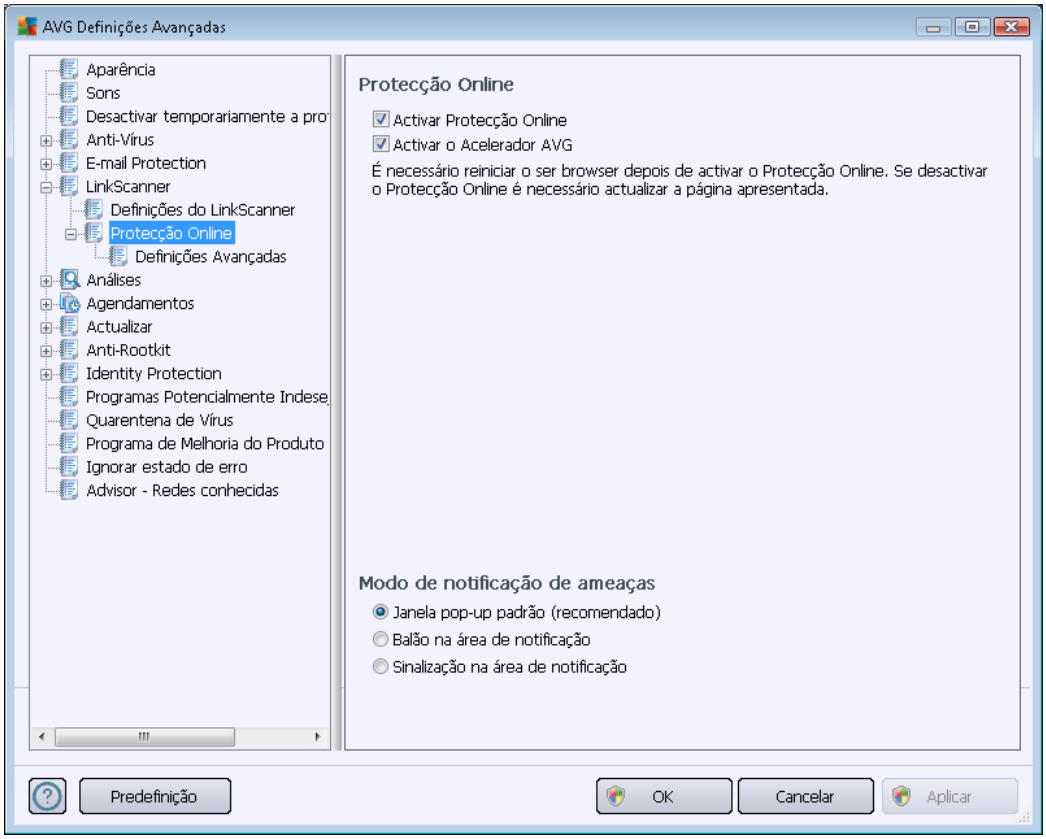
A janela ***Definições do LinkScanner*** permite-lhe activar/desactivar as funcionalidades elementares do LinkScanner:



- ***Activar o Search-Shield*** – (*activado por predefinição*): ícones de notificação relativos às pesquisas efectuadas com o Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ou SlashDot: tendo verificado antecipadamente o conteúdo dos websites devolvidos pelo motor de busca.

- ***Activar o Surf-Shield*** – (*activado por predefinição*): protecção activa (*em tempo real*) contra websites maliciosos à medida que estes são acedidos. Ligações de websites maliciosos conhecidos são bloqueados à medida que são acedidos pelo utilizador via um browser Web (*ou qualquer outra aplicação que utilize HTTP*).

10.6.2. Protecção Online



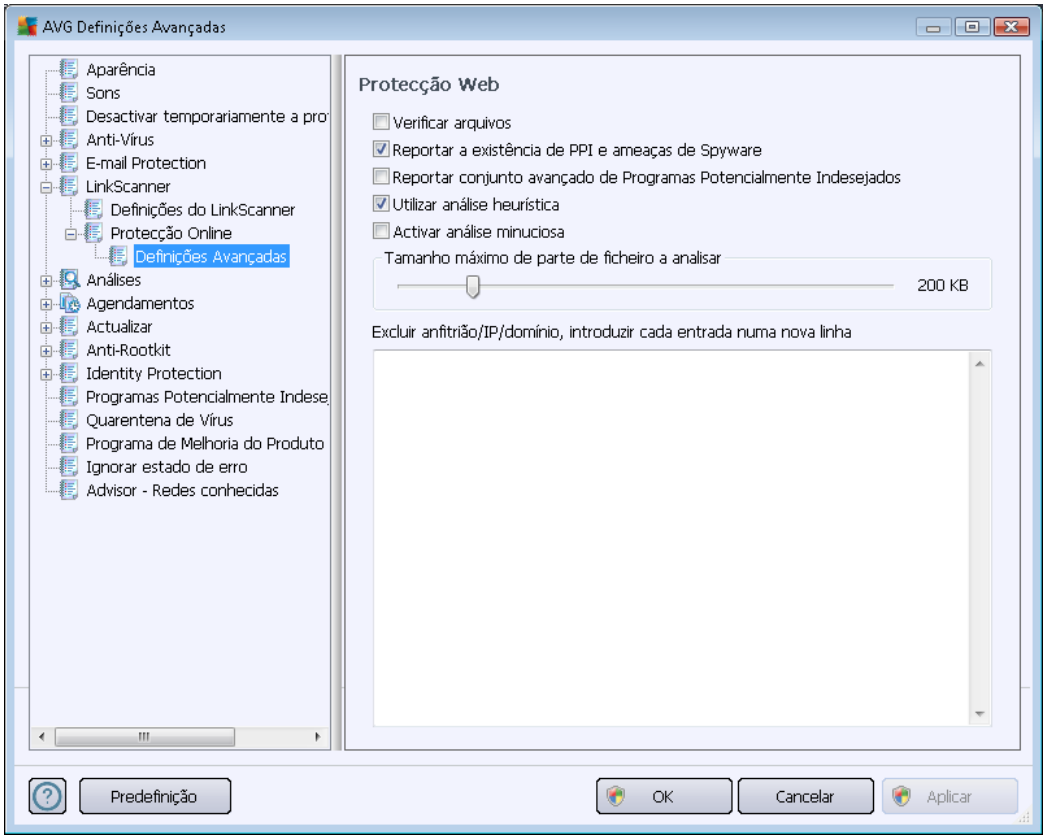
A janela ***Protecção Online*** apresenta as seguintes opções:

- ***Activar a Protecção Online*** *(activado por predefinição)* – Activar/desactivar por completo o serviço ***Protecção Online***. Para definições avançadas da ***Protecção Online*** , continue para a janela seguinte da janela apelidada Protecção na Internet.

- ***Activar o Acelerador AVG*** *(activado por predefinição)* - Activar/desactivar o serviço ***Acelerador AVG*** que permite uma reprodução de vídeos mais fluida e facilita as transferências.

Modo de notificação de ameaças

Na parte inferior da janela, seleccione de que forma pretende ser informado de possíveis ameaças detectadas: através de uma janela pop-up padrão, através de uma notificação de balão, ou através de informação do ícone na Barra de Tarefas.



Na janela ***Protecção na Internet*** pode editar a configuração do componente em relação à análise do conteúdo de websites. A interface de edição permite-lhe configurar as seguintes opções elementares:

- ***Activar a Protecção na Internet*** – esta opção confirma que a***Protecção Online*** deve analisar o conteúdo das páginas www. Uma vez que esta opção está activada (*por predefinição*), pode ainda activar/desactivar estes itens:
    - ***Verificar arquivos*** – (*desactivado por predefinição*): analisar o conteúdo de arquivos possivelmente incluídos na página www a ser apresentada.
    - ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** – (*activado por predefinição*) – marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.
    - ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** – (*desactivado por predefinição*): marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos

maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

- ***Utilizar a análise heurística***- (*activado por predefinição*): analisar o conteúdo da página a ser apresentada utilizando o método análise heurística (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*).
- ***Activar análise minuciosa*** (*desactivado por predefinição*) – em situações específicas (*suspeita de infecção do computador*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.
- ***Tamanho máximo de ficheiro a ser analisado*** – se os ficheiros incluídos estiverem presentes na página apresentada também pode analisar o seu conteúdo antes de estes serem transferidos para o seu computador. No entanto, analisar um ficheiro grande demora algum tempo e a transferência da página Web pode ser abrandada significativamente. Pode utilizar o cursor para especificar o tamanho máximo de um ficheiro que esteja para ser analisado pela***Protecção Online***. Mesmo que o ficheiro transferido seja superior ao tamanho especificado e, como tal, não será analisado com a Protecção Online, ainda está protegido: na eventualidade do ficheiro estar infectado, a ***Protecção Residente*** detectará imediatamente.
- ***Excluir anfitrião/IP/domínio*** – pode digitar no campo de texto o nome exacto de um servidor (*anfitrião, endereço de IP, endereço de IP com máscara, ou URL*)ou um domínio que não deverá ser analisado pela ***Protecção Online***. Como tal, exclua somente anfitriões que tenha a certeza absoluta que nunca providenciarão conteúdo perigoso.

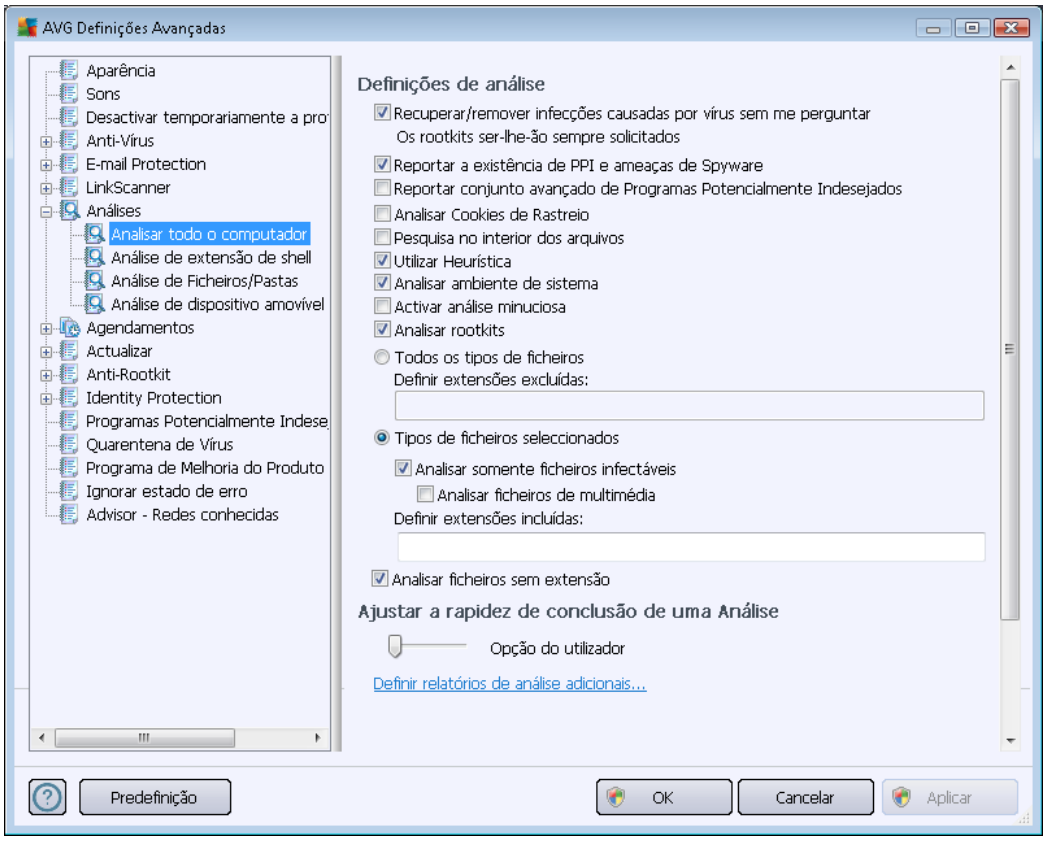
10.7. Análises

As definições avançadas de análise estão divididas em quatro categorias que se referem a tipos específicos de análises conforme definidas pelo fornecedor do software:

- ***Análise de Todo o Computador*** - análise padrão predefinida de todo o computador
- ***Análise em Contexto*** - análise específica de um objecto seleccionado directamente no ambiente do Explorador do Windows
- ***Análise de Ficheiros/Pastas*** – análise padrão predefinida de áreas seleccionadas do seu computador
- ***Análise de Dispositivo Amovível*** – análise específica de dispositivos amovíveis conectados ao seu computador

10.7.1. Análise de todo o computador

A opção ***Análise de todo o computador*** permite-lhe editar os parâmetros de uma das análises predefinidas pelo fornecedor do software, a Análise de todo o computador:



Definições de análise

A secção ***Definições de análise*** faculta uma lista de parâmetros de análise que podem ser opcionalmente activados/desactivados.

- ***Recuperar/remover infecções causadas por vírus sem me perguntar*** (*activado por predefinição*) – se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Se o ficheiro infectado não puder ser restaurado automaticamente, o objecto infectado será movido para a Quarentena de Vírus.

- ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** (*activado por predefinição*) – marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado*

por predefinição) – marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

- ***Analisar a existência de Cookies de Rastreio*** (*desactivado por predefinição*) – este parâmetro do componente Anti-Spyware define que as cookies deverão ser detectadas durante a análise; (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação especifica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos*)

- ***Analisar no interior de arquivos*** (*desactivado por predefinição*) – este parâmetro define que a análise deve verificar todos os ficheiros mesmo os que estão armazenados no interior de arquivos, ex. ZIP, RAR,...

- ***Utilizar Heurística*** (*activado por predefinição*) – a análise heurística (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a detecção de vírus durante a análise.

- ***Analisar o ambiente do sistema*** (*activado por predefinição*) – a análise verificará também as áreas de sistema do seu computador.

- ***Activar análise minuciosa*** (*desactivado por predefinição*) – em situações específicas (*suspeita de infecção do computador*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.

- ***Analisar a existência de rootkits*** (*activado por predefinição*) – a análise Anti-Rootkit analisa o computador em busca de eventuais rootkits, ou seja, programas e tecnologias que podem ocultar actividade de malware no computador. Se for detectado um rootkit, isto não significa necessariamente que o computador esteja infectado. Em alguns casos, podem ser erroneamente detectados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Além disso deve decidir se pretende que sejam analisados

- ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções para a análise ao providenciar uma listagem extensões de ficheiro separadas por vírgula (*uma vez guardada, as vírgulas mudam para ponto e vírgula*) que não devem ser analisadas;

- ***Tipos de ficheiros seleccionados*** – pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infectados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser analisados.

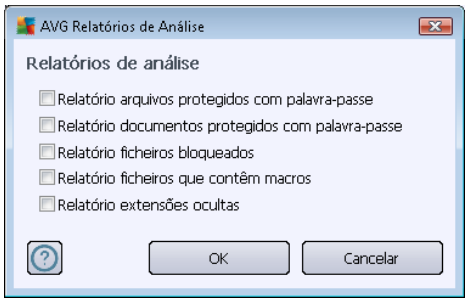
- Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

Ajustar a rapidez de conclusão de uma Análise

Na secção ***Ajustar a rapidez de conclusão de uma análise*** pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. O valor desta opção está, por predefinição, definido para o nível *definida pelo utilizador* de utilização automática de recursos. Se quiser que a análise seja executada mais rapidamente, esta demorará menos tempo mas a utilização de recursos do sistema aumentará significativamente durante a sua execução, e diminuirá o desempenho de outras actividades no seu PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir a utilização dos recursos do sistema prolongando a duração da análise.

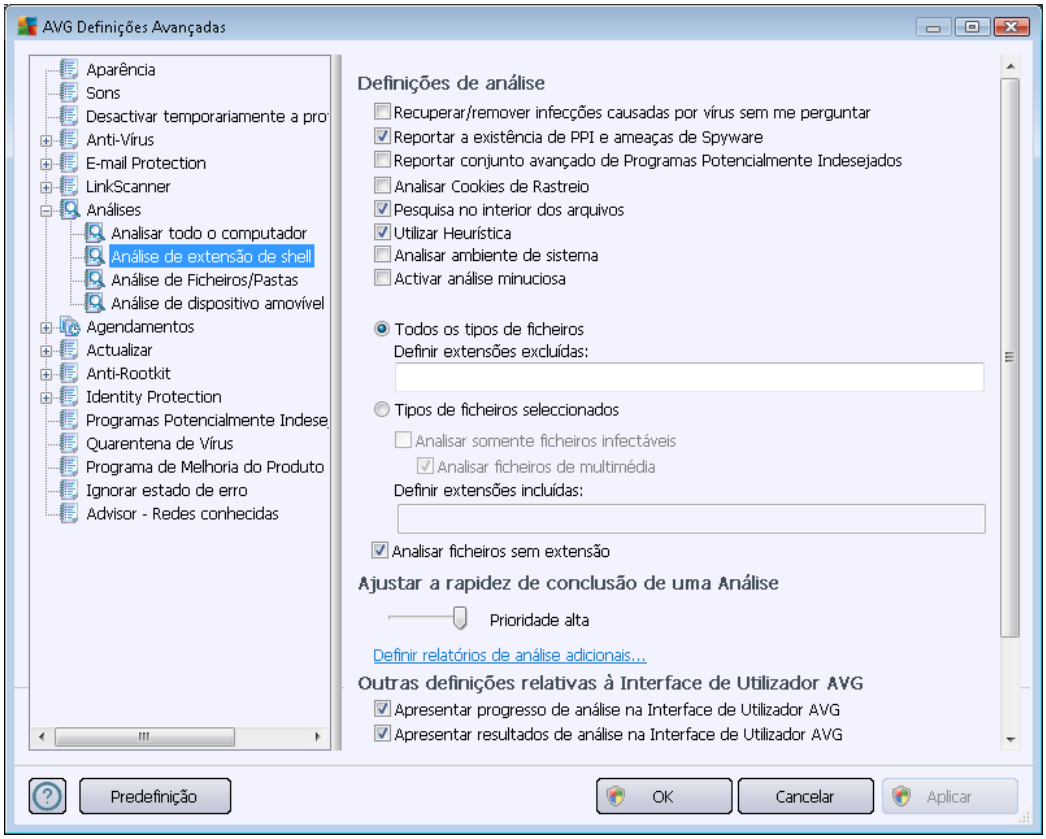
Definir relatórios de análise adicionais...

Clique no link ***Configurar relatórios de análise adicionais ...*** para abrir uma janela independente apelidada ***Relatórios de análise*** onde pode seleccionar vários itens para definir quais as detecções que deverão ser reportadas:



10.7.2. Análise em Contexto

À semelhança do item anterior, a Análise de todo o computador, este item apelidado ***Análise em Contexto*** também oferece várias opções para edição da análise predefinida pelo fornecedor do software. Desta vez a configuração está relacionada com a análise de objectos específicos executada directamente a partir ambiente do Explorador do Windows (*Análise em Contexto*), consulte o capítulo Analisar no Explorador do Windows:



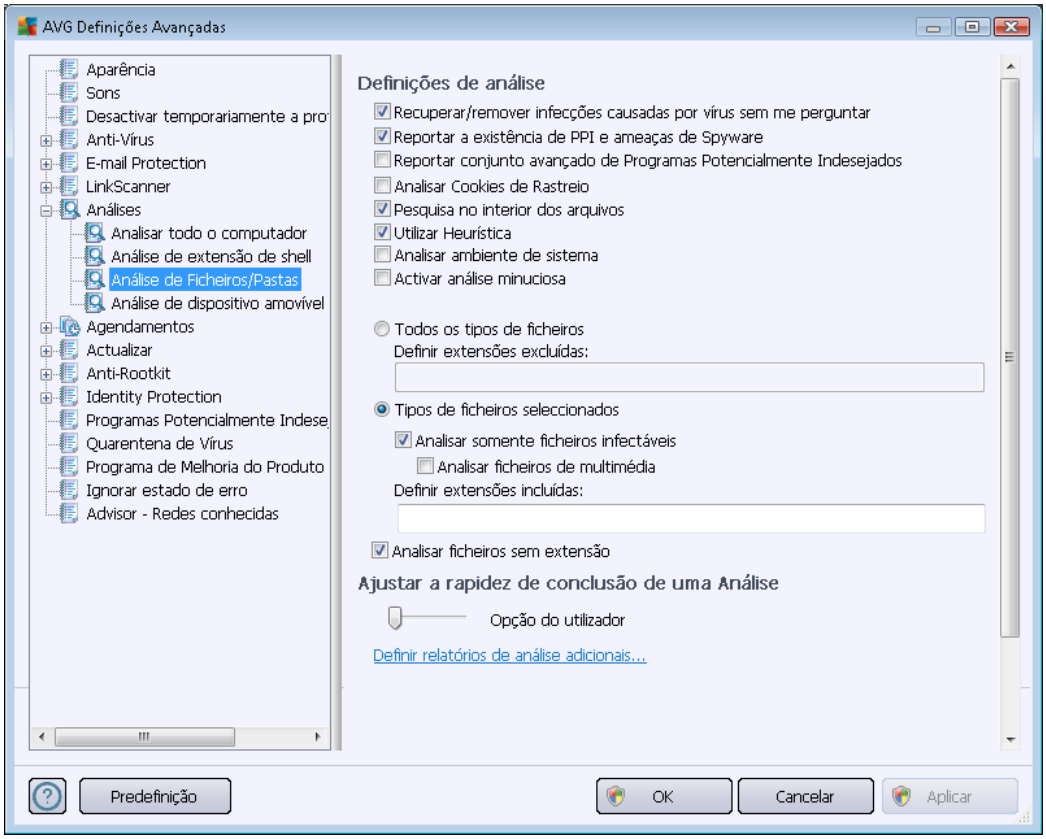
A lista de parâmetros é idêntica aos disponíveis para a análise Analisar todo o computador. No entanto, as predefinições diferem (*por exemplo, a Análise de todo o computador não verifica os arquivos por predefinição, mas verifica o ambiente do sistema; a Análise em contexto é o oposto*).

Nota: *Para uma descrição de parâmetros específicos, por favor consulte o capítulo Definições Avançadas do AVG / Análises / Análise de Todo o Computador.*

Comparativamente à janela Análise de todo o computador, a janela ***Análise em contexto*** também inclui a secção ***Outras definições relativas à Interface do Utilizador do AVG***, onde pode especificar se pretende que o progresso e os resultados da análise sejam acessíveis a partir da interface do utilizador do AVG. Além disso, pode definir que o resultado da análise só deve ser apresentado na eventualidade da detecção de uma infecção durante a análise.

10.7.3. Análise de Ficheiros/Pastas

A interface de edição para a opção ***Analisar pastas ou ficheiros específicos*** é idêntica à janela de edição da Análise de todo o computador. Todas as opções de configuração são as mesmas; no entanto, as definições padrão são mais rígidas para a análise Analisar todo o computador:

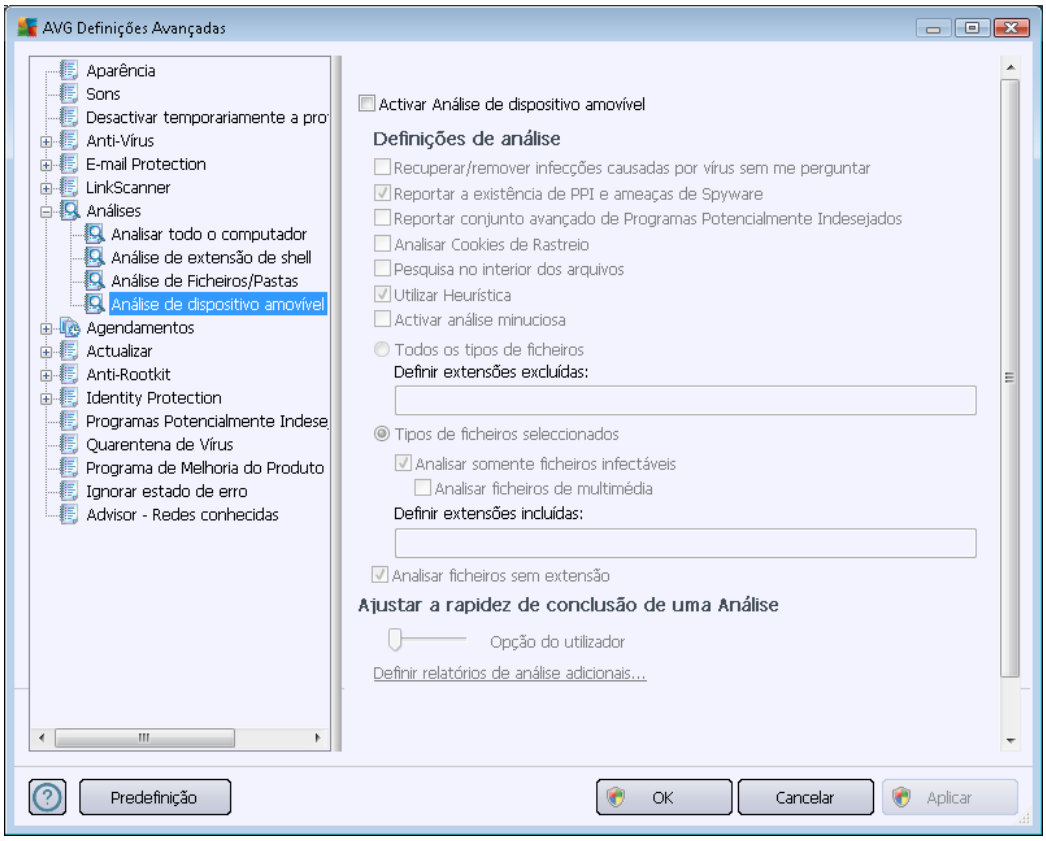


Todos os parâmetros definidos nesta janela de configuração aplicam-se apenas às áreas seleccionadas para análise com a Análise de ficheiros/pastas!

Nota: *Para uma descrição de parâmetros específicos, por favor consulte o capítulo Definições Avançadas do AVG / Análises / Análise de Todo o Computador.*

10.7.4. Análise de dispositivo amovível

A interface de edição da ***Análise de dispositivo amovível*** também é muito semelhante à janela de edição da Análise de Todo o Computador:



A ***Análise de dispositivo amovível*** é iniciada automaticamente quando um dispositivo amovível é conectado ao seu computador. Por predefinição, esta análise está desactivada. No entanto, é crucial que seja efectuada a análise de dispositivos amovíveis por potenciais ameaças uma vez que estes são das maiores fontes de infecção. Para que esta análise esteja pronta e seja iniciada automaticamente quando necessário, seleccione a opção ***Activar a Análise de dispositivo amovível*** .

Nota: *Para uma descrição de parâmetros específicos, por favor consulte o capítulo Definições Avançadas do AVG / Análises / Análise de Todo o Computador.*

10.8. Agendamentos

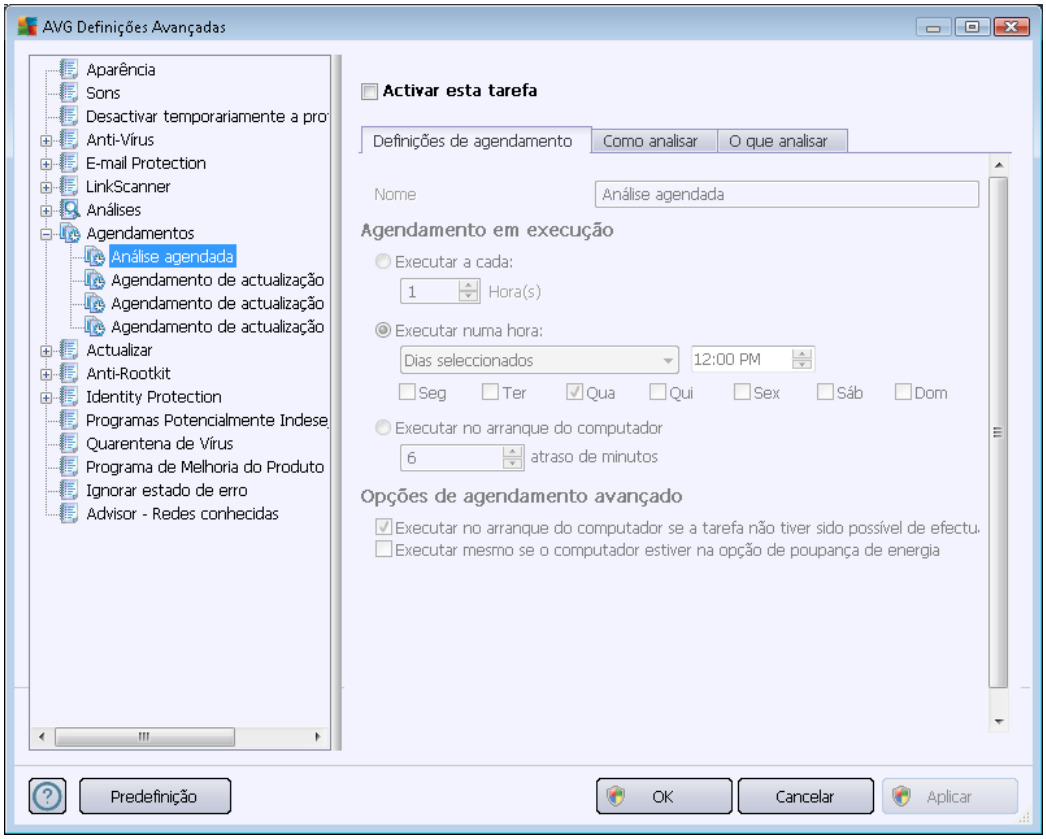
Na secção ***Agendamentos*** pode editar as definições predefinidas do:

- Análise agendada
- Agendamento de actualização de definições
- Agendamento de actualização do programa

- Agendamento de Actualização do Anti-Spam

10.8.1. Análise agendada

Os parâmetros da análise agendada podem ser editados (*ou configurado um novo agendamento*) nos três separadores. Em cada separador pode marcar/desmarcar o item ***Activar esta tarefa*** para desactivar temporariamente a análise agendada, e voltar a activá-la conforme necessário



De seguida, no campo de texto ***Nome*** ((*desactivado para todos os agendamentos predefinidos*) encontra o nome atribuído ao agendamento actual pelo fornecedor do software. Para agendamentos novos (*o utilizador pode adicionar novos agendamentos ao clicar com o botão direito do rato sobre o item* ***Análise agendada*** *na árvore de navegação à esquerda*) o utilizador pode especificar um nome da sua preferência, e nessas situações o campo de texto estará aberto para edição. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir.

Exemplo:*Não é adequado nomear uma análise com o nome "Nova análise" ou "A minha análise" uma vez que estes nomes não referem o que a análise efectivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc. Também não é necessário especificar no nome da análise se é a análise de todo o computador ou somente de ficheiros e pastas seleccionados – as suas próprias análises serão sempre uma versão específica da análise de ficheiros e pastas seleccionados.*

Nesta janela pode ainda definir os seguintes parâmetros de análise:

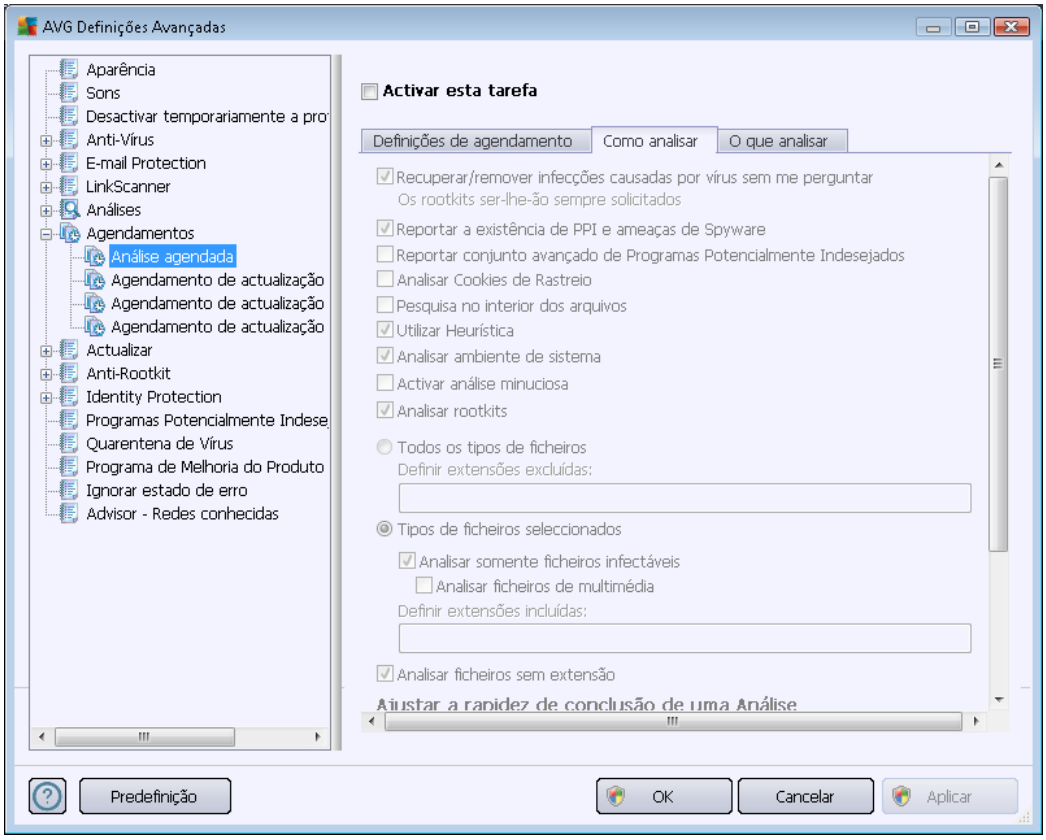
Agendamento em execução

Aqui, pode especificar os intervalos de tempo para a execução do novo agendamento de análise. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (***Executar a cada ...***) ou definindo uma data e hora precisas (***Executar a uma hora específica ...***), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Executar aquando do arranque do computador***).

Opções de agendamento avançado

Esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca. Uma vez iniciada a análise agendada à hora especificada, será informado deste facto através de uma janela pop-up aberta no ícone da Barra de Tarefas do AVG:

Será então apresentado um novo ícone AVG na barra de tarefas (*de cor cheia com uma lanterna – veja a imagem acima*) a informá-lo de que a análise agendada está em execução. Clique com o botão direito do rato sobre o ícone do AVG da análise em execução para abrir um menu de contexto onde pode optar por pausar. ou inclusivamente parar, a análise em execução; também pode alterar a prioridade da análise em questão.



No separador ***Como analisar*** encontrará uma lista de parâmetros de análise que podem ser opcionalmente activados/desactivados. A maioria dos parâmetros estão activados por predefinição e a funcionalidade será aplicada durante a análise. ***A menos que tenha uma razão válida para alterar estas definições, recomendamos que mantenha a configuração predefinida***:

- ***Recuperar/remover infecções causadas por vírus sem me perguntar*** *(activado por predefinição):* se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Se o ficheiro infectado não puder ser restaurado automaticamente, o objecto infectado será movido para a Quarentena de Vírus.

- ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** *(activado por predefinição):* marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado por predefinição*): marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por

predefinição.

- ***Analisar a existência de Cookies de Rastreio*** (*desactivado por predefinição*): este parâmetro do componente Anti-Spyware define que as cookies deverão ser detectadas durante a análise (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação especifica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos*)

- ***Analisar no interior de arquivos*** (*desactivado por predefinição*): este parâmetro define que a análise deverá verificar todos os ficheiros mesmo se estes estiverem comprimidos em arquivos, ex. ZIP, RAR,...

- ***Utilizar Heurística*** (*activado por predefinição*): a análise heurística (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a detecção de vírus durante a análise.

- ***Analisar o ambiente do sistema*** (*activado por predefinição*): a análise verificará também as áreas de sistema do seu computador;

- ***Activar análise minuciosa*** (*desactivado por predefinição):* em situações específicas (*suspeita de infecção do computador*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.

- ***Analisar a existência de rootkits*** *(activado por predefinição): a análise* Anti-Rootkit analisa o computador em busca de eventuais rootkits, ou seja, programas e tecnologias que podem ocultar actividade de malware no computador. Se for detectado um rootkit, isto não significa necessariamente que o computador esteja infectado. Em alguns casos, podem ser erroneamente detectados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Além disso deve decidir se pretende que sejam analisados

- ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções para a análise ao providenciar uma listagem extensões de ficheiro separadas por vírgula (*uma vez guardada, as vírgulas mudam para ponto e vírgula*) que não devem ser analisadas;

- ***Tipos de ficheiros seleccionados*** – pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infectados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser analisados.

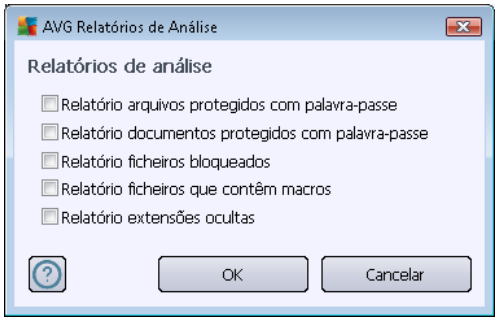
- Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

Ajustar a rapidez de conclusão de uma Análise

Na secção ***Ajustar a rapidez de conclusão de uma análise*** pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. O valor desta opção está, por predefinição, definido para o nível *definida pelo utilizador* de utilização automática de recursos. Se quiser que a análise seja executada mais rapidamente, esta demorará menos tempo mas a utilização de recursos do sistema aumentará significativamente durante a sua execução, e diminuirá o desempenho de outras actividades no seu PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir a utilização dos recursos do sistema prolongando a duração da análise.

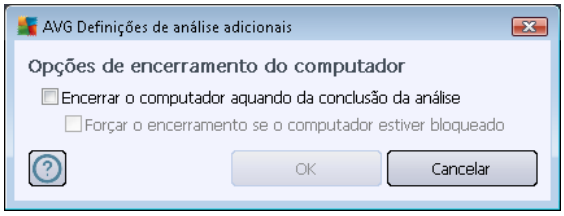
Definir relatórios de análise adicionais

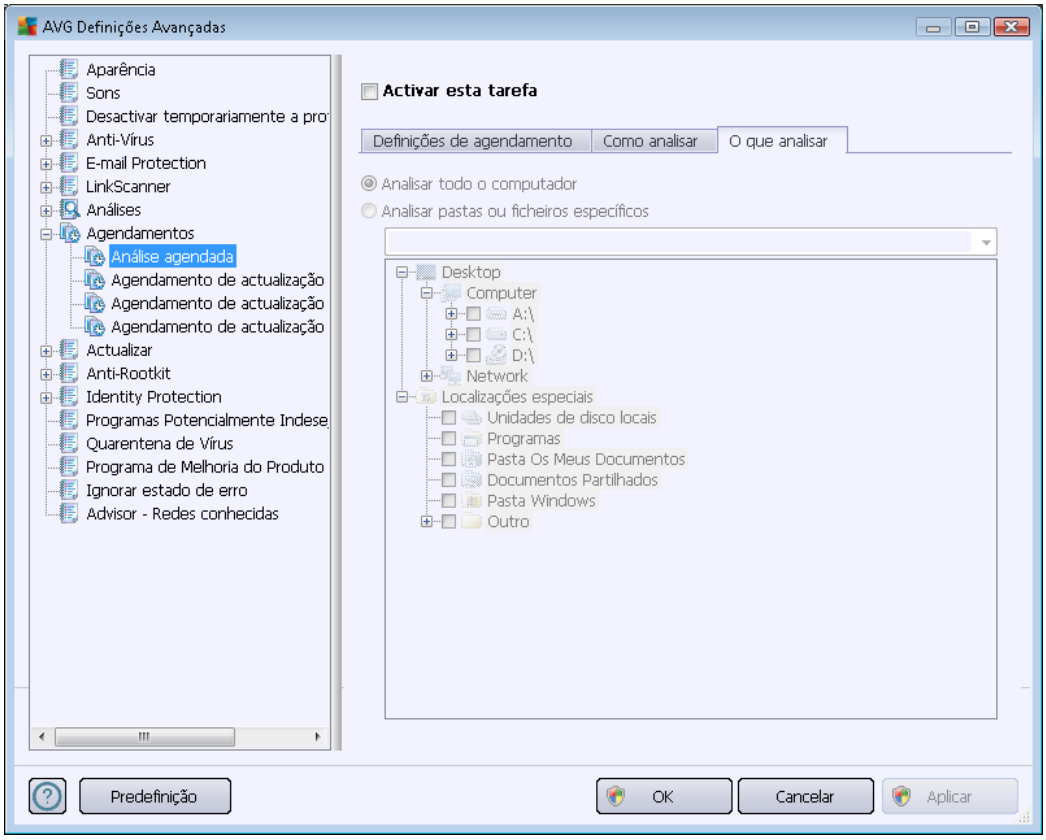
Clique no link ***Configurar relatórios de análise adicionais ...*** para abrir uma janela independente apelidada ***Relatórios de análise*** onde pode seleccionar vários itens para definir quais as detecções que deverão ser reportadas:



Definições de análise adicionais

Clique nas ***Definições de análise adicionais...***para abrir uma nova janela de ***Opções de encerramento do computador*** onde pode decidir se o computador deve ser encerrado automaticamente aquando do término do processo de análise. Tendo confirmado esta opção (***Encerrar o computador aquando do término da análise***), será activada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar encerramento se o computador estiver bloqueado***).

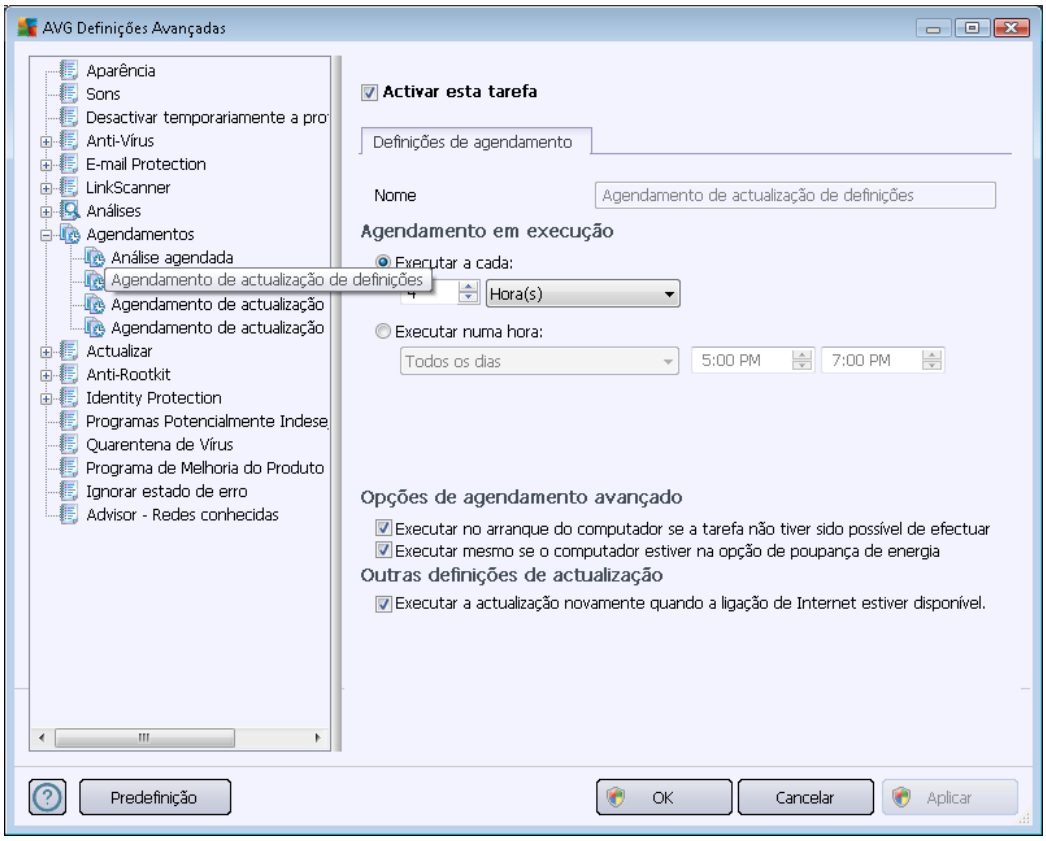




No separador ***O que analisar*** pode definir se pretende agendar uma análise a todo o computador ou analisar ficheiros e pastas específicos. Na eventualidade de seleccionar a análise de ficheiros/ pastas, na parte inferior desta janela é activada a estrutura da árvore apresentada e pode especificar pastas a serem analisadas.

10.8.2. Agendamento de Actualização de Definições

Se for ***realmente necessário***, pode desmarcar o item ***Activar esta tarefa*** para desactivar temporariamente a actualização de definições e activá-lo novamente mais tarde:



Nesta janela pode configurar alguns parâmetros detalhados do agendamento de actualização de definições. No campo de texto ***Nome*** (*desactivado para todos os agendamentos predefinidos*) encontra o nome atribuído ao agendamento actual pelo fornecedor do software.

Agendamento em execução

Nesta secção, especifique o intervalo de tempo para a execução do novo agendamento de actualização de definições. A temporização pode ser definida pela execução repetida da actualização após um determinado período de tempo (***Executar a cada...***) ou definindo uma data e hora específicas (***Executar à hora específica...***).

Opções de agendamento avançado

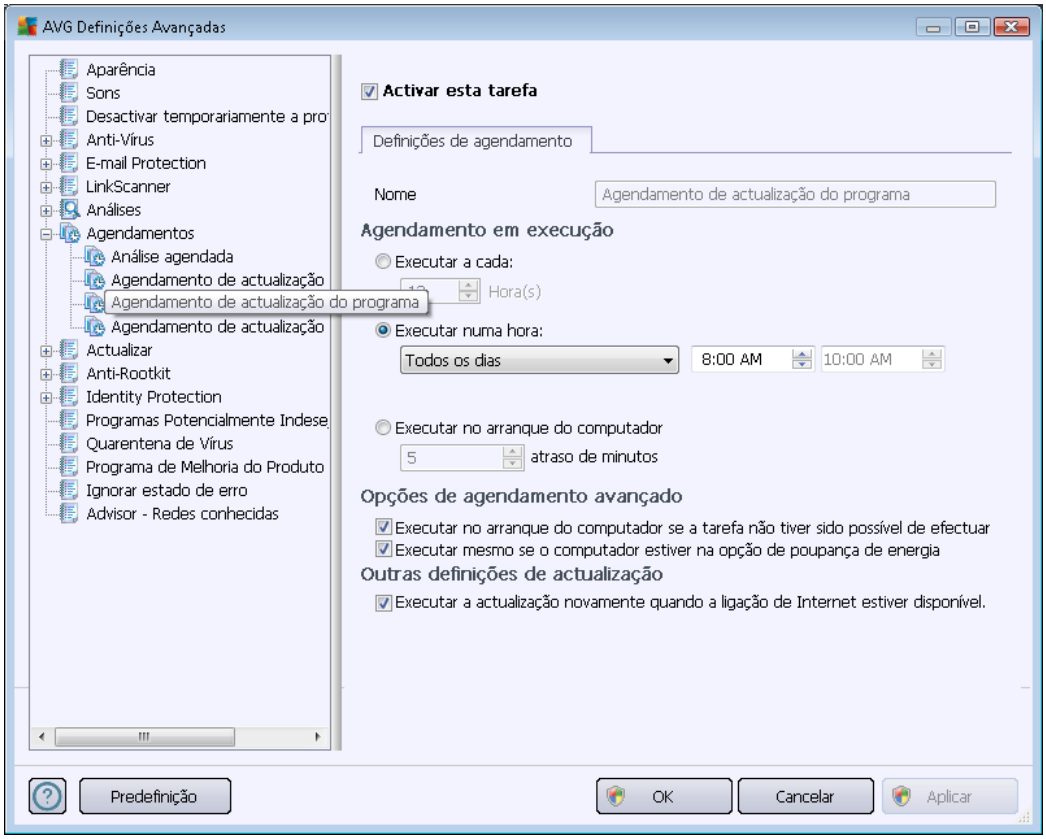
Esta secção permite-lhe definir em que condições a actualização de definições deverá/não deverá ser executada se o computador estiver em modo de bateria fraca ou desligado.

Outras definições de actualização

Finalmente, marque a opção ***Executar a actualização novamente assim que a ligação Internet estiver disponível*** para certificar-se de que se o processo de actualização ou a ligação à Internet falharem, a actualização será executada de novo imediatamente após o restabelecimento da ligação à Internet. Uma vez iniciado o agendamento à hora especificada, será avisado deste facto através de uma janela de pop-up aberta no ícone do AVG na Barra de Tarefas considerando que tenha mantido a configuração predefinida da janela *Definições Avançadas/Aparência*.

10.8.3. Agendamento de actualização do programa

Se for ***efectivamente necessário***, pode desmarcar o item ***Activar esta tarefa*** para desactivar temporariamente a actualização do programa agendada e voltar a activá-la posteriormente:



No campo de texto ***Nome*** (*desactivado para todos os agendamentos predefinidos*) encontra o nome atribuído ao agendamento actual pelo fornecedor do software.

Agendamento em execução

Aqui, especifique os intervalos de tempo para a execução do novo agendamento de actualização do programa. A temporização pode ser definida pela execução repetida da actualização após um determinado período de tempo (***Executar a cada ...***) ou definindo uma data e hora precisas (

Executar a uma hora específica ...), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Acção baseada no arranque do computador***).

Opções de agendamento avançado

Esta secção permite-lhe definir em que condições a actualização do programa deverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

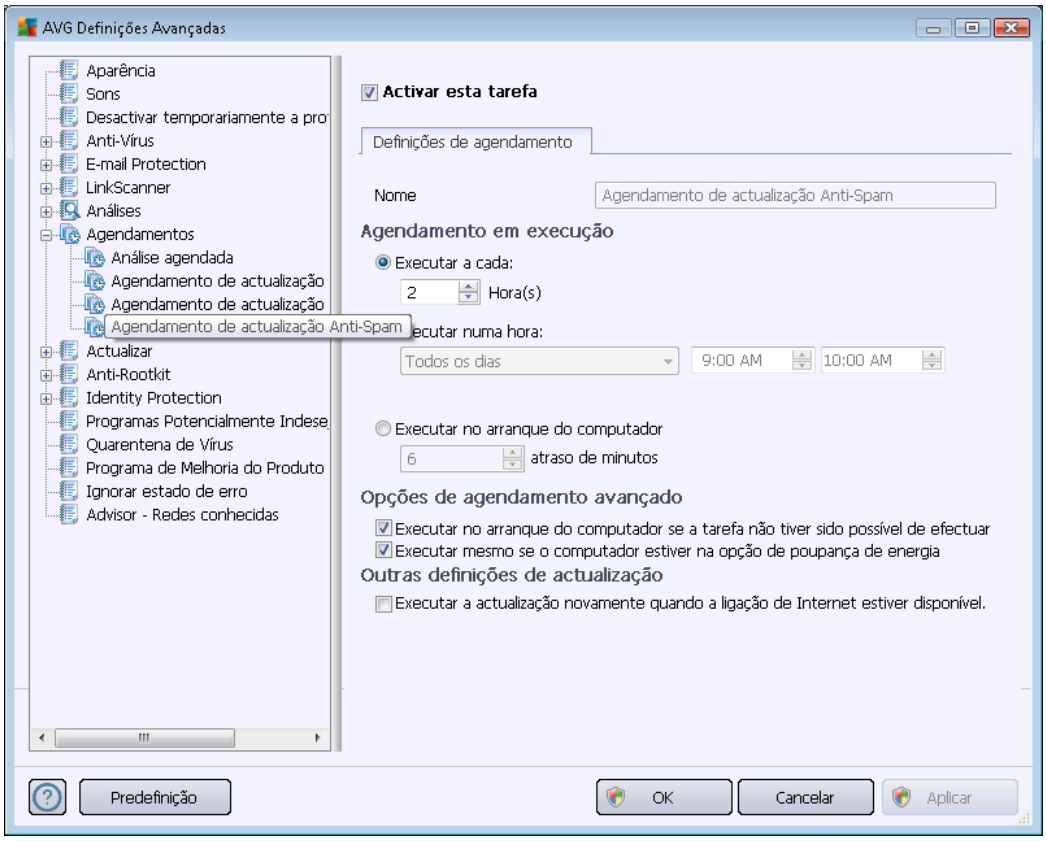
Outras definições de actualização

Marque a opção ***Executar a actualização novamente assim que a ligação Internet estiver disponível*** para certificar-se de que se o processo de actualização ou a ligação à Internet falharem, a actualização será executada de novo imediatamente após o restabelecimento da ligação à Internet. Uma vez iniciado o agendamento à hora especificada, será avisado sobre este facto através de uma janela de pop-up aberta no ícone do AVG na barra de tarefas (*considerando que tenha mantido a configuração predefinida da janela Definições Avançadas/Aparência*).

Nota: *Se ocorrer uma coincidência temporal de execução de um agendamento de actualização do programa e de um agendamento de uma análise, o processo de actualização terá precedência e a análise será interrompida.*

10.8.4. Agendamento de Actualização do Anti-Spam

Se for necessário, pode desmarcar o item ***Activar esta tarefa*** , simplesmente para desactivar a actualização agendada do Anti-Spam temporariamente e activá-la novamente mais tarde:



Nesta janela pode configurar alguns parâmetros detalhados do agendamento de actualização. No campo de texto ***Nome*** (*desactivado para todos os agendamentos predefinidos*) encontra o nome atribuído ao agendamento actual pelo fornecedor do software.

Agendamento em execução

Aqui, especifique os tempos de intervalo para a execução de novos agendamentos de actualização do Anti-Spam. A temporização pode ser definida pela execução repetida da actualização do Anti-Spam após um determinado período de tempo (***Executar a cada ...***) ou definindo uma data e hora precisas (***Executar a uma hora específica ...***), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Acção baseada no arranque do computador***).

Opções de agendamento avançado

Esta secção permite-lhe definir em que condições a actualização do Anti-Spam deverá/não deverá ser executada se o computador estiver em modo de bateria fraca ou desligado.

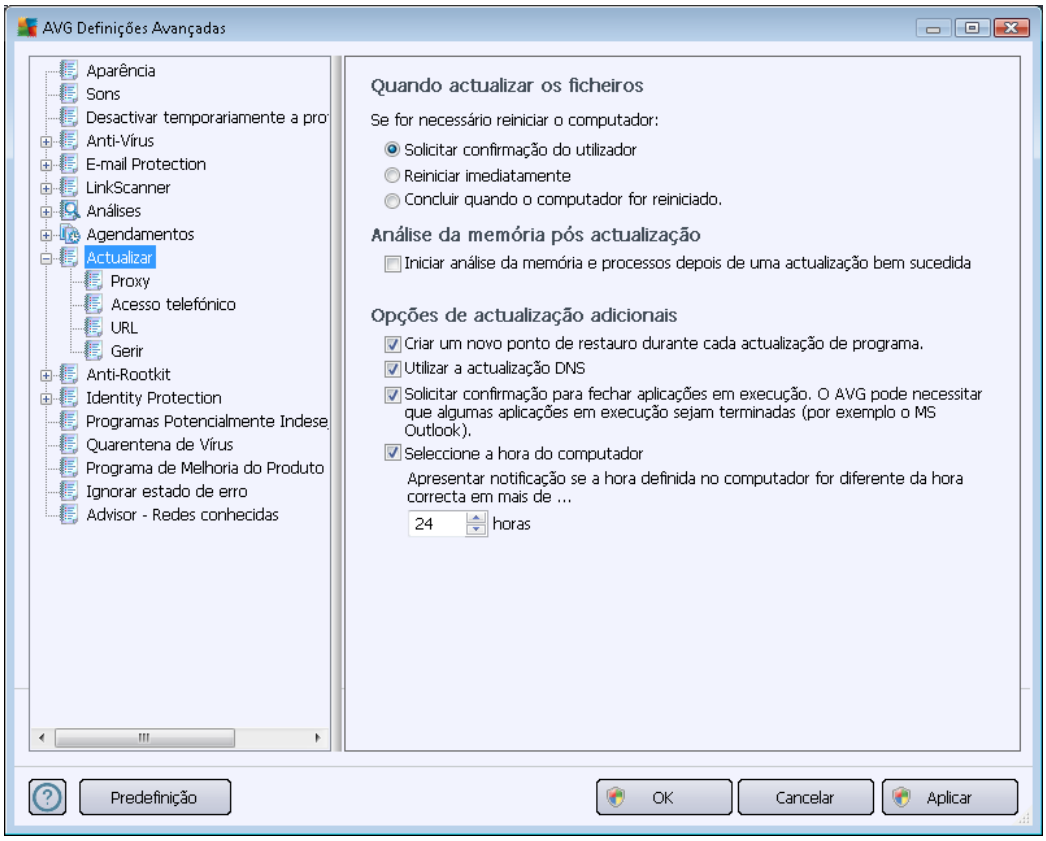
Outras definições de actualização

Marque a opção ***Executar a actualização novamente assim que a ligação Internet estiver disponível*** para certificar-se de que, se o processo de actualização do componente Anti-Spam ou a ligação à Internet falharem, a actualização será executada, de novo, imediatamente após o restabelecimento da ligação à Internet.

Uma vez iniciada a análise agendada à hora especificada, será avisado sobre este facto através de uma janela de pop-up aberta no ícone do AVG na Barra de Tarefas (*considerando que tenha mantido a configuração predefinida da janela Definições Avançadas/Aparência*).

10.9. Actualizar

O item de navegação ***Actualizar*** abre uma nova janela onde pode especificar parâmetros gerais relativos à actualização do AVG:



Quando actualizar os ficheiros

Nesta secção pode optar entre três alternativas a serem usadas caso o processo de actualização requeira a reinicialização do PC. A conclusão do processo de actualização pode ser agendada para o próximo arranque do PC, ou pode executar a reinicialização imediatamente:

- ***Requerer confirmação ao utilizador*** *(activado por predefinição)* - ser-lhe-á pedido que aprove um reinicio do PC necessário para finalizar o processo de actualização

- ***Reiniciar imediatamente*** – o computador será reiniciado automaticamente após o processo de actualização terminar, e a sua aprovação não será necessária

- ***Concluir quando o computador for reiniciado*** – a conclusão do processo de actualização será adiada até ao próximo arranque do computador. Tenha em conta que esta opção só é recomendada se tiver a certeza de que o computador é ligado e desligado com regularidade, pelo menos uma vez por dia!

Análise da memória pós actualização

Marque esta caixa para definir se pretende iniciar uma nova análise da memória após cada actualização bem sucedida. A actualização transferida pode conter novas definições de vírus, e estas podem ser aplicadas na análise imediatamente.

Opções de actualização adicionais

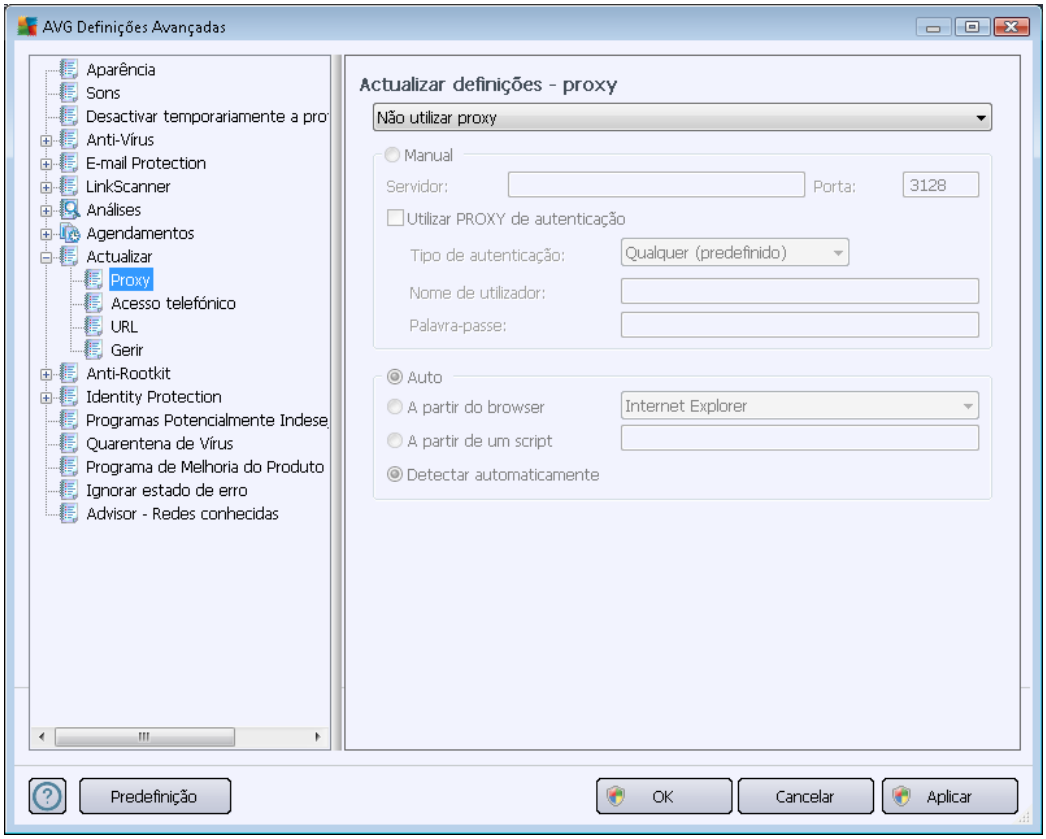
- ***Criar um novo ponto de restauro do sistema durante cada actualização de programa*** – antes da execução de cada actualização de Programa do AVG, o sistema criará um ponto de restauro do sistema. Na eventualidade do processo de actualização falhar e o seu sistema operativo falhar pode sempre restaurar o seu SO para a configuração original a partir deste ponto. Esta opção é acessível via Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauro do Sistema , mas quaisquer alterações são recomendadas apenas a utilizadores avançados! Mantenha esta caixa seleccionada se quiser utilizar esta funcionalidade.

- ***Utilizar a actualização DNS*** (*activado por predefinição*) – com este item marcado, o seu **AVG Internet Security 2012** consulta as informações relativas à última versão da base de dados de vírus e à mais recente versão do programa no servidor DNS. Então, só são transferidos, e aplicados, os ficheiros de actualização mais pequenos e indispensáveis. Desta forma, a quantidade total de dados transferidos é minimizada e o processo de actualização é executado mais depressa.

- ***Requerer confirmação para fechar aplicações em execução*** (*activado por predefinição*) estará a certificar-se de que não serão fechadas quaisquer aplicações actualmente em utilização sem a sua permissão – se necessário para que o processo de actualização seja concluído.

- ***Verificar a hora do computador*** – seleccione esta opção para especificar que pretende que seja apresentada uma notificação na eventualidade de a hora do computador ser diferente da hora correcta além do número de horas especificado.

10.9.1. Proxy



O servidor proxy é um servidor autónomo ou um serviço executado no computador que garante uma ligação mais segura à Internet. De acordo com as regras de rede especificadas, pode aceder à Internet directamente ou através do servidor proxy; as duas possibilidades podem ser permitidas em simultâneo. Depois, no primeiro item da janela ***Definições de actualização – proxy*** pode seleccionar a partir do menu da janela de sequência se pretender:

- ***Utilizar proxy***
- ***Não usar proxy*** – predefinições
- ***Tentar ligação utilizando proxy e se falhar, ligar directamente***

Se seleccionar qualquer opção utilizando o servidor proxy, terá de especificar mais alguns dados. As definições do servidor podem ser configuradas manualmente ou automaticamente.

Configuração manual

Se seleccionar a configuração manual (verifique *a **opção Manual** para activar a secção respectiva da janela*) tem de especificar os seguintes itens:

- ***Servidor*** - especifique o endereço IP do servidor ou o nome do servidor

- ***Porta*** - especifique o número da porta que permite aceder directamente à Internet (*por predefinição, este número está configurado para 3128 mas pode ser configurado para um número diferente -se não tiver a certeza, contacte o administrador da rede*)

O servidor proxy também pode ter regras específicas configuradas para cada utilizador. Se o seu servidor proxy estiver configurado desta forma, seleccione a opção ***Utilizar PROXY de autenticação*** para verificar se o seu nome de utilizador e palavra-passe são válidos para estabelecer ligação à Internet via o servidor proxy.

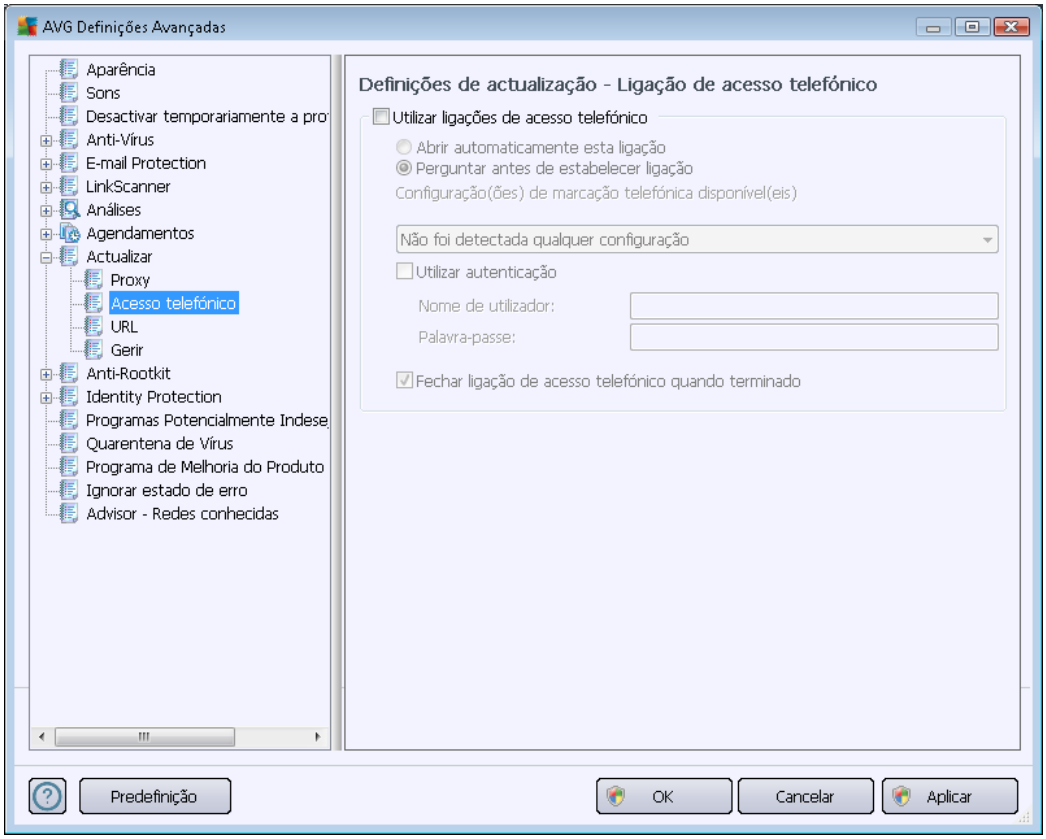
Configuração automática

Se seleccionar a configuração automática *(marque a opção **Auto** para activar a secção respectiva da janela*) e depois por favor seleccione de onde a configuração proxy deve ser retirada:

- ***A partir do browser*** - a configuração será lida a partir do seu browser predefinido
- ***Do script*** – a configuração será lida a partir do script transferido com a função a devolver o endereço do proxy
- ***Auto-detecção*** – a configuração será detectada automática e directamente a partir do servidor proxy

10.9.2. Acesso telefónico

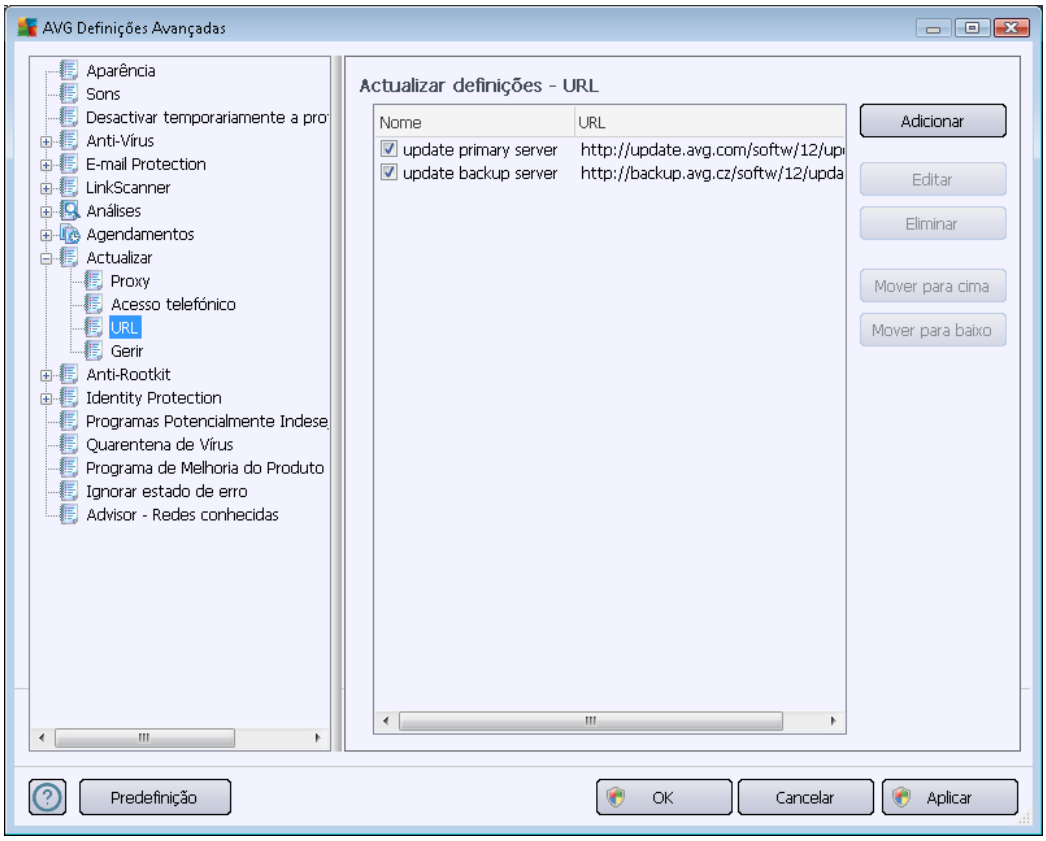
Todos os parâmetros definidos na janela ***Definições de Actualização – Ligação de acesso telefónico*** referem-se à ligação à Internet de Acesso telefónico. Os campos do separador estão inactivos até que seja marcada a opção ***Utilizar ligações de Acesso Telefónico*** que activa os campos:



Especifique se pretende ligar à Internet automaticamente (***Abrir automaticamente esta ligação***) ou se pretende confirmar manualmente a ligação (***Perguntar antes de estabelecer ligação***). Para que a ligação seja estabelecida automaticamente deve ainda seleccionar se a mesma deverá concluir após a actualização estar terminada (***Fechar ligação de acesso telefónico quando terminado***).

