



AVG Internet Security 2011

Manual do Utilizador

Revisão do documento 2011.21 (16.5.2011)

Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.
Todas as outras marcas comerciais são propriedade dos respectivos proprietários.

Este produto utiliza o Algoritmo MD5 Message-Digest da RSA Data Security, Inc., Copyright (C) 1991-2, RSA Data Security, Inc. Criado em 1991.

Este produto utiliza código da biblioteca C-SaCzec, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Este produto utiliza a biblioteca de compressão zlib, Copyright (c) 1995-2002 Jean-loup Gailly e Mark Adler.
Este produto utiliza a biblioteca de compressão libbzip2, Copyright (c) 1996-2002 Julian R. Seward.



Índice

1. Introdução	8
2. Requisitos de Instalação do AVG	9
2.1 Sistemas Operativos Suportados	9
2.2 Requisitos Mínimos e Recomendados de Hardware	9
3. Opções de Instalação do AVG	10
4. Processo de Instalação do AVG	11
4.1 Bem-vindo	11
4.2 Activar a sua licença do AVG	12
4.3 Seleccione o tipo de instalação	13
4.4 Opções Personalizadas	14
4.5 Instalar a Barra de Ferramentas de Segurança AVG	15
4.6 Progresso da instalação	16
4.7 A instalação foi concluída com sucesso	16
5. Após a Instalação	18
5.1 Registo do produto	18
5.2 Aceder à Interface do Utilizador	18
5.3 Análise de todo o computador	18
5.4 Teste Eicar	18
5.5 Configuração predefinida do AVG	19
6. Interface de Utilizador AVG	20
6.1 Menu de Sistema	21
6.1.1 Ficheiro	21
6.1.2 Componentes	21
6.1.3 Histórico	21
6.1.4 Ferramentas	21
6.1.5 Ajuda	21
6.2 Informação de Estado de Segurança	24
6.3 Links Rápidos	25
6.4 Síntese de Componentes	25
6.5 Estatísticas	27
6.6 Ícone da barra de tarefas	27
6.7 Gadget do AVG	28



7. Componentes do AVG	31
7.1 Anti-Vírus	31
7.1.1 <i>Princípios de Anti-Vírus</i>	31
7.1.2 <i>Interface do Anti-vírus</i>	31
7.2 Anti-Spyware	32
7.2.1 <i>Princípios de Anti-Spyware</i>	32
7.2.2 <i>Interface do Anti-Spyware</i>	32
7.3 Anti-Spam	34
7.3.1 <i>Princípios do Anti-Spam</i>	34
7.3.2 <i>Interface do Anti-Spam</i>	34
7.4 Firewall	35
7.4.1 <i>Princípios da Firewall</i>	35
7.4.2 <i>Perfis da Firewall</i>	35
7.4.3 <i>Interface da Firewall</i>	35
7.5 Link Scanner	39
7.5.1 <i>Princípios do Link Scanner</i>	39
7.5.2 <i>Interface do Link Scanner</i>	39
7.5.3 <i>Search-Shield</i>	39
7.5.4 <i>Surf-Shield</i>	39
7.6 Protecção Residente	43
7.6.1 <i>Princípios da Protecção Residente</i>	43
7.6.2 <i>Interface da Protecção Residente</i>	43
7.6.3 <i>Deteção da Protecção Residente</i>	43
7.7 Family Safety	48
7.8 AVG LiveKive	48
7.9 Verificador de E-mail	48
7.9.1 <i>Princípios do Verificador de E-mail</i>	48
7.9.2 <i>Interface do Verificador de E-mail</i>	48
7.9.3 <i>Deteção de verificador de E-mail</i>	48
7.10 Actualizações	52
7.10.1 <i>Princípios de Actualizações</i>	52
7.10.2 <i>Interface de Actualizações</i>	52
7.11 Licença	54
7.12 Administração Remota	55
7.13 Protecção Online	56
7.13.1 <i>Princípios da Protecção Online</i>	56
7.13.2 <i>Interface da Protecção Online</i>	56



7.13.3 Detecção da Protecção Online	56
7.14 Anti-Rootkit	59
7.14.1 Princípios do Anti-Rootkit	59
7.14.2 Interface do Anti-Rootkit	59
7.15 Ferramentas	61
7.15.1 Processos	61
7.15.2 Ligações de Rede	61
7.15.3 Arranque automático	61
7.15.4 Extensões do Browser	61
7.15.5 Visualizador LSP	61
7.16 Analisador do PC	66
7.17 Protecção de Identidade	68
7.17.1 Princípios da Protecção de Identidade	68
7.17.2 Interface da Protecção de Identidade	68
7.18 Barra de Ferramentas de Segurança	70
8. Barra de Ferramentas de Segurança AVG	72
8.1 Interface da Barra de Ferramentas de Segurança AVG	72
8.1.1 Botão de logótipo do AVG	72
8.1.2 Caixa de pesquisa do AVG Secure Search (powered by Google)	72
8.1.3 Estado da Página	72
8.1.4 Notícias do AVG	72
8.1.5 Notícias	72
8.1.6 Eliminar histórico	72
8.1.7 Notificador de E-mail	72
8.1.8 Informação Meteorológica	72
8.1.9 Facebook	72
8.2 Opções da Barra de Ferramentas de Segurança AVG	79
8.2.1 Separador Geral	79
8.2.2 Separador Botões Úteis	79
8.2.3 Separador Segurança	79
8.2.4 Separador Opções Avançadas	79
9. Definições Avançadas do AVG	84
9.1 Aparência	84
9.2 Sons	86
9.3 Ignorar Condições de Erro	88
9.4 Protecção de Identidade	89
9.4.1 Definições da Protecção de Identidade	89



9.4.2 Lista de Permissões	89
9.5 Quarentena de Vírus	93
9.6 Excepções PUP	93
9.7 Anti-Spam	95
9.7.1 Definições	95
9.7.2 Desempenho	95
9.7.3 RBL	95
9.7.4 Lista Branca	95
9.7.5 Lista Negra	95
9.7.6 Definições Avançadas	95
9.8 Protecção Online	107
9.8.1 Protecção na Internet	107
9.8.2 Mensagens Instantâneas	107
9.9 Link Scanner	111
9.10 Análises	112
9.10.1 Analisar todo o computador	112
9.10.2 Análise em contexto	112
9.10.3 Analisar pastas ou ficheiros específicos	112
9.10.4 Análise de Dispositivo Amovível	112
9.11 Agendamentos	117
9.11.1 Análise agendada	117
9.11.2 Agendamento de actualização da base de dados de vírus	117
9.11.3 Agendamento de actualização do programa	117
9.11.4 Agendamento de Actualização do Anti-Spam	117
9.12 Verificador de E-mail	129
9.12.1 Certificação	129
9.12.2 Filtro de Correio	129
9.12.3 Servidores	129
9.13 Protecção Residente	138
9.13.1 Definições Avançadas	138
9.13.2 Itens excluídos	138
9.14 Servidor de Memória Cache	142
9.15 Anti-Rootkit	143
9.16 Actualizar	144
9.16.1 Proxy	144
9.16.2 Acesso telefónico	144
9.16.3 URL	144
9.16.4 Gerir	144



9.17 Desactivar temporariamente a protecção do AVG	151
9.18 Programa de Melhoria do Produto	152
10. Definições da Firewall	155
10.1 Geral	155
10.2 Segurança	156
10.3 Áreas e perfis de Adaptadores	157
10.4 IDS	158
10.5 Registos	160
10.6 Perfis	162
11. Análise do AVG	164
11.1 Interface de Análise	164
11.2 Análises Predefinidas	165
11.2.1 Análise de todo o computador	165
11.2.2 Analisar pastas ou ficheiros específicos	165
11.2.3 Análise Anti-Rootkit	165
11.3 A analisar no Explorador do Windows	175
11.4 Análise da Linha de Comandos	176
11.4.1 Parâmetros da Análise CMD	176
11.5 Agendamento de Análise	178
11.5.1 Definições de agendamento	178
11.5.2 Como Analisar	178
11.5.3 O que Analisar	178
11.6 Resumo dos Resultados da Análise	188
11.7 Detalhes dos Resultados da Análise	189
11.7.1 Separador Resumo dos Resultados	189
11.7.2 Separador Infecções	189
11.7.3 Separador Spyware	189
11.7.4 Separador Avisos	189
11.7.5 Separador Rootkits	189
11.7.6 Separador Informações	189
11.8 Quarentena de Vírus	197
12. Actualizações do AVG	199
12.1 Níveis de Actualização	199
12.2 Tipos de Actualização	199
12.3 Processo de Actualização	199



13. Histórico de Eventos	201
14. FAQ e Suporte Técnico	203



1. Introdução

Este manual do utilizador disponibiliza informação completa para o **AVG Internet Security 2011**.

Parabéns pela sua aquisição do AVG Internet Security 2011!

O **AVG Internet Security 2011** é um entre um leque de premiados produtos AVG desenvolvidos para lhe proporcionar descanso e segurança absoluta para o seu PC. Como todos os produtos AVG, o **AVG Internet Security 2011** foi completamente redesenhado, de raiz, para proporcionar a renomeada e acreditada protecção de segurança de uma forma nova, mais fácil de utilizar e mais eficiente. O seu novo produto **AVG Internet Security 2011** tem uma interface fácil de utilizar combinada com análises mais agressivas e mais rápidas. Foram automatizadas mais funcionalidades de segurança para a sua conveniência, e foram incluídas novas e inteligentes opções de utilizador para que possa adequar as nossas funcionalidades de segurança ao seu estilo de vida. Sem mais utilizações comprometedoras para a sua segurança!

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

Todos os produtos AVG oferecem

- Protecção que é relevante para a forma como utiliza o computador e a Internet: banca e compras on-line, navegação e pesquisas, conversação e e-mails, ou transferência de ficheiros e utilização das redes sociais - a AVG tem um produto de protecção adequado para si
- Protecção despreocupada que é da confiança de mais de 110 milhões de pessoas em todo o mundo e potenciada por uma rede global de investigadores altamente experientes
- Protecção que é apoiada por uma equipa de suporte profissional contínuo



2. Requisitos de Instalação do AVG

2.1. Sistemas Operativos Suportados

O **AVG Internet Security 2011** 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 2011 mas sem o componente PID.

2.2. Requisitos Mínimos e Recomendados de Hardware

Requisitos mínimos de hardware para o **AVG Internet Security 2011**:

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

Requisitos recomendados de hardware para o **AVG Internet Security 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB de memória RAM
- 1400 MB de espaço livre no disco rígido (para propósitos de instalação)



3. Opções de Instalação do AVG

O AVG pode ser instalado a partir do ficheiro de instalação disponível no CD de instalação, ou pode transferir o ficheiro de instalação mais recente a partir do website da AVG (<http://www.avg.com/>).

Antes de iniciar a instalação do AVG, recomenda-se vivamente que visite o website da AVG (<http://www.avg.com/>) para verificar a existência de um novo ficheiro de instalação. Desta forma tem a certeza de que instala a mais recente versão disponível do AVG Internet Security 2011.

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



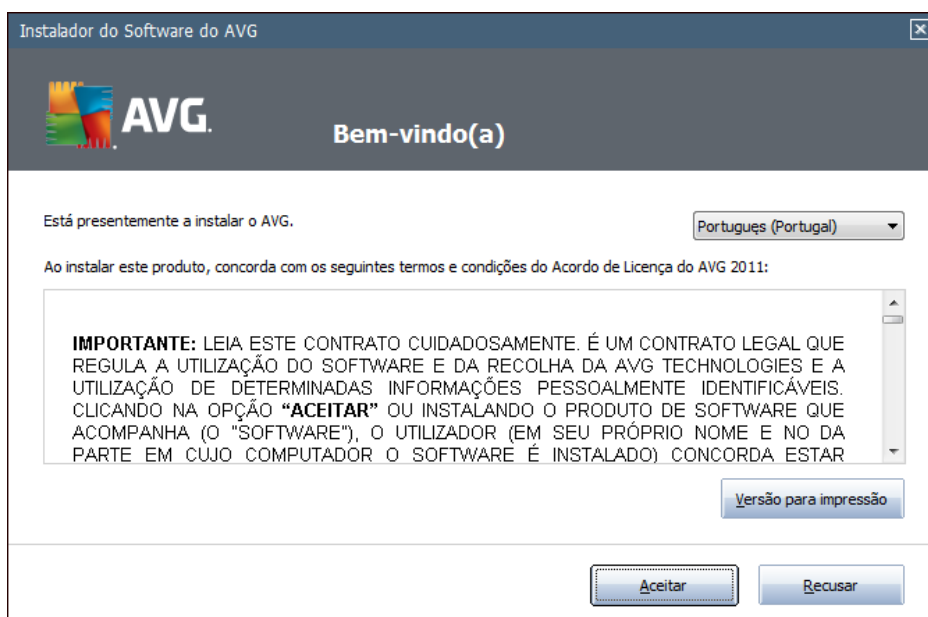
4. Processo de Instalação do AVG

Para instalar o **AVG Internet Security 2011** no seu computador, precisa de transferir o ficheiro de instalação mais recente. Pode utilizar o ficheiro de instalação a partir do CD facultado na caixa da sua edição, mas este ficheiro pode estar desactualizado. Como tal, recomendamos que obtenha o ficheiro de instalação mais recente ficheiro on-line. Pode transferir o ficheiro a partir do website da AVG (<http://www.avg.com/>), na secção [Centro de Suporte / Transferências](#).