10.9.3. URL

A janela ***URL*** apresenta uma lista de endereços da Internet a partir dos quais pode transferir os ficheiros de actualização:



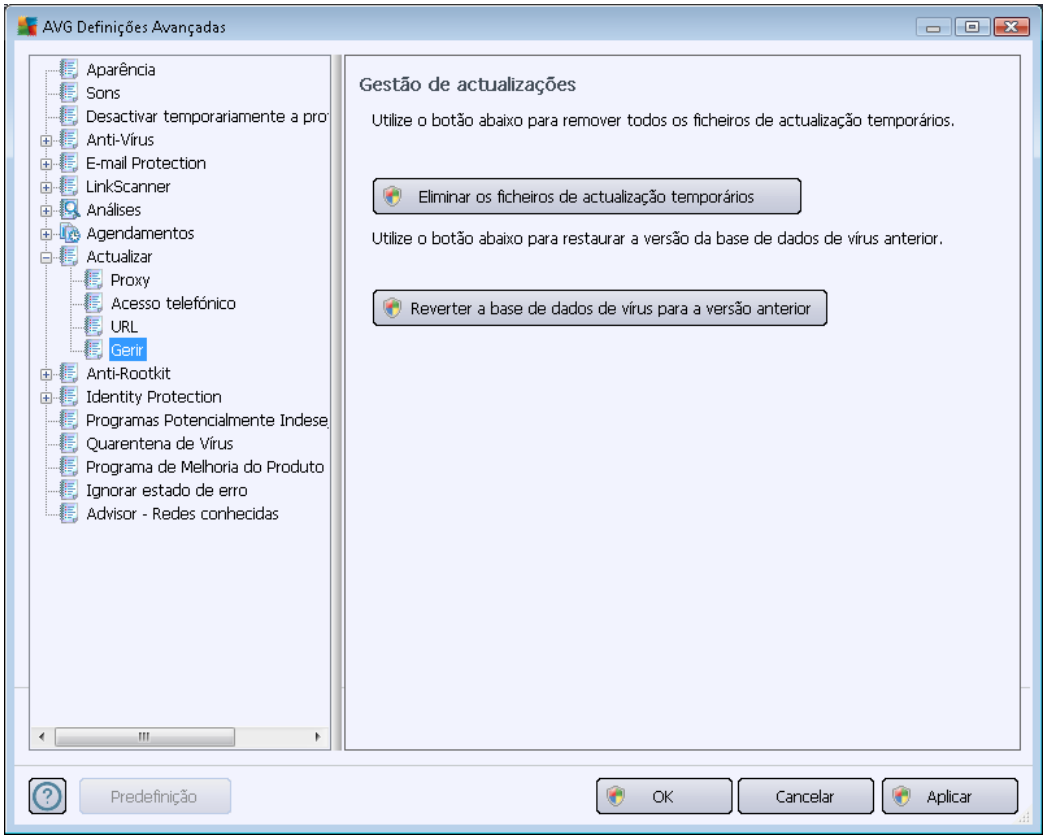
Botões de controlo

A lista e os respectivos itens podem ser modificados, utilizando os botões de controlos seguintes:

- ***Adicionar*** – abre uma janela onde pode especificar um novo URL a adicionar à lista
- ***Editar*** – abre uma janela onde pode editar os parâmetros do URL seleccionado
- ***Eliminar*** – elimina o URL seleccionado da lista
- ***Mover para cima*** – move o URL seleccionado uma posição para cima na lista
- ***Mover para baixo*** – move o URL seleccionado uma posição para baixo na lista

10.9.4. Gerir

A janela ***Gestão de actualizações*** faculta duas opções acessíveis via dois botões:

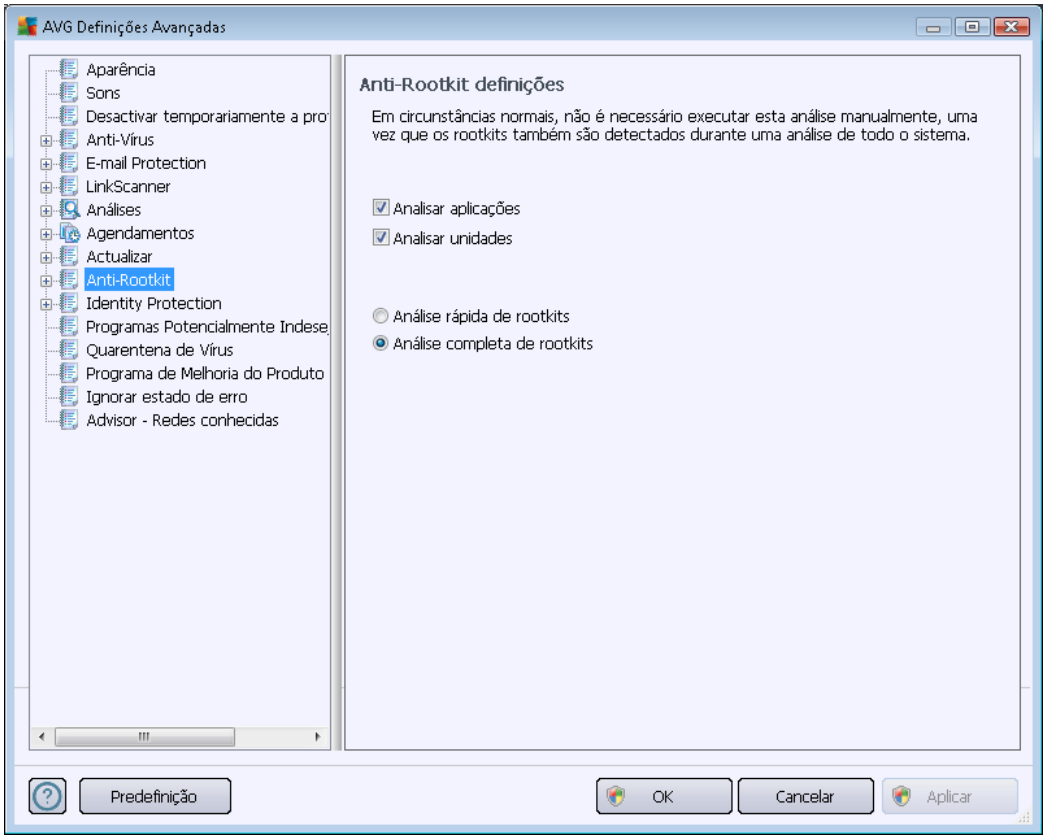


- ***Eliminar os ficheiros de actualização temporários*** - prima este botão para eliminar todos os ficheiros de actualização redundantes do seu disco rígido (*por predefinição, estes ficheiros são guardados durante 30 dias*)

- ***Reverter a base de dados de vírus para a versão anterior*** - prima este botão para eliminar a última versão da base de dados de vírus do seu disco rígido e para regressar à versão anteriormente guardada (*a nova versão de base de dados de vírus fará parte da actualização seguinte*)

10.10. Anti-Rootkit

Na janela de ***Definições do Anti-Rootkit***, pode editar a configuração do componente Anti-Rootkit e parâmetros específicos da análise anti-rootkit. A análise anti-rootkit é um processo predefinido incluído na Análise de todo o computador:



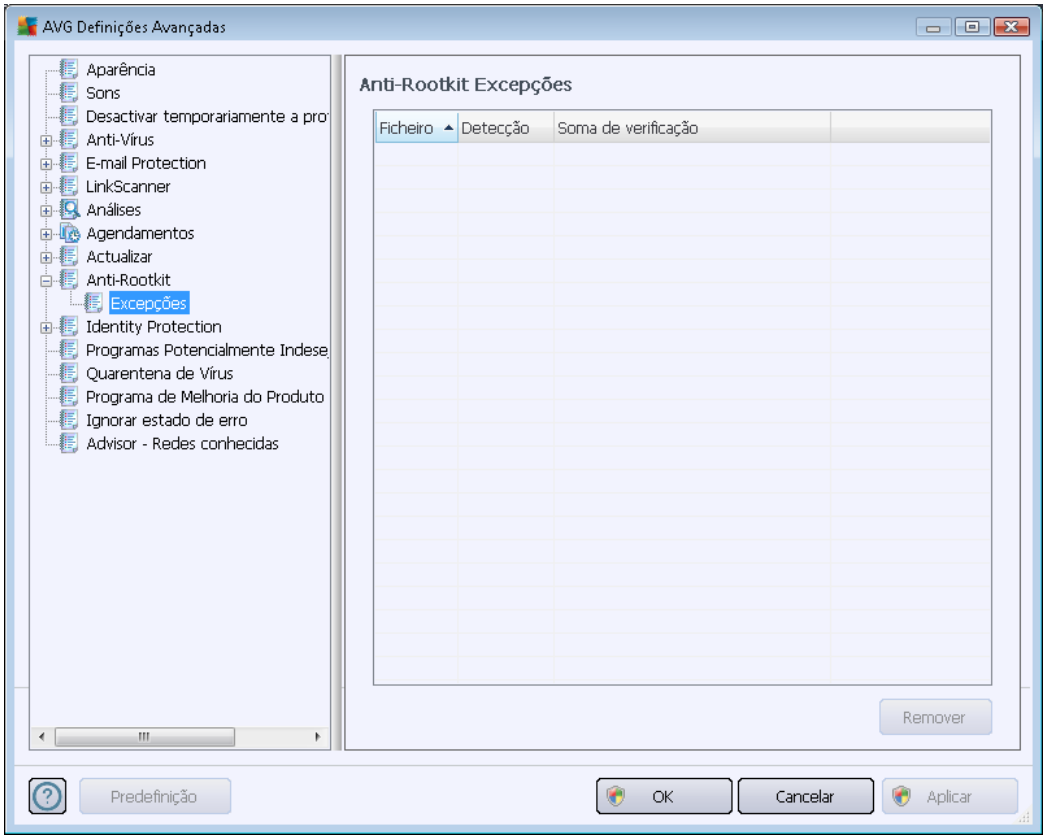
A edição de todas as funções do componente Anti-Rootkit, conforme dispostas nesta janela, também é acessível directamente a partir da interface do componente Anti-Rootkit.

Analisar aplicações e ***Analisar controladores*** permitem-lhe especificar detalhadamente o que deve ser incluído na análise anti-rootkit. Estas definições são destinadas a utilizadores avançados; recomendamos que mantenha todas as opções activadas. Posteriormente, pode escolher o modo de análise de rootkits:

- ***Análise rápida de rootkits*** – analisa todos os processos em execução, controladores carregados e a pasta de sistema (*normalmente c:\Windows*)
- ***Análise completa de rootkits*** – analisa todos os processos em execução, controladores carregados, a pasta de sistema (*normalmente c:\Windows*), e todos os discos locais (*incluindo unidades flash mas excluindo unidades de disquete/CD*)

10.10.1. Excepções

Na janela ***Excepções do Anti-Rootkit*** pode definir ficheiros específicos *(por exemplo, alguns controladores que possam ser falsos positivos detectados como rootkits)* que deverão ser excluídos desta análise:

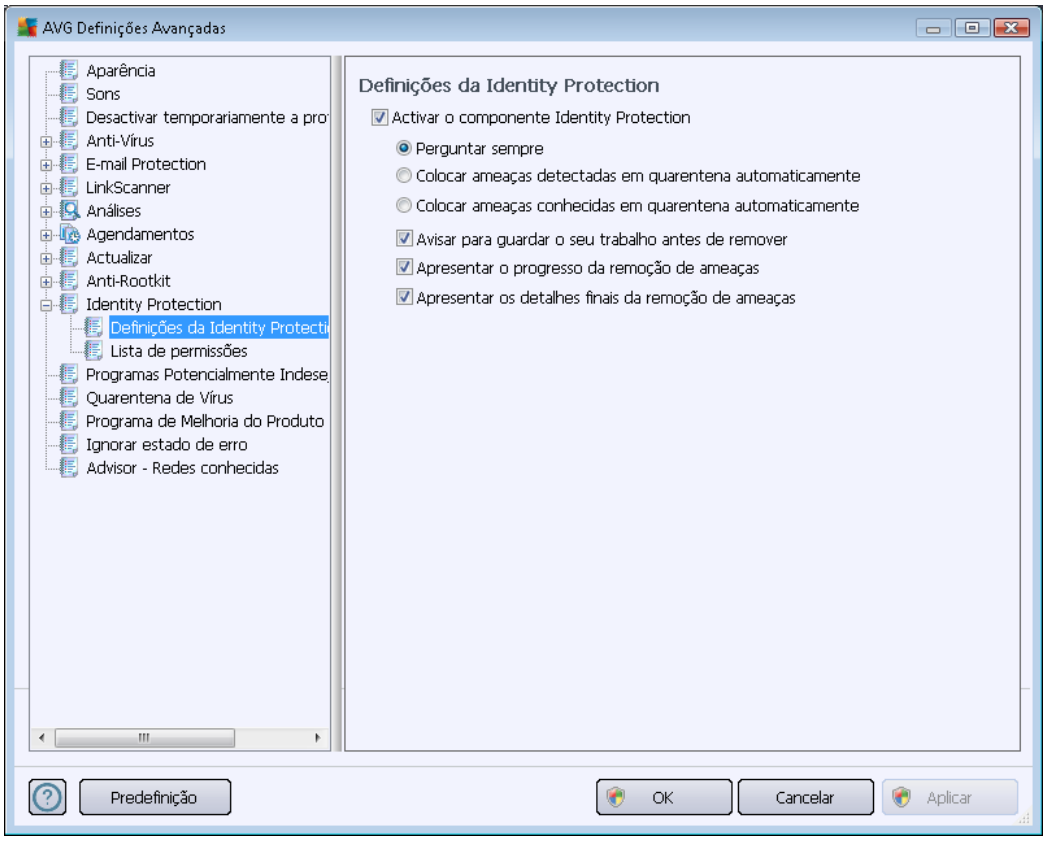


10.11. Protecção de Identidade

Protecção de Identidade é um componente anti-malware que o protege de todos os tipos de malware (*spyware, bots, roubos de identidade, etc.*) utilizando tecnologias comportamentais e proporciona protecção imediata contra novos vírus *(para ver uma descrição detalhada da funcionalidade do componente, consulte o capítulo Protecção de Identidade*).

10.11.1. Definições da Protecção de Identidade

A janela ***Definições da Protecção de Identidade*** permite-lhe activar/desactivar as funcionalidades elementares do componente Protecção de Identidade:



Activar a Protecção de Identidade (*activado por predefinição*) – desmarque para desactivar o componente Protecção de Identidade.

Recomendamos vivamente que não faça isto a menos que seja indispensável!

Quando a Protecção de Identidade está activada, pode especificar que acção tomar quando uma ameaça é detectada:

- ***Perguntar sempre*** (*activado por predefinição*) – quando uma ameaça for detectada, ser-lhe-á solicitado que decida se a mesmo deve ser movida para a quarentena para garantir que não são removidas aplicações que pretende ter em execução.
- ***Colocar ameaças detectadas em quarentena automaticamente*** - marque esta caixa para definir que pretende que todas as ameaças eventualmente detectadas movidas para o espaço seguro da Quarentena de Vírus do imediatamente. Se mantiver as predefinições, quando uma ameaça for detectada, ser-lhe-á solicitado que decida se a mesma deve ser movida para a quarentena para garantir que não são removidas aplicações que pretende ter em execução.
- ***Colocar ameaças conhecidas em quarentena automaticamente*** – mantenha este item

marcado se quiser que todas as aplicações detectadas como potencial malware sejam automática e imediatamente movidas para a Quarentena de Vírus do.

Pode, ainda, atribuir itens específicos para activar mais funcionalidades opcionais da Protecção de Identidade:

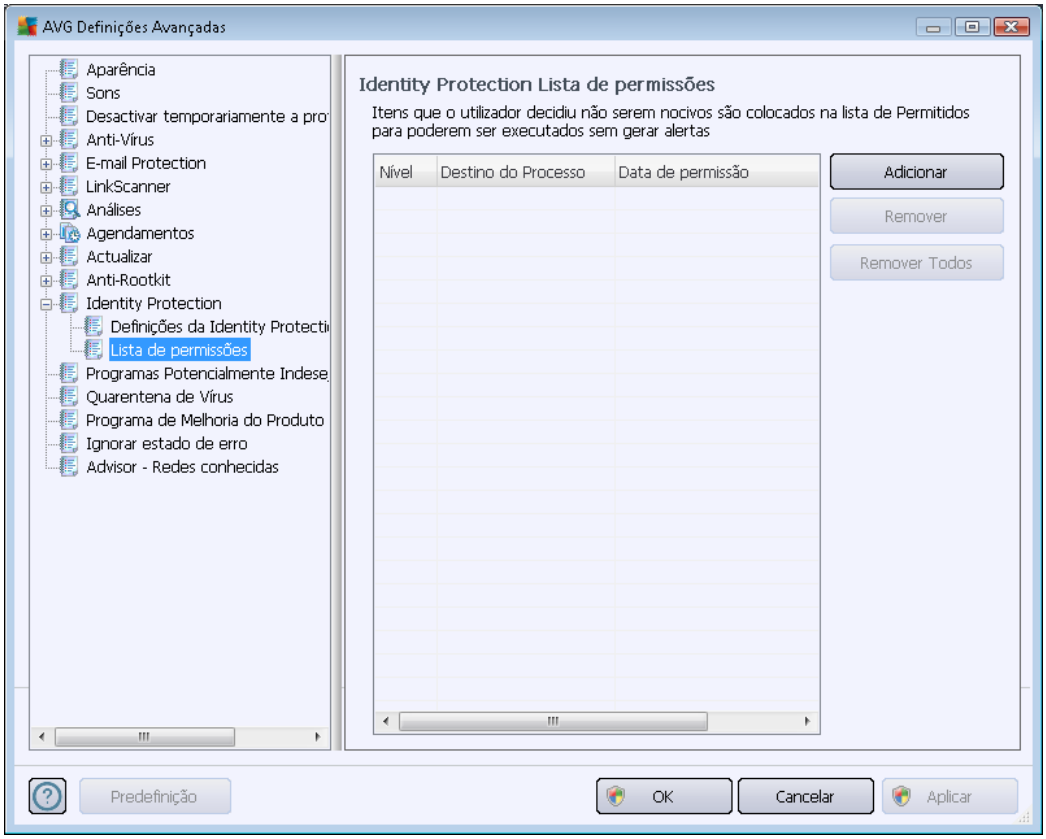
- ***Avisar para guardar o seu trabalho antes de remover*** - (*activado por predefinição*) – marque este item se pretender ser avisado antes de a aplicação detectada como possível malware ser retirada para a quarentena. Caso esteja a trabalhar com a aplicação, o seu projecto pode perder-se e é necessário guardá-lo primeiro. Por predefinição, este item está activado e recomendamos vivamente que o mantenha assim.

- ***Apresentar o progresso da remoção de ameaças*** - (*activado por predefinição*) – com este item activado, assim que é detectado um possível malware, abre-se uma nova janela de diálogo para mostrar o progresso de remoção do malware para a quarentena.

- ***Apresentar os detalhes finais da remoção de ameaças*** - (*activado por predefinição*) – com este item activado, a ***Protecção de Identidade*** apresenta informações detalhadas sobre cada objecto movido para a quarentena (*grau de gravidade, localização, etc.*).

10.11.2. Lista de Permissões

Se, na janela ***definições da Protecção de Identidade***, decidir manter o item ***Colocar ameaças detectadas em quarentena automaticamente*** desmarcado, sempre que for detectado software potencialmente perigoso será inquirido sobre a intenção de remoção do mesmo. Se, em seguida, indicar como segura a aplicação suspeita (*detectada com base no seu comportamento*) e confirmar que a mesma deve continuar instalada no computador, a aplicação será adicionada à ***Lista de permissões da Protecção de Identidade*** e não voltará a ser identificada como potencialmente perigosa:



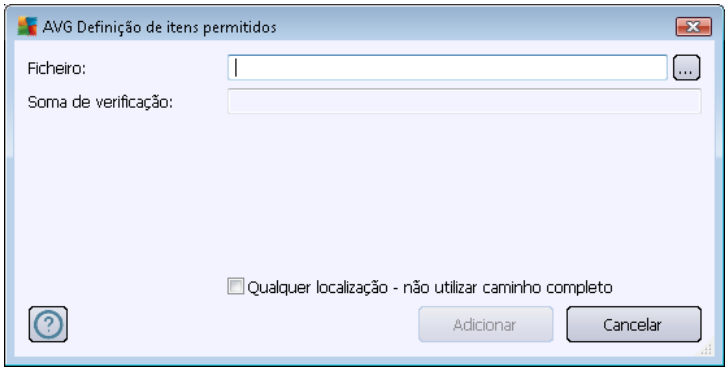
A ***Lista de permissões da Protecção de Identidade*** disponibiliza as seguintes informações sobre cada aplicação:

- ***Nível*** – identificação gráfica da gravidade do processo respectivo numa escala de quatro níveis, do menos grave (■□□□) até ao crítico (■■■■)
- ***Localização do processo*** - localização do ficheiro executável da aplicação (*processo*)
- ***Data de permissão*** – data em que classificou manualmente a aplicação como segura.

Botões de controlo

Os botões de controlo disponíveis na janela de ***Lista de permissões da Protecção de Identidade*** são os seguintes:

- ***Adicionar*** - prima este botão para adicionar uma nova aplicação à lista de permissões. É apresentada a seguinte janela:

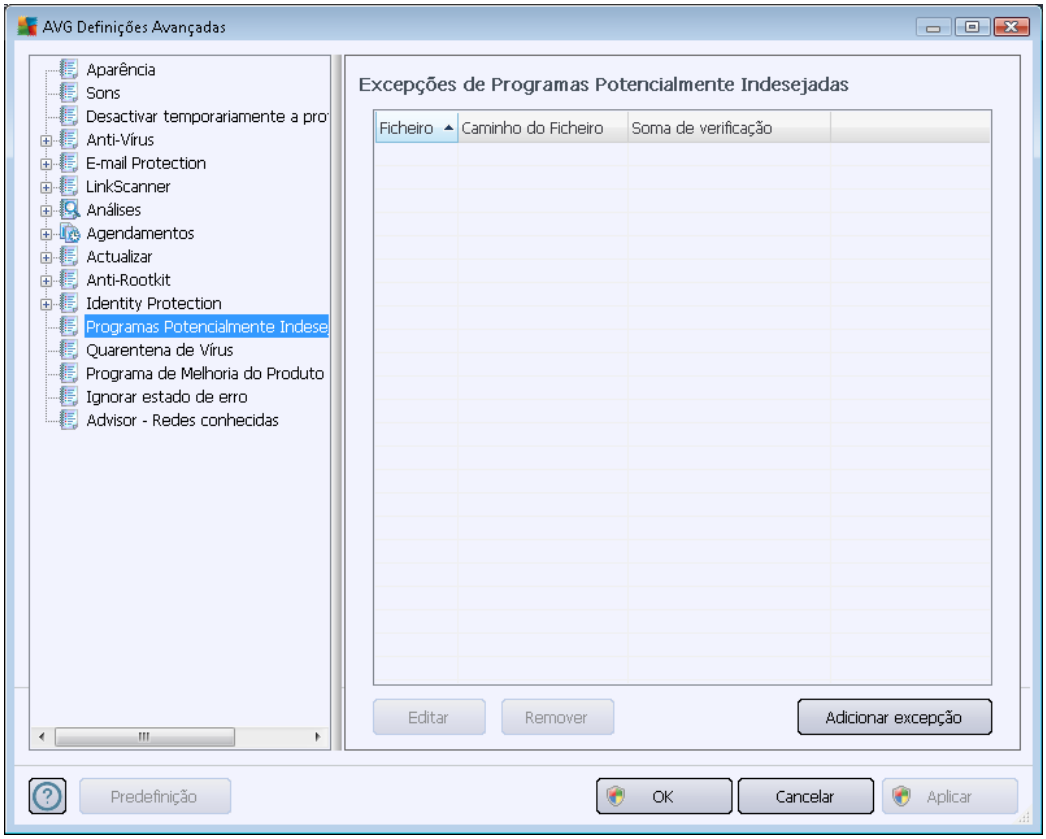


- ***Ficheiro*** – digite o caminho completo do ficheiro (*aplicação*) que pretende marcar como excepção
- ***Soma de verificação*** – apresenta a 'assinatura' única do ficheiro seleccionado. Esta soma de verificação é uma cadeia de caracteres gerada automaticamente, que permite ao AVG distinguir inequivocamente o ficheiro seleccionado dos outros ficheiros. A soma de verificação é gerada e apresentada depois do ficheiro ser correctamente adicionado.
- ***Qualquer localização – não utilize a localização completa*** – se pretender definir este ficheiro como uma excepção para a localização específica, deixe esta caixa desmarcada

- ***Remover*** - prima para remover a aplicação seleccionada da lista
- ***Remover todos*** - prima para remover todas as aplicações listadas

10.12. Programas Potencialmente Indesejados

O **AVG Internet Security 2012** possui a capacidade de analisar e detectar aplicações executáveis ou bibliotecas DLL que poderão ser potencialmente indesejadas no sistema. Em alguns casos, o utilizador pode pretender manter alguns programas indesejados no computador (programas que foram instalados propositadamente). Alguns programas, especialmente programas gratuitos, incluem adware. Esse adware pode ser detectado e reportado pelo **AVG Internet Security 2012** como *programa potencialmente indesejado*. Se pretender manter um tal programa no computador, pode defini-lo como uma Excepção de Programa Potencialmente Indesejado:

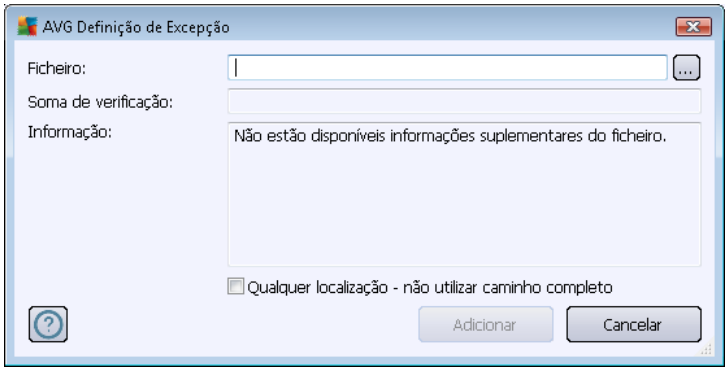


A janela das ***Excepções de Programas Potencialmente Indesejados*** apresenta uma lista de excepções actualmente válidas e já definidas de programas potencialmente indesejados. Pode editar a lista, eliminar itens existentes, ou adicionar novas excepções. As seguintes informações podem ser encontradas na lista para todas as excepções:

- ***Ficheiro*** - faculta o nome exacto da aplicação respectiva
- ***Localização do Ficheiro*** - apresenta a localização da aplicação
- ***Soma de verificação*** – apresenta a 'assinatura' única do ficheiro seleccionado. Esta soma de verificação é uma cadeia de caracteres gerada automaticamente, que permite ao AVG distinguir inequivocamente o ficheiro seleccionado dos outros ficheiros. A soma de verificação é gerada e apresentada depois do ficheiro ser correctamente adicionado.

Botões de controlo

- ***Editar*** – abre uma janela de edição (*idêntica à janela para definição de novas excepções, veja abaixo*) de uma excepção já definida, onde pode alterar os parâmetros de excepção
- ***Remover*** – elimina o item seleccionado da lista de excepções
- ***Adicionar excepção*** – abre uma janela de edição onde pode definir os parâmetros da nova excepção a ser criada:



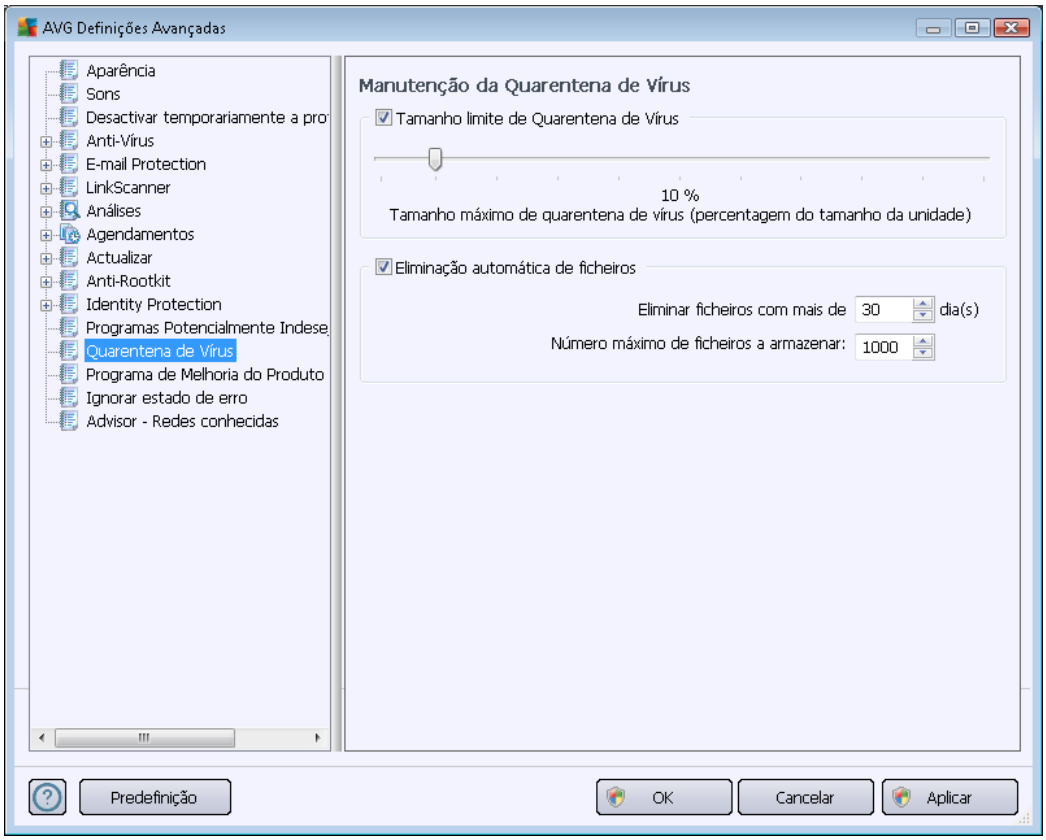
- ***Ficheiro*** – digite o caminho completo do ficheiro que pretende marcar como excepção

- ***Soma de verificação*** – apresenta a 'assinatura' única do ficheiro seleccionado. Esta soma de verificação é uma cadeia de caracteres gerada automaticamente, que permite ao AVG distinguir inequivocamente o ficheiro seleccionado dos outros ficheiros. A soma de verificação é gerada e apresentada depois do ficheiro ser correctamente adicionado.

- ***Informação do ficheiro*** - apresenta qualquer informação adicional disponível acerca do ficheiro *(informações de licença/versão, etc.)*

- ***Qualquer localização – não utilize a localização completa*** – se pretender definir este ficheiro como uma excepção para a localização específica, deixe esta caixa desmarcada. Se a caixa estiver marcada, o ficheiro especificado é definido como excepção independentemente da sua localização *(no entanto, é necessário introduzir a localização completa do ficheiro em causa; o ficheiro será então usado como exemplo único para o caso de surgirem dois ficheiros com o mesmo nome no sistema)*.

10.13. Quarentena de Vírus



A janela ***Manutenção da Quarentena de Vírus*** permite-lhe definir vários parâmetros em relação à administração dos objectos armazenados na Quarentena de Vírus:

- ***Tamanho Limite da Quarentena de Vírus*** – Utilize o cursor para definir o tamanho máximo da Quarentena de Vírus. O tamanho é especificado proporcionalmente ao tamanho do seu disco local.

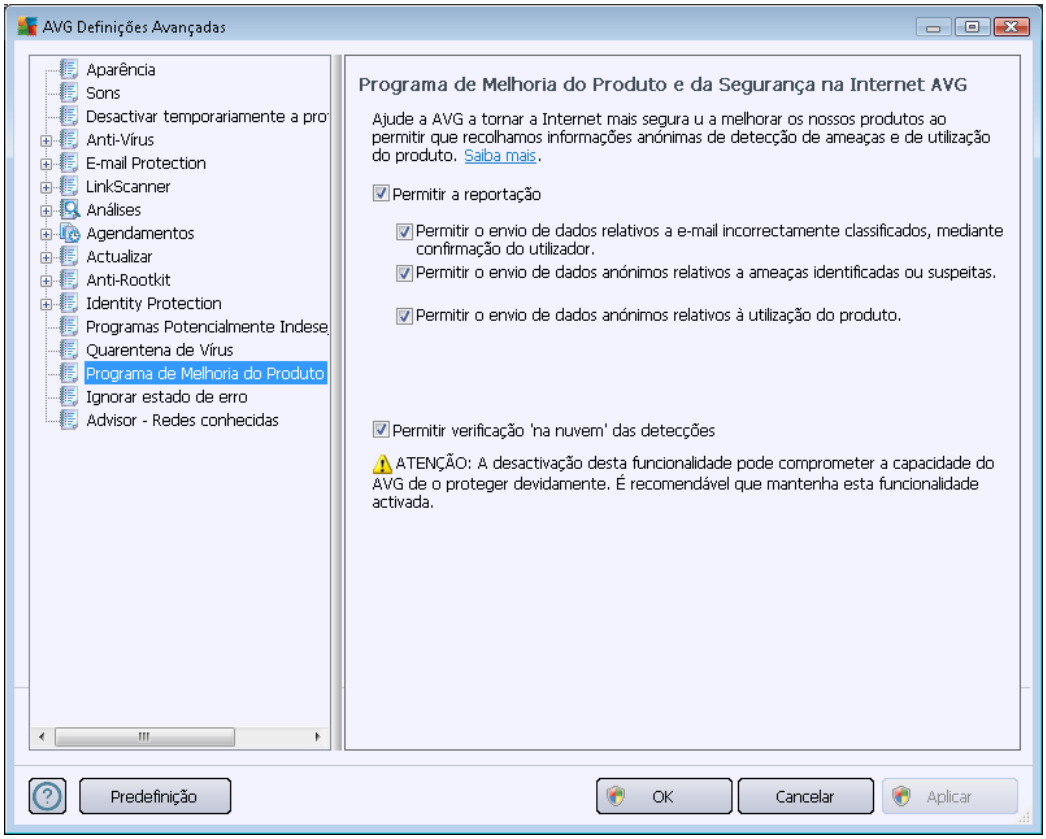
- ***Eliminação automática de ficheiro*** – Nesta secção defina o tempo máximo que os objectos deverão ficar armazenados na Quarentena de Vírus (***Eliminar ficheiros mais antigos do que ...dias***), e o número máximo de ficheiros a serem armazenados na Quarentena de Vírus (***Número máximo de ficheiros a serem armazenados***).