A instalação é uma sequência de janelas com uma breve descrição do que deve fazer em cada passo. De seguida facultamos uma explicação para cada janela:

4.1. Bem-vindo

O processo de instalação inicia com a janela **Bem-vindo**. Aqui pode seleccionar o idioma usado para o processo de instalação e o idioma predefinido da interface do utilizador do AVG. Na secção superior da janela encontra um menu de opções com uma lista dos idiomas que pode escolher:



Atenção: Aqui, está a escolher o idioma para o processo de instalação. O idioma que seleccionar será instalado como idioma predefinido da interface do utilizador do AVG, juntamente com o idioma Inglês que é instalado automaticamente. Se quiser instalar idiomas adicionais para a interface do utilizador, defina-os na janela de configuração [Opções Personalizadas](#).

Além disso, esta janela faculta o texto integral do acordo de licença do AVG. Leia-o atentamente. 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.



4.2. Activar a sua licença do AVG

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

O número de venda pode ser encontrado na caixa do CD do seu **AVG Internet Security 2011**. O número de licença estará na mensagem de e-mail de confirmação que recebeu após comprar o seu **AVG Internet Security 2011** 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.

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

4.3. Seleccione o tipo de instalação



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

Para a maioria dos utilizadores, é recomendável a **Instalação Rápida** padrão, que instala o AVG em modo totalmente automático com as definições predefinidas pelo fornecedor do programa. Esta configuração proporciona a segurança máxima combinada com uma utilização de recursos otimizada. Futuramente, se houver necessidade de alterar a configuração, tem sempre a possibilidade de o fazer directamente na aplicação AVG. Se optar pela **Instalação Rápida**, prima o botão **Seguinte** para continuar para a janela seguinte: [Instalar a Barra de Ferramentas de Segurança AVG](#).

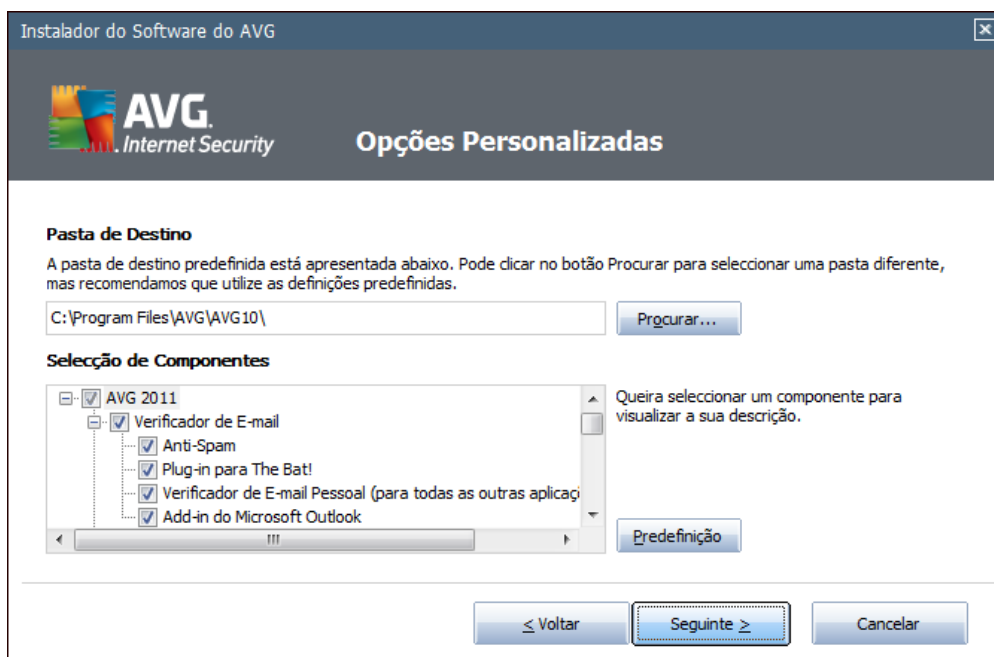
A **Instalação Personalizada** só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o AVG com definições que não as padrão; ex. para corresponder a requisitos do sistema específicos. Depois de seleccionar esta opção, prima o botão **Seguinte** para prosseguir para a janela [Opções Personalizadas](#).

Na parte direita da janela pode encontrar a caixa associada ao [Gadget do AVG](#) (suportado no Windows Vista/Windows 7). Se quiser instalar o gadget, marque a caixa correspondente. O [Gadget do AVG](#) ficará então disponível na Barra Lateral do Windows, proporcionando acesso imediato às funcionalidades mais importantes do seu **AVG Internet Security 2011**, ou seja, [análises](#) e [actualizações](#).



4.4. Opções Personalizadas

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



Pasta de Destino

Na secção **Pasta de Destino** da janela deverá especificar a localização onde o **AVG Internet Security 2011** deverá ser instalado. O AVG será instalado por predefinição na pasta de ficheiros de programas localizada na unidade C:. Se quiser alterar esta localização, utilize o botão **Procurar** para visualizar a estrutura da unidade, e seleccione a respectiva pasta.

Seleção de Componentes

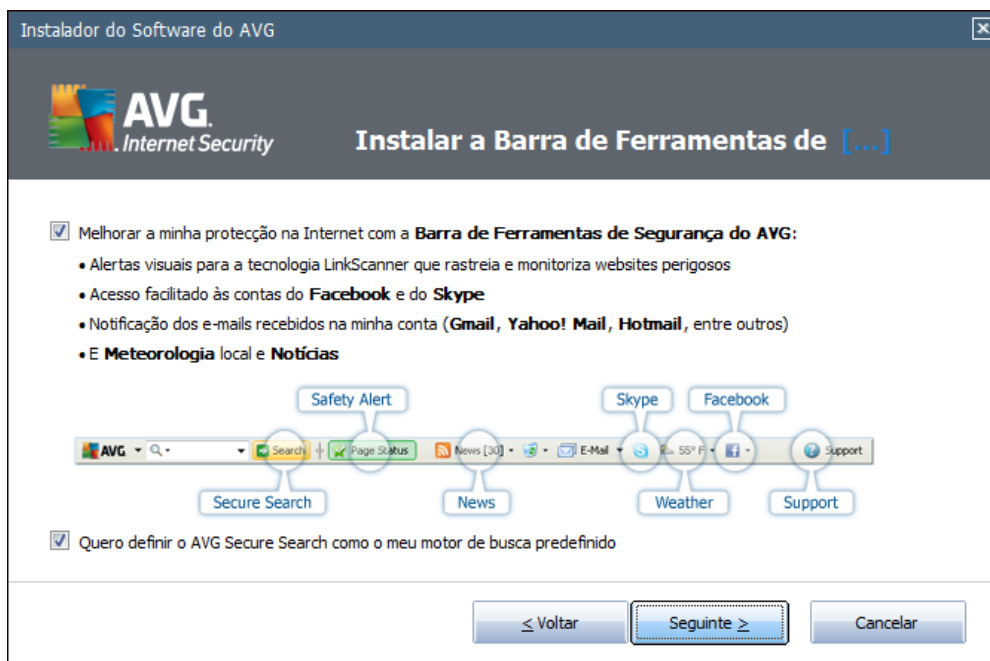
A secção **Seleção de Componentes** apresenta uma síntese de todos os componentes do **AVG Internet Security 2011** que podem ser instalados. Se as definições predefinidas não forem da sua conveniência, pode remover/adicionar componentes específicos.

No entanto, só pode seleccionar entre os componentes que estão incluídos na edição do AVG que adquiriu!

Realce qualquer um dos itens na lista **Seleção 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**.

Clique no botão **Seguinte** para continuar.

4.5. 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.



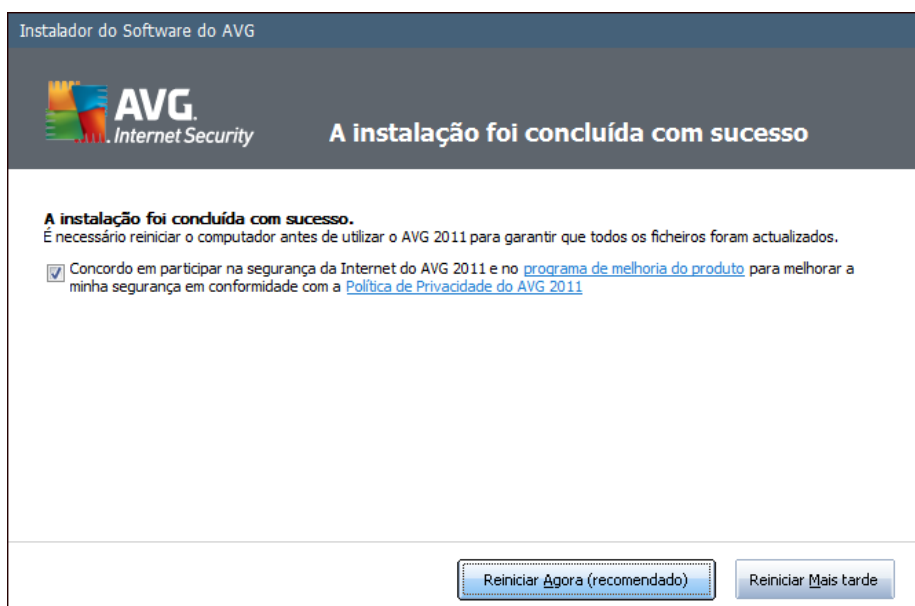
4.6. Progresso da instalação

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 automaticamente redireccionado para a janela seguinte.

4.7. A instalação foi concluída com sucesso





A janela **A instalação foi concluída com sucesso** confirma que o seu **AVG Internet Security 2011** foi totalmente instalado e configurado.

Nesta janela, queira providenciar as suas informações de contacto para que possa receber todas as informações e notícias relativas ao produto. Abaixo do formulário de registo, encontra as duas opções seguintes:

- **Sim, mantenham-me informado sobre actualizações de segurança e ofertas especiais do AVG 2011 por e-mail** - marque a caixa para declarar que pretende ser informado sobre as novidades na esfera da segurança na Internet e que pretende receber informações sobre ofertas especiais relativas a produtos AVG, melhorias e actualizações, etc.
- **Concordo em participar no Programa de Melhoria do Produto e Segurança na Internet do AVG 2011...** - marque esta caixa para manifestar o seu anuimento em 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 ameaças detectadas de forma a aumentar o nível geral de segurança na Internet.

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**.

Nota: Se estiver a usar uma licença comercial do AVG, e caso tenha seleccionado o item *Administração Remota para instalação* (consulte [Opções Personalizadas](#)), a janela *A instalação foi concluída com sucesso* será apresentada com a seguinte interface:

*É preciso especificar os parâmetros do Centro de Dados AVG - providencie a cadeia de caracteres de ligação do Centro de Dados AVG no formato servidor:porta. Se não dispuser destas informações de momento, deixe o campo em branco e poderá definir a configuração posteriormente na janela **Definições Avançadas / Administração Remota**. Para informações detalhadas sobre a Administração Remota AVG, queira consultar o manual do utilizador do AVG Business Edition, que pode ser transferido a partir do Website da AVG (<http://www.avg.com/>).*



5. Após a Instalação

5.1. Registo do produto

Estando terminada a instalação do **AVG Internet Security 2011**, por favor registe o seu produto on-line no website da AVG (<http://www.avg.com/>), **Página de registo** (siga as instruções facultadas directamente na página). 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.

5.2. Aceder à Interface do Utilizador

A [Interface do Utilizador do AVG](#) pode ser acedida de várias 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
- fazendo duplo clique sobre a linha de estado localizada na secção inferior do [gadget do AVG \(se instalado; suportado pelo Windows Vista/ Windows 7\)](#)
- a partir do menu **Iniciar/Todos os Programas/AVG 2011/Interface do Utilizador do AVG**
- A partir da [Barra de Ferramentas de Segurança AVG](#) através da opção **Iniciar o AVG**

5.3. 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 2011**. Por este motivo deve executar uma análise [Analisar todo o computador](#) para se certificar de que não existem infecções no seu PC.

Para instruções relativas à execução de [Analisar todo o computador](#) por favor consulte o capítulo [Análise do AVG](#).

5.4. Teste Eicar

Para confirmar que o **AVG Internet Security 2011** 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** guardá-lo no disco local. Imediatamente após a confirmação da transferência do ficheiro de teste, a [Protecção On-line](#) 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 'vírus' 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** 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!**

5.5. Configuração predefinida do AVG

A configuração predefinida (ou seja, a forma como a aplicação está configurada imediatamente após a instalação) do **AVG Internet Security 2011** está configurada pelo fornecedor do software de forma a que todos os componentes e funções estejam afinados para proporcionarem um desempenho excelente.