10.14. Programa de Melhoria do Produto

A janela ***Programa de Melhoria do Produto e Segurança na Internet AVG*** convida-o a participar no programa de melhoria do produto da AVG e ajudar-nos a aumentar o nível de segurança na Internet em geral. Mantenha a opção ***Permitir a reportação*** marcada para permitir a reportação de ameaças detectadas aos laboratórios da AVG. Esta acção ajuda a recolher informação actualizada relativa às mais recentes ameaças de participantes de todo o mundo e, em troca, podemos melhorar a protecção para todos.

A reportação é processada automaticamente, como tal não lhe causa qualquer inconveniente.

Não são incluídos nos relatórios quaisquer dados de identificação pessoal. A reportação de ameaças detectadas é opcional; contudo, pedimos que mantenha esta opção activada. Ajuda-nos a melhorar a protecção para o utilizador em particular e todos os utilizadores do AVG em geral.



Nesta janela, estão disponíveis as seguintes opções de configuração:

- ***Permitir a reportação*** *(activado por predefinição)* - Se quiser ajudar-nos a melhorar ainda mais o **AVG Internet Security 2012**, mantenha a caixa seleccionada. Desta forma activa a reportação de todas as ameaças detectadas à AVG, para que possamos recolher informações actualizadas sobre malware de todos os participantes a nível mundial e, como compensação, melhorar a protecção para todos. A reportação é processada automaticamente, como tal não lhe causa qualquer inconveniente, e não são incluídos nos relatórios quaisquer dados de identificação pessoal.
    - ***Permitir o envio de dados relativos a e-mail incorrectamente classificados, mediante confirmação do utilizador*** *(activado por predefinição)* – enviar informações sobre mensagens de e-mail incorrectamente identificadas como spam, ou sobre mensagens de spam que não foram detectadas pelo componente Anti-Spam. Ao enviar este tipo de informações, ser-lhe-á pedida confirmação.
    - ***Permitir o envio de dados anónimos relativos a ameaças identificadas ou suspeitas*** *(activado por predefinição)* – enviar informações sobre qualquer código suspeito, ou identificado como perigoso, ou padrão de comportamento *(pode ser vírus, spyware ou uma página Web maliciosa a que esteja a tentar aceder)*

detectado no seu computador.

- ***Permitir o envio de dados anónimos relativos à utilização do produto*** *(activado por predefinição)* – enviar estatísticas básicas sobre a utilização da aplicação, tais como o número de detecções, análises executadas, actualizações bem/mal sucedidas, etc.

- ***Permitir verificação 'na nuvem' das detecções*** *(activado por predefinição)* – as ameaças detectadas serão verificadas em termos efectivos de infecção, para identificar falsos positivos.

Ameaças mais comuns

Hoje em dia, existem muito mais ameaças do que vírus propriamente ditos. Os autores de códigos maliciosos e websites perigosos são muito inovadores e surgem novos tipos de ameaças com grande frequência, sendo que a maioria ocorre na Internet. Estas são algumas das mais comuns:

- Yμ ***vírus*** é um código malicioso que se copia e dissemina, muitas vezes indetectado até o mal estar feito. Alguns vírus são sérias ameaças, eliminando ou deliberadamente alterando ficheiros, enquanto que alguns vírus podem fazer algo aparentemente inofensivo, como reproduzir um trecho musical. No entanto, alguns vírus são perigosos devido à habilidade básica de se multiplicarem – mesmo um vírus mais simples pode utilizar toda a memória do computador num instante e levar a uma falha fatal do computador.

- Yμ ***worm*** é uma subcategoria de vírus que, ao contrário dos vírus, não precisa de um objecto "hospedeiro" para se juntar; envia-se si próprio para outros computadores autonomamente, normalmente via e-mail, e em resultado sobrecarrega os servidores de e-mail e sistemas de rede.

- ***Spyware é normalmente definido como sendo uma categoria de malware (****malware = qualquer software malicioso, incluindo vírus*) ocultos em programas – regra geral Trojan horses – com o objectivo de recolherem informações pessoais, palavras-passe, números de cartão de crédito, ou para infiltrarem num computador e permitirem ao hacker tomar o controlo do mesmo remotamente; obviamente, tudo sem o conhecimento ou consentimento do proprietário do computador.

- ***Programas potencialmente indesejados*** são um tipo de spyware que pode ser, embora não necessariamente, perigoso para o seu computador. Um exemplo específico de um PUP é o adware, software concebido para distribuir publicidade, normalmente apresentando pop-ups publicitários; irritantes, mas não propriamente prejudiciais.

- ***As cookies de rastreio*** também podem ser consideradas um tipo de spyware, uma vez que estes pequenos ficheiros, guardados no browser da Internet e enviados automaticamente para o website proveniente quando o visitar novamente, podem conter dados como o seu histórico de navegação e outras informações semelhantes.

- ***Exploit*** é um código malicioso que se aproveita de uma falha ou vulnerabilidade num sistema operativo, browser da Internet, ou outro programa essencial.

- O ***Phishing*** é uma tentativa de obtenção de dados pessoais sensíveis simulando uma

organização fidedigna e reputada. Normalmente, as potenciais vítimas são contactadas por um e-mail de grupo a pedir, por exemplo, que actualizem os detalhes da sua conta bancária. Para o fazer, são convidadas a seguir o link que então os encaminha para um website falso do banco.

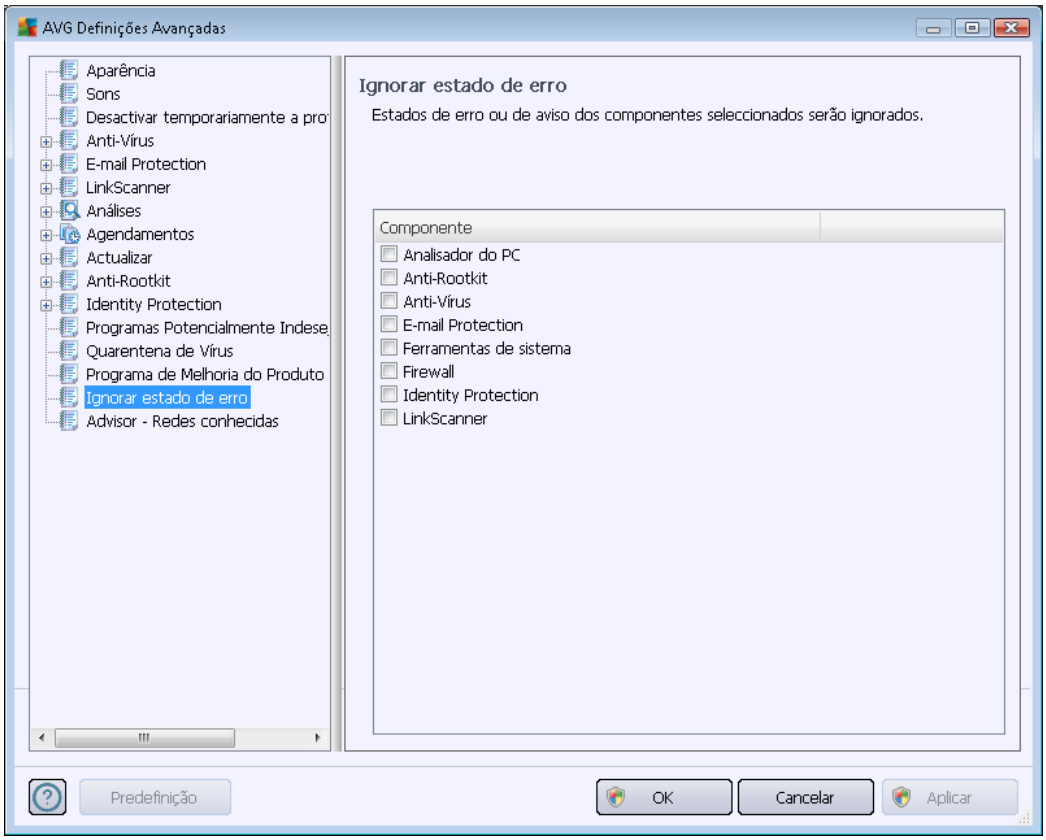
- ***Embuste – é um e-mail em massa que contém informações perigosas, alarmantes ou meramente aborrecidas e inúteis.*** Muitas da ameaças acima utilizam mensagens de e-mail de embuste para se propagarem.

- ***Os websites maliciosos*** são aqueles que instalam deliberadamente software malicioso no seu computador e os websites infectados fazem exactamente o mesmo, com a diferença de que estes são websites legítimos que foram subjugados para infectarem os visitantes.

Para o proteger contra todos estes diferentes tipos de ameaças, o AVG Internet Security 2012 integra componentes especializados. Para uma breve descrição dos mesmos, consulte o capítulo Síntese de Componentes.

10.15. Ignorar estado de erro

Na janela ***Ignorar estado de erro*** pode seleccionar os componentes sobre os quais não quer ser informado:



Por predefinição, nenhum dos componentes na lista está seleccionado. O que significa que se algum componente obtiver um estado de erro, será informado imediatamente dessa situação

através:

- ícone da Barra de Tarefas – enquanto todas os componentes do AVG estiverem a funcionar devidamente o ícone é apresentado com quatro cores; no entanto, se ocorrer um erro, os ícones serão apresentados com um ponto de exclamação amarelo,
- uma descrição textual do problema existente na secção Informação de Estado de Segurança da janela principal do AVG

Pode ocorrer uma situação em que, por alguma razão, necessite de desactivar um componente temporariamente (*isto não é recomendável, deverá tentar ao máximo manter todos os componentes constantemente activados e na configuração predefinida, mas pode acontecer*. Nesse caso, o ícone da Barra de Tarefas reporta automaticamente o estado de erro do componente. No entanto, nesta situação não podemos considerar um erro efectivo uma vez que o utilizador ocasionou-o deliberadamente, e tem consciência do risco potencial. Em simultâneo, uma vez apresentado a cinzento, o ícone não poderá apresentar quaisquer outros erros que possam surgir.

Nesta eventualidade, pode seleccionar componentes que possam estar em estado de erro (*ou desactivados*) na janela acima e estabelecer que não pretende ser informado dos mesmos. A mesma opção *(Ignorar estado do componente)* também está disponível para componentes específicos directamente a partir da síntese dos componentes na janela principal do AVG.

10.16. Advisor – Redes conhecidas

O AVG Advisor inclui uma funcionalidade que monitoriza as redes às quais o utilizador estabelece ligação e, se for encontrada uma nova rede *(com um nome de rede que já é utilizado, o que pode ser confuso)*, avisa o utilizador e recomenda a verificação da segurança da rede. Se o utilizador decidir que é seguro estabelecer ligação à nova rede, pode também guardá-la nesta lista; o AVG Advisor memoriza então os atributos exclusivos da rede *(especificamente o endereço MAC)* e não volta a apresentar a notificação.

Nesta janela de diálogo, pode verificar quais foram as redes que guardou anteriormente como sendo redes conhecidas. Pode eliminar entradas individuais clicando no botão ***Remover***; a rede respectiva será então considerada desconhecida e possivelmente perigosa.

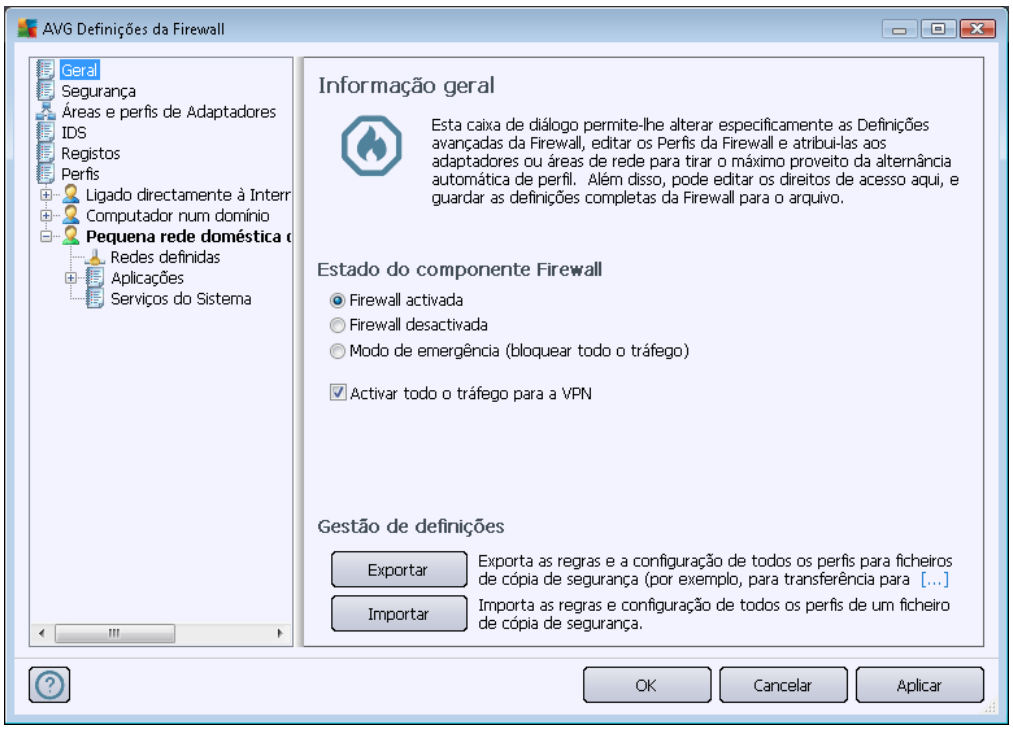
11. Definições da Firewall

A configuração da Firewall abre numa nova janela onde pode configurar através de várias janelas parâmetros muito avançados do componente.

Tenha em atenção: O fornecedor do software configurou todos os componentes do AVG Internet Security 2012 para um desempenho optimizado. Não altere a configuração predefinida a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente por um utilizador avançado!

11.1. Geral

A janela ***Informação geral*** está dividida em duas secções:



Estado da Firewall

Na secção ***Estado da Firewall*** pode alterar o estado da Firewall conforme necessário:

- ***Firewall activada*** – marque esta opção para permitir a comunicação para as aplicações que estão atribuídas como "permitidas" no conjunto de regras definidas no perfil da Firewall seleccionado.
- ***Firewall desactivada*** – esta opção desactiva a Firewall por completo, todo o tráfego de rede é permitido mas não verificado!
- ***Modo de emergência (bloquear todo o tráfego de internet)*** – seleccione esta opção

para bloquear todo o tráfego em todas as portas de rede; a Firewall ainda está em execução mas todo o tráfego de rede está parado.

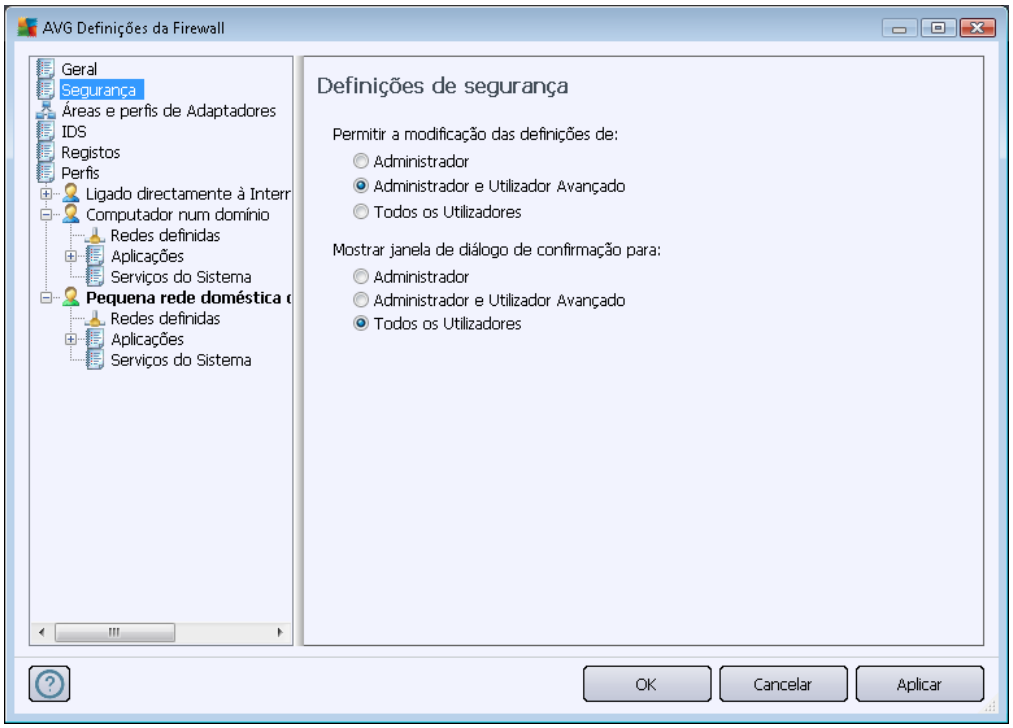
- ***Activar todo o tráfego para a VPN*** *(activado por predefinição)* – se usar uma ligação VPN *(Virtual Private Network – Rede Privada Virtual)*, ex. para se ligar ao escritório a partir de casa, recomendamos que marque a caixa.***A Firewal AVG*** procurará automaticamente pelos adaptadores de rede, detectará os que são usados para a ligação VPN e permitirá que todas as aplicações estabeleçam ligação à rede pretendida *(aplicável apenas para aplicações que não tenham regras específicas da Firewall atribuídas)*. Num sistema padrão com adaptadores de rede comuns, este simples passo poupa-lhe o trabalho de configurar uma regra detalhada para cada aplicação que precisar de usar através da VPN.

Nota: *Para activar a ligação VPN é necessário permitir a comunicação aos seguintes protocolos de sistema: GRE, ESP, L2TP, PPTP. Isto pode ser feito na janela Serviços do sistema.*

Gestão de definições

Na janela ***Gestão de definições*** pode ***Exportar*** ou ***Importar*** a configuração da Firewall; ou seja, exportar as regras e definições da Firewall definidas para ficheiros de cópia de segurança ou, por outro lado, importar a totalidade do ficheiro da cópia de segurança.

11.2. Segurança



Na janela ***Definições de segurança*** pode definir regras gerais do comportamento da Firewall independentemente do perfil seleccionado:

- ***Permitir modificação de definições para*** . especifique a quem é permitido alterar a configuração da Firewall.

- ***Apresentar janelas de confirmação para*** – especifique a quem a janela de confirmação (*janelas a solicitar uma decisão numa situação que não está prevista por uma regra da Firewall*) deve ser apresentada.

Pode atribuir o direito específico, em ambas as situações, a um dos seguintes grupos de utilizadores:

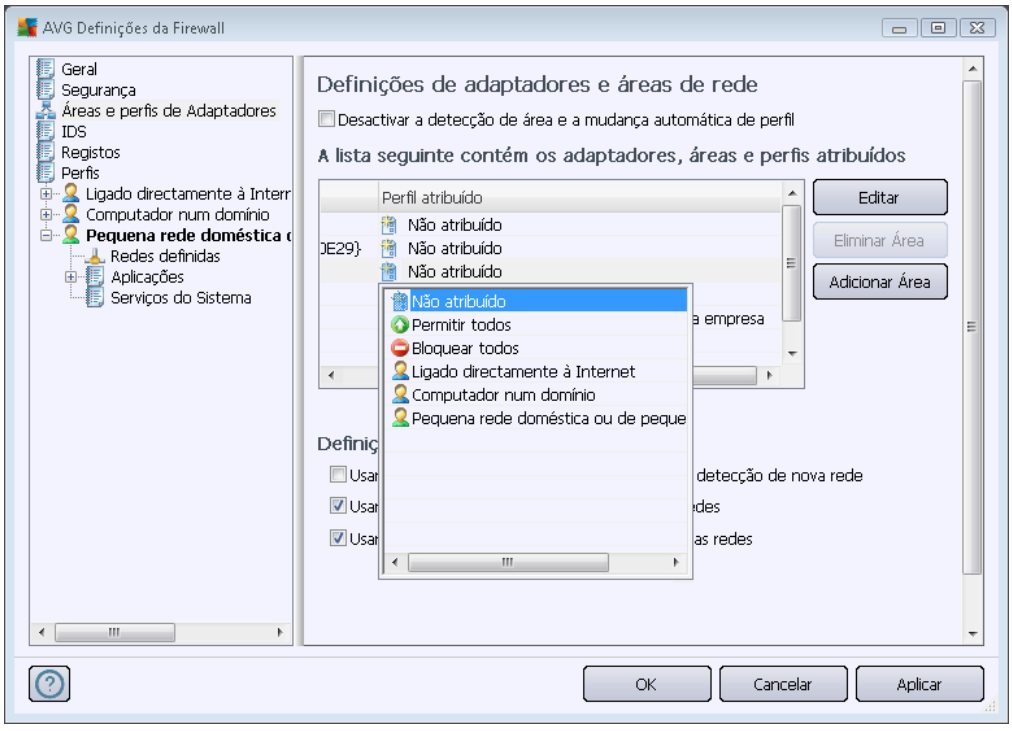
- ***Administrador*** – controla completamente o PC e tem o direito de associar cada utilizador a grupos com níveis de autoridade especificamente definidos.

- ***Administrador e Utilizador Avançado*** – o administrador pode incluir qualquer utilizador num determinado grupo (*Utilizador Avançado*) e definir autorizações para os membros desse grupo.

- ***Todos os Utilizadores*** – outros utilizadores não associados a nenhum grupo específico.

11.3. Áreas e perfis de Adaptadores

Na janela ***Definições de adaptadores e áreas de rede*** pode editar definições relativas à atribuição de perfis definidos a adaptadores específicos e redes referentes e respectivas:



- ***Desactivar a detecção de área e a mudança automática de perfil*** *(desactivado por*

predefinição) - Pode ser atribuído um dos perfis definidos a cada tipo de interface de rede, respectivamente a cada área. Se não quiser definir perfis específicos, será usado um perfil comum. No entanto, se decidir distinguir perfis e atribuí-los a adaptadores e áreas específicas, e posteriormente – por alguma razão – quiser mudar esta definição temporariamente, seleccione a opção ***Desactivar detecção de área e mudança automática de perfil***.

- ***Lista de adaptadores, áreas e perfis atribuídos*** – Nesta lista pode encontrar uma síntese de adaptadores e áreas detectados. Pode atribuir um perfil específico a cada um a partir do menu dos perfis definidos. Para abrir este menu, clique com o botão esquerdo do rato sobre o item respectivo na lista de adaptadores *(na coluna Perfil atribuído)* e seleccione o perfil a partir do menu de contexto.

Definições avançadas

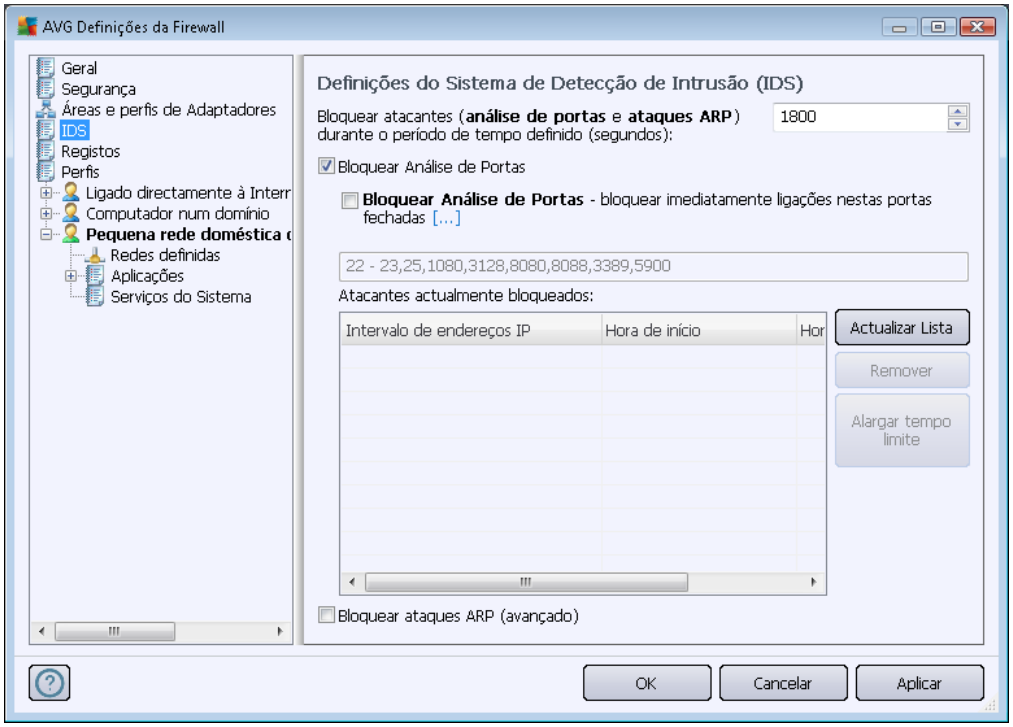
- ***Usar sempre um perfil predefinido e não apresentar a detecção de uma nova área de rede*** – sempre que o computador ligar a uma nova rede, a Firewall alerta-o e apresenta uma janela a solicitar que seleccione um tipo de ligação de rede e que lhe atribua um Perfil da Firewall. Se não quiser que essa janela seja apresentada, marque esta caixa.

- ***Usar a heurística AVG para detecção de novas redes*** - Permite a recolha de informações sobre uma rede recém detectada com o mecanismo do AVG (*no entanto, esta opção só está disponível do SO Vista, ou superior*).

- ***Usar a heurística Microsoft para detecção de novas redes*** - Permite a recolha de algumas informações sobre uma rede recém detectada a partir do Serviço do Windows (*esta opção só está disponível no Windows Vista ou superior*).

11.4. IDS

O Sistema de Detecção de Intrusão (IDS) é uma funcionalidade especial de análise de comportamento destinada a identificar e bloquear tentativas de comunicação suspeitas através de portas específicas do seu computador. Pode configurar os parâmetros do IDS na janela ***Definições do Sistema de Detecção de Intrusão (IDS)***:



A janela ***definições do Sistema de Detecção de Intrusão (IDS)*** disponibiliza as seguintes opções de configuração:

- ***Bloquear (Análise de portas e ataques ARP) os atacantes durante um período de tempo definido*** – Aqui pode especificar durante quantos segundos deverá a porta ser bloqueada sempre que for detectada uma tentativa de comunicação suspeita na mesma. Por predefinição, o tempo de intervalo está definido para 1800 segundos (*30 minutos*).

- ***Bloquear Análise de Portas*** *(activado por predefinição)* – Marque a caixa para bloquear tentativas de comunicação em todas as portas TCP e UDP provenientes do exterior para o computador. Para essas ligações, são permitidas cinco tentativas e a sexta é bloqueada. O item está activado por predefinição e recomendamos que mantenha essa configuração. Se mantiver a opção ***Bloquear Análise de Portas*** activada, estão disponíveis opções de configuração adicionais *(caso contrário, o item seguinte estará desactivado)*:

    - ***Bloquear Análise de Portas*** – Marque a caixa para bloquear imediatamente quaisquer tentativas de comunicação através das portas especificadas no campo de texto abaixo. As portas individuais ou intervalos de portas deverão ser separados por vírgula. Existe uma lista predefinida de portas recomendadas, caso pretenda usar esta funcionalidade.

    - Atacantes actualmente bloqueados – Esta secção lista quaisquer tentativas de comunicação que estejam actualmente bloqueadas pela Firewall. O histórico completo de tentativas bloqueadas pode ser consultado na janela Registos (*separador Registo de análise de portas*).

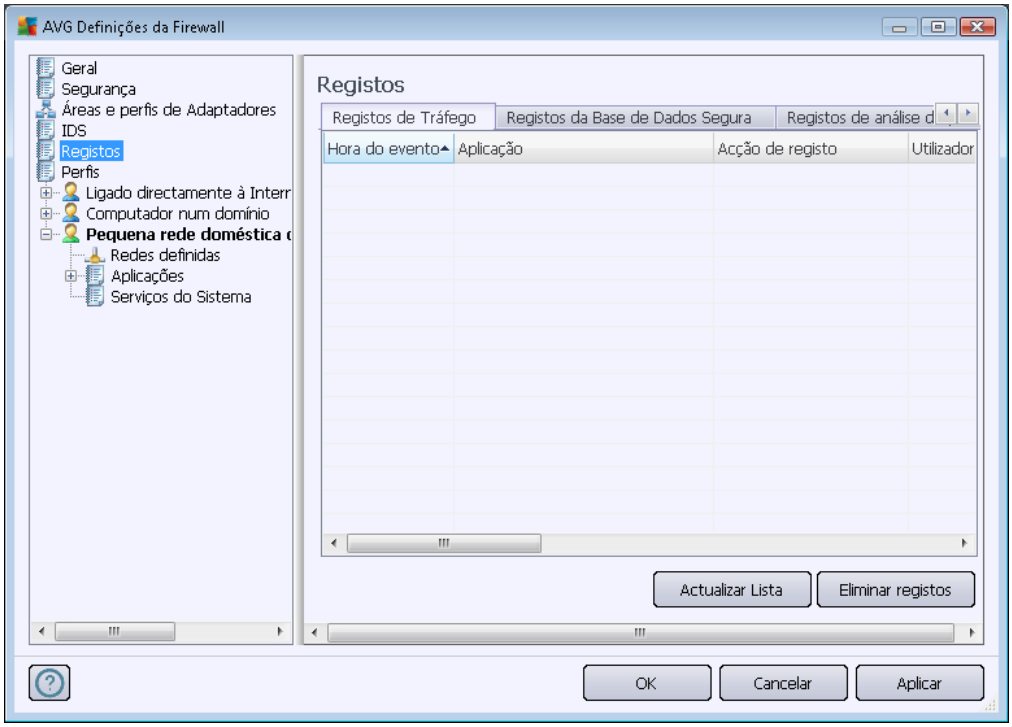
- ***Bloquear ataques ARP (avançado)****(desactivado por predefinição)* - Marque esta opção para activar o bloqueio de tipos especiais de tentativas de comunicação na rede local

detectadas pelo ***IDS*** como potencialmente perigosas. Será aplicada a temporização definida na opção ***Bloquear atacantes durante um período de tempo definido.*** Recomendamos que somente utilizadores avançados, familiarizados com o tipo e nível de risco da sua rede local, utilizem esta funcionalidade.

Botões de controlo

- ***Actualizar lista*** – prima este botão para actualizar a lista (*para incluir quaisquer tentativas bloqueadas recentemente*)
- ***Remover*** - prima para cancelar um bloqueio seleccionado
- ***Alargar tempo limite*** – prima para prolongar o período de tempo durante o qual uma tentativa seleccionada será bloqueada. Será apresentada uma nova janela com opções alargadas que lhe permite especificar a hora e a data, ou uma duração ilimitada.

11.5. Registos



A janela ***Registos*** permite-lhe rever a listagem de todas as acções e eventos registados pela Firewall com uma descrição detalhada dos parâmetros relevantes (*hora do evento, nome da aplicação, acção do registo respectiva, nome de utilizador, PID, sentido de tráfego, tipo de protocolo, números das portas remota e local, etc.*) em quatro separadores:

- ***Registos de Tráfego*** - providencia informações sobre a actividade de todas as aplicações que tentaram ligar à rede.

- ***Registos da Base de Dados Segura*** - *A Base de Dados Segura* é uma base de dados interna do AVG que recolhe informações sobre aplicações certificadas e seguras que podem ter sempre permissão para comunicar on-line. Da primeira vez que uma nova aplicação tentar conectar à rede (*ou seja, quando ainda não existe nenhuma regra da firewall especificada para esta aplicação*), é necessário descobrir se a comunicação na rede deve ser permitida para a respectiva aplicação. Primeiro, o AVG procura na *Base de Dados Segura*, e, se a aplicação estiver listada, ser-lhe-á concedido acesso à rede automaticamente. Só depois disso, se não houver qualquer informação sobre a aplicação disponível na base de dados, será o utilizador inquirido, por meio de uma janela independente, sobre se pretende que a aplicação aceda à rede.

- ***Registos de análise de portas*** – providencia registo de todas as actividades do Sistema de Detecção de Intrusão.

- ***Registos ARP*** – registo de informações sobre o bloqueio de tipos especiais de tentativas de comunicação numa rede local (opção *Bloquear ataques ARP*) detectadas pelo Sistema de Detecção de Intrusão como potencialmente perigosas.

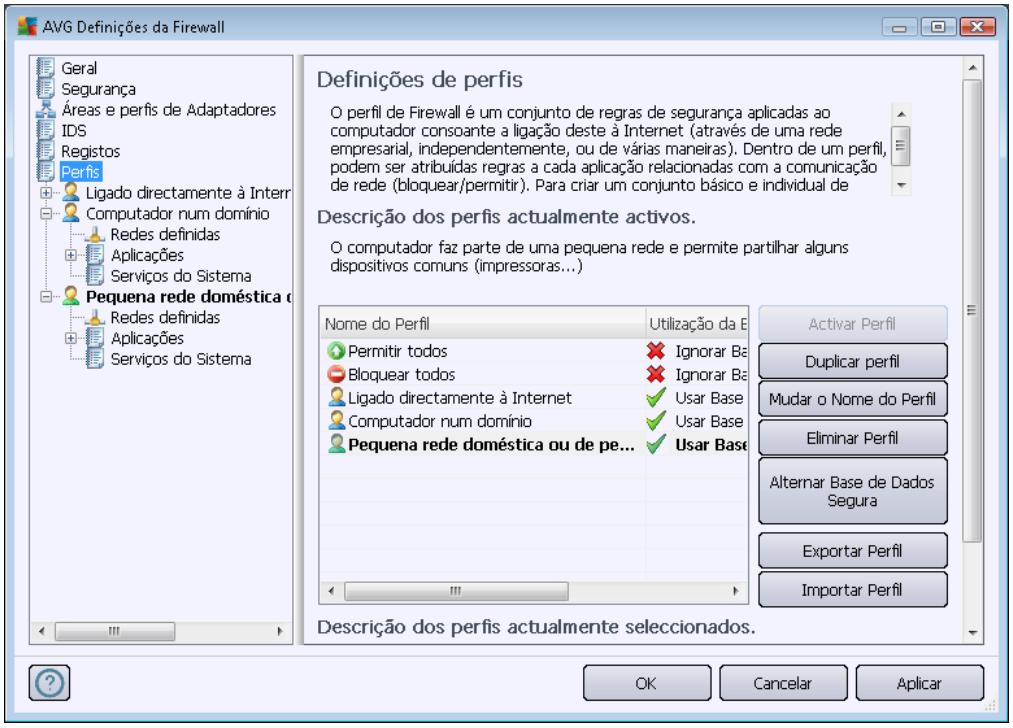
Botões de controlo

- ***Actualizar lista*** -Todos os parâmetros registados podem ser ordenados consoante o atributo seleccionado: cronologicamente (*datas*) ou alfabeticamente (*outras colunas*) – basta clicar no cabeçalho da coluna respectiva. Use o botão ***Actualizar lista*** para actualizar a informação actualmente apresentada.

- ***Eliminar registos*** - Clique para eliminar todas as entradas da tabela.

11.6. Perfis

Na janela ***Definições de perfis*** pode encontrar uma lista de todos os perfis disponíveis:



Os perfis do sistema *(Permitir Todos, Bloquear Todos)* não podem ser editados. No entanto, todos os perfis personalizados *(Ligado directamente à Internet, Computador num domínio, Pequena rede doméstica ou de pequena empresa)* podem ser editados directamente nesta janela por meio dos botões de controlo:

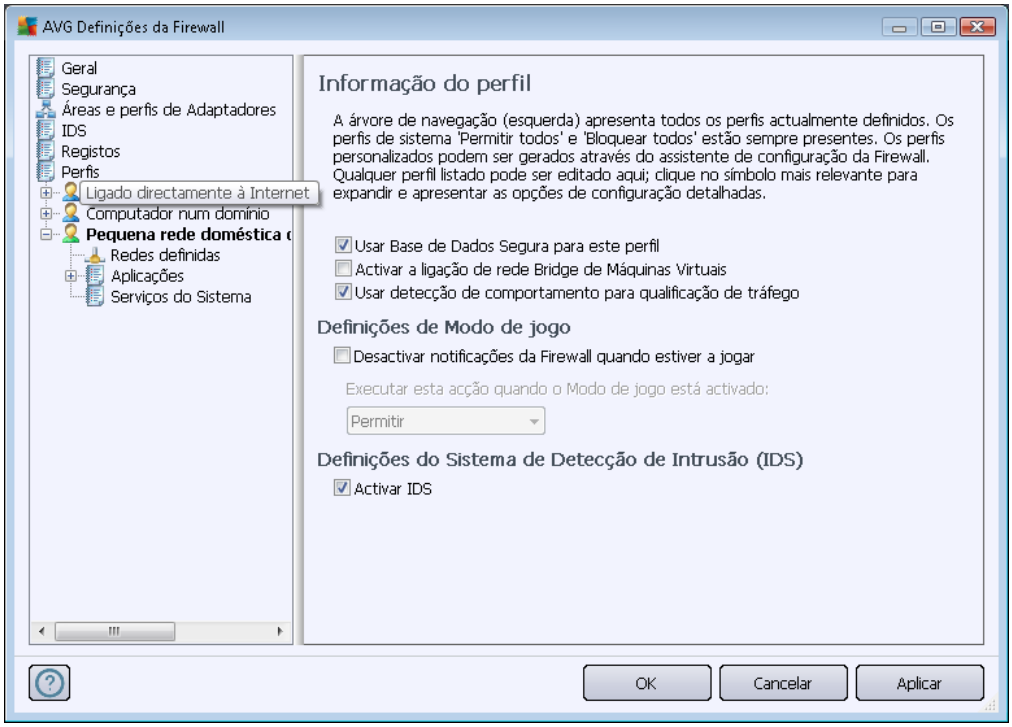
- ***Activar perfil*** – Este botão define o perfil seleccionado como activo, o que significa que a configuração do perfil seleccionado será usada pela Firewall para controlar o tráfego de rede.
- ***Duplicar perfil*** - Cria uma cópia idêntica do perfil seleccionado; pode editar e renomear a cópia para criar um novo perfil com base no perfil duplicado original.
- ***Mudar o Nome do Perfil*** – Permite-lhe definir um novo nome para um perfil seleccionado.
- ***Eliminar perfil*** - Elimina o perfil seleccionado da lista.
- ***Alternar Base de Dados Segura*** - Para o perfil seleccionado, pode decidir se pretende utilizar as informações constantes da *Base de Dados Segura* (A*Base de Dados Segura é uma base de dados interna do AVG que recolhe dados sobre aplicações certificadas e seguras que podem sempre ter permissão para comunicar on-line*).
- ***Exportar perfil*** - Grava a configuração do perfil seleccionado para um ficheiro que será guardado para possível utilização posterior.

- ***Importar perfil*** - Configura as definições do perfil seleccionado com base nos dados exportados da cópia de segurança do ficheiro de configuração.

Na secção inferior da janela tem à sua disposição a descrição de um perfil que esteja actualmente seleccionado na lista acima.

Consoante o número de perfis definidos que são mencionados na lista na janela ***Perfil***, a estrutura do menu de navegação à esquerda será alterada em conformidade. Cada perfil definido cria uma secção específica no item ***Perfil***. Podem ser editados perfis específicos nas seguintes janelas (*que são idênticas para todos os perfis*):

11.6.1. Informação do perfil



A janela ***Informação do perfil*** é a primeira janela da secção onde pode editar a configuração de cada perfil em janelas separadas referentes a parâmetros específicos do perfil.

- ***Usar a Base de Dados Segura para este perfil*** (*activado por predefinição*) – Marque esta opção para activar a *Base de Dados Segura* (*ou seja, a base de dados interna do AVG que recolhe informações sobre aplicações certificadas e seguras que comunicam on-line. Se ainda não houver nenhuma regra especificada para a aplicação, é necessário descobrir se pode ser concedida permissão à aplicação para aceder à rede. O AVG pesquisa na Base de Dados Segura primeiro, e, se a aplicação estiver listada, será considerada segura e ser-lhe-á concedida permissão para comunicar através da rede. Caso contrário, o utilizador será inquirido sobre se pretende que a aplicação tenha permissão para comunicar através da rede*) para o respectivo perfil

- ***Activar a Ligação de Rede Bridge de Máquinas Virtuais*** (*desactivado por predefinição*) - Marque este item para permitir que máquinas virtuais em ambiente VMware conectem

directamente à rede.

- ***Usar detecção de comportamento para qualificação de tráfego*** (*activado por predefinição*) – Marque esta opção para permitir que a Firewall use a funcionalidade Protecção de Identidade aquando da avaliação de uma aplicação – a Protecção de Identidade pode identificar se a aplicação apresenta algum comportamento suspeito, ou se pode ser considerada segura para comunicar on-line.

Definições do Modo de Jogo

Na secção ***Definições do Modo de Jogo*** pode decidir e confirmar ao seleccionar o item respectivo se pretende receber mensagens informativas da Firewall apresentadas mesmo enquanto uma aplicação de ecrã inteiro está em execução no seu computador (*normalmente jogos, mas aplica-se a qualquer aplicação de ecrã inteiro, ex. apresentações de Power Point*), uma vez que as mensagens informativas podem ser interruptivas.

Se seleccionar o item ***Desactivar notificações da Firewall quando jogar jogos***, no menu de opções, então seleccione que acção deve ser tomada na eventualidade de uma nova aplicação sem regras especificadas tentar comunicar através da Internet (*aplicações que normalmente resultariam numa janela de pedido*) todas estas aplicações podem ser permitidas ou bloqueadas.

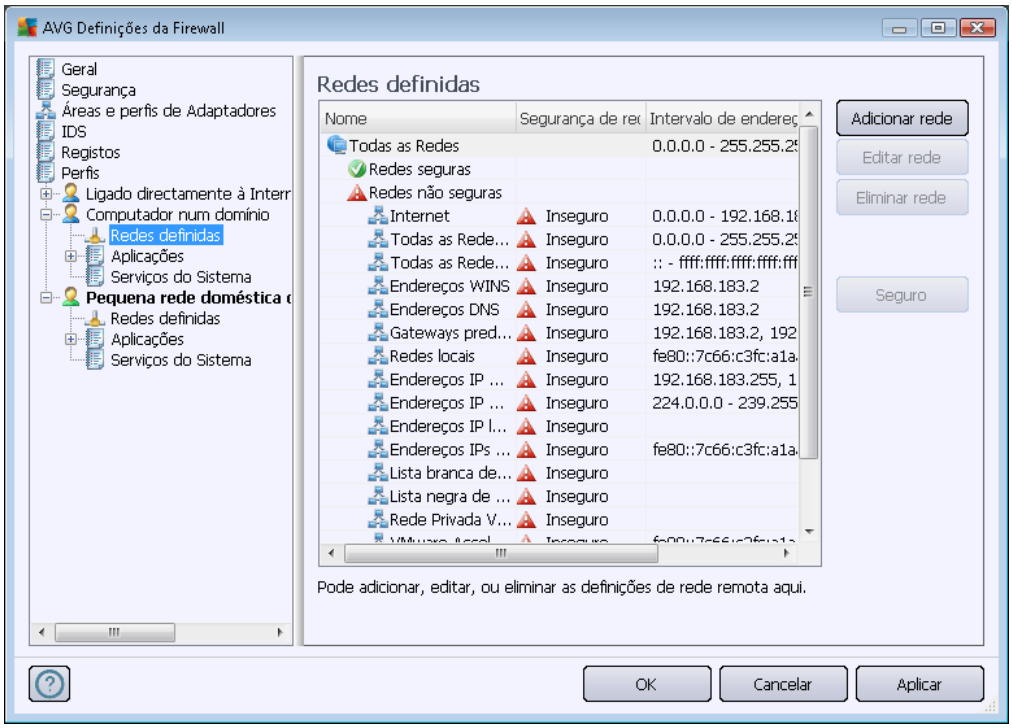
Com o modo de jogo activado, todas as tarefas agendadas (*análises, actualizações*) são adiadas até ao encerramento da aplicação.

Definições do Sistema de Detecção de Intrusão (IDS)

Marque a caixa ***Activar IDS*** para activar a funcionalidade de análise comportamental especial destinada a identificar e bloquear tentativas de comunicação suspeitas através das portas do seu computador *(para mais informações sobre as definições desta funcionalidade, consulte o capítulo IDS deste documento).*

11.6.2. Redes definidas

A janela ***Redes definidas*** faculta uma lista de todas as redes às quais o seu computador está conectado.

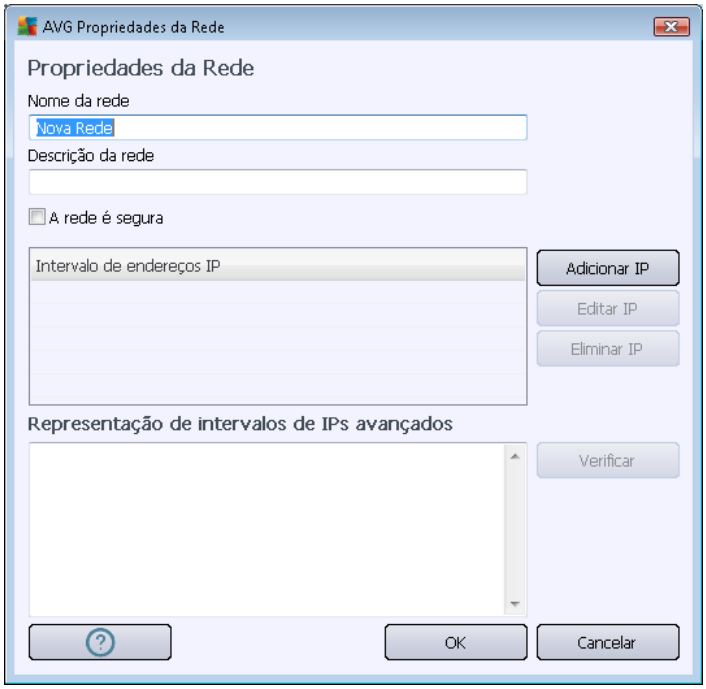


A lista apresenta as seguintes informações relativas a cada rede detectada:

- ***Redes*** - Apresenta uma lista de nomes de todas as redes às quais o computador está conectado.
- ***Segurança da Rede*** - Por predefinição todas as redes são consideradas não seguras, e somente se tiver a certeza que a respectiva rede é segura, pode atribui-la como tal ((*clique na lista de itens referente à rede respectiva e seleccione Seguro no menu de contexto*) – todas as redes seguras serão então incluídas no grupo daquelas através das quais a aplicação pode comunicar com o conjunto de regras da aplicação definido para Permitir para seguro.
- ***Intervalo de endereços IP*** - Cada rede será detectada automaticamente e especificada na forma de intervalo de endereço IP

Botões de controlo

- ***Adicionar rede*** – Abre a janela ***Propriedades de rede*** onde pode editar parâmetros da rede recentemente definida:



Nesta janela, pode especificar o ***Nome da rede*** , facultar a ***Descrição da rede*** e possivelmente atribuir a rede como segura. A nova rede pode ser definida manualmente numa janela independente aberta via o botão ***Adicionar IP***(alternativamente ***Editar IP***/ ***Eliminar IP***, nesta janela pode especificar a rede ao facultar o Intervalo ou máscara de IP. Para um número de redes mais amplo que devem ser definidas como parte da rede recentemente criada, pode usar a opção da ***Representação avançada de Intervalo de IPs*** : introduza a lista de todas as redes no campo de texto respectivo (*qualquer formato standard é suportado*) e clique no botão ***Verificar*** para se certificar de que o formato pode ser reconhecido. Depois clique em ***OK*** para confirmar e guardar os dados.

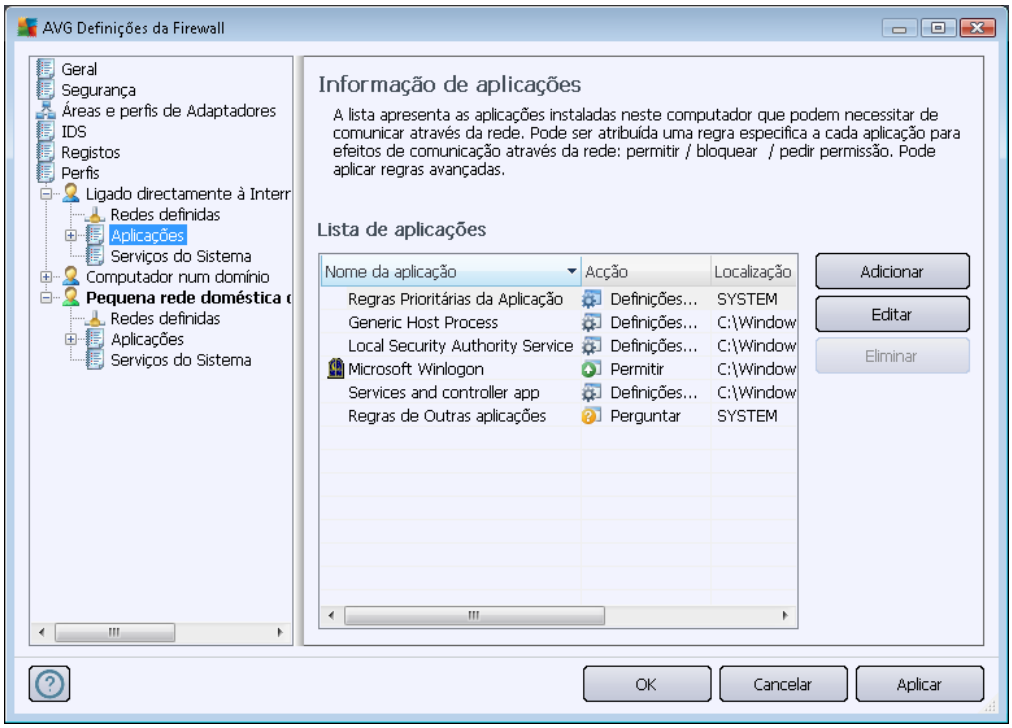
- ***Editar rede*** – Abre a janela ***Propriedades de rede*** (*veja acima*) onde pode editar parâmetros de uma rede já definida (*a janela é idêntica à janela para adicionar uma nova rede, consulte a descrição no parágrafo anterior*).

- ***Eliminar rede*** – Remove o visto de uma rede seleccionada da lista de redes.

- ***Marcar como segura*** – Por predefinição, todas as redes são consideradas não seguras e , no caso de ter a certeza de que a rede respectiva é segura, pode usar este botão para a marcar como tal (*e vice-versa, uma vez atribuída a rede como segura, o texto do botão altera para "Marcar como não segura"*).

11.6.3. Aplicações

A janela ***Informações de aplicações*** lista todas as aplicações instaladas que possam precisar de comunicar através da rede e ícones respeitantes à acção atribuída:



As aplicações na ***Lista de aplicações*** são as que foram detectadas no computador (*e atribuídas acções respectivas*). Podem ser usados os seguintes tipos de acção:

- - Permitir comunicação para todas as redes
- – Permitir comunicação somente para redes definidas como Seguras
- – Bloquear comunicação
- – Apresentar janela de solicitação (*o utilizador poderá decidir se pretende permitir ou bloquear a comunicação quando a aplicação tenta comunicar através da rede*)
- – Definições avançadas definidas

Por favor tenha em atenção que só foram detectadas aplicações já instaladas, portanto se instalar uma nova aplicação mais tarde, terá de definir regras da Firewall para ela. Por predefinição, quando uma nova aplicação tenta conectar através da rede pela primeira vez, a Firewall cria uma nova regra automaticamente em conformidade com a Base de Dados Segura, ou pergunta-lhe se pretende bloquear ou permitir a comunicação. Na última situação, o utilizador poderá guardar a sua resposta como uma regra permanente (que ficará depois listada nesta janela).

Obviamente, também pode definir regras para a nova aplicação imediatamente – nesta janela, clique

em ***Adicionar*** e preencha os detalhes da aplicação.

Para além das aplicações, a lista também contém dois itens especiais:

- ***Regras Prioritárias da Aplicação*** (*no topo da lista*) são preferenciais e são sempre aplicadas antes das regras de qualquer aplicação individual.
- ***Outras Regras da Aplicação*** (*no fundo da lista*) são usadas como "último recurso", quando nenhuma regra da aplicação for aplicável, ex. para uma aplicação desconhecida e indefinida. Seleccione a acção que deve ser activada quando uma aplicação desse género tentar comunicar através da rede:
  - *Bloquear* – a comunicação será sempre bloqueada.
  - *Permitir* – a comunicação será permitida em qualquer rede.
  - *Perguntar* – poderá decidir se pretende permitir ou bloquear a comunicação.

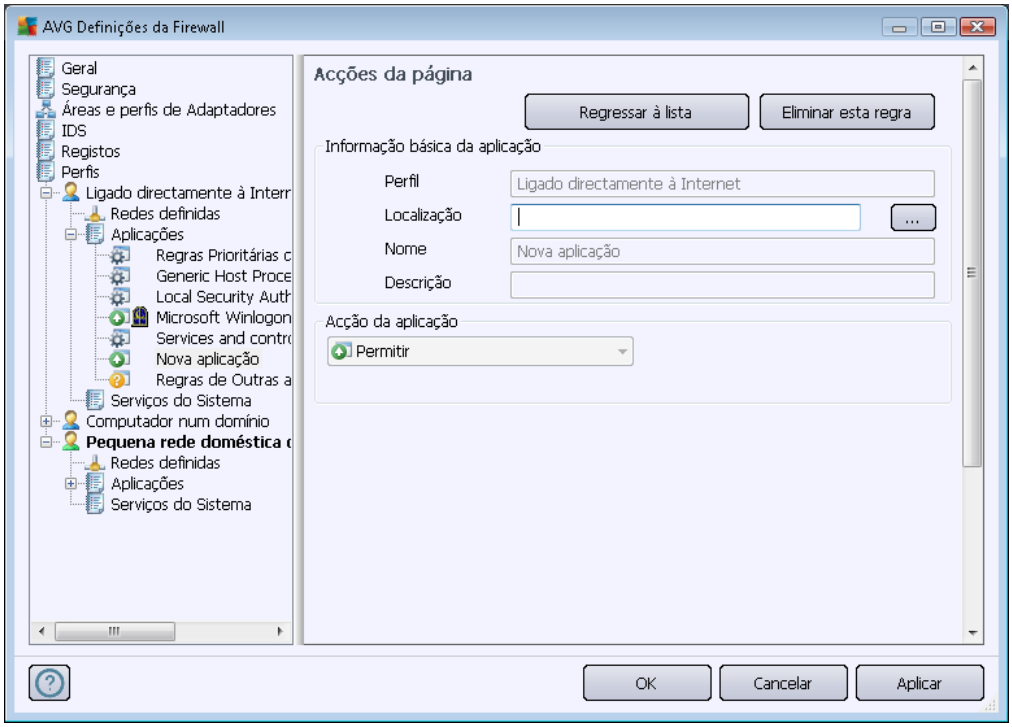
Estes itens têm opções de configuração diferentes das aplicações comuns e são destinados exclusivamente a utilizadores experientes. Recomendamos vivamente que não modifique estas definições!

Botões de controlo

A lista pode ser editada usando os seguintes botões de controlo:

- ***Adicionar*** – Abre uma janela de Acções da Página em branco para definição de novas regras de aplicações.
- ***Editar*** - Abre a mesma janela de Acções da Página com dados disponibilizados para edição de um conjunto de regras de aplicações existente.
- ***Eliminar*** - Remove a aplicação seleccionada da lista.

Na janela ***Acções de Página***, o utilizador pode configurar detalhadamente definições para a respectiva aplicação:



Botões de controlo

Há dois botões de controlo disponíveis no topo da janela:

- ***Regressar à lista*** – Clique neste botão para apresentar a síntese de todas as regras de aplicação definidas.
- ***Eliminar esta regra*** – Clique neste botão para eliminar a regra de aplicação actualmente apresentada. ***Tenha em atenção que esta acção não pode ser anulada!***

Informação básica da aplicação

Nesta secção, preencha o ***Nome*** da aplicação, e opcionalmente uma ***Descrição*** (*um breve comentário para sua informação*). No campo ***Caminho***, introduza a localização completa para a aplicação (*o ficheiro executável*) no disco; alternativamente, pode localizar a aplicação convenientemente na estrutura em árvore depois de clicar no botão "***...***".

Acção da aplicação

No menu de opções, pode seleccionar a regra da Firewall para a aplicação, ou seja, o que a Firewall

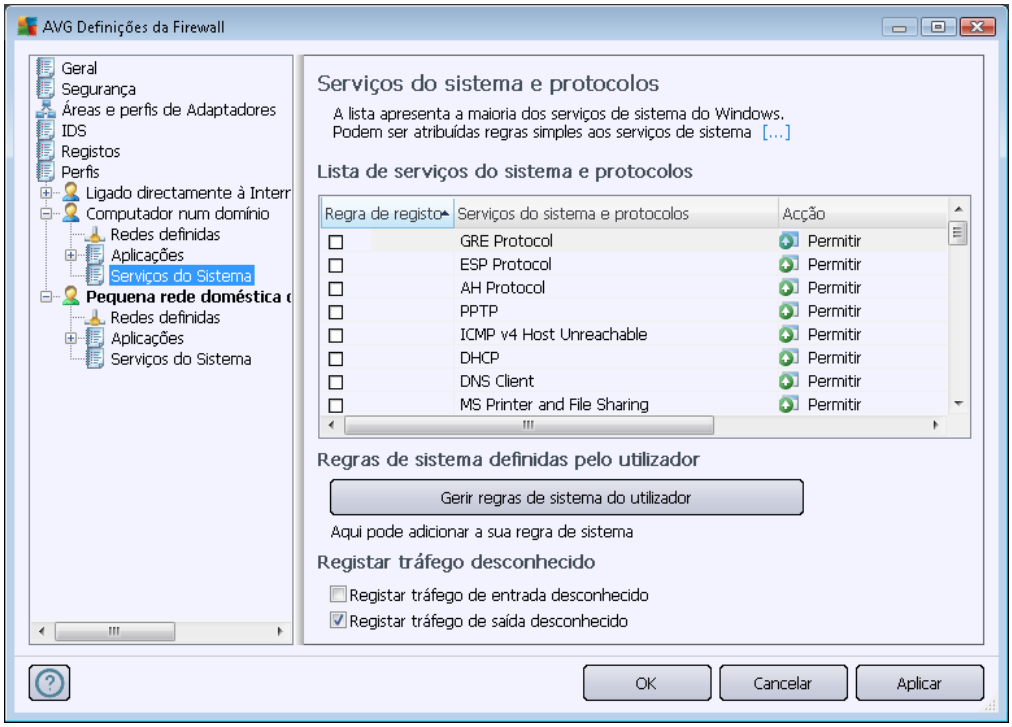
deve fazer quando a aplicação tenta comunicar através da rede:

- ***Permitir para todos*** – Permite que a aplicação comunique através de todas as redes e adaptadores definidos, sem quaisquer limitações.
- ***Permitir para seguros*** – Só permitirá que a aplicação comunique através das redes definidas como seguras *(fiáveis)*.
- ***Bloquear*** – Interdita a comunicação automaticamente; a aplicação não poderá ligar-se a nenhuma rede.
- ***Perguntar*** – Apresenta uma janela que lhe permite decidir se quer permitir ou bloquear a tentativa de comunicação actual.
- ***Definições avançadas*** – Apresenta opções de definições mais alargadas e mais detalhadas na parte inferior da janela na secção ***Detalhes das regras de aplicação***. Os detalhes serão aplicados consoante a ordem da lista, sendo que pode ***Mover para cima*** ou ***Mover para baixo*** as regras na lista conforme necessário para estabelecer a sua precedência. Depois de seleccionar uma regra específica na lista, a síntese dos detalhes da regra serão apresentados na parte inferior da janela. Qualquer valor sublinhado a azul pode ser alterado na janela de definições respectiva. Para eliminar a regra seleccionada, clique em ***Remover***. Para definir uma nova regra utilize o botão ***Adicionar*** para abrir a janela ***Alterar detalhe da regra*** que lhe permite especificar todos os detalhes necessários.

11.6.4. Serviços do Sistema

Qualquer edição na janela Serviços de sistema e protocolos, é recomendável APENAS PARA UTILIZADORES EXPERIENTES!

A janela ***Serviços de sistema e protocolos*** lista os serviços de sistema e protocolos padrão do Windows que possam precisar de comunicar através da rede:



Lista de serviços do sistema e protocolos

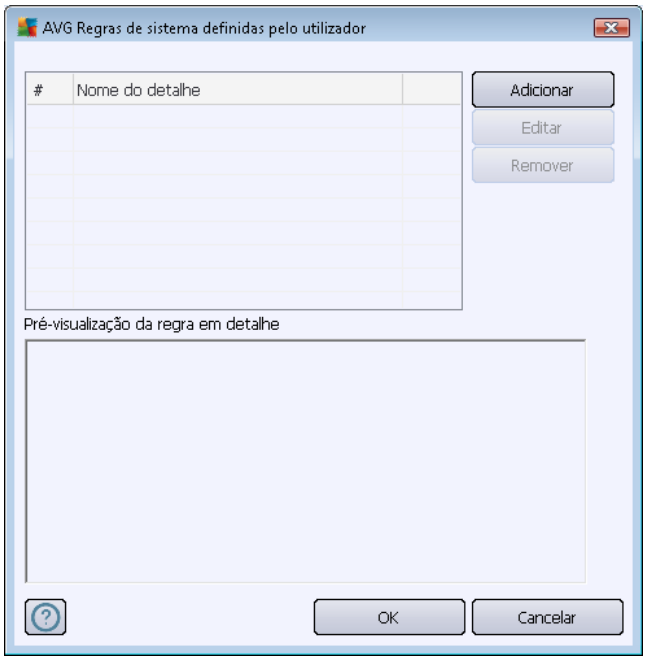
A tabela é composta por duas colunas:

- ***Registo de acção de regra*** – Esta caixa permite-lhe activar o registo de todas as regras de aplicações nos Registos.
- ***Serviço de sistema e protocolos*** – Esta coluna apresenta o nome do serviço de sistema respectivo.
- ***Acção*** – Esta coluna apresenta um ícone para a acção atribuída:
  - Permitir comunicação para todas as redes
  - Permitir comunicação somente para redes definidas como Seguras
  - Bloquear comunicação
- ***Redes*** – Esta coluna detalha em que rede específica a regra de sistema é aplicável.

Para editar qualquer item da lista (*incluindo as acções atribuídas*), clique com o botão direito do rato e seleccione ***Editar***.***No entanto, a edição de regras do sistema deve ser efectuada exclusivamente por utilizadores avançados e é vivamente recomendável não editar regras do sistema!***

Regras de sistema definidas pelo utilizador

Para abrir uma nova janela para definição das suas próprias regras do serviço do sistema (*consulte a imagem abaixo*), prima o botão ***Gerir regras de sistema do utilizador***. A secção superior da janela ***Regras de sistema definidas pelo utilizador*** apresenta um resumo de todos os detalhes da regra de sistema actualmente em edição; a parte inferior apresenta o detalhe seleccionado. Os detalhes da regra definida pelo utilizador podem ser editados, adicionados, ou eliminados por meio do botão respectivo; os detalhes de regras definidas pelo fabricante só podem ser editados:



Tenha em atenção que as definições de detalhes de regras são avançadas, destinadas principalmente a administradores de redes que precisam de ter controlo absoluto sobre a configuração da Firewall. Se não estiver familiarizado com tipo de protocolos de comunicação, números de portas de rede, definições de endereços IP, etc., é favor não modificar estas definições! Se precisar realmente de alterar a configuração, consulte por favor os ficheiros de ajuda da janela respectiva para informações específicas.

Registar tráfego desconhecido

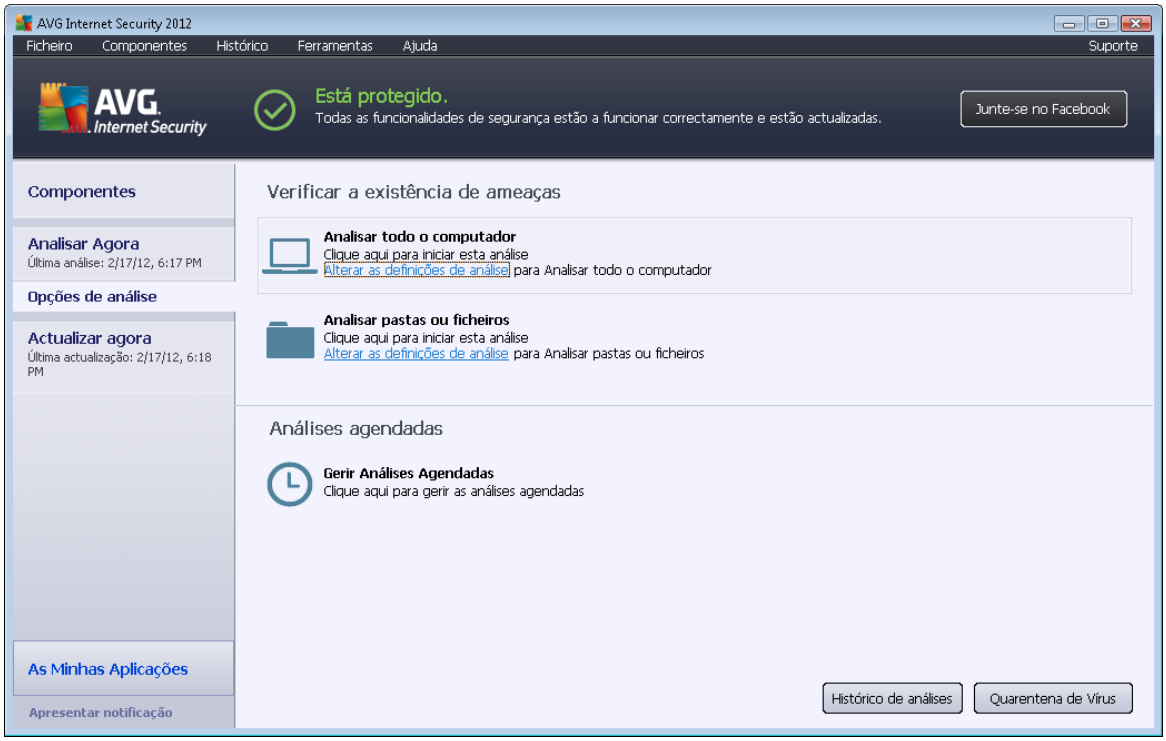
- ***Registar tráfego de entrada desconhecido*** *(desactivado por predefinição)* – Marque a caixa para registar nos Registos cada tentativa de ligação desconhecida do exterior para o seu computador.

- ***Registar tráfego de saída desconhecido*** *(activado por predefinição)* – Marque a caixa para registar nos Registos cada tentativa de ligação desconhecida do seu computador para uma localização externa.

12. Análise do AVG

Por predefinição, o **AVG Internet Security 2012** não executa qualquer análise, uma vez, que após a análise inicial, o utilizador deverá ficar devidamente protegido pelos componentes residentes do **AVG Internet Security 2012** que estão sempre alerta e não permitem que nenhum código malicioso aceda ao computador. Obviamente, o utilizador pode agendar uma análise para execução a intervalos regulares, ou iniciar uma análise manualmente consoante as necessidades pontuais.

12.1. Interface de Análise



A interface de análise do AVG é acessível via o link rápido ***Opções de análise***. Clique neste link para mudar para a janela ***Analisar a existência de ameaças***. Nesta janela encontrará o seguinte:

- síntese das análises predefinidas - existem três tipos de análises definidas pelo fornecedor do software e que estão prontas a serem utilizadas imediatamente seja manualmente ou por agendamento:
    - Análise de todo o computador
    - Analisar pastas ou ficheiros específicos
- Secção Análises agendadas – onde pode definir novos testes e criar novos agendamentos consoante necessário.

Botões de controlo

Os botões de controlo disponíveis na interface de testes são os seguintes:

- ***Histórico de análises*** - apresenta a janela Síntese dos resultados da análise com todos o históricos de análises
- ***Apresentar Quarentena de Vírus*** - abre uma nova janela com a Quarentena de Vírus – um espaço onde as infecções detectadas são colocadas em quarentena

12.2. Análises Predefinidas

Uma das principais funcionalidades do **AVG Internet Security 2012** é a análise manual. Os testes a pedido são concebidos para analisar várias partes do computador sempre que existam suspeitas de uma possível infecção por vírus. De qualquer modo, recomenda-se vivamente que esses testes sejam efectuados regularmente, mesmo que considere que não serão detectados vírus no computador.