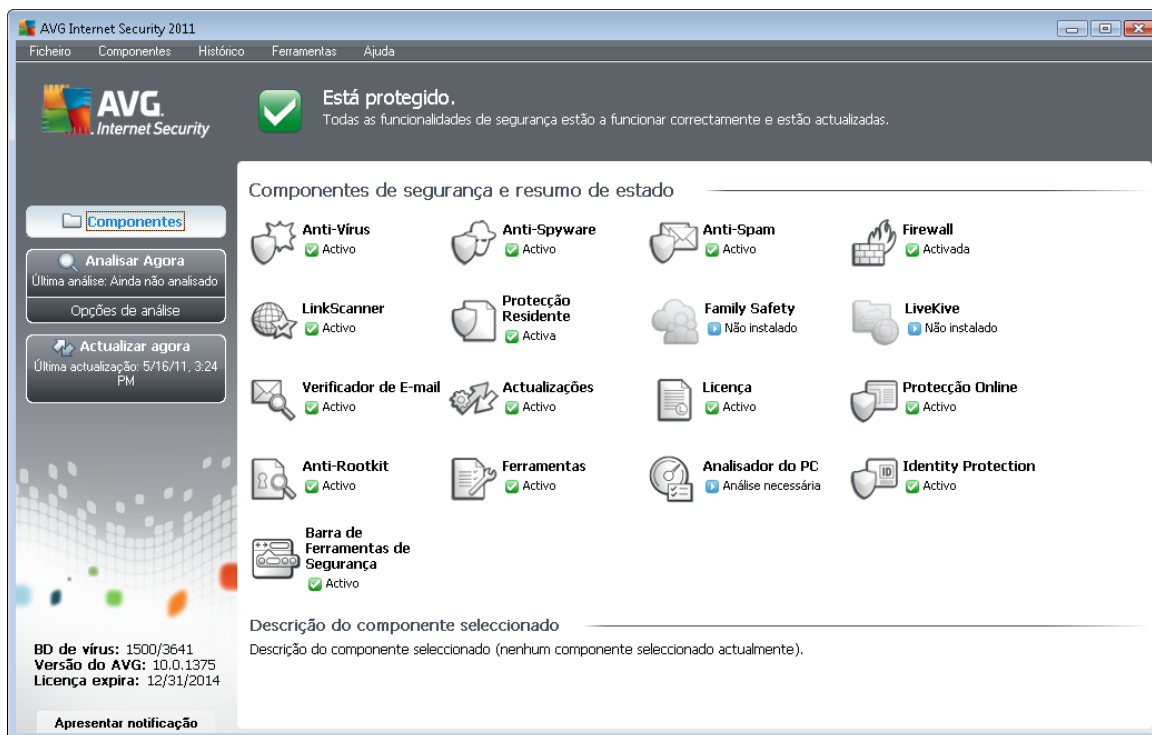
Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente por um utilizador avançado.

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.



6. Interface de Utilizador AVG

O AVG Internet Security 2011 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 - [detalhes >>](#)
- **Informação de Estado de Segurança** (secção superior da janela) faculta-lhe informação relativa ao estado actual do seu programa AVG - [detalhes >>](#)
- **Links rápidos** (secção esquerda da janela) permite-lhe aceder rapidamente às tarefas mais importantes e utilizadas mais frequentemente do AVG - [detalhes >>](#)
- **Síntese de Componentes** (secção central da janela) faculta uma síntese de todos os componentes instalados do AVG - [detalhes >>](#)
- **Estatísticas** (secção inferior esquerda da janela) fornece-lhe todos os dados estatísticos relativos ao funcionamento do programa - [detalhes >>](#)
- **Ícone da Barra de Notificação do Sistema** (canto inferior direito do monitor, na barra de notificação do sistema) indica o estado actual do AVG - [detalhes >>](#)
- **O Gadget do AVG** (barra lateral do Windows, suportado no Windows Vista/7) permite-lhe aceder rapidamente às análises e actualizações do AVG - [detalhes >>](#)



6.1. Menu de Sistema

O **menu de sistema** é a navegação padrão utilizada em todas as aplicações do Windows. Está localizado na parte superior da janela principal do **AVG Internet Security 2011**. 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:

6.1.1. Ficheiro

- **Sair** - fecha a interface do utilizador do **AVG Internet Security 2011**. No entanto, a aplicação AVG continuará a ser executada em segundo plano e o seu computador continuará protegido!

6.1.2. 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** assegura que o seu computador está protegido contra vírus que tentam aceder ao seu computador - [detalhes >>](#)
- **Anti-Spyware** assegura que o seu computador está protegido contra spyware e adware - [detalhes >>](#)
- **Anti-Spam** verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. - [detalhes >>](#)
- **Firewall** Controla a forma como é efectuada a comunicação de dados entre o seu computador e outros computadores da Internet ou da rede local - [detalhes >>](#)
- **Link Scanner** analisa os resultados de busca apresentados no seu browser - [detalhes >>](#)
- **Verificador de E-mail** verifica todo o e-mail a receber e a enviar pela existência de vírus - [detalhes >>](#)
- **Family Safety** ajuda-o a monitorizar as actividades on-line dos seus filhos e a protegê-las contra conteúdos inapropriados - [detalhes >>](#)
- **LiveKive** efectua cópias de segurança automáticas dos seus dados on-line - [detalhes >>](#)
- **Protecção Residente** é executada em segundo plano e analisa ficheiros à medida que estes são copiados, abertos ou guardados - [detalhes >>](#)
- **Actualizações** controla todas as actualizações do AVG - [detalhes >>](#)
- **Licença** apresenta o número, tipo e data de expiração da licença - [detalhes >>](#)



- **Protecção On-line** analisa todos os dados transferidos por um browser - [detalhes >>](#)
- **Anti-Rootkit** detecta programas e tecnologias que tentam camuflar malware - [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** - componente anti-malware que se destina a evitar que ladrões de identidade roubem os seus valores digitais pessoais - [detalhes >>](#)
- **Barra de Ferramentas de Segurança** permite-lhe usar funcionalidades seleccionadas do AVG directamente a partir do seu Browser - [detalhes >>](#)
- **A Administração Remota** só é apresentada nas edições AVG Business caso tenha especificado durante o [processo de instalação](#) a instalação deste componente

6.1.3. Histórico

- **Resultados da análise** - muda para a interface de teste do AVG, mais especificamente para a janela [Síntese de Resultados de Análise](#)
- **Deteção da Protecção Residente** - abre uma janela com a síntese das ameaças detectadas pela [Protecção Residente](#)
- **Deteção do Verificador de E-mail** - abre a janela com a síntese dos anexos das mensagens de e-mail identificados como perigosos pelo componente [Verificador de E-mail](#)
- **Deteção da Protecção On-line** - abre uma janela com a síntese das ameaças detectadas pela [Protecção Online](#)
- **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 2011** registadas
- **Firewall** - abre a interface das definições da Firewall no separador [Registos](#) com uma síntese detalhada de todas as acções da Firewall

6.1.4. Ferramentas

- **Análise do computador** - muda para a [Interface de análise do AVG](#) e 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 uma análise manual a um único ficheiro seleccionado a partir da estrutura em árvore do seu disco.
- **Actualizar** - inicia automaticamente o processo de actualização do **AVG Internet Security 2011**.
- **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 2011** . 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** .

6.1.5. Ajuda

- **Conteúdos**- abre os ficheiros de ajuda do AVG
- **Obter Ajuda On-line** - abre o website da AVG (<http://www.avg.com/>) na página do centro de apoio ao cliente
- **Web do 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 (*o número 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 2011**, os dois últimos itens aparecem como **Comprar agora** e **Activar**, permitindo-lhe comprar a versão completa do programa imediatamente. Para produtos **AVG Internet Security 2011** instalados com um número de venda, os itens são apresentados como **Registar** e **Activar**. Para mais informações, queira consultar a secção **Licença** desta documentação.

- **Acerca do AVG** - abre a janela **Informações** com cinco separadores que facultam dados



sobre o nome do programa, versão do programa e da base de dados de vírus, informação de sistema, acordo de licenciamento e informações de contacto da **AVG Technologies CZ**.

6.2. Informação de Estado de Segurança

A secção **Informação de Estado de Segurança** está localizada na parte superior da janela principal do AVG. Nesta secção encontra sempre informações relativas ao estado de segurança actual do seu **AVG Internet Security 2011**. Por favor veja uma síntese dos ícones possivelmente apresentados, e a respectiva descrição:



- O ícone verde indica que o seu AVG está perfeitamente funcional. O computador está totalmente protegido, actualizado e todos os componentes instalados estão a funcionar correctamente.



- O ícone laranja 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 e provavelmente decidiu desactivar algum componente por alguma razão. Ainda está protegido pelo AVG. No entanto, por favor preste atenção às definições do componente problemático! O nome do mesmo será facultado na secção **Informação de Estado de Segurança**.

Este ícone 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 a partir do menu de contexto aberto com um clique direito do rato sobre o ícone do componente respectivo na síntese de componentes da janela principal do AVG). Pode ter de usar esta opção numa situação específica mas é especialmente recomendado desactivar a opção "**Ignorar estado do componente**" assim que possível.



- O ícone vermelho indica que o AVG está em estado crítico! Um ou mais componentes não estão a funcionar devidamente e o AVG não consegue proteger o seu 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 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 para um desempenho optimizado e obter o nível máximo de segurança!

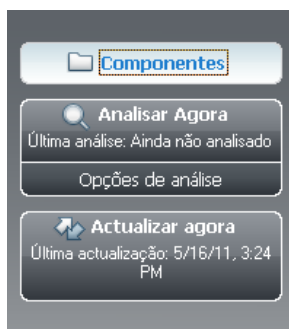
É recomendável que preste atenção à Informação de Estado de Segurança e que na eventualidade do relatório indicar algum problema, tente resolvê-lo imediatamente. Caso contrário, o seu computador está em risco!

Nota: A informação de estado do AVG também pode ser obtida a qualquer momento a partir do [ícone da barra de notificação](#).



6.3. Links Rápidos

Links rápidos (na secção à esquerda da [Interface do utilizador do AVG](#)) permite-lhe aceder imediatamente às características mais importantes e mais frequentemente utilizadas do AVG:



- **Componentes** - utilize este link para alternar entre a interface do AVG actualmente aberta para a interface padrão com uma síntese de todos os componentes instalados - consulte o capítulo [Síntese de Componentes >>](#)
- **Analisar agora** - por predefinição, o botão disponibiliza informações (*tipo de análise, data da última execução*) da última análise executada. Pode executar o comando **Analisar agora** para iniciar a mesma análise novamente, ou seguir o link **Opções de análise** para abrir a interface de análise do AVG onde pode executar análises ou editar os parâmetros das mesmas - consulte o capítulo [Análise do AVG>>](#)
- **Actualizar agora** - o link disponibiliza a data da última execução do processo de actualização. Prima o botão para abrir a interface de actualização e executar o processo de actualização do AVG imediatamente - consulte o capítulo [Actualizações do AVG>>](#)

Estes links estão constantemente acessíveis a partir da interface do utilizador. Quando utilizar um link específico para executar um processo específico, o GUI alternará para uma nova janela mas os links rápidos continuarão disponíveis. Além disso, o processo em execução é representado graficamente.

6.4. Síntese de Componentes

A secção **Síntese de Componentes** está localizada na parte central da [Interface do Utilizador do AVG](#). A secção está dividida em duas partes:

- Síntese de todos os componentes instalados que consiste em um painel com o ícone dos componentes e a informação se o respectivo componente está activo ou inactivo
- Descrição de um componente seleccionado

No **AVG Internet Security 2011**, a secção **Síntese de Componentes** contém informações sobre os seguintes componentes:

- **Anti-Vírus** assegura que o seu computador está protegido contra vírus que tentam aceder ao seu computador - [detalhes >>](#)



- **Anti-Spyware** assegura que o seu computador está protegido contra spyware e adware - [detalhes >>](#)
- **Anti-Spam** verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. - [detalhes >>](#)
- **Firewall** Controla a forma como é efectuada a comunicação de dados entre o seu computador e outros computadores da Internet ou da rede local - [detalhes >>](#)
- **Link Scanner** analisa os resultados de busca apresentados no seu browser - [detalhes >>](#)
- **Verificador de E-mail** verifica todo o e-mail a receber e a enviar pela existência de vírus - [detalhes >>](#)
- **Protecção Residente** é executada em segundo plano e analisa ficheiros à medida que estes são copiados, abertos ou guardados - [detalhes >>](#)
- **Family Safety** ajuda-o a monitorizar as actividades on-line dos seus filhos e a protegê-las contra conteúdos inapropriados - [detalhes >>](#)
- **LiveKive** efectua cópias de segurança automáticas dos seus dados on-line - [detalhes >>](#)
- **Actualizações** controla todas as actualizações do AVG - [detalhes >>](#)
- **Licença** apresenta o número, tipo e data de expiração da licença - [detalhes >>](#)
- **Protecção On-line** analisa todos os dados transferidos por um browser - [detalhes >>](#)
- **Anti-Rootkit** detecta programas e tecnologias que tentam camuflar malware - [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** - componente anti-malware que se destina a evitar que ladrões de identidade roubem os seus valores digitais pessoais - [detalhes >>](#)
- **Barra de Ferramentas de Segurança** permite-lhe usar funcionalidades seleccionadas do AVG directamente a partir do seu Browser - [detalhes >>](#)
- **A Administração Remota** só é apresentada nas edições AVG Business caso tenha especificado durante o [processo de instalação](#) a instalação deste componente

Clique uma vez no ícone de qualquer componente para o realçar na síntese de componentes. É apresentada simultaneamente uma descrição da funcionalidade básica do componente na parte inferior da interface do utilizador. Clique duas vezes no ícone 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 o menu de contexto: além de abrir a interface gráfica do componente também pode seleccionar **Ignorar o estado do componente**. Selecciona 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 notificação](#).

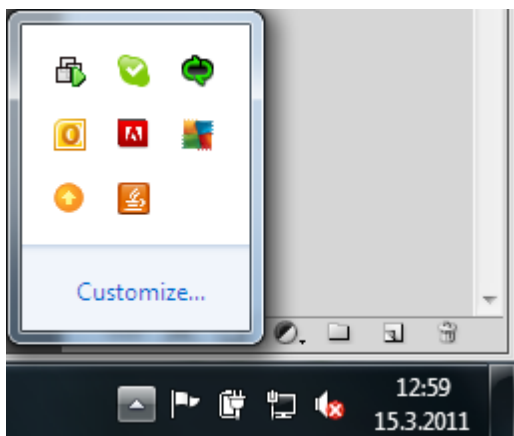
6.5. Estatísticas

A secção **Estatísticas** está localizada na parte inferior esquerda da [Interface do Utilizador do AVG](#). Faculta uma lista de informações relativas ao funcionamento do programa:

- **BD de vírus** - informa-o acerca da versão da base de dados de vírus actualmente instalada
- **Versão do AVG** - informa-o acerca da versão do AVG instalada(o número está no formato de 10.0.xxxx, em que 10.0 é a versão da linha do produto, e xxxx representa o número de compilação)
- **A licença expira** - faculta a data de expiração da licença do seu AVG

6.6. Ícone da barra de tarefas

Ícone da Barra de Notificação (na barra de tarefas do Windows) indica o estado actual do seu **AVG Internet Security 2011**. É visível constantemente na sua barra de notificação, independentemente de a janela principal do AVG estar aberta ou fechada:



Se apresentar a cor preenchida , o **Ícone da Barra de Notificação** indica que todos os componentes do AVG estão activos e perfeitamente funcionais. Além disso, o ícone da barra de notificação do AVG pode ser apresentado em cor cheia se o AVG tiver um estado de erro mas o utilizador tiver plena consciência e tiver decidido deliberadamente [ignorar o estado do componente](#). Um ícone com um ponto de exclamação  indica um problema (*componente inactivo, estado de erro, etc.*). Clique duas vezes no **Ícone da Barra de Notificação** para abrir a janela principal e editar um componente.

O ícone da barra de notificação informa-o ainda de actividades actuais do AVG e possíveis alterações de estado no programa (ex. *execução automática de uma análise agendada ou uma actualização, 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 notificação do AVG:



O **Ícone da Barra de Notificação** também pode ser utilizado como link rápido para aceder à janela principal do AVG a qualquer momento - duplo clique sobre o ícone. Ao clicar com o botão direito do rato sobre o **Ícone da Barra de Notificação** 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](#)
- **Análises** - clique para abrir o menu de contexto do
- **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](#)
- **Executar o Analisador do PC** - clique para executar o componente [Analisador do PC](#)
- **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*.
- **Actualizar agora** - inicia imediatamente uma [actualização](#)
- **Ajuda** - abre o ficheiro de ajuda na página inicial

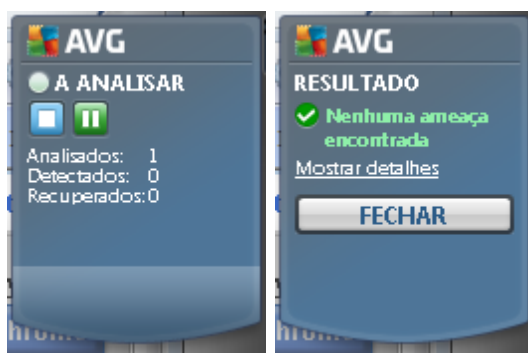
6.7. Gadget do AVG

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 2011**, ou seja, [análises](#) e [actualizações](#):

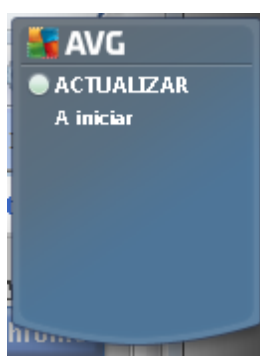


O **Gadget do AVG** disponibiliza as seguintes opções de acesso rápido:

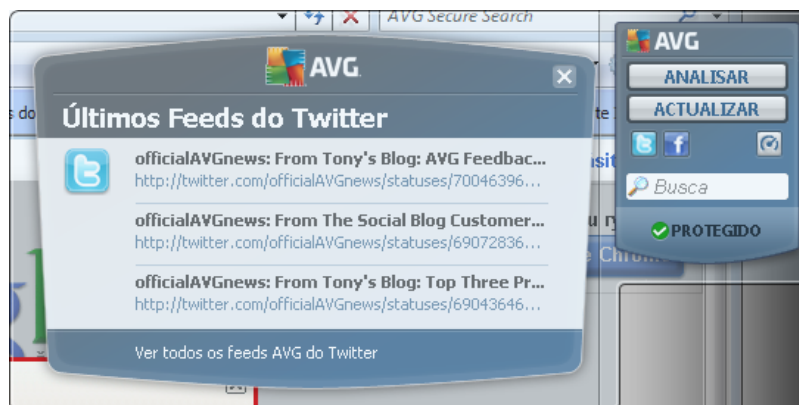
- **Analisar agora** - clique no link **Analisar agora** para iniciar a [análise de todo o computador](#) directamente. Pode consultar o progresso do processo de análise na interface alternada do utilizador no gadget. Um breve resumo das estatísticas apresenta informações sobre o número de objectos analisados, 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 AVG directamente a partir do gadget:



- **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, conquanto tenha instalado o AVG com recurso a uma das licenças da edição **AVG Business Editions**), e este abrir o seu browser no website da **AVG SMB Community** na rede social LinkedIn
- **Analizador do PC**  - abre a interface do utilizador no componente [Analizador do PC](#)
- **Caixa de pesquisa** - digite uma palavra-chave e obtenha os resultados imediatamente numa nova janela do seu browser predefinido.



7. Componentes do AVG

7.1. Anti-Vírus

7.1.1. Princípios de Anti-Vírus

O componente de análise do software anti-vírus analisa todos os ficheiros e actividades de ficheiros (abrir/fechar ficheiros, etc.) pela existência de vírus conhecidos. Quaisquer vírus detectados serão impedidos de tomarem qualquer acção e serão eliminados ou colocados em quarentena. 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.

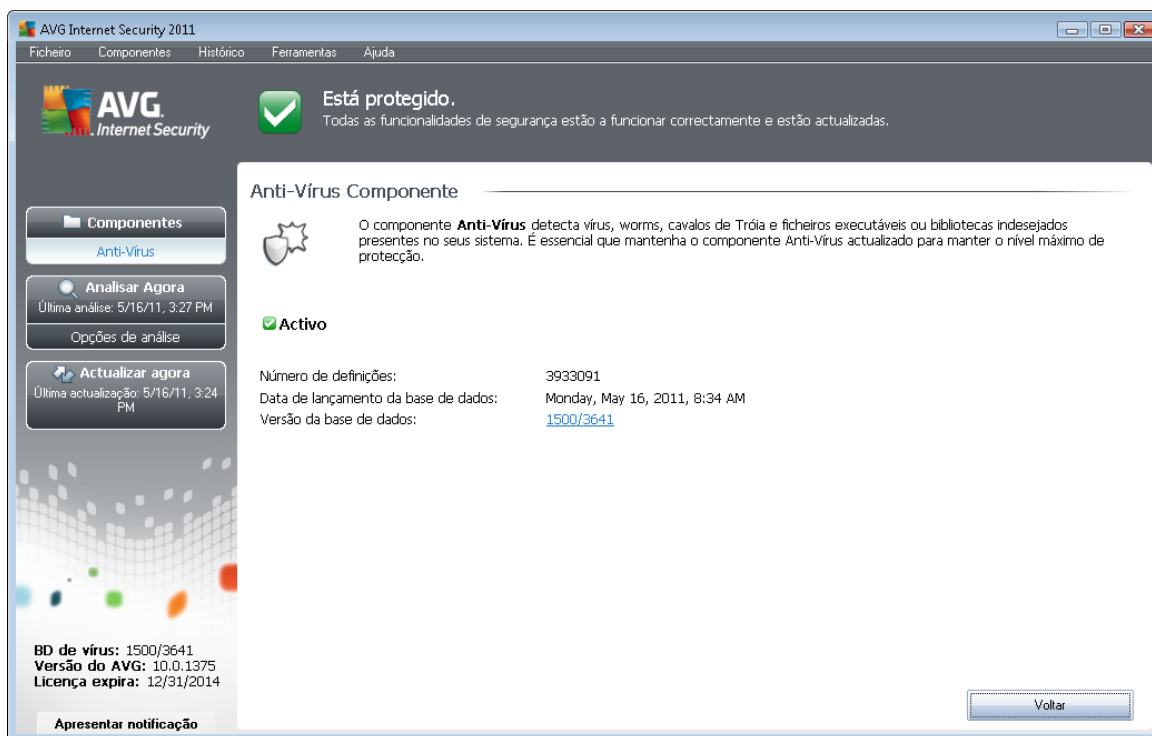
A característica mais importante da protecção anti-vírus é que nenhum vírus conhecido pode ser executado no computador!

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:

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

O AVG possui ainda 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 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.

7.1.2. Interface do Anti-vírus



O interface do componente **Anti-Vírus** faculta alguma informação básica relativa à funcionalidade do componente, informação acerca do estado actual do componente (*O componente Anti-Vírus está activo.*) e uma sucinta síntese de estatísticas relativas ao **Anti-vírus**:

- **Número de definições** - o número faculta a contagem de definições de vírus na versão actualizada da base de dados de vírus
- **Lançamento da base de dados** - especifica quando e a que horas a base de dados de vírus foi actualizada
- **Versão da base de dados** - define o número da versão mais recente base de dados de vírus e este número aumenta com cada actualização da base de dados de vírus

Existe apenas um botão disponível na interface deste componente (**Retroceder**) - prima o botão para retroceder para a [Interface do utilizador do AVG padrão](#) (*síntese dos componentes*).

7.2. Anti-Spyware

7.2.1. Princípios de Anti-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,

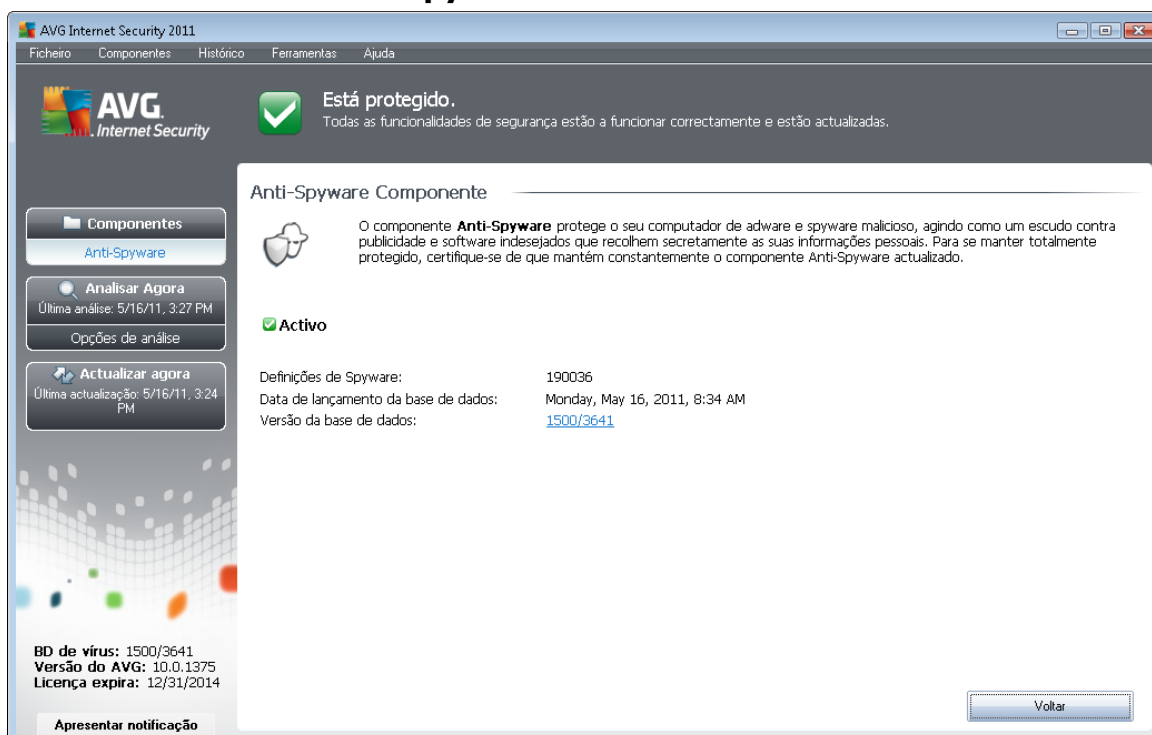


incluem anúncios, janelas de pop-up ou outros tipos de software desagradável.