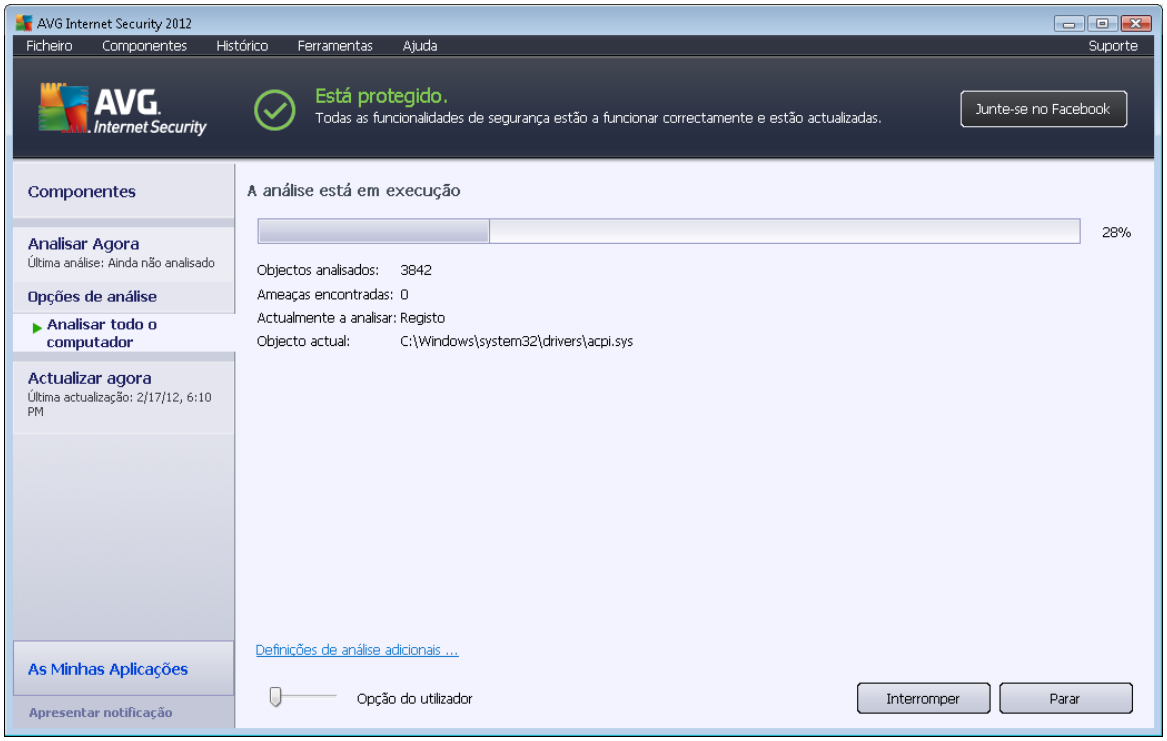
No **AVG Internet Security 2012** encontrará os seguintes tipos de análises predefinidas pelo fornecedor do software:

12.2.1. Análise de todo o computador

Análise de todo o computador - analisa todo o computador pela existência de possíveis infecções e/ou programas potencialmente indesejados. Este teste analisará todas os discos rígidos no seu computador, detectará e recuperará qualquer vírus encontrado, ou removerá a infecção detectada para a Quarentena de Vírus. A Análise a todo o computador deve ser agendada no posto de trabalho pelo menos uma vez por semana.

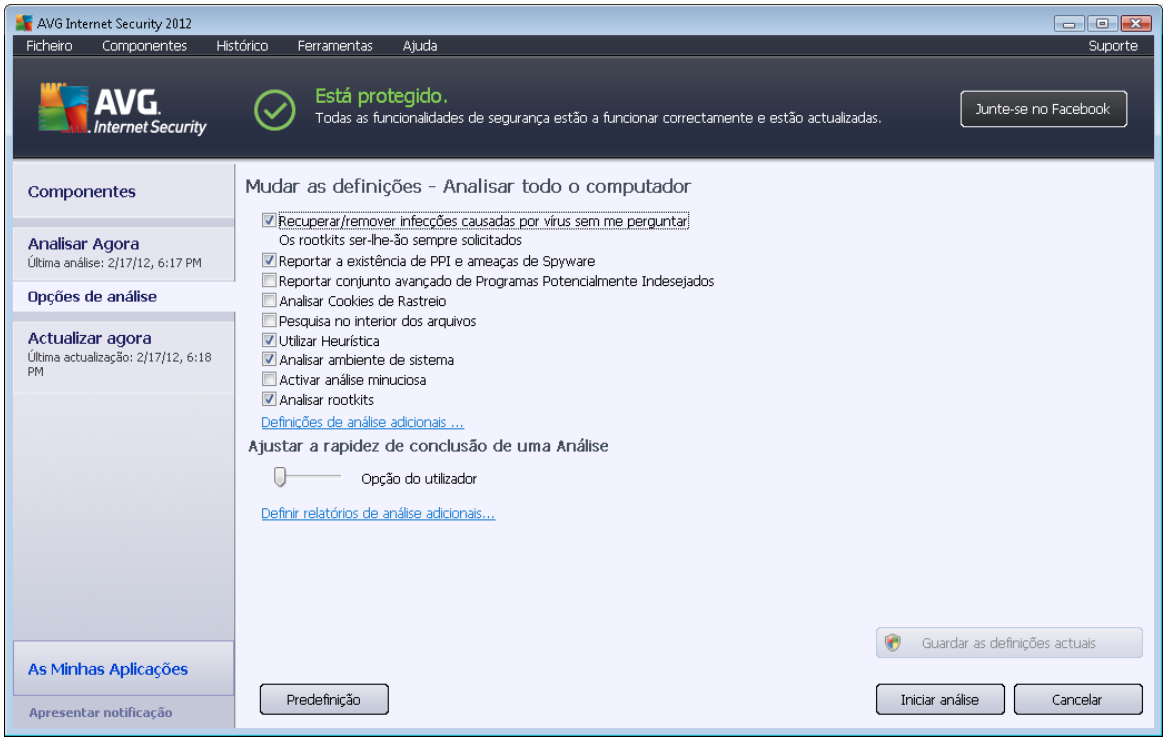
Início de análise

A ***Análise de todo o computador*** pode ser iniciada directamente a partir da interface de análise clicando no ícone da análise. Não é necessário configurar mais quaisquer definições adicionais para este tipo de análise, a análise iniciará imediatamente na janela ***A análise está em execução*** (*consulte a captura de ecrã*). A análise pode ser temporariamente interrompida (***Suspender***) ou cancelada (***Cancelar***) se necessário.



Edição da configuração de análise

Tem a opção de editar as predefinições da análise da ***Análise de todo o computador***. Clique no link ***Alterar as definições de análise*** para aceder à janela ***Alterar as definições de análise da Análise de todo o computador*** *(acessível a partir da interface de análise através do link Alterar as definições de análise da Análise de todo o computador)*. ***É recomendável que mantenha das definições padrão a menos que tenha uma razão válida para as alterar!***



- ***Parâmetros de análise*** – na lista de parâmetros de análise pode activar/desactivar parâmetros específicos consoante necessário:

  - ***Recuperar/remover infecções causadas por vírus sem me perguntar*** (*activado por predefinição*) – Se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Se o ficheiro infectado não puder ser restaurado automaticamente, o objecto infectado será movido para a Quarentena de Vírus.

  - ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** (*activado por predefinição*) – Marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

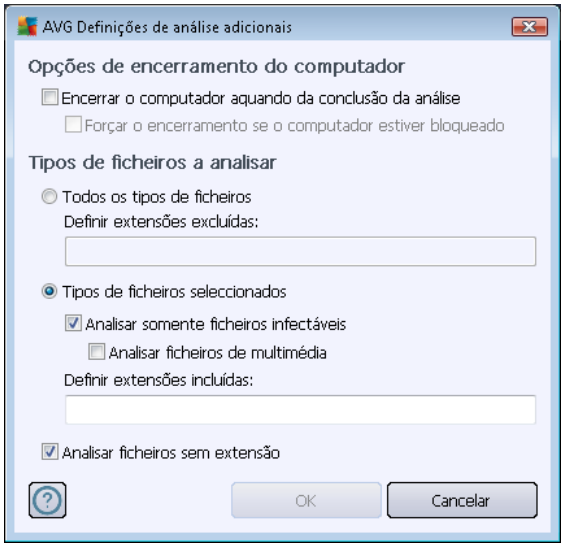
  - ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado por predefinição*) – Marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

  - ***Analisar a existência de Cookies de Rastreio*** (*desactivado por predefinição*) – Este parâmetro do componente Anti-Spyware define que as cookies deverão ser

detectadas durante a análise; (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação especifica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos*).

- ***Analisar no interior de arquivos*** (*desactivado por predefinição*) – Este parâmetro define que a análise deve verificar todos os ficheiros mesmo os que estão armazenados no interior de arquivos, ex. ZIP, RAR, ...
- ***Utilizar Heurística*** (*activado por predefinição*) – A análise heurística (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a detecção de vírus durante a análise.
- ***Analisar o ambiente do sistema*** (*activado por predefinição*) – A análise verificará também as áreas de sistema do seu computador.
- ***Activar análise minuciosa*** (*desactivado por predefinição*) – Em situações específicas (*suspeita de infecção do computador*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.
- ***Analisar a existência de rootkits*** (*activado por predefinição*) – a análise Anti-Rootkit analisa o computador em busca de eventuais rootkits, ou seja, programas e tecnologias que podem ocultar actividade de malware no computador. Se for detectado um rootkit, isto não significa necessariamente que o computador esteja infectado. Em alguns casos, podem ser erroneamente detectados controladores específicos ou secções de aplicações seguras como sendo rootkits.

- ***Definições de verificação adicionais*** – a ligação abre uma nova janela de ***Definições de verificação adicionais*** onde pode especificar os seguintes parâmetros:



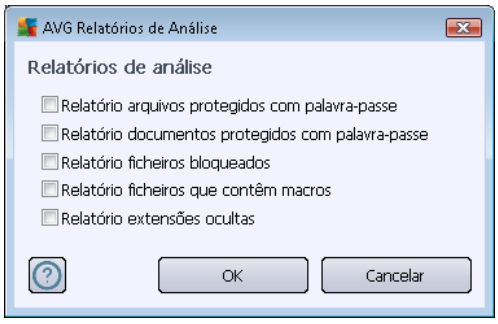
- ***Opções de encerramento do computador*** – decida se o computador deve ser

encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção (***Encerrar o computador aquando do término da análise***), será activada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar encerramento se o computador estiver bloqueado***).

- ***Definir tipos de ficheiros para análise*** – deve decidir ainda se pretende que sejam analisados:
  - ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;
  - ***Tipos de ficheiros seleccionados*** – pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infectados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser analisados.
  - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

- ***Ajustar a rapidez de conclusão de uma Análise*** – pode usar o cursor para alterar a prioridade do processo de análise. O valor desta opção está, por predefinição, definido para o nível *Definida pelo utilizador* de utilização automática de recursos. Em alternativa, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*ex. quando o computador não está a ser utilizado*).

- ***Definir relatórios de análise adicionais*** – a ligação abre uma nova janela de ***Relatórios de Análise*** onde pode seleccionar que tipos de possíveis detecções deverão ser reportadas:



Aviso: *Estas definições de análise são idênticas aos parâmetros de uma análise nova – conforme descrito no capítulo Análise do AVG / Agendamento de análises / Como Analisar . Na eventualidade*

*de decidir alterar a configuração padrão da análise **Analisar todo o computador** pode guardar as suas novas definições como a definição padrão a ser utilizada para todas as análises de todo o computador.*

12.2.2. Analisar pastas ou ficheiros específicos

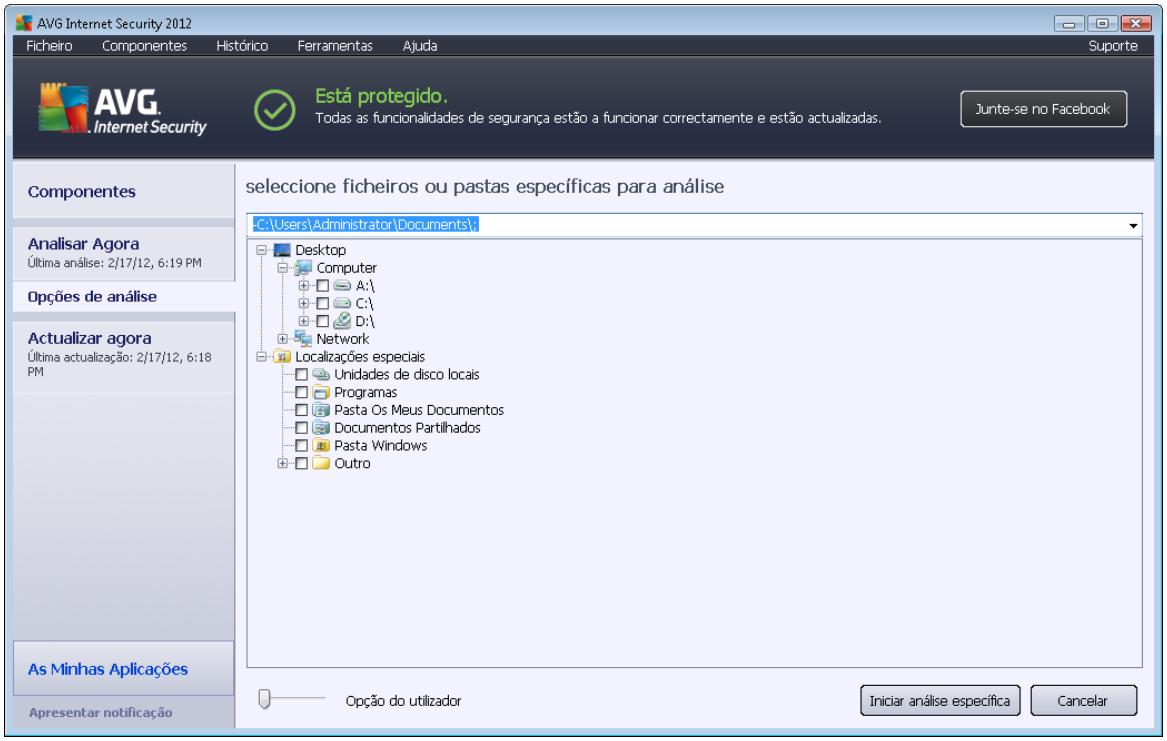
Analisar pastas ou ficheiros específicos – analisa apenas as áreas do seu computador que tiver seleccionado para o efeito (*pastas seleccionadas, discos rígidos, unidades de disquetes, CDs, etc.*). O progresso da análise na eventualidade da detecção de vírus e o seu tratamento é o mesmo que o da análise Analisar todo o computador: qualquer infecção detectada é recuperada ou removida para a Quarentena de Vírus. A análise de ficheiros ou pastas específicos pode ser utilizada para configurar os seus próprios testes e os seus agendamentos consoante as suas necessidades.

Início de análise

A ***Análise de ficheiros ou pastas específicos*** pode ser iniciada directamente a partir da interface de análise clicando no ícone de análise. Será apresentada uma nova janela apelidada ***Seleccionar ficheiros ou pastas específicos a analisar*** . Na estrutura em árvore do seu computador seleccione as pastas que pretende analisar. O caminho para cada pasta será gerado automaticamente e aparecerá na caixa de texto na parte superior da janela.

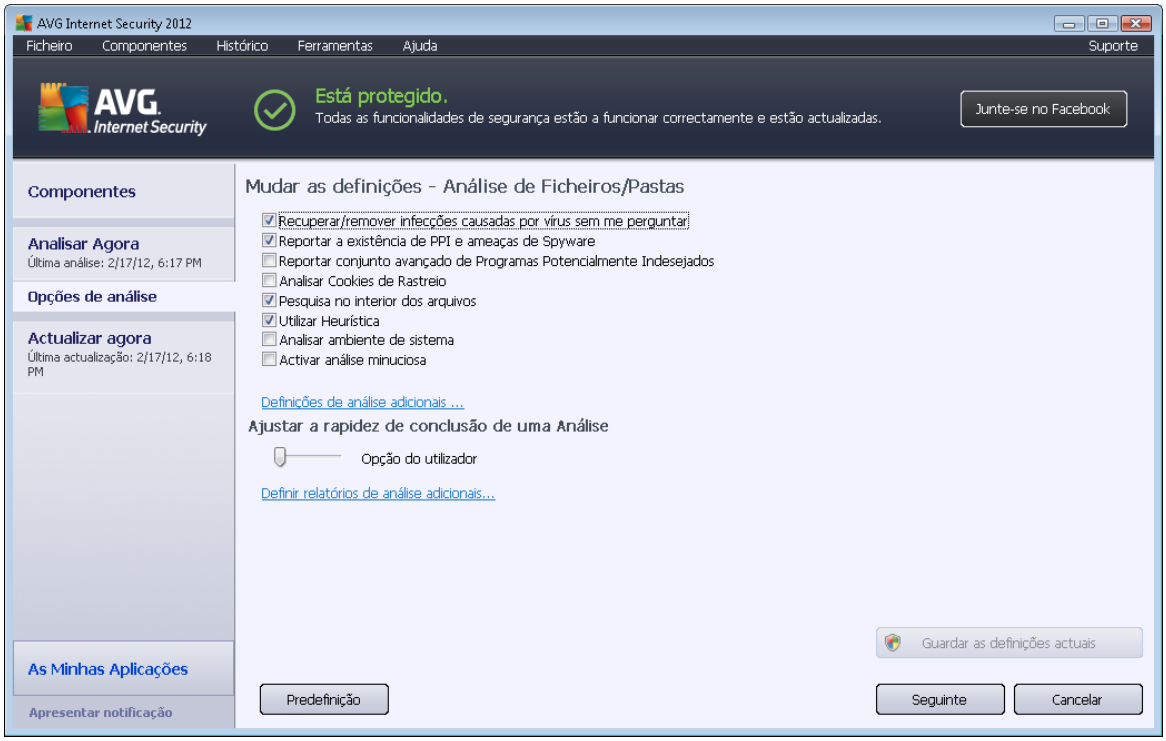
Também existe a possibilidade de analisar uma pasta específica excluindo todas as sub-pastas desta da análise; para isso deverá escrever um sinal de menos "**-**" à frente do caminho gerado automaticamente (*veja a captura de ecrã*). Para excluir toda a pasta da análise utilize o "!" parâmetro.

Finalmente, para iniciar a análise, clique no botão ***Iniciar análise***; o processo de análise em si é idêntico ao da Análise de todo o computador.



Edição da configuração de análise

Tem a opção de editar as definições padrão predefinidas da análise ***Analisar ficheiros e pastas específicos***. Clique no link ***Alterar definições de análise*** para ir para a janela ***alterar definições de análise para a Análise de ficheiros/pastas***. ***É recomendável que mantenha das definições padrão a menos que tenha uma razão válida para as alterar!***



- ***Parâmetros de análise*** – na lista de parâmetros de análise pode activar/desactivar parâmetros específicos consoante necessário:

  - ***Recuperar/remover infecções causadas por vírus sem me perguntar*** (*activado por predefinição*) – se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Se o ficheiro infectado não puder ser restaurado automaticamente, o objecto infectado será movido para a Quarentena de Vírus.

  - ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** (*activado por predefinição*) – marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

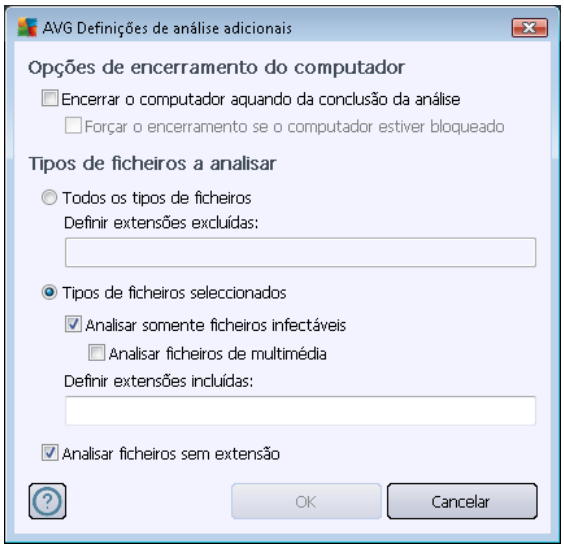
  - ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado por predefinição*) – marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

  - ***Analisar a existência de Cookies de Rastreio*** (*desactivado por predefinição*) – este parâmetro do componente Anti-Spyware define que as cookies deverão ser

detectadas durante a análise (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação especifica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos*).

- ***Analisar no interior de arquivos*** (*activado por predefinição*) – este parâmetro define que a análise deve verificar todos os ficheiros mesmo os que estão armazenados no interior de arquivos, ex. ZIP, RAR,...
- ***Utilizar Heurística*** (*activado por predefinição*) – a análise heurística (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a detecção de vírus durante a análise.
- ***Analisar o ambiente do sistema*** (*desactivado por predefinição*) – a análise verificará também as áreas de sistema do seu computador.
- ***Activar análise minuciosa*** (*desactivado por predefinição*) – em situações específicas (*suspeita de infecção do computador*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.

- ***Definições de verificação adicionais*** – a ligação abre uma nova janela de ***Definições de verificação adicionais*** onde pode especificar os seguintes parâmetros:



- ***Opções de encerramento do computador*** – decida se o computador deve ser encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção (***Encerrar o computador aquando do término da análise***), será activada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar encerramento se o computador estiver bloqueado***).
- ***Tipos de ficheiros para análise*** – deve decidir ainda se pretende que sejam

analisados:

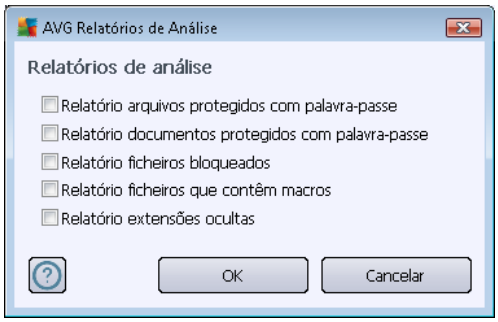
- ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

- ***Tipos de ficheiros seleccionados*** – pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infectados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser analisados.

- Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

- ***Prioridade do processo de análise*** – pode usar o cursor para alterar a prioridade do processo de análise. O valor desta opção está, por predefinição, definido para o nível *Definida pelo utilizador* de utilização automática de recursos. Em alternativa, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*ex. quando o computador não está a ser utilizado*).

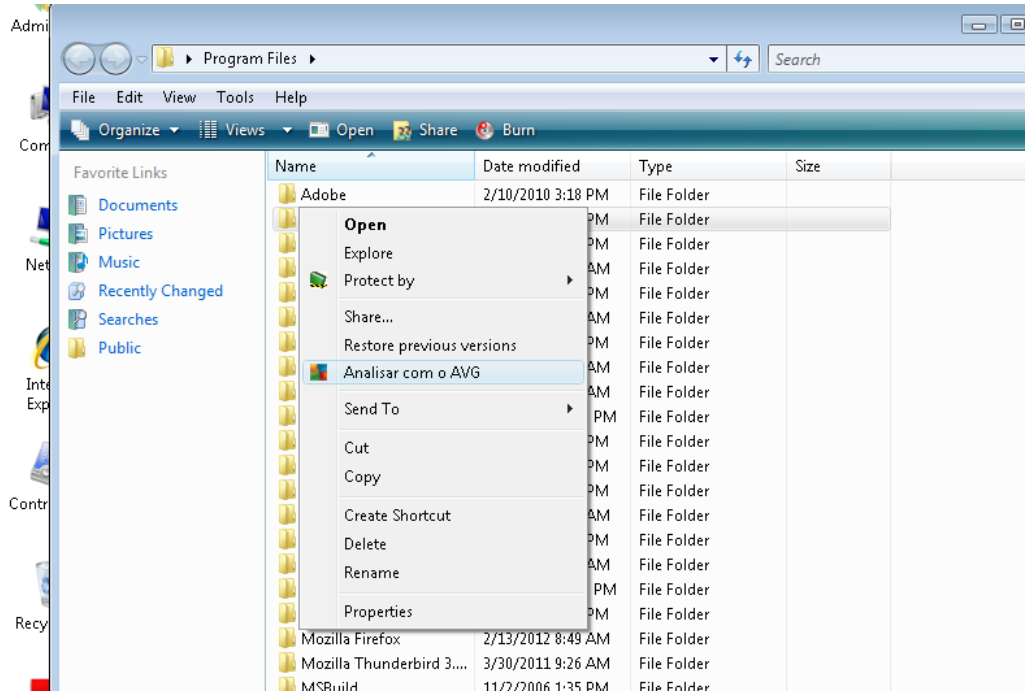
- ***Definir relatórios de análise adicionais*** – o link abre uma nova janela de ***Relatórios de Análise*** onde pode seleccionar que tipos de possíveis detecções deverão ser reportadas:



Aviso: *Estas definições de análise são idênticas aos parâmetros de uma análise nova – conforme descrito no capítulo Análise do AVG / Agendamento de análises / Como Analisar . Na eventualidade de decidir alterar a configuração padrão da análise* ***Analisar pastas ou ficheiros específicos*** *pode guardar as suas novas definições como a definição padrão a ser utilizada para todas as análises de ficheiros e pastas específicos. Além disso, esta configuração será utilizada como modelo para todos os novos agendamentos de análise (todas as análises personalizadas são baseadas na configuração actual da análise Analisar ficheiros e pastas específicos).*

12.3. A analisar no Explorador do Windows

Para além das análises predefinidas executadas para todo o computador ou as suas áreas seleccionadas, o **AVG Internet Security 2012** também disponibiliza a opção de análise rápida de um objecto específico directamente no ambiente do Explorador do Windows. Se quiser abrir um ficheiro desconhecido e não estiver seguro do seu conteúdo, pode querer analisá-lo manualmente. Siga estes passos:



- No Explorador do Windows seleccione o ficheiro *(ou pasta)* que pretende analisar
- Clique com o botão direito do rato sobre o objecto para abrir o menu de contexto
- Seleccione a opção ***Analisar com o*** para proceder à análise do ficheiro com o **AVG Internet Security 2012**

12.4. Análise da Linha de Comandos

No **AVG Internet Security 2012** existe ainda a opção de executar a análise a partir da linha de comandos. Pode utilizar esta opção em servidores por exemplo, ou ao criar um batch script a ser executado automaticamente após o arranque do computador. Pode iniciar a análise a partir da linha de comandos com várias parâmetros, como na interface gráfica do utilizador do AVG.

Para iniciar a análise do AVG a partir da linha de comandos, execute o seguinte comando na pasta em que o AVG está instalado:

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

Sintaxe do comando

A sintaxe do comando é a seguinte:

- ***avgscanx /parâmetro*** ... ex. ***avgscanx /comp*** para analisar todo o computador
- ***avgscanx /parâmetro /parâmetro*** .. com vários parâmetros, estes deverão estar alinhados numa linha e separados por espaço e o símbolo "barra"
- se um parâmetro requerer que seja facultado um valor específico (ex. o parâmetro ***/scan*** que requer informação acerca das áreas seleccionadas do seu computador a serem analisadas, e o utilizador tiver de facultar a localização exacta da secção seleccionada), os valores são divididos por ponto e vírgula, por exemplo: ***avgscanx /scan=C:\;D:***

Parâmetros de digitalização

Para visualizar uma síntese integral dos parâmetros disponíveis, digite o comando respectivo com o parâmetro /? ou /HELP (ex. ***avgscanx /?***). O único parâmetro obrigatório é /SCAN para especificar que áreas do computador devem ser analisadas. Para uma explicação mais detalhada das opções consulte a síntese de parâmetros da linha de comandos.

Para executar a análise prima ***Enter***. Pode parar o processo durante a análise via as combinações ***Ctrl+C*** ou ***Ctrl+Pause***.

Análise CMD iniciada a partir da interface gráfica

Ao iniciar o computador no Modo de Segurança do Windows, também existe a possibilidade de iniciar a análise da linha de comandos a partir da interface gráfica do utilizador. A análise em si será iniciada a partir da linha de comandos, a janela ***Compositor de Linhas de Comando*** só permite especificar a maioria dos parâmetros de análise no conforto da interface gráfica.

Uma vez que esta janela só é acessível no Modo de Segurança do Windows, para uma descrição detalhada desta janela queira por favor consultar o ficheiro de ajuda que pode ser aberto directamente a partir da janela.

12.4.1. Parâmetros da Análise CMD

A listagem seguinte oferece-lhe uma lista de todos os parâmetros disponíveis para a análise da linha de comandos:

- ***/SCAN*** Analisar pastas ou ficheiros específicos */SCAN=path;path (e.g. /SCAN=C:\;D:\)*
- ***/COMP*** Análise de todo o computador
- ***/HEUR*** Usar análise heurística

- ***/EXCLUDE*** Excluir localização ou ficheiros da análise
- ***/@*** Ficheiro de comandos /nome de ficheiro/
- ***/EXT*** Analisar estas extensões /por exemplo EXT=EXE,DLL/
- ***/NOEXT*** Não analisar estas extensões /por exemplo NOEXT=JPG/
- ***/ARC*** Analisar arquivos
- ***/CLEAN*** Limpar automaticamente
- ***/TRASH*** Mover ficheiros infectados para a Quarentena de Vírus
- ***/QT*** Teste Rápido
- ***/LOG*** Gerar um ficheiro com os resultados da análise
- ***/MACROW*** Reportar macros
- ***/PWDW*** Reportar ficheiros protegidos por palavra-passe
- ***/ARCBOMBSW*** Reportar bombas de arquivos *(arquivos comprimidos repetidamente)*
- ***/IGNLOCKED*** Ignorar ficheiros bloqueados
- ***/REPORT*** Reportar para ficheiro /nome de ficheiro/
- ***/REPAPPEND*** Anexar ao ficheiro de relatório
- ***/REPOK*** Reportar ficheiros não infectados como OK
- ***/NOBREAK*** Não permitir CTRL-BREAK para abortar
- ***/BOOT*** activar verificação MBR/BOOT
- ***/PROC*** Analisar processos activos
- ***/PUP*** Reportar Programas potencialmente indesejados
- ***/PUPEXT*** Reportar conjunto avançado de Programas potencialmente indesejados
- ***/REG*** Analisar registo
- ***/COO*** Analisar cookies
- ***/?*** Apresentar ajuda neste tópico
- ***/HELP*** Apresentar ajuda acerca deste tópico

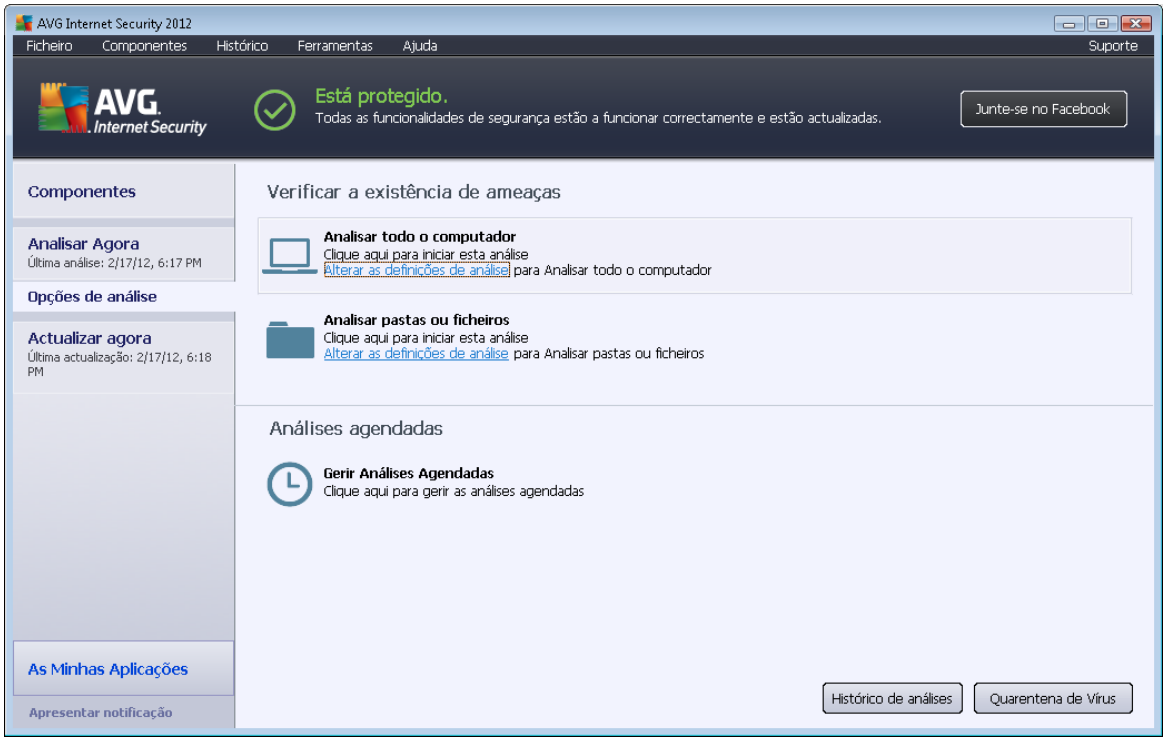
- ***/PRIORITY*** Defina a prioridade de análise /Baixa, Auto, Elevada/ *(consulte a secção Definições avançadas / Análises)*
- ***/SHUTDOWN*** Encerrar o computador aquando da conclusão da análise
- ***/FORCESHUTDOWN*** Forçar o encerramento do computador após o término da análise
- ***/ADS*** Analisar Fluxos de Dados Alternados *(somente NTFS)*
- ***/HIDDEN*** Reportar ficheiros com extensão oculta
- ***/INFECTABLEONLY*** Analisar apenas ficheiros com extensões infectáveis
- ***/THOROUGHSCAN*** Activar análise minuciosa
- ***/CLOUDCHECK*** Verificar a existência de falsos positivos
- ***/ARCBOMBSW*** Reportar ficheiros de arquivo recomprimidos

12.5. Agendamento de Análise

Com o **AVG Internet Security 2012** pode executar análises manualmente (por exemplo quando suspeita que uma infecção contagiou o seu computador) ou baseado num agendamento planeado. É vivamente recomendável que execute as análises baseado num agendamento: desta forma pode assegurar que o seu computador está protegido de quaisquer possibilidade de ser infectado, e não terá de se preocupar com quando e se iniciar uma análise.