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.

Existe igualmente o risco potencial de ter sido transmitido malware ao computador antes da instalação do AVG, ou que tenha negligenciado as actualizações do **AVG Internet Security 2011** com as [bases de dados e actualizações do programa](#) mais recentes. Por este motivo, o AVG permite a verificação completa da existência de malware/spyware no computador, através da funcionalidade de análise. Detecta também malware latente e inactivo, isto é, malware que foi transferido mas ainda não foi activado.

7.2.2. Interface do Anti-Spyware



A interface do componente **Anti-Spyware** faculta uma sucinta síntese da funcionalidade do componente, informações acerca do estado actual do componente e algumas estatísticas do **Anti-Spyware**.

- **Definições de Spyware** - o número faculta a contagem das amostras de spyware definidas na última versão da base de dados de spyware
- **Lançamento da base de dados** - especifica quando e a que horas a base de dados de spyware foi actualizada
- **Versão da base de dados** - especifica o número da versão mais recente base de dados e



este número aumenta com cada actualização da base de dados de vírus

Existe apenas um botão disponível na interface deste componente (**Retroceder**) - prima o botão para retroceder para a [Interface do utilizador do AVG padrão \(síntese dos componentes\)](#).

7.3. Anti-Spam

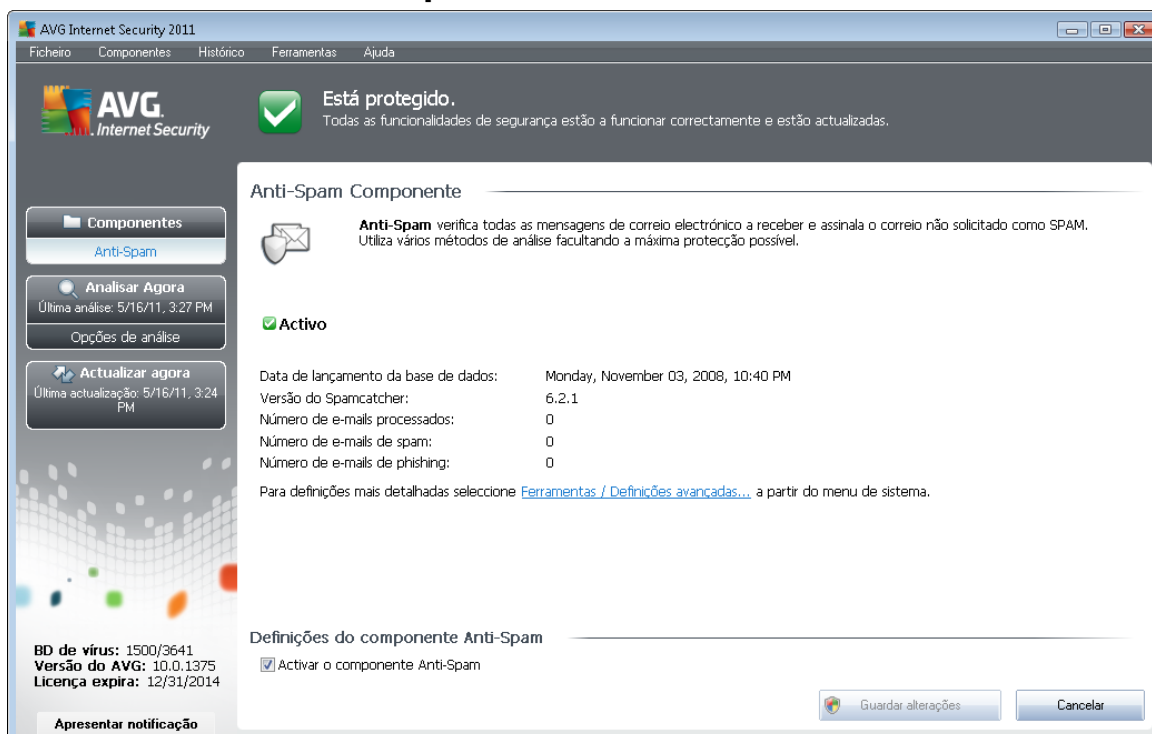
Spam refere-se a correio electrónico não solicitado, que normalmente publicita um produto ou serviço e que é enviado em massa para um grande número de endereços de e-mail sobrecarregando as caixas de correio dos destinatários. Spam não se refere a correio electrónico comercial legítimo, consentido pelos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

7.3.1. Princípios do Anti-Spam

O componente AVG Anti-Spam verifica todo e-mail a receber e assinala o e-mail solicitado como spam. O **AVG Anti-Spam** pode modificar o assunto do e-mail (que foi identificado como sendo spam) ao adicionar uma linha de texto especial. Depois poderá facilmente filtrar os seus e-mails no seu cliente de e-mail.

O componente AVG Anti-Spam utiliza vários métodos de análise para processar cada e-mail, oferecendo o máximo de protecção possível contra e-mail indesejado. O **AVG 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).

7.3.2. Interface do Anti-Spam





Na janela do componente **Anti-Spam** encontrará um sucinto texto com a descrição da funcionalidade do componente, informação acerca do seu estado actual e as seguintes estatísticas:

- **Data de lançamento da base de dados** - especifica quando e a que horas a base de dados foi actualizada e aplicada
- **Versão do Spamcatcher** - define o número da última versão do componente anti-spam
- **Número de e-mails processados** - especifica a quantidade de mensagens de e-mail que foram analisadas desde a última execução do componente anti-spam
- **Número de e-mails de spam** - entre todos os e-mails analisados, especifica quantas mensagens foram assinaladas como spam
- **Número de e-mails de phishing** - entre todos os e-mails analisados, especifica quantas mensagens foram consideradas tentativas de phishing

A janela **Anti-Spam** apresenta ainda o link [Ferramentas/Definições Avançadas](#). Use o link para aceder às configurações avançadas de todos os componentes do **AVG Internet Security 2011**.

Por favor tenha em atenção: 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.

Existe apenas um botão disponível na interface deste componente (**Retroceder**) - prima o botão para retroceder para a [Interface do utilizador do AVG](#) padrão (síntese dos componentes).

7.4. Firewall

Uma firewall é um sistema que implementa uma política de controlo de acesso entre duas ou mais redes, bloqueando/autorizando o tráfego. Cada 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 cada porta da 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.

Firewall protege a sua informação de identificação pessoal de ser enviada 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 de ataques desencadeados por utilizadores internos noutros computadores da rede.

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.

7.4.1. Princípios da Firewall

No AVG, o componente **Firewall** controla todo o tráfego em cada porta 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.

Nota: 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

7.4.2. 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 política 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 personalizados:**

- o **Ligado directamente à Internet** - adequado para computadores de secretária domésticos comuns ligados directamente à Internet ou portáteis que ligam à Internet fora da rede segura da empresa. Seleccione esta opção se se ligar à Internet a partir de casa, ou se estiver numa pequena rede empresarial sem controlo central. Além disso, seleccione esta opção aquando de viagens e ligação à Internet com o seu portátil em vários locais desconhecidos e potencialmente perigosos (*ciber-cafés, quarto de hotel, etc.*). Serão criadas regras mais restritivas uma vez que se parte do princípio que estes computadores não possuem protecção adicional e necessitam, como tal, do máximo de protecção.
- o **Computador num domínio** - adequado para computadores numa rede local, ex., escola ou rede empresarial. Parte-se do princípio que o computador está protegido por algumas medidas adicionais de maneira que o nível de segurança pode ser inferior que num computador independente.
- o **Pequena rede doméstica ou empresarial** - adequado para computadores em pequenas redes, ex., em casa ou numa pequena empresa. Normalmente, só alguns computadores ligados entre si, sem um administrador "central".

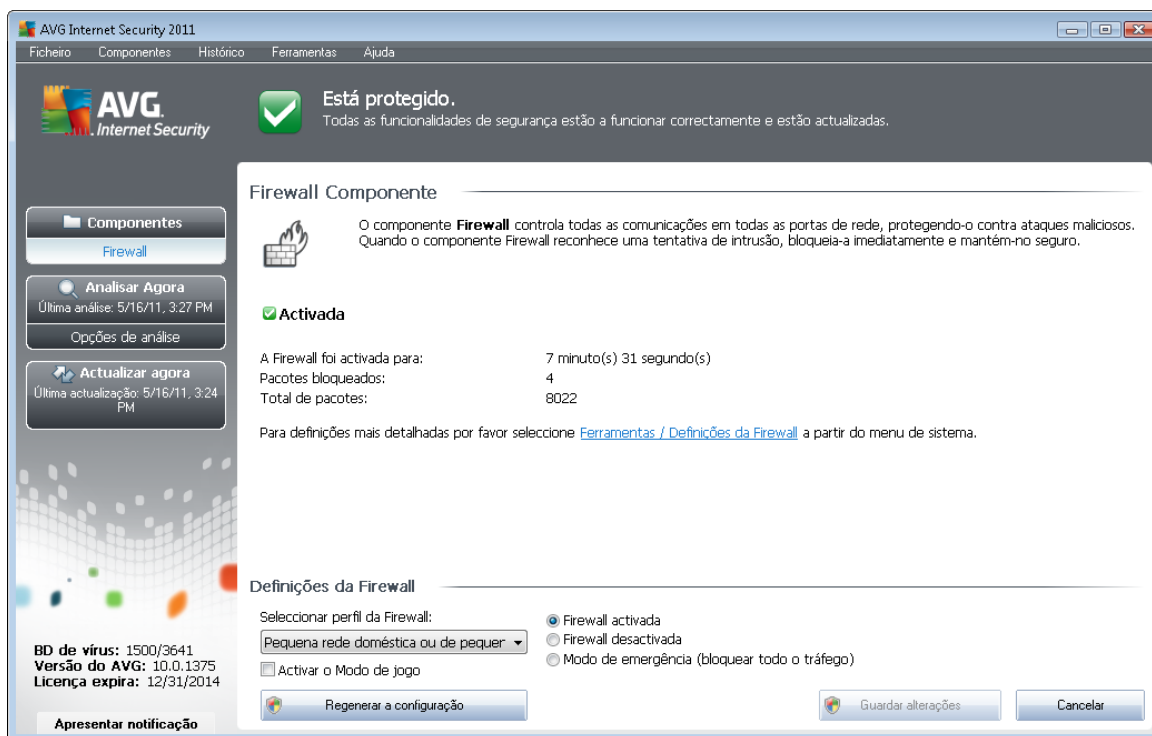
Mudança de perfil

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.

7.4.3. Interface da Firewall



A interface do componente **Firewall** faculta alguma informação básica acerca da funcionalidade do componente, o seu estado e uma breve síntese das estatísticas da **Firewall**:

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

Firewall definições

- **Selecione perfil de Firewall** - selecione um dos perfis definidos a partir do menu de opções - estão dois perfis constantemente disponíveis (os *perfis definidos apelidados Permitir tudo e Bloquear tudo*), foram adicionados outros perfis manualmente por edição de perfil na janela [Perfis](#) nas [Definições 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.

- **Estado da Firewall:**

- o **Firewall activada** - 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
- o **Firewall desactivada** - esta opção desactiva a [Firewall](#) por completo, todo o tráfego de rede é permitido mas não verificado!
- o **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

Por favor tenha em atenção: 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 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 [Interface do utilizador do AVG](#) padrão (síntese dos componentes)

7.5. Link Scanner

7.5.1. Princípios do 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.

A tecnologia do **LinkScanner** consiste em duas funcionalidades, o [Search-Shield](#) e o [Surf-Shield](#):

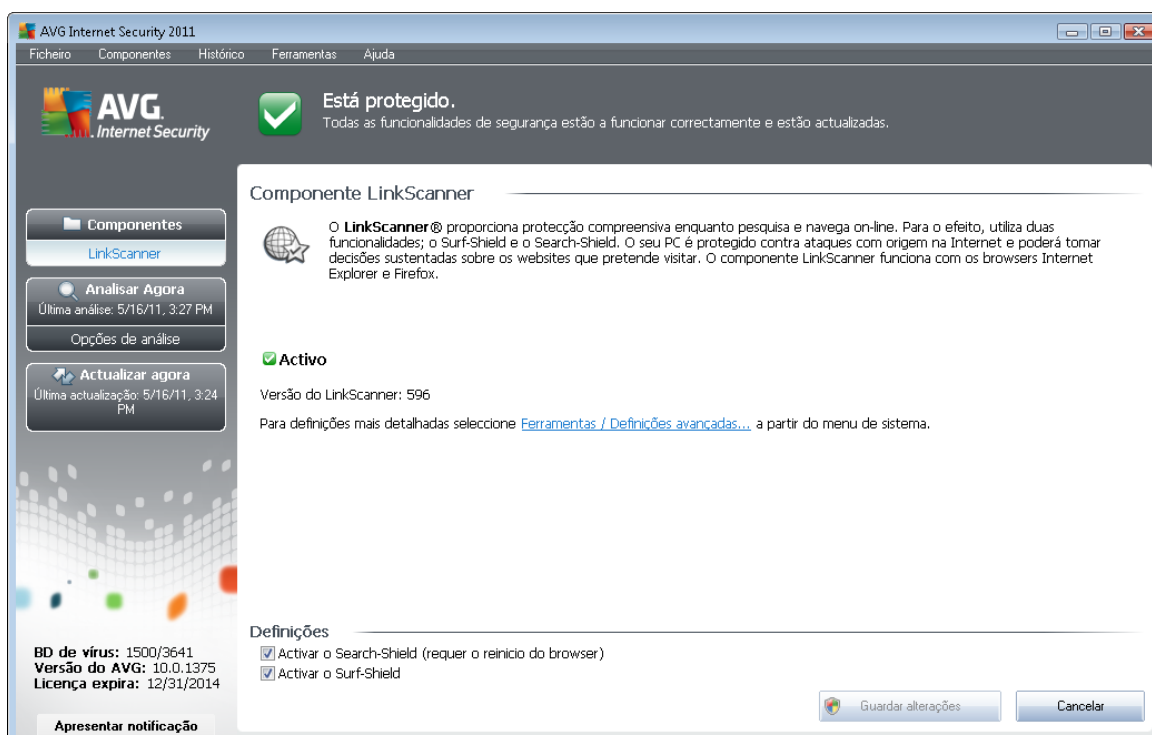


- **O Search-Shield** contém uma lista de websites (*endereços URL*) que são conhecidos como sendo perigosos. Ao pesquisar com o Google, Yahoo!, JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ou SlashDot, todos os resultados de pesquisa são verificados contra esta lista e é apresentado um veredicto (*para resultados de pesquisa do Yahoo! só são apresentados os ícones de veredicto "website infectado"*).
- **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.

Nota: O Link Scanner não se destina a plataformas de servidores!

7.5.2. Interface do Link Scanner

A interface do componente **LinkScanner** providencia uma breve descrição das funcionalidades do componente e informações relativas ao seu estado actual. Além disso, pode encontrar informações sobre o número da mais recente versão da base de dados do **LinkScanner** (Versão do | **Link Scanner**).



Definições do LinkScanner

Na parte inferior da janela pode editar várias opções:



- **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).

7.5.3. 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 **[AVG Link Scanner](#)** 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 do link é segura (este ícone não será apresentado para resultados de pesquisa Resultados de pesquisa do JP).

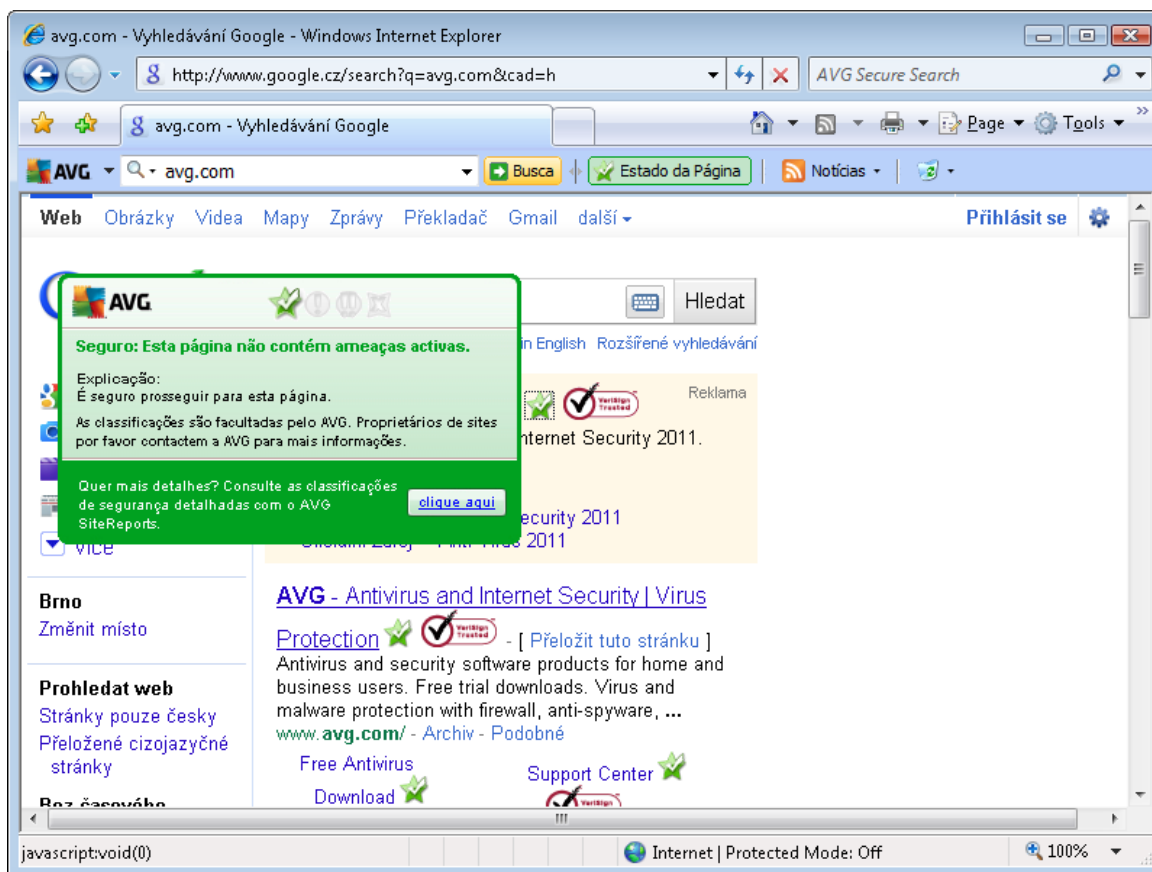
 A página de destino não contém ameaças mas é algo suspeita (*questionável em termos de origem ou motivo, como tal, não é recomendável para compras on-line, etc.*).

 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.

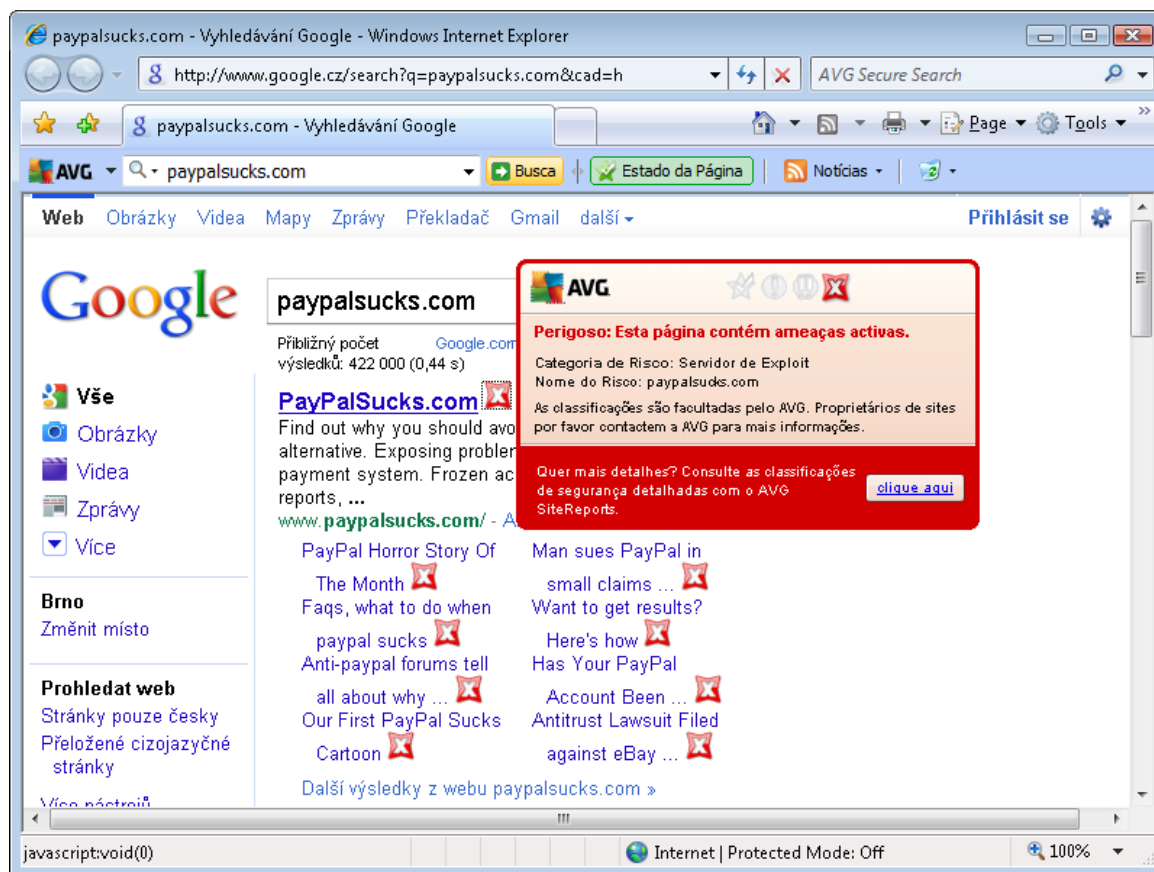
Colocar o cursor sobre um ícone de classificação individual apresentará detalhes acerca do link em questão. As informações incluem detalhes adicionais sobre a ameaça (se for o caso):



7.5.4. 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 [AVG Link Scanner](#) não permitirá que o seu browser a apresente.

Se se deparar com um website malicioso, o [AVG LinkScanner](#) avisa-o no seu browser por meio de uma janela semelhante a:



Aceder a esse website é extremamente perigoso e completamente desaconselhável!

7.6. Protecção Residente

7.6.1. Princípios da Protecção Residente

O componente **Protecção Residente** proporciona protecção permanente ao seu computador. Analisa todos os ficheiros que são abertos, guardados, ou copiados e protege as áreas de sistema do computador. Quando a **Protecção Residente** detecta um vírus num ficheiro acedido, interrompe a operação em curso, não permitindo a activação do vírus. Normalmente, o utilizador nem sequer se apercebe do processo, uma vez que este é executado em "segundo plano", e só é notificado quando são encontradas ameaças; em simultâneo a **Protecção Residente** bloqueia a activação da ameaça e remove-a. A **Protecção Residente** é carregada na memória do seu computador durante o arranque do sistema.

O que a Protecção Residente pode fazer:

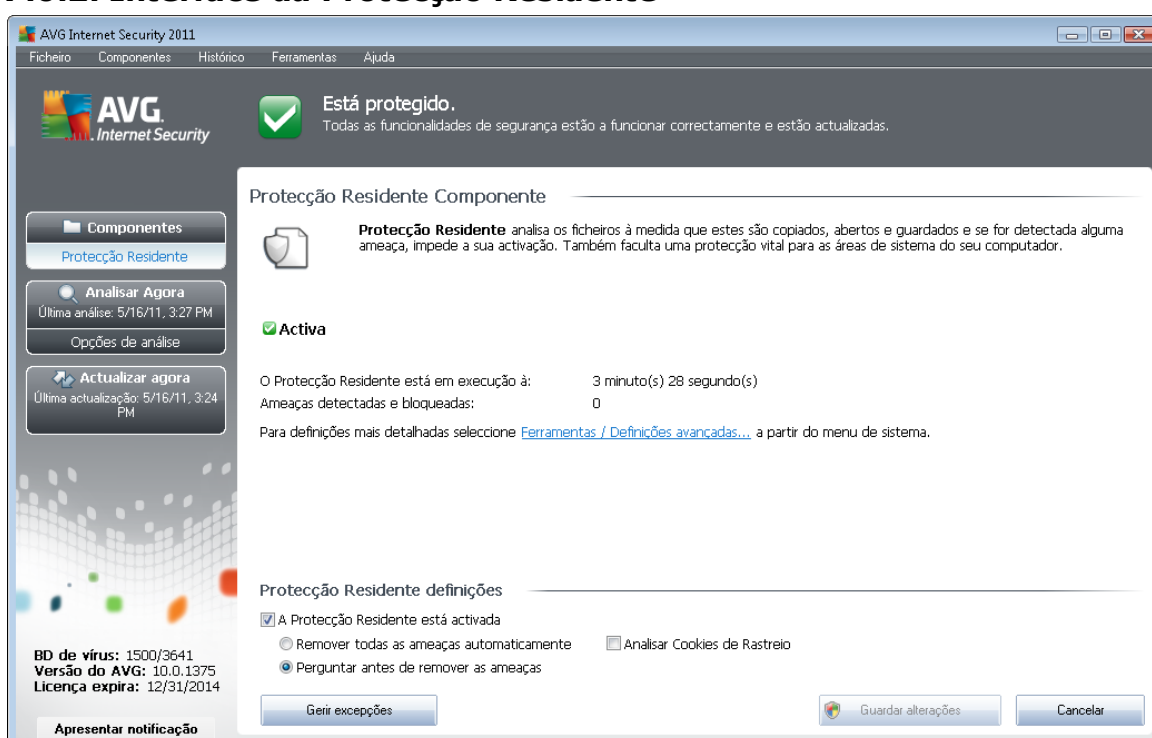
- Verificar a existência de tipos específicos de possíveis ameaças
- Analisar dispositivos amovíveis (*unidades flash, etc.*)



- Analisar ficheiros com extensões específicas ou sem extensão
- Permitir excepções às análises - ficheiros ou pastas específicos que nunca devem ser analisados

Aviso: A Protecção Residente é carregada na memória do seu computador durante o arranque do sistema, e é vital que a mantenha continuamente activada!