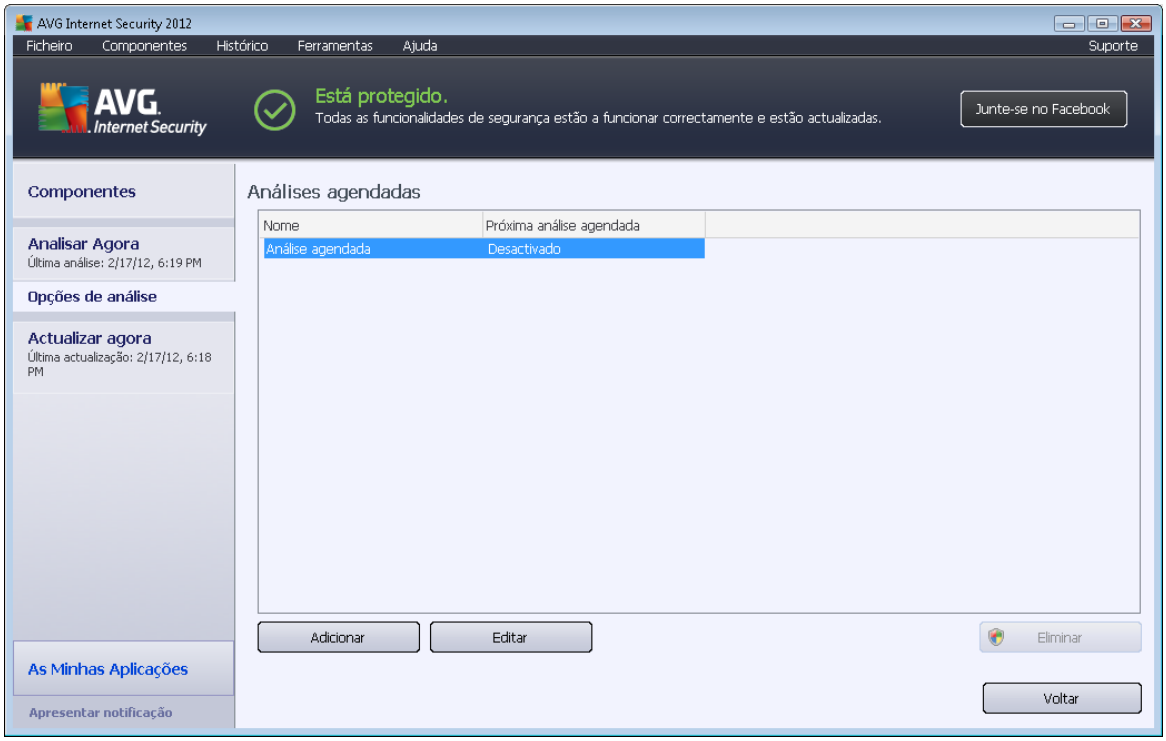
Deve executar a Análise de todo o computador regularmente, pelo menos uma vez por semana. No entanto, se possível, execute a análise de todo computador diariamente – conforme configurado na configuração de agendamento de análise predefinida. Se o computador estiver "sempre ligado" então pode agendar análises fora das horas de expediente. Se o computador for desligado ocasionalmente, então agende as análises para ocorrerem aquando do arranque do computador quando a tarefa não tiver sido executada atempadamente.

Para criar novos agendamentos de análise, consulte a interface de análise do AVG e veja na secção inferior apelidada ***Agendamento de Análises***:



Análises agendadas

Clique no ícone gráfico na secção ***Análises agendadas*** para abrir uma nova janela de ***Análises agendadas*** onde pode encontrar uma listagem de todas as análises actualmente agendadas:



Pode editar / adicionar análises por meio dos seguintes botões de controlo:

- ***Adicionar agendamento de análise*** – o botão abre a janela ***Definições para agendamento de análises*** , separador Definições de agendamento. Nesta janela pode especificar os parâmetros do teste definido.

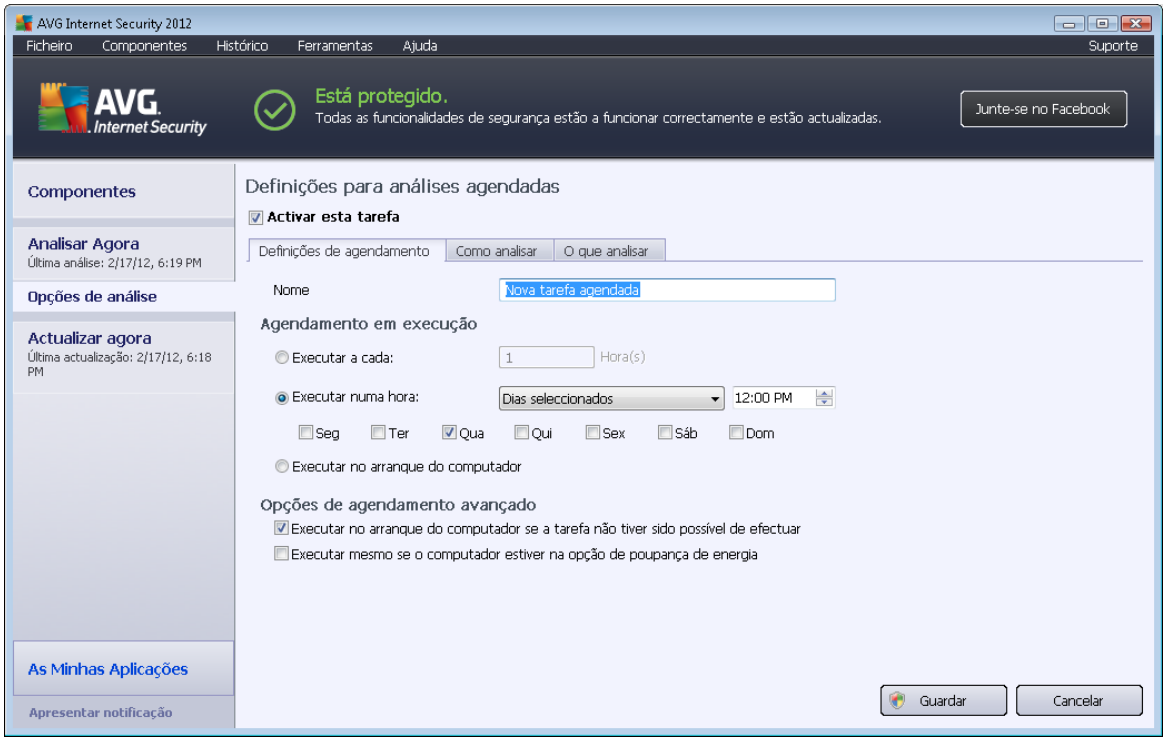
- ***Editar agendamento de análise*** – este botão só pode ser utilizado se já tiver seleccionado um teste existente a partir da lista de testes agendados. Nesse caso o botão aparece como activo e pode clicar nele para alternar para a janela ***Definições para análise agendada*** , separador Definições de agendamento. Os parâmetros do teste seleccionado já estão especificados e podem ser editados.

- ***Eliminar agendamento de análise*** – este botão só pode ser utilizado se já tiver seleccionado um teste existente a partir da lista de testes agendados. Este teste pode então ser eliminado da lista clicando no botão de controlo. No entanto, só pode remover os teste que tiver criado; o ***Agendamento de análise a todo o computador*** predefinido nas configurações padrão nunca pode ser eliminado.

- ***Retroceder*** – regressar à interface de análise do AVG

12.5.1. Definições de agendamento

Se quiser agendar um novo teste e a sua execução regular, aceda à janela ***Definições para teste agendado*** (*clique no botão* ***Adicionar agendamento de análise*** *na janela* ***Agendar análises***). A janela está dividida em três separadores: ***Definições de agendamento*** *(consulte a imagem abaixo; o separador predefinido para o qual será automaticamente redireccionado*), Como analisar e O que analisar.



No separador ***Definições de agendamento*** pode seleccionar/desseleccionar primeiro o item ***Activar esta tarefa*** para desactivar temporariamente a análise agendada, e voltar a activá-lo conforme necessário.

De seguida atribua um nome à análise que está em vias de criar e agendar. Digite o nome no campo de texto ao lado do item ***Nome***. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir.

Exemplo:*Não é adequado nomear uma análise com o nome "Nova análise" ou "A minha análise" uma vez que estes nomes não referem o que a análise efectivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc. Também não é necessário especificar no nome da análise se é a análise de todo o computador ou somente de ficheiros e pastas seleccionados – as suas próprias análises serão sempre uma versão específica da análise de ficheiros e pastas seleccionados.*

Nesta janela pode ainda definir os seguintes parâmetros de análise:

- ***Agendamento em execução*** - especifique os intervalos de tempo para a execução do novo agendamento de análise. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (***Executar a cada ...***ou definindo uma data e hora precisas (***Executar a uma hora específica ...***), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Acção baseada no arranque do computador***).

- ***Opções de agendamento avançado*** – esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

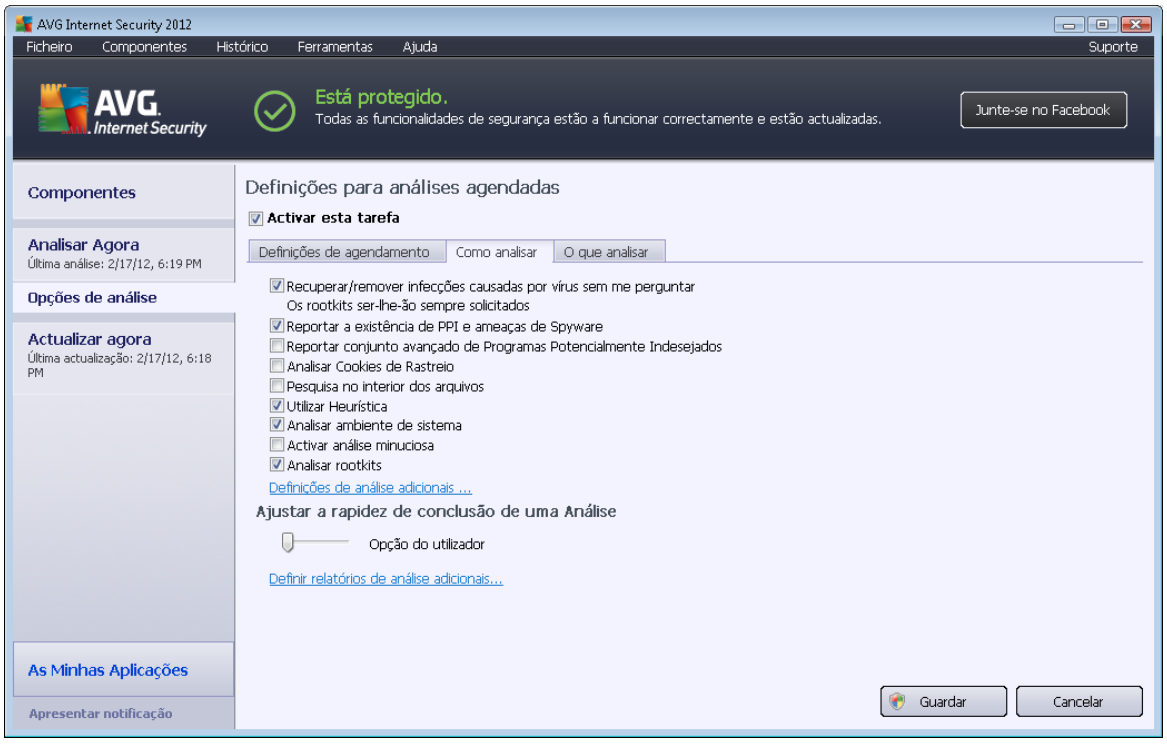
Botões de controlo da janela de Definições para análises agendadas

Existem dois botões de controlo disponíveis nos três separadores da janela ***Definições para análises agendadas*** (*Definições de agendamento, Como analisar e O que analisar*) e estes têm as mesmas funcionalidades independentemente do separador activo:

- ***Guardar*** – guarda todas as alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG. Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos

- ***Cancelar*** – cancela quaisquer alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG.

12.5.2. Como Analisar



No separador ***Como analisar*** encontrará uma lista de parâmetros de análise que podem ser opcionalmente activados/desactivados. A maioria dos parâmetros estão activados por predefinição e a funcionalidade será aplicada durante a análise. A menos que tenha uma razão válida para alterar estas definições, recomendamos que mantenha a configuração predefinida:

- ***Recuperar/remover infecções causadas por vírus sem me perguntar*** (*activado por predefinição*): se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Na eventualidade de o ficheiro infectado não poder ser recuperado automaticamente, ou se decidir desactivar esta opção, será notificado aquando da detecção de um vírus e terá de decidir o que fazer com a infecção

detectada. A acção recomendada é a remoção do ficheiro infectado para a Quarentena de Vírus.

- ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** (*activado por predefinição*): marque para activar o componente Anti-Spyware e analisar a existência de spyware assim como de vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** (*desactivado por predefinição*): marque para detectar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

- ***Analisar a existência de Cookies de Rastreio*** (*activado por predefinição*): este parâmetro do componente Anti-Spyware define que as cookies deverão ser detectadas durante a análise (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação especifica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos*).

- ***Analisar no interior de arquivos*** (*desactivado por predefinição*): este parâmetro define que a análise deverá verificar todos os ficheiros mesmo se estes estiverem comprimidos em arquivos, ex. ZIP, RAR, ...

- ***Utilizar Heurística*** (*activado por predefinição*): a análise heurística (*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a detecção de vírus durante a análise.

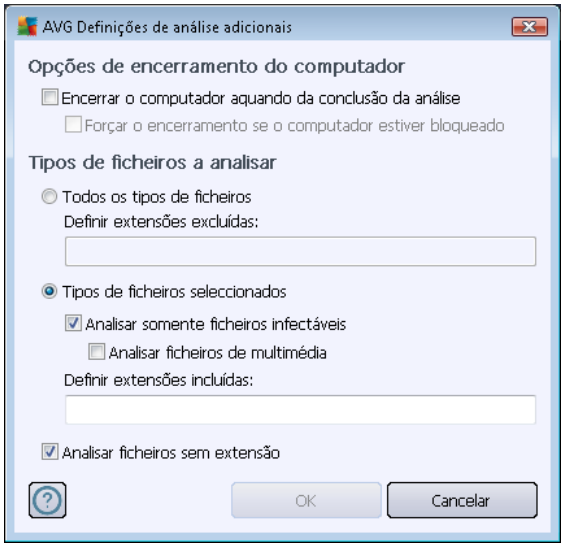
- ***Analisar o ambiente do sistema*** (*activado por predefinição*): a análise verificará também as áreas de sistema do seu computador.

- ***Activar análise minuciosa*** (*desactivado por predefinição*) – em situações específicas (*suspeita de infecção do computador*) pode marcar esta opção para activar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, inclusivamente as que dificilmente poderão ser infectadas, só para o caso. Tenha em consideração que este método é bastante demorado.

- ***Analisar a existência de rootkits*** (*activado por predefinição*): a análise Anti-Rootkit analisa o computador em busca de eventuais rootkits, ou seja, programas e tecnologias que podem ocultar actividade de malware no computador. Se for detectado um rootkit, isto não significa necessariamente que o computador esteja infectado. Em alguns casos, podem ser erroneamente detectados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Depois, pode alterar a configuração de análise da seguinte forma:

- ***Definições de verificação adicionais*** – a ligação abre uma nova janela de ***Definições de verificação adicionais*** onde pode especificar os seguintes parâmetros:



- ***Opções de encerramento do computador*** – decida se o computador deve ser encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção (***Encerrar o computador aquando do término da análise***), será activada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar encerramento se o computador estiver bloqueado***).

- ***Definir tipos de ficheiros para análise*** – deve decidir ainda se pretende que sejam analisados:

  - ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

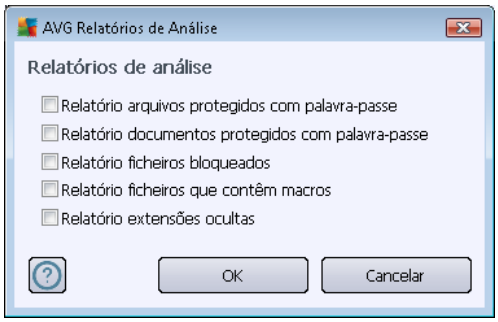
  - ***Tipos de ficheiros seleccionados*** – pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infectados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser analisados.

  - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

- ***Ajustar a rapidez de conclusão de uma Análise*** – pode usar o cursor para alterar a prioridade do processo de análise. O valor desta opção está, por predefinição, definido para o nível *Definida pelo utilizador* de utilização automática de recursos. Em alternativa, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador*

mas não se preocupa com a duração da análise), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*ex. quando o computador não está a ser utilizado*).

- ***Definir relatórios de análise adicionais*** – a ligação abre uma nova janela de ***Relatórios de Análise*** onde pode seleccionar que tipos de possíveis detecções deverão ser reportadas:



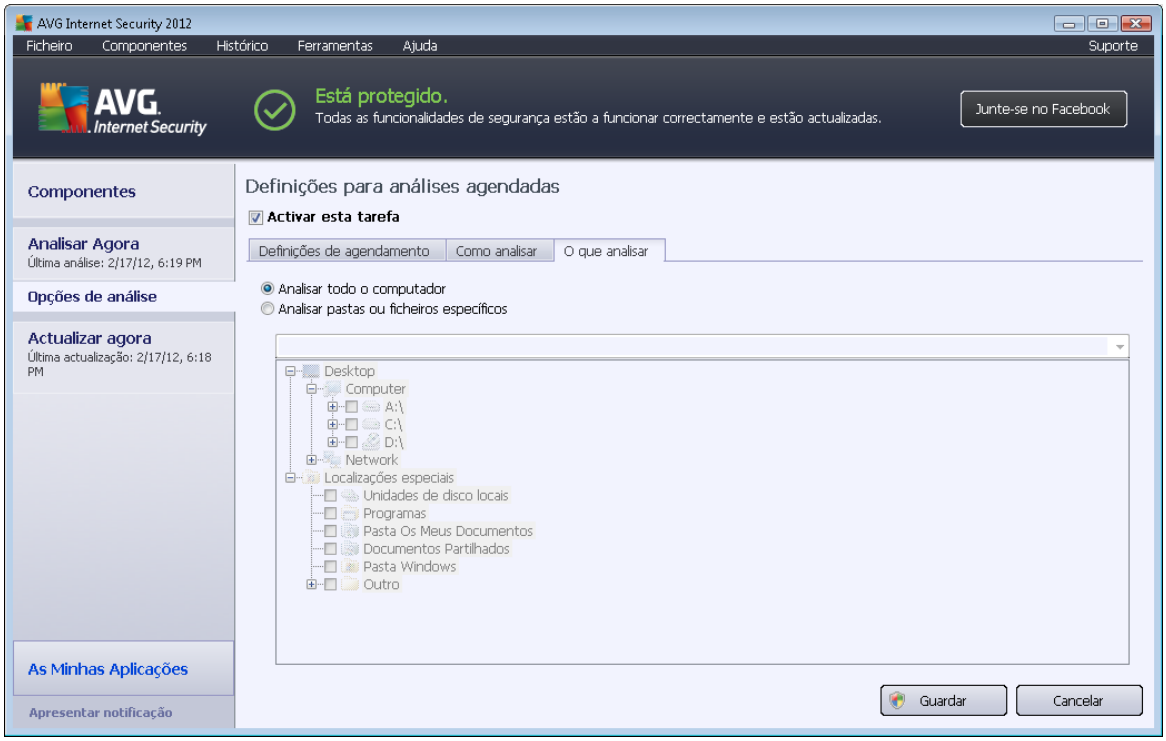
Botões de controlo

Existem dois botões de controlo disponíveis nos três separadores da janela ***Definições para análises agendadas*** (*Definições de agendamento*, *Como analisar* e *O que analisar*) e estes têm as mesmas funcionalidades independentemente do separador activo:

- ***Guardar*** – guarda todas as alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG. Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos

- ***Cancelar*** – cancela quaisquer alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG.

12.5.3. O que Analisar



No separador ***O que analisar*** pode definir se pretende agendar uma análise a todo o computador ou analisar ficheiros e pastas específicos.

Na eventualidade de seleccionar a análise de ficheiros ou pastas específicos, a estrutura em árvore apresentada na parte inferior desta janela é activada e pode especificar as pastas a serem analisadas (*expanda os itens ao clicar no 'mais' até encontrar a pasta que pretende analisar*). Pode seleccionar várias pastas ao seleccionar as caixas respectivas. As pastas seleccionadas irão aparecer no campo de texto no topo da janela, e a lista de opções guardará o histórico das suas análises seleccionadas para utilização futura. Em alternativa, pode introduzir a localização completa da pasta pretendida manualmente (*se introduzir várias localizações, é necessário separá-los com ponto e vírgula sem quaisquer espaços adicionais*).

Na estrutura em árvore pode igualmente visualizar uma secção com a identificação ***Localizações especiais***. De seguida, dispõe de uma lista de localizações que serão analisadas se a respectiva caixa estiver marcada:

- ***Unidades de disco locais*** - todas as unidades de disco do seu computador
- ***Ficheiros de Programas***
  - C:\Ficheiros de Programas\
  - *na versão de 64 bits* C:\Ficheiros de Programas (x86)
- ***Pasta Os Meus Documentos***

- *para o Win XP:* C:\Documents and Settings\Default User\Os Meus Documentos\
- *para o Windows Vista/7*: C:\Users\utilizador\Documentos\

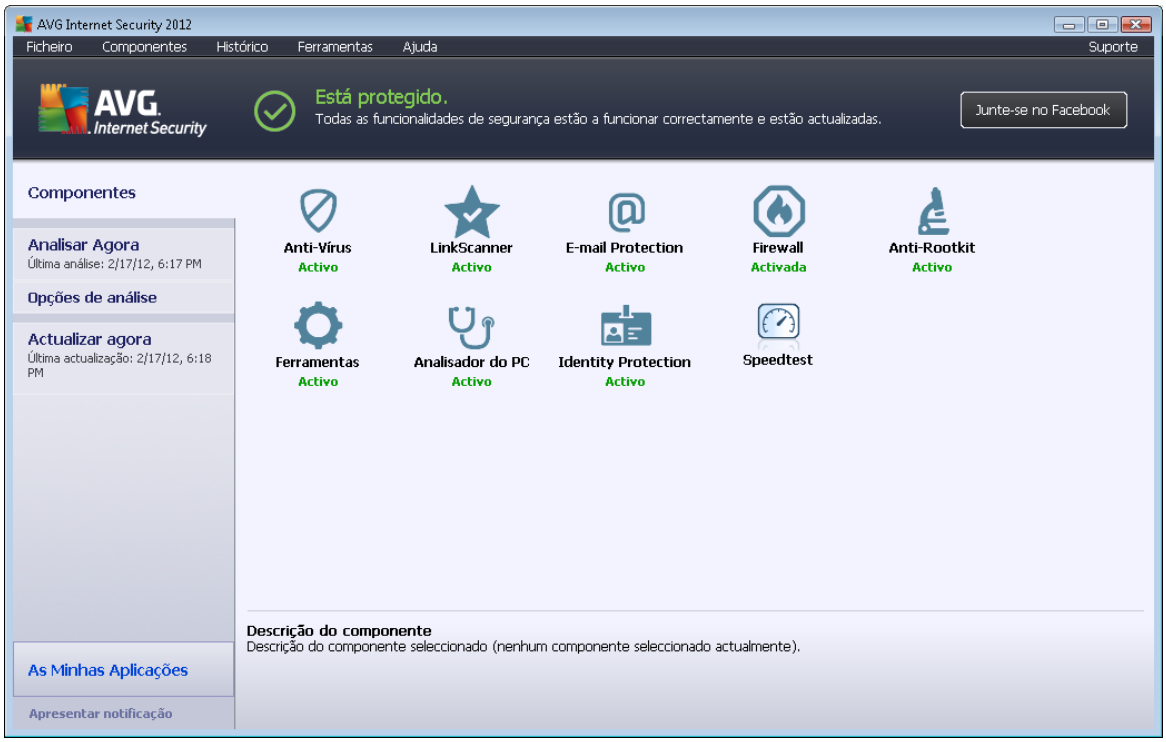
- ***Documentos Partilhados***
  - *para o Win XP*: C:\Documents and Settings\All Users\Documentos\
  - *para o Windows Vista/7*: C:\Users\Public\Documentos\
- ***Pasta Windows*** – C:\Windows\
- ***Outra***
  - *Unidade de sistema* – a unidade de disco rígido na qual o sistema operativo está instalado (normalmente C:)
  - *Pasta de sistema* – C:\Windows\System32\
  - *Pasta dos Ficheiros Temporários* – C:\Documents and Settings\User\Local\ (*Windows XP*); ou C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Ficheiros Temporários da Internet* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); ou C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Botões de controlo

Os mesmo dois botões de controlo estão disponíveis em todos os três separadores do janela ***Definições para análises agendadas*** (*Definições de agendamento*, *Como analisar* e *O que analisar)*:

- ***Guardar*** – guarda todas as alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG. Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos
- ***Cancelar*** – cancela quaisquer alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG.

12.6. Resumo dos Resultados da Análise



A janela ***Síntese dos resultados da análise*** é acessível a partir da interface de análise do AVG via o botão ***Histórico de análises***. A janela faculta uma lista de todas as análises executadas anteriormente e informações relativas aos seus resultados:

- ***Nome*** – designação da análise; pode ser o nome de uma das análises predefinidas ou um nome que tenha atribuído à sua própria análise agendada. Cada nome inclui um ícone indicando o resultado da análise.

  – ícone verde informa que não foram detectadas quaisquer infecções durante a análise

  – ícone azul anuncia que foi detectada uma infecção durante a análise mas que o objecto infectado foi removido automaticamente

  – ícone vermelho avisa que foi detectada uma infecção durante a análise e que não pôde ser removida!

  Cada ícone pode ser sólido ou cortado ao meio – o ícone sólido representa uma análise que foi concluída devidamente; o ícone cortado ao meio significa que a análise foi cancelada ou interrompida.

  Atenção:*Para informações detalhadas de cada análise por favor consulte a janela Resultados da Análise acessível via o botãoVer detalhes (na parte inferior desta janela).*

- ***Hora de inicio*** – data e hora em que a análise foi iniciada
- ***Hora de término*** – data e hora em que a análise foi terminada
- ***Objectos testados*** – número de objectos que foram verificados durante a análise
- ***Infecções*** – número de infecções de vírus detectadas / removidas
- ***Spyware*** – número de spyware detectado / removido
- ***Avisos*** – número de objectos suspeitos
- ***Rootkits*** – número de rootkits
- ***Informação de registo de análise*** – informações relativas ao decurso da análise e resultados (normalmente sobre a sua finalização ou interrupção)

Botões de controlo

Os botões de controlo para a janela ***Resumo dos resultados da análise***são:

- ***Ver detalhes*** - clique para mudar para a janela Resultados da Análise para ver dados detalhados da análise seleccionada
- ***Eliminar resultado*** - clique para remover o item seleccionado da síntese de resultados de análise
- ***Retroceder*** – alterna para a janela padrão da interface de análise do AVG

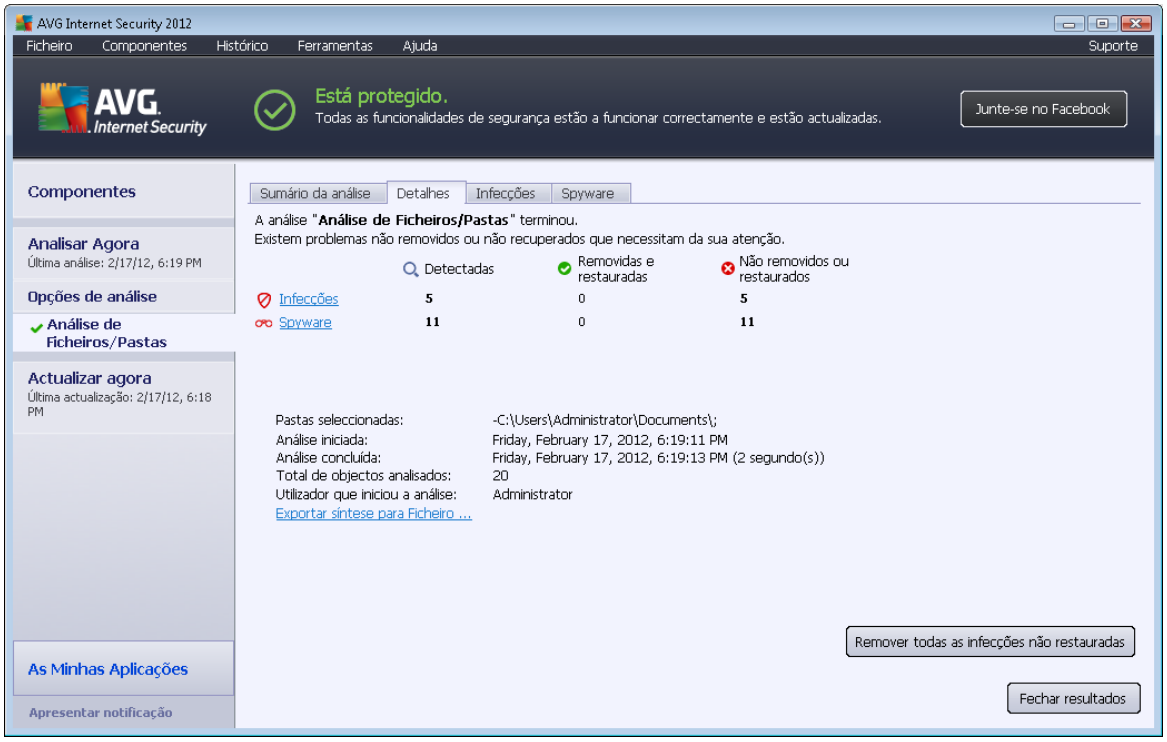
12.7. Detalhes dos Resultados da Análise

Se, na janela Síntese dos Resultados da Análise, estiver seleccionado um item específico, pode então clicar no botão ***Ver detalhes*** para alternar para a janela ***Resultados de Análise*** que providencia dados detalhados relativos ao decurso e resultado da análise seleccionada. A janela de diálogo está dividida em vários separadores:

- Síntese de Resultados – este separador é apresentado constantemente e faculta dados estatísticos que descrevem o progresso da análise
- Infecções – este separador só é apresentado se tiver sido detectada alguma infecção de vírus durante a análise
- Spyware – este separador só é apresentado se tiver sido detectado algum spyware durante a análise
- Avisos – este separador é apresentado, por exemplo, se tiverem sido detectados cookies durante a análise
- Rootkits – este separador só é apresentado se tiver sido detectado algum rootkit durante a análise

- Informação – este separador só é apresentado se tiverem sido detectadas ameaças potenciais mas que não podem ser classificadas em qualquer das categorias acima descritas; nesse caso o separador faculta mensagem de aviso aquando da detecção. Além disso, encontrará aqui informações sobre objectos que não foi possível analisar *(ex. arquivos protegidos por palavra-passe)*.

12.7.1. Separador Resumo dos Resultados



No separador ***Resultados da Análise*** pode encontrar estatísticas detalhadas com informação relativa a:

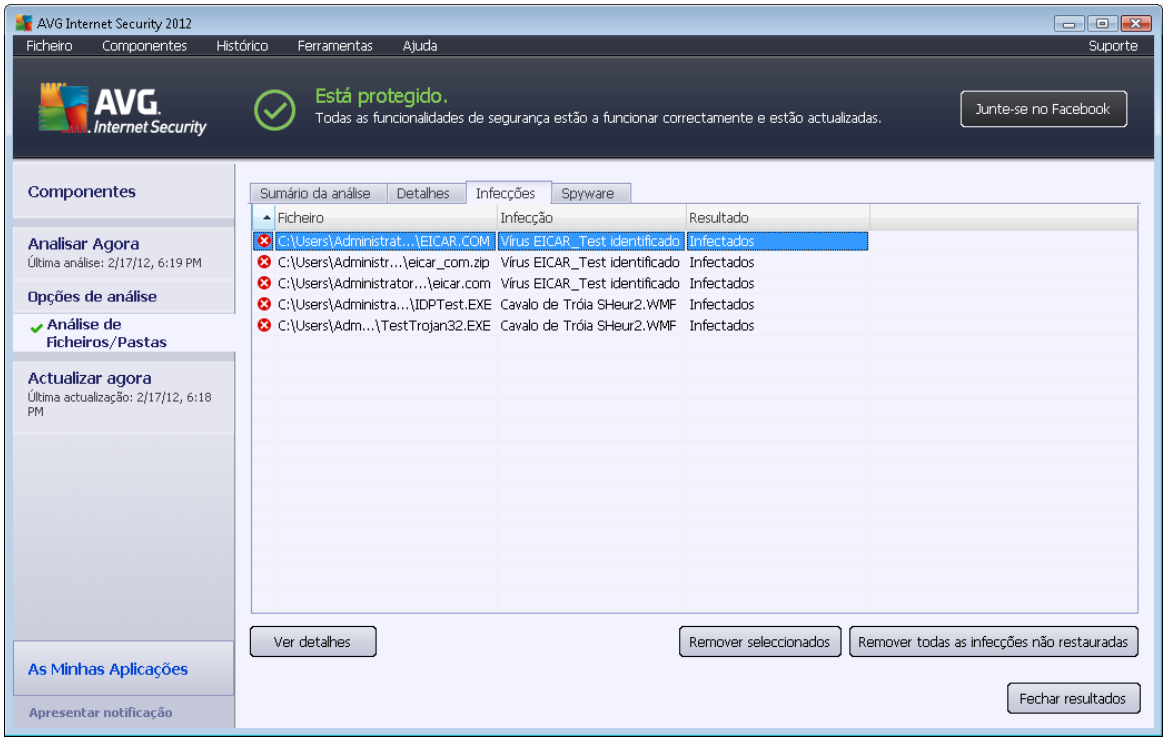
- infecções de vírus/spyware detectadas
- infecções de vírus/spyware removidas
- o número de infecções de vírus / spyware que não podem ser removidas ou recuperadas

Adicionalmente, encontrará informações relativas à data e hora exacta do inicio da análise, ao número total de objectos analisados, à duração da análise e ao número de erros que tenham ocorrido durante a análise.

Botões de controlo

Existe um botão de controlo disponível nesta janela. O botão ***Fechar resultados*** remete para a janela Resumo dos resultados da análise.