7.6.2. Interface da Protecção Residente



Para além de uma síntese da funcionalidade da **Protecção Residente** e a informação do estado do componente, a interface da **Protecção Residente** também disponibiliza alguns dados estatísticos:

- **A Protecção Residente está activa há** - faculto o tempo decorrido desde a inicialização do componente
- **Ameaças detectadas e bloqueadas** - número de infecções detectadas que foram impedidas de executar/abrir (se necessário, este valor pode ser restaurado; ex. para propósitos estatísticos - Restaurar valor)

Protecção Residente definições

Na parte inferior da janela encontrará a secção apelidada **Definições da Protecção Residente** onde pode editar algumas definições básicas da funcionalidade do componente (está disponível uma configuração detalhada, como em todos os outros componentes, via o item *Ferramentas/Definições avançadas* do menu de sistema).



A opção **Protecção Residente está activa** permite-lhe activar/desactivar facilmente a protecção da Protecção Residente. Por predefinição, a função está activa. Com a protecção residente pode ainda decidir como deverão ser tratadas as infecções possivelmente detectadas (removidas):

- ☐ automaticamente (**Remover todas as ameaças automaticamente**)
- ☐ ou somente depois da aprovação do utilizador (**Perguntar antes de remover as ameaças**)

Esta opção não tem impacto no nível de segurança, e só reflecte as suas preferências.

Em ambas as situações, pode ainda seleccionar se pretende **Analisar a existência de cookies de rastreio**. Em casos específicos pode activar esta opção para obter níveis de segurança máximos, no entanto, está desactivada por predefinição. (*cookies = 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*).

Por favor tenha em atenção: 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.

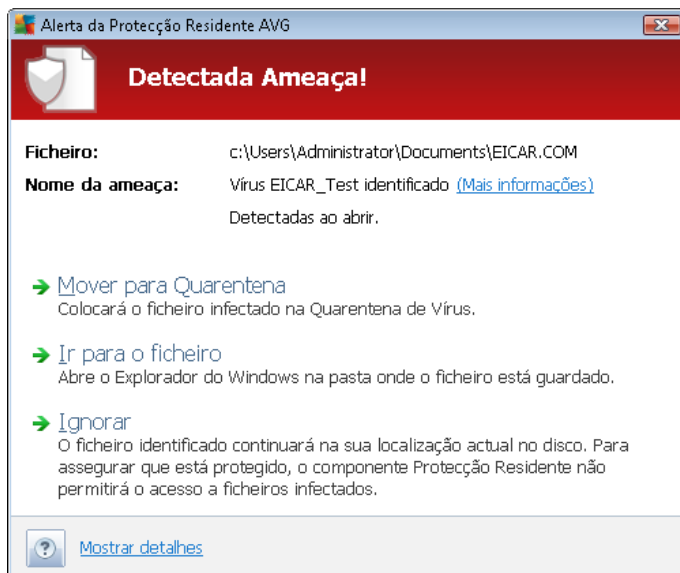
Botões de controlo

Os botões de controlo disponíveis na interface do **Protecção Residente** são os seguintes:

- **Gerir excepções** - abre a janela [Protecção Residente - Itens Excluídos](#) onde pode definir pastas e ficheiros que não devem ser verificados pela análise da [Protecção Residente](#)
- **Guardar alterações** - clique neste botão para guardar e aplicar quaisquer alterações efectuadas nesta janela
- **Cancelar** - clique neste botão para retroceder para a [Interface do utilizador do AVG](#) padrão (síntese dos componentes)

7.6.3. Detecção da 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 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 exercer no momento - estão disponíveis as seguintes opções:

Tenha em atenção que em determinadas condições (que tipo de ficheiro está infectado e onde está localizado), nem todas as opções estarão sempre disponíveis!

- **Remover a ameaça como Utilizador Avançado**- seleccione a caixa se verificar que não tem direitos suficientes para remover a ameaça enquanto utilizador comum. Os Utilizadores Avançados possuem direitos de acesso expandidos, e se a ameaça estiver localizada numa determinada pasta de sistema, pode ter de utilizar esta caixa de verificação para a remover com sucesso.
- **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 a Quarentena** - o vírus será movido para a [Quarentena de Vírus do AVG](#)
- **Ir para o ficheiro** - esta opção redirecciona-o para a localização exacta do objecto suspeito (*abre uma nova janela do Explorador do Windows*)
- **Ignorar** - recomendamos vivamente que NÃO utilize esta opção a menos que tenha uma razão verdadeiramente válida para isso!

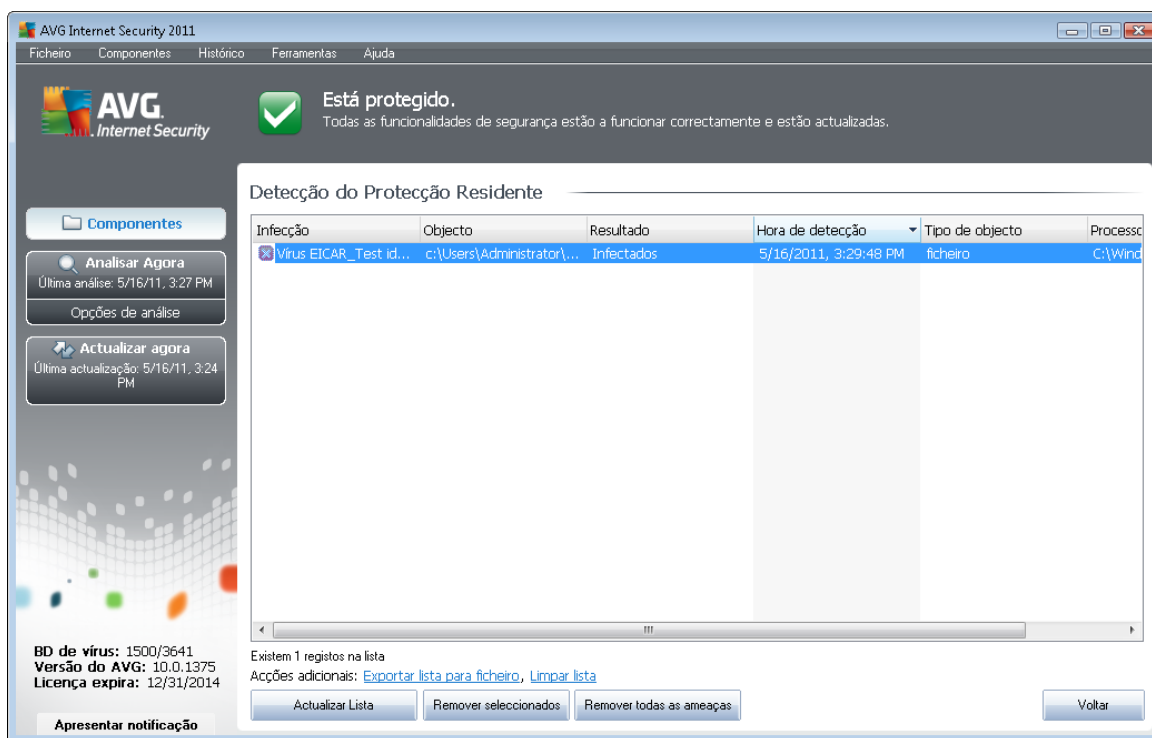
Nota: Pode ocorrer que o tamanho do objecto detectado exceda o limite de espaço livre na Quarentena de Vírus. Se isso acontecer, será informado por meio de um pop-up sobre a questão quando tentar mover o objecto infectado para a Quarentena de Vírus. Contudo, o tamanho da



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 Avançadas 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.

A síntese integral de todas as ameaças detectadas pela [Protecção Residente](#) pode ser encontrada na janela **Deteccção da Protecção Residente** acessível a partir da opção do menu do sistema [Histórico / detecccões da Protecção Residente](#):



A **Deteccção 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 detecccão** - 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*).

7.7. Family Safety

A **Segurança Familiar AVG** ajuda-o a proteger os seus filhos de websites, conteúdos multimédia e pesquisas on-line inapropriados, proporcionando-lhe relatórios relativos à actividade deles on-line. Pode 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.

O componente só estará activo quando o produto **Segurança Familiar AVG** estiver instalado no seu computador. Se não tiver o produto **Segurança Familiar AVG** instalado, clique no ícone correspondente na interface do utilizador **AVG Internet Security 2011** e será encaminhado para o website do produto onde pode consultar todas as informações necessárias.

7.8. AVG LiveKive

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 componente só estará activo quando o produto **AVG LiveKive** estiver instalado no seu computador. Se não tiver o produto **AVG LiveKive** instalado, clique no ícone correspondente na interface do utilizador **AVG Internet Security 2011** e será encaminhado para o website do produto onde pode consultar todas as informações necessárias.

7.9. Verificador 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.

7.9.1. Princípios do 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 e The Bat*). A sua função primária é a utilização com aplicações de e-



mail como o Outlook Express, o Mozilla, O Incredimail, etc.

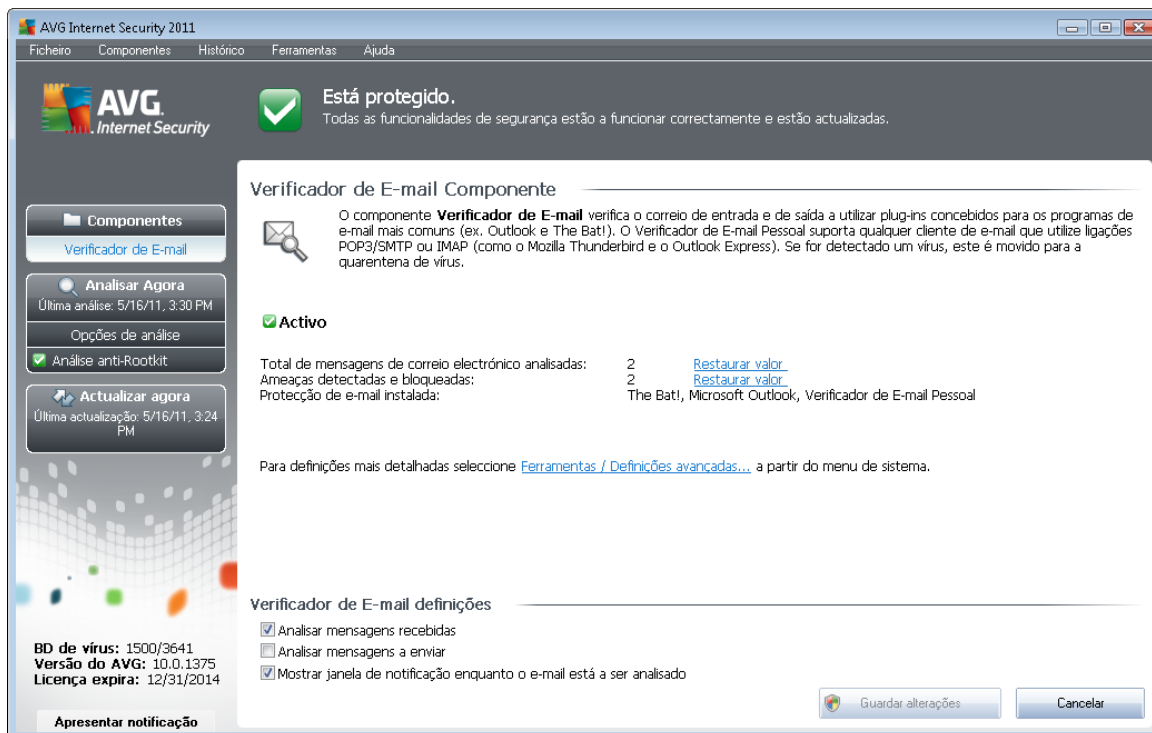
Durante a [instalação](#) do AVG são criados servidores automáticos para controlo das mensagens de e-mail: um para verificar e-mails a receber e um segundo para verificar e-mails a enviar. A utilização destes dois servidores é automaticamente associada às portas 110 e 25 (*portas padrão para o envio/recepção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

Nota: O Verificador de E-mail do AVG não se destina a plataformas de servidores!

7.9.2. Interface do Verificador de E-mail



Na janela do componente **Verificador de E-mail** encontrará um sucinto texto com a descrição da funcionalidade do componente, informação acerca do seu estado actual e as seguintes estatísticas:

- **Total de mensagens de E-mail analisadas** - quantas mensagens de foram analisadas



desde que o **Verificador de E-mail** foi executado pela última vez (se necessário, este valor pode ser restaurado; ex. para propósitos estatísticos - Restaurar valor)

- **Ameaças detectadas e bloqueadas** - faculta o número de infecções detectadas nas mensagens de desde a última execução do **Verificador de E-mail**
- **Protecção de e-mail instalada** - informações acerca de um plug-in específico de protecção de e-mail respeitante ao seu cliente de e-mail predefinido instalado

Verificador de E-mail definições

Na parte inferior da janela pode encontrar a secção **Definições do Verificador de E-mail**, onde pode editar algumas características básicas da funcionalidade do componente:

- **Analisar mensagens recebidas** - marque o item para especificar que todas as mensagens entregues na sua conta devem ser analisadas pela existência de vírus. Este item está activado por predefinição, e é recomendável que não altere esta definição!
- **Analisar mensagens a enviar** - seleccione este item para especificar que todas as mensagens de correio electrónico enviadas a partir da sua conta devem ser analisadas pela existência de vírus (este item está desactivado por predefinição.
- **Apresentar ícone de notificação durante a análise da mensagem de e-mail** - 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 pelo componente [Verificador de E-mail](#) . Por predefinição, este item está activado e é recomendável que não altere esta definição!

A configuração avançada do componente **Verificador de E-mail** está acessível via o item **Ferramentas/Definições Avançadas** no menu de sistema; contudo a configuração avançada é recomendada apenas para utilizadores avançados!

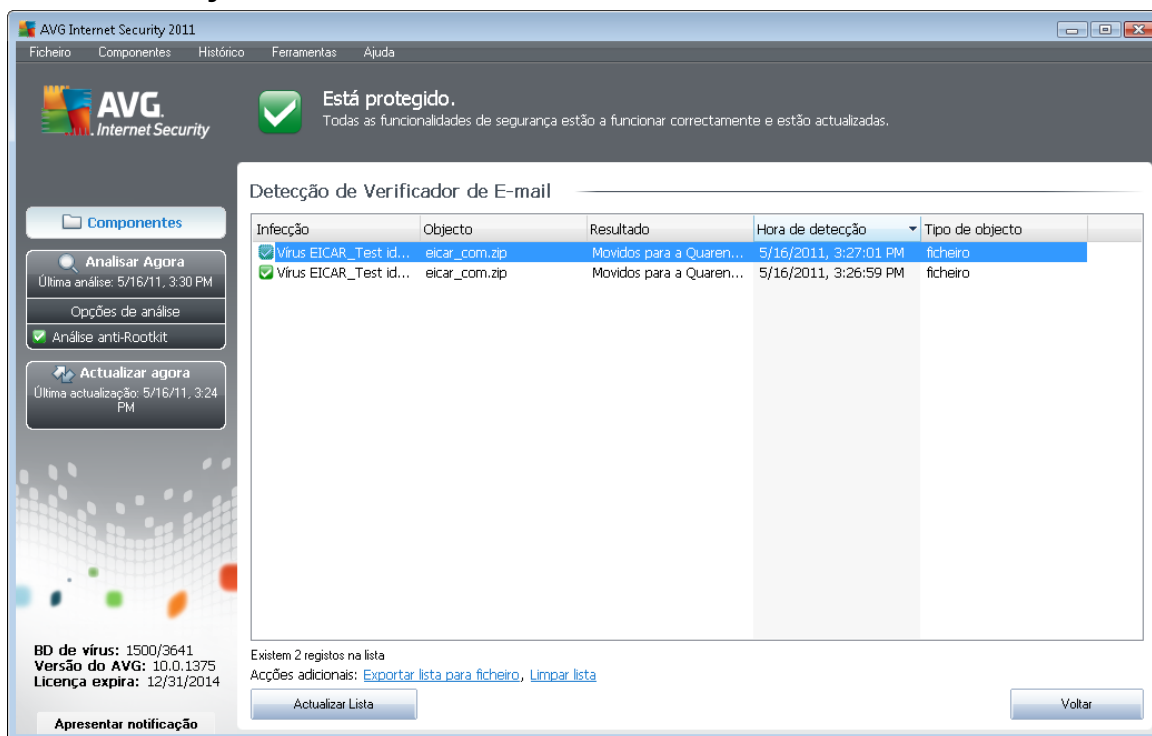
Por favor tenha em atenção: O fornecedor do software configurou todos os componentes do AVG de forma a estes proporcionarem um excelente desempenho. Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente 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 interface **Verificador de E-mails** 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 [Interface do utilizador do AVG](#) padrão (síntese dos componentes)

7.9.3. Detecção de verificador de E-mail



Na janela **Detecção do Verificador de E-mail** (acessível via a opção do menu de sistema **Histórico / Detecção do Verificador de E-mail**) poderá ver uma lista de todas as infecções encontradas pelo componente **Verificador 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-mails** são os seguintes:

- **Actualizar lista** - actualiza a lista de ameaças detectadas



- **Retroceder** - regressa à janela apresentada anteriormente

7.10. Actualizações

7.10.1. Princípios de Actualizações

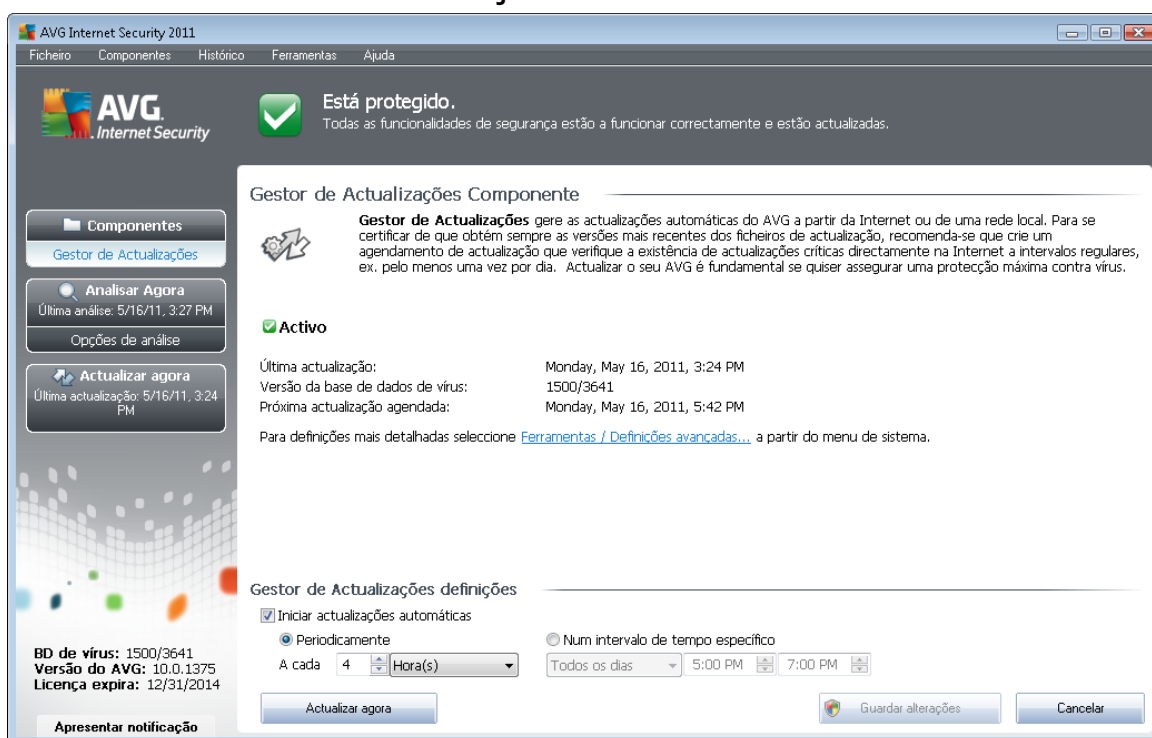
Nenhum software de segurança pode garantir uma protecção efectiva de vários tipos de ameaças a menos que seja actualizado regularmente! Os criadores de vírus estão constantemente à espreita de novas falhas que possam explorar tanto em software como nos sistemas operativos. Novos vírus, novo malware, 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.

É essencial actualizar o seu AVG regularmente!

O **Actualizações** ajuda-o a controlar as actualizações regulares. Neste componente pode agendar transferências automáticas de ficheiros de actualização a partir da Internet, ou da rede local. As actualizações de definições de vírus essenciais deverão ser diárias se possível. As menos urgentes actualizações do programa podem ser semanais.

Nota: Por favor preste atenção ao capítulo [Actualizações do AVG](#) para mais informações relativas a tipos de actualizações e níveis!

7.10.2. Interface de Actualizações





A interface do **Gestor de Actualizações** apresenta informações sobre a funcionalidade do componente e o seu estado actual, assim como dados estatísticos:

- **Última actualização** - especifica a data e hora da última actualização da base de dados
- **Versão da base de dados de vírus** - define o número da versão mais recente base de dados de vírus e este número aumenta com cada actualização da base de dados de vírus
- **Próxima actualização agendada** - especifica a data e hora da próxima actualização da base de dados

Gestor de Actualizações definições

Na parte inferior da janela pode encontrar a secção **Definições de Actualizações** onde pode proceder a algumas alterações às regras de execução do processo de actualização. Pode definir se pretende que os ficheiros de actualização sejam transferidos automaticamente (**Iniciar actualizações automáticas**) ou somente manualmente. Por predefinição, a opção **Iniciar actualizações automáticas** está activada e recomendamos que a mantenha neste estado! A transferência regular dos mais recentes ficheiros de actualização é essencial para o funcionamento apropriado de qualquer software de segurança!

Pode ainda definir quando a actualização deve ser executada:

- o **Periodicamente** - define o intervalo de tempo
- o **Num intervalo de tempo específico** - define a hora exacta do dia a que a actualização deve ser executada

Por predefinição, a actualização está definida para ser executada a cada 4 horas. É vivamente recomendável que mantenha esta definição a menos que tenha uma razão muito forte para a alterar!

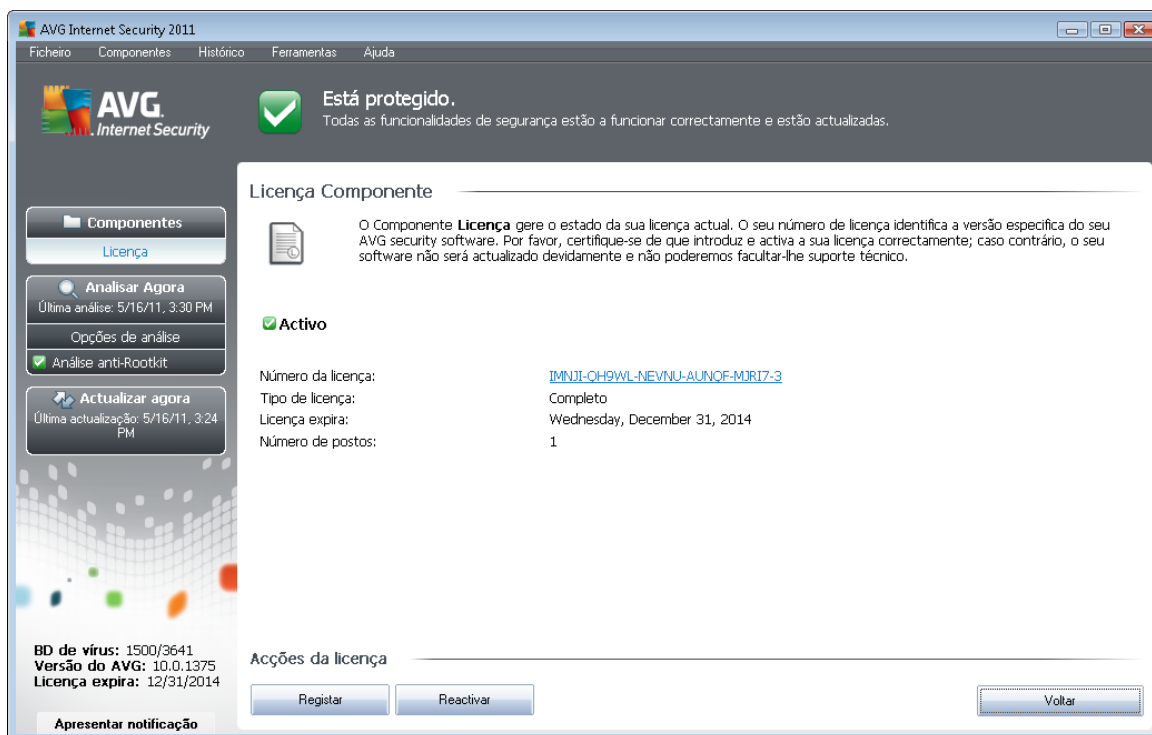
Por favor tenha em atenção: O fornecedor do software configurou todos os componentes do AVG de forma a estes proporcionarem um excelente desempenho. Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efectuadas exclusivamente 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 interface de **Actualizações** são os seguintes:

- **Actualizar agora** - inicia uma [actualização imediata](#) manualmente
- **Guardar alterações** - clique neste botão para guardar e aplicar quaisquer alterações