12.7.2. Separador Infecções



O separador ***Infecções*** só é apresentado na janela ***Resultados da Análise*** se tiver sido detectada alguma infecçãodurante a análise. O separador está dividido em três secções que facultam a seguinte informação:

- ***Ficheiro*** – localização original completa do objecto infectado
- ***Infecções*** – nome do vírus detectado (*para detalhes específicos relativos a vírus por favor consulte a Enciclopédia de vírus on-line*)
- ***Resultado*** – define o estado actual do objecto infectado que foi detectado durante a análise:
    - ***Infectado*** – o objecto infectado foi detectado e mantido na sua localização original (*por exemplo se tiver desactivado a opção de recuperação automática nas definições de uma análise específica*)
    - ***Recuperado*** – o objecto infectado foi recuperado automaticamente e mantido na sua localização original
    - ***Movido para a Quarentena de Vírus*** – o objecto infectado foi movido para a Quarentena de Vírus
    - ***Eliminado*** – o objecto infectado foi eliminado
    - ***Adicionado às excepções PUP*** - a detecção foi avaliada como sendo uma

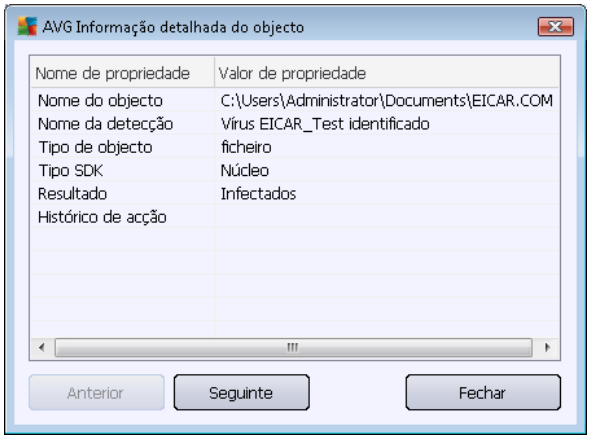
excepção e adicionada à lista de excepções PUP *(configurada na janela Excepções PUP das definições avançadas)*

- ***Ficheiro bloqueado – não testado*** – o objecto detectado está bloqueado e o AVG não o consegue analisar
- ***Objecto potencialmente perigoso*** - o objecto foi detectado como sendo potencialmente perigoso mas não infectado(*pode conter macros, por exemplo*); a informação deverá ser entendida como sendo um aviso
- ***É necessário reiniciar para concluir a acção*** – o objecto infectado não pode ser removido, para o remover por completo tem de reiniciar o seu computador

Botões de controlo

Existem três botões de controlo disponíveis nesta janela:

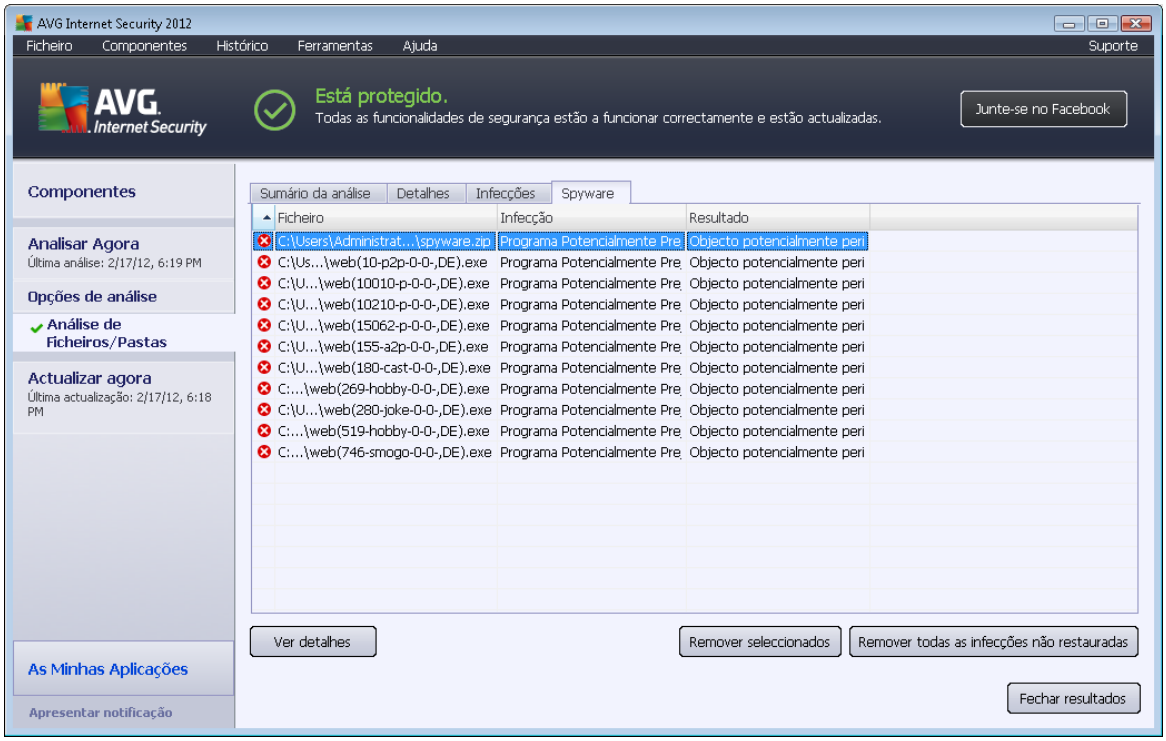
- ***Ver detalhes*** – o botão abre uma nova janela apelidada ***Informação detalhada de objecto*** :



  Nesta janela pode encontrar informações detalhadas sobre o objecto infeccioso detectado (*ex. nome e localização do objecto infectado, tipo de objecto, tipo SDK, resultado da detecção e histórico das acções associadas ao objecto detectado*). Ao utilizar os botões ***Anterior***/***Seguinte*** pode visualizar informações relativas a detecções especificas. utilizar o botão ***Fechar*** para fechar esta janela.

- ***Remover seleccionadas*** – utilize o botão para mover as detecções seleccionadas para a Quarentena de Vírus
- ***Remover todas as não recuperadas*** – este botão elimina todas as detecções que não possam ser recuperadas ou movidas para a Quarentena de Vírus
- ***Fechar resultados*** – conclui a síntese de informações detalhadas e retorna à janela Resumo dos resultados da análise

12.7.3. Separador Spyware



O separador ***Spyware*** só é apresentado na janela ***Resultados da Análise*** se tiver sido detectado spyware durante a análise. O separador está dividido em três secções que facultam a seguinte informação:

- ***Ficheiro*** – localização original completa do objecto infectado
- ***Infecções*** – nome do spyware detectado *(para detalhes relativos a vírus específicos por favor consulte a Enciclopédia de vírus on-line)*
- ***Resultado*** – define o estado actual do objecto infectado que foi detectado durante a análise:
    - ***Infectado*** – *o objecto infectado foi detectado e mantido na sua localização original (por exemplo se tiver desactivado a opção de recuperação automática nas definições de uma análise específica)*
    - ***Recuperado*** – o objecto infectado foi recuperado automaticamente e mantido na sua localização original
    - ***Movido para a Quarentena de Vírus*** – o objecto infectado foi movido para a Quarentena de Vírus
    - ***Eliminado*** – o objecto infectado foi eliminado
    - ***Adicionado às excepções PUP*** - a detecção foi avaliada como sendo uma excepção e adicionada à lista de excepções PUP *(configurada na janela Excepções*

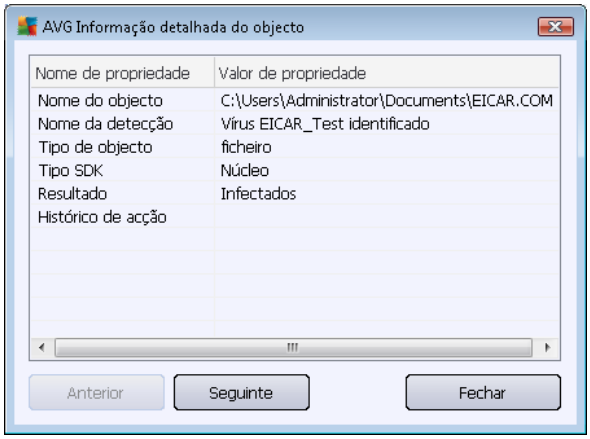
PUP das definições avançadas)

- ***Ficheiro bloqueado – não testado*** – o objecto detectado está bloqueado e o AVG não o consegue analisar
- ***Objecto potencialmente perigoso*** - o objecto foi detectado como sendo potencialmente perigoso mas não infectado (pode conter macros, por exemplo); a informação deverá ser entendida como sendo um aviso
- ***É necessário reiniciar para concluir a acção*** – o objecto infectado não pode ser removido, para o remover por completo tem de reiniciar o seu computador

Botões de controlo

Existem três botões de controlo disponíveis nesta janela:

- ***Ver detalhes*** – o botão abre uma nova janela apelidada ***Informação detalhada de objecto*** :



  Nesta janela pode encontrar informações detalhadas sobre o objecto infeccioso detectado (*ex. nome e localização do objecto infectado, tipo de objecto, tipo SDK, resultado da detecção e histórico das acções associadas ao objecto detectado*). Ao utilizar os botões ***Anterior***/***Seguinte*** pode visualizar informações relativas a detecções especificas. Utilize o botão ***Fechar*** para fechar esta janela.

- ***Remover seleccionadas*** – utilize o botão para mover as detecções seleccionadas para a Quarentena de Vírus
- ***Remover todas as não recuperadas*** – este botão elimina todas as detecções que não possam ser recuperadas ou movidas para a Quarentena de Vírus
- ***Fechar resultados*** – conclui a síntese de informações detalhadas e retorna à janela Resumo dos resultados da análise

12.7.4. Separador Avisos

O separador ***Avisos*** apresenta informações acerca de objectos "suspeitos" (*normalmente ficheiros*) detectados durante as análises. Ao serem detectados pela Protecção Residente, o acesso a estes ficheiros é bloqueado. Exemplo típicos deste tipo de detecções são: ficheiros ocultos, cookies, chaves de registo suspeitas, documentos ou arquivos protegidos por palavra-passe, etc. Esses ficheiros não representam qualquer ameaça directa para o seu computador ou a segurança do mesmo. As informações sobre estes ficheiros são úteis na eventualidade de ser detectado um adware ou um spyware no seu computador. Se, nos resultados de teste, só forem detectados avisos pelo **AVG Internet Security 2012**, não é necessária qualquer acção.

Esta é uma breve descrição dos exemplos mais comuns desses objectos:

- ***Ficheiros ocultos*** - Os ficheiros ocultos não são, por predefinição, visíveis no Windows, e alguns vírus ou outras ameaças podem evitar a sua detecção ao guardarem os seus ficheiros com este atributo. Se o seu **AVG Internet Security 2012** reportar um ficheiro oculto que o utilizador suspeite ser malicioso, pode movê-lo para a Quarentena de Vírus do AVG.

- ***Cookies*** – As cookies são ficheiros de texto simples que são usados pelos websites para guardar informações específicas relativas ao utilizador e que são posteriormente usadas para carregar esquemas de página predefinidos, preenchimento do nome de utilizador, etc.

- ***Chaves de registo suspeitas*** - Algum malware guarda as suas informações no Registo do Windows para assegurar que é carregado no arranque ou para alargar o seu efeito sobre o sistema operativo.

12.7.5. Separador Rootkits

O separador ***Rootkits*** apresenta informações sobre os rootkits detectados durante a análise anti-rootkit incluída na Análise de todo o computador.

Um rootkit é um programa concebido para assumir controlo do sistema do computador, sem a autorização dos proprietários e gestores legítimos do mesmo. O acesso ao hardware é raramente necessário uma vez que um rootkit destina-se a assumir o controlo do sistema operativo em execução no hardware. Regra geral, os rootkits agem de forma a ocultar a sua presença no sistema através de subversões ou evasões dos mecanismos de segurança padrão dos sistemas operativos. Acontece que estes também são frequentemente Trojans; como tal, enganam os utilizadores para que estes pensem que os mesmos podem ser executados em segurança nos seus sistemas. As técnicas utilizadas para este efeito podem incluir ocultar processos em execução de programas de monitorização, ou esconder ficheiros ou dados de sistema do sistema operativo.

A estrutura deste separador é basicamente a mesma do separador Infecções ou do separador Spyware.

12.7.6. Separador Informações

O separador ***Informação*** contém dados acerca dessas "detecções" que não podem ser categorizadas como infecções, spyware, etc. Não podem ser positivamente etiquetadas como perigosas mas contudo carecem da sua atenção. A análise do **AVG Internet Security 2012** consegue detectar ficheiros que podem não estar infectados, mas que são suspeitos. Estes ficheiros são reportados como Aviso, ou como Informação.

O nível de gravidade ***Informação*** pode ser reportado por uma das seguintes razões.

- ***Executável compilado*** – O ficheiro foi compilado com um dos compiladores de executáveis menos comuns, o que pode indicar uma tentativa de evitar a análise desse ficheiro. No entanto, nem todas as reportações desse ficheiro indicam um vírus.

- ***Executável compilado recursivo*** – semelhante ao anterior, no entanto menos frequente entre o software comum. Tais ficheiros são suspeitos e deve ser considerada a sua remoção ou submissão para análise.

- ***Arquivo ou documento protegidos por palavra-passe*** - Os ficheiros protegidos por palavra-passe não podem ser analisados pelo **AVG Internet Security 2012** (*ou qualquer outros programa anti-malware*).

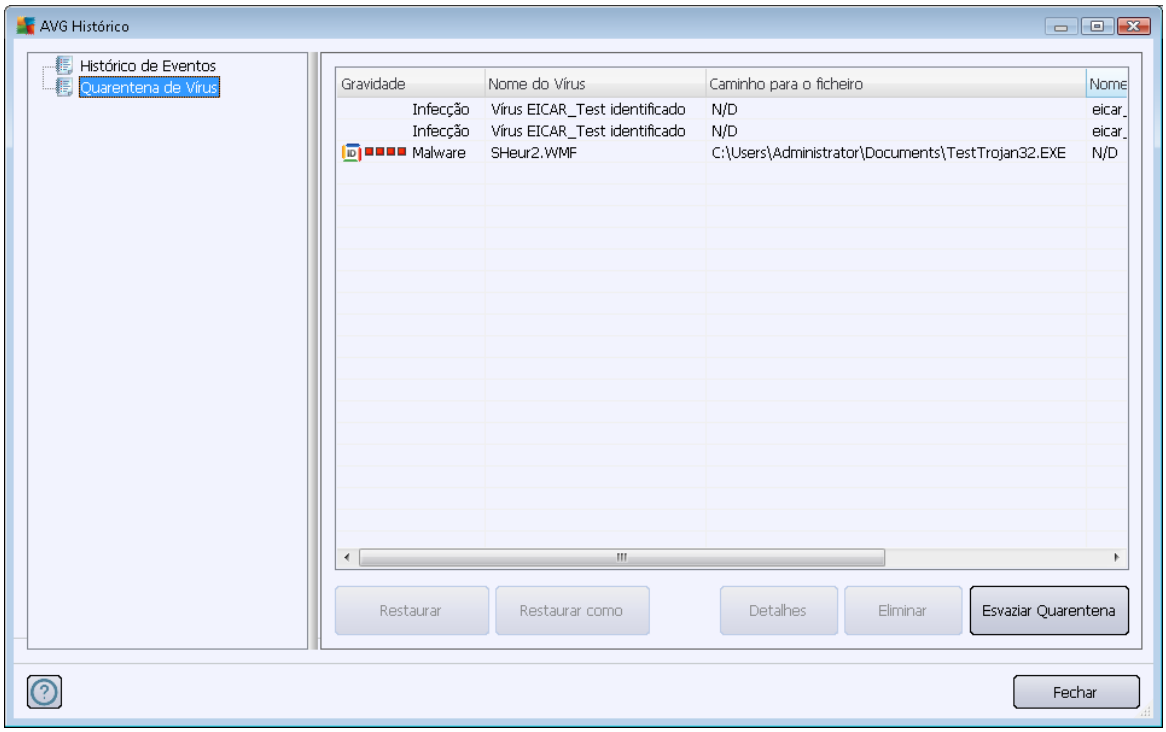
- ***Documentos com macros*** – o documento contém macros, que podem ser maliciosas.

- ***Extensão oculta*** - Ficheiros com extensão oculta podem aparentar ser, por exemplo, imagens, mas serem na verdade ficheiros executáveis (*ex. imagem.jpg.exe*). A segunda extensão não é visível no Windows por predefinição, e o **AVG Internet Security 2012** reporta esses ficheiros para evitar a abertura acidental dos mesmos.

- ***Localização do ficheiro inadequada*** – Se algum ficheiro de sistema importante estiver a ser executado a partir de outra localização que não a predefinida (*ex. winlogon.exe a ser executado de outra pasta que não a pasta Windows*), o **AVG Internet Security 2012** reporta esta discrepância. Em alguns casos, os vírus usam nomes de processos do sistema tradicionais para tornarem a sua presença menos evidente no sistema.

- ***Ficheiro bloqueado*** – O ficheiro está bloqueado e, como tal, não pode ser analisado pelo **AVG Internet Security 2012**. Isto normalmente significa que existe um ficheiro que está constantemente a ser usado pelo sistema (*ex. ficheiro swap*).

12.8. Quarentena de Vírus



A Quarentena de Vírus é um ambiente seguro para a gestão de objectos suspeitos/infectados detectados durante os testes AVG. Se um objecto infectado for detectado durante a análise e o AVG não puder recuperá-lo automaticamente, deverá decidir o que fazer com o objecto suspeito. A solução recomendada consiste em mover o objecto para a ***Quarentena de Vírus*** para tratamento futuro. O propósito principal da ***Quarentena de Vírus*** é manter qualquer ficheiro eliminado durante um determinado período de tempo, para que possa certificar-se de que já não necessita do ficheiro na localização original. Se, porventura, descobrir que a ausência do ficheiro causa problemas, pode enviar o ficheiro em questão para análise ou restaurá-lo para a localização original.

A interface da ***Quarentena de vírus*** abre numa janela separada e oferece uma síntese da informação dos objectos infectados colocados em quarentena:

- ***Gravidade*** – na eventualidade de decidir instalar o componente Protecção de Identidade integrado no **AVG Internet Security 2012**, será apresentada nesta secção uma identificação gráfica da gravidade da detecção respectiva numa escala de quatro níveis desde inofensiva (■□□□) até muito perigosa (■■■■); e a informação sobre o tipo de infecção (*com base no nível de infecção – todos os objectos listados podem estar positiva ou potencialmente infectados*)

- ***Nome do vírus*** – especifica o nome da infecção detectada de acordo com a Enciclopédia de vírus *(on-line)*

- ***Localização do ficheiro*** – localização original do ficheiro infeccioso detectado

- ***Nome original do objecto*** – todos os objectos detectados listados na tabela foram

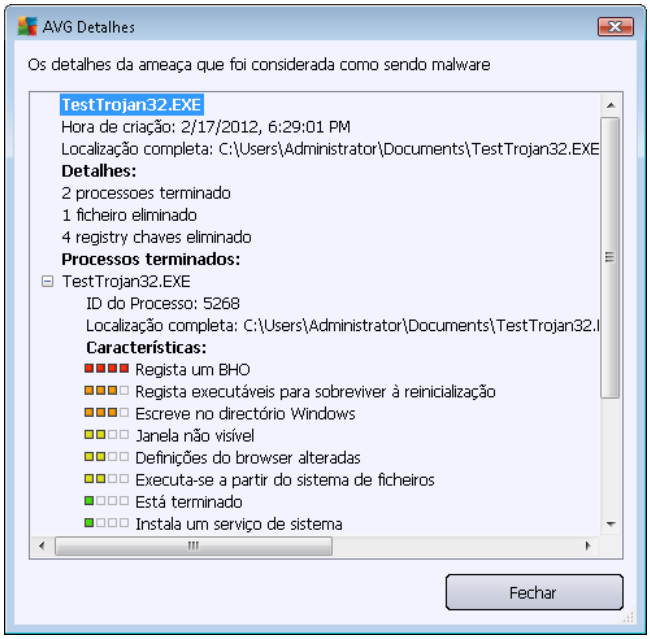
etiquetados com o nome padrão dado pelo AVG durante o processo de análise. Na eventualidade de o objecto ter um nome específico que seja conhecido (*ex. o nome de um anexo de e-mail que não corresponde ao conteúdo efectivo do anexo*), este será facultado nesta coluna.

- ***Data de armazenamento*** – data e hora em que o ficheiro suspeito foi detectado e removido para a Quarentena de Vírus

Botões de controlo

Os seguintes botões de controlo estão acessíveis a partir da interface da ***Quarentena de Vírus***:

- ***Restaurar*** – repõe o ficheiro infectado à sua localização original no seu disco rígido
- ***Restaurar Como*** – move o ficheiro infectado para a pasta seleccionada
- ***Detalhes*** – este botão só é aplicável a ameaças detectadas pela Protecção de Identidade. Ao clicar, apresenta uma síntese sinóptica das informações da ameaça (*que ficheiros/ processos foram afectados, características do processo, etc.)*). Tenha em atenção que para todos os restantes itens que não tenham sido detectados pela PID, este botão será apresentado a cinzento e inactivo!



- ***Eliminar*** - remove o ficheiro infectado da ***Quarentena de Vírus*** completa e irreversivelmente
- ***Quarentena vazia*** – remover todos ***Quarentena de Vírus*** conteúdo completamente. Ao remover os ficheiros da ***Quarentena de Vírus***, esses ficheiros são irremediavelmente removidos do disco (*não movidos para a Reciclagem*).

13. Actualizações do AVG

Nenhum software de segurança pode garantir uma protecção efectiva contra vários tipos de ameaças a menos que seja actualizado regularmente! Os criadores de vírus estão constantemente à espreita de novas falhas que possam explorar, tanto em software como nos sistemas operativos. Novos vírus, novo malware, novos ataques de intrusão surgem todos os dias. Por isso, os vendedores de software estão constantemente a lançar actualizações e correcções, para solucionar quaisquer falhas de segurança que sejam descobertas.

Tendo em conta todas as novas ameaças informáticas que surgem, e a velocidade a que se disseminam, é totalmente essencial actualizar o seu **AVG Internet Security 2012** regularmente. A melhor solução é manter as configurações predefinidas do programa. Tenha em conta que se a base de dados de vírus do seu **AVG Internet Security 2012** não estiver actualizada, o programa não poderá detectar as ameaças mais recentes!

É essencial actualizar o seu AVG regularmente! As actualizações de definições de vírus essenciais deverão ser diárias, se possível. As actualizações do programa menos urgentes podem ser semanais.

13.1. Execução de actualização

Para proporcionar o máximo de segurança possível, o **AVG Internet Security 2012** está agendado, por predefinição, para procurar novas actualizações a cada quatro horas. Uma vez que as actualizações do AVG não são lançadas com base num intervalo específico, mas antes em função da quantidade e severidade das novas ameaças, esta verificação é extremamente importante para garantir que a base de dados de vírus do seu AVG está constantemente actualizada.

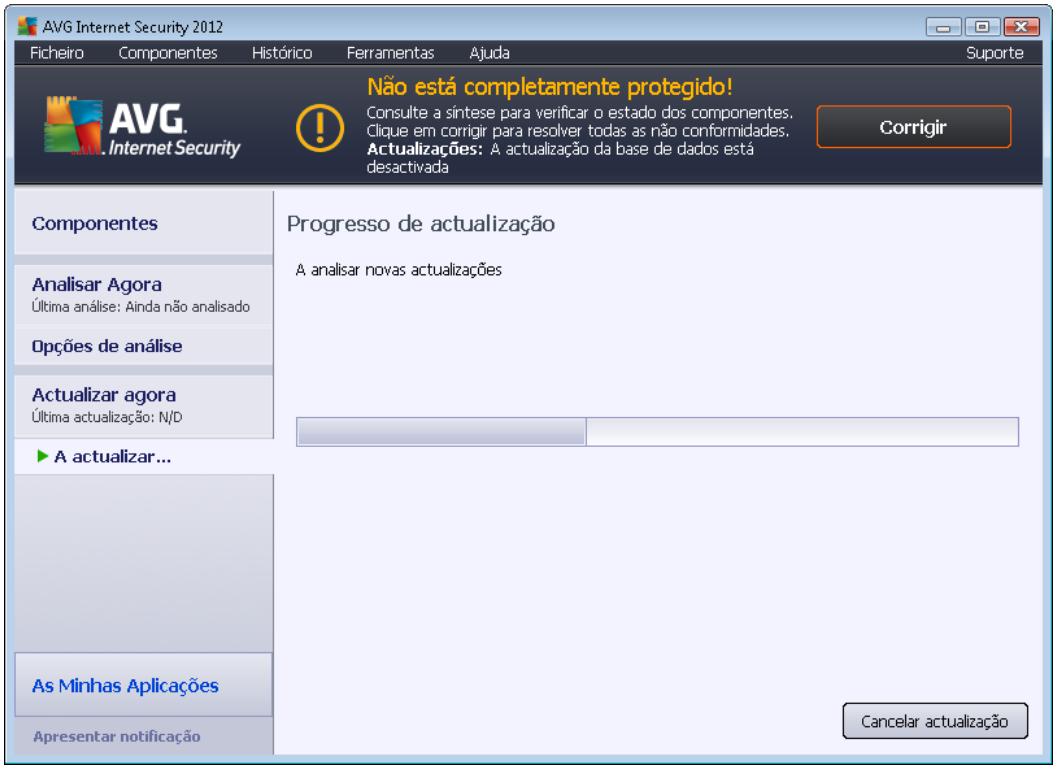
Se quiser reduzir o número de execuções da actualização, pode configurar os seus próprios parâmetros de actualização. No entanto, recomendamos imperativamente que execute a actualização um mínimo de uma vez por dia! A configuração pode ser editada na secção Definições avançadas/Agendamentos, especificamente nas seguintes janelas:

- Agendamento de actualização de definições
- Agendamento de actualização do programa
- Agendamento de Actualização do Anti-Spam

Caso pretenda verificar a existência de novos ficheiros imediatamente, use o link rápido Actualizar agora na janela principal do AVG. Este link está constantemente disponível a partir de qualquer janela da Interface do utilizador do .

13.2. Progresso de actualização

Assim que inicia a actualização, o AVG verifica a existência de novos ficheiros de actualização disponíveis. Se for o caso, o **AVG Internet Security 2012** começará a transferi-los e inicia o processo de transferência propriamente dito. Durante o processo de actualização será redireccionado para a interface de ***Actualização*** onde pode ver o progresso do processo na sua representação gráfica, assim como numa síntese de parâmetros estatísticos relevantes *(tamanho do ficheiro de actualização, dados recebidos, velocidade de transferência, tempo decorrido, etc.)*:



***Nota**: Antes da iniciação da actualização do programa AVG será criado um ponto de restauro. Na eventualidade do processo de actualização falhar e o seu sistema operativo falhar pode sempre restaurar o seu sistema operativo para a configuração original a partir deste ponto. Esta opção é acessível através do menu do Windows: Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauro do Sistema. Recomendado apenas para utilizadores experientes!*

13.3. Níveis de actualização

O **AVG Internet Security 2012** disponibiliza dois níveis de actualização passíveis de selecção:

- ***Definições de actualização*** contém alterações necessárias para uma protecção anti-vírus, anti-spam e anti-malware fiável. Normalmente, não inclui alterações ao código e apenas actualiza a base de dados de definições. Esta actualização deve ser aplicada logo que esteja disponível.

- ***Actualização do programa*** contém várias alterações do programa, soluções e melhorias.

Aquando do agendamento de uma actualização, é possível definir parâmetros específicos para ambos os níveis de actualização:

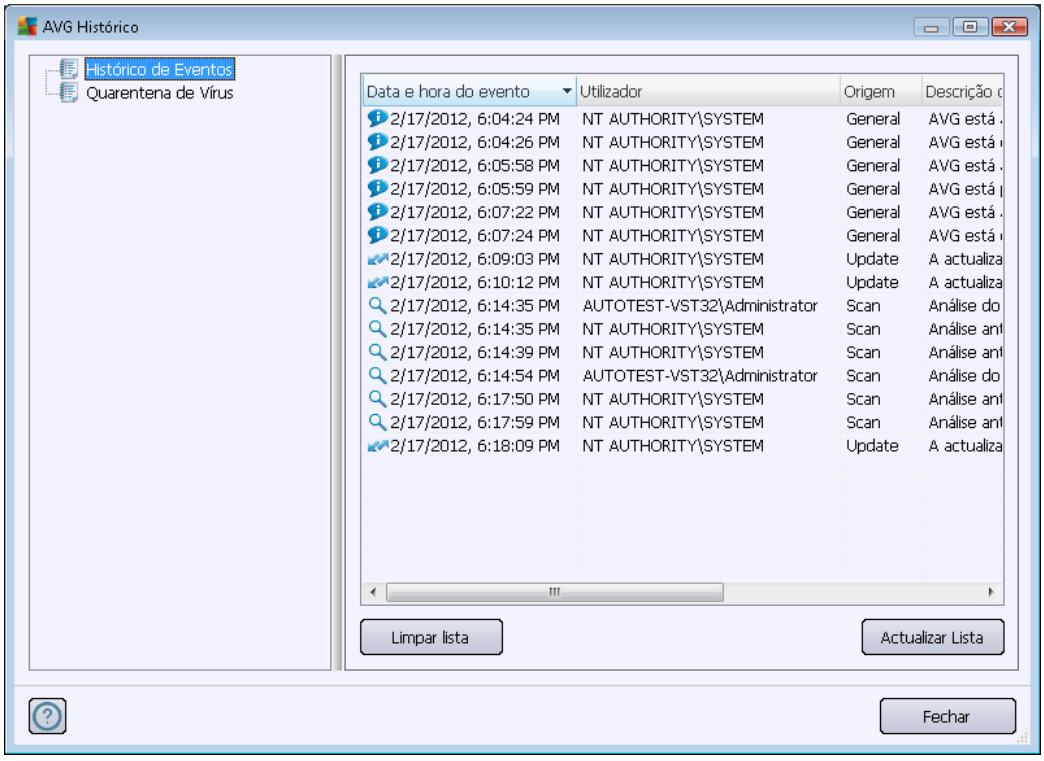
- Agendamento de actualização de definições

- Agendamento de actualização do programa

***Nota:** Se ocorrer uma coincidência temporal de execução de um agendamento de actualização do programa e de um agendamento de uma análise, o processo de actualização terá precedência e a*

análise será interrompida.

14. Histórico de Eventos



A janela ***Histórico*** é acessível a partir do menu de sistema via o item ***Histórico/Registo do Histórico de Eventos***. Nesta janela poderá encontrar um resumo dos eventos importantes ocorridos durante o funcionamento do **AVG Internet Security 2012**. ***O Histórico*** regista os seguintes tipos de eventos:

- Informações acerca das actualizações da aplicação do AVG
- Informações relativas ao início, conclusão ou interrupção de análises (*incluindo as análises executadas automaticamente*)
- Informações relativas à detecção de vírus (*seja pela Protecção Residente ou por uma análise*) incluindo a localização da ocorrência
- Outros eventos importantes

Para cada evento, são apresentadas as seguintes informações:

- ***Data e hora do evento*** apresenta a data e a hora exactas a que o evento ocorreu
- ***Utilizador*** especifica o nome do utilizador com sessão iniciada no momento em que ocorreu o evento
- ***Origem*** apresenta as informações relativas ao componente de origem, ou outra parte do sistema AVG, que despoletou o evento

- ***Descrição do evento*** apresenta um breve resumo do que de facto aconteceu

Botões de controlo

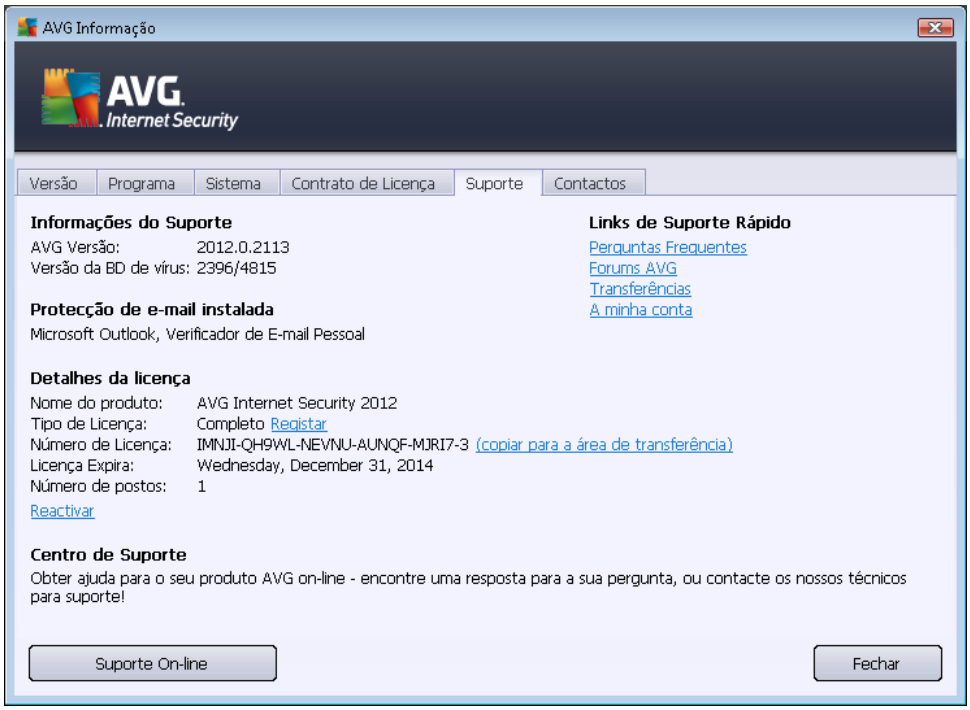
- ***Lista vazia*** - clique neste botão para eliminar todas as entradas da lista de eventos
- ***Actualizar lista*** – clique neste botão para actualizar todas as entradas da lista de eventos

15. FAQ e Suporte Técnico

Na eventualidade de ter alguma dúvida ou problema de ordem comercial ou técnica com o seu **AVG Internet Security 2012** , há várias formas de obter ajuda. Queira escolher entre as seguintes opções:

- ***Obter suporte***: dentro da aplicação AVG, pode aceder a uma página dedicada de apoio ao cliente no website da AVG (http://www.avg.com/). Seleccione o item ***Ajuda / Obter suporte*** no menu principal para ser encaminhado para o website da AVG com as opções de suporte disponíveis. Para continuar, queira seguir as instruções apresentadas na página.

- ***Suporte (hiperligação do menu principal)***: O menu do AVG (*no topo da interface do utilizador*) inclui a hiperligação ***Suporte*** que abre uma nova janela com todos os tipos de informações de que possa precisar quando procura ajuda. A janela inclui dados básicos sobre o seu programa AVG (*programa / versão da base de dados*), informações da licença e uma lista de hiperligações de suporte rápido:



- ***Resolução de problemas no ficheiro de ajuda***: está disponível uma nova secção de ***Resolução de problemas*** directamente no ficheiro de ajuda incluído no **AVG Internet Security 2012** *(para abrir o ficheiro de ajuda, carregue na tecla F1 em qualquer janela da aplicação)*. Esta secção providencia uma lista das situações que ocorrem com maior frequência e que motivam a procura de ajuda profissional por parte de um utilizador. Queira seleccionar a situação que melhor descreve o seu problema e clique sobre a mesma para abrir instruções detalhadas que solucionam o problema.

- ***Centro de Suporte do Website da AVG***: Em alternativa, pode consultar a solução para o seu problema no website da AVG (http://www.avg.com/). Na secção ***Centro de Suporte*** pode encontrar uma síntese estruturada de grupos temáticos que tratam de questões

técnicas e comerciais.

- ***Perguntas Frequentes***: no Website da AVG (http://www.avg.com/) também pode encontrar uma secção à parte e elaboradamente estruturada de perguntas frequentes. Esta secção é acessível através da opção do menu ***Centro de Suporte / Perguntas Frequentes***. Mais uma vez, todas as perguntas estão divididas de forma ordenada em categorias comercial, técnica e de vírus.

- ***Acerca de Vírus e Ameaças***: um capítulo específico do website da AVG (http://www.avg.com/) é dedicado a questões relativas a vírus *(é possível aceder à página Web a partir do menu principal, através da opção Ajuda / Acerca de Vírus e Ameaças)*. No menu, seleccione ***Centro de Suporte / Acerca de Vírus e Ameaças*** para aceder a uma página que apresenta uma vista estruturada de informações relativas a ameaças online. Também encontra instruções para a remoção de vírus, spyware e conselhos sobre como se manter protegido.

- ***Fórum de debate***: Também pode usar o fórum de debate dos utilizadores do AVG em http://forums.avg.com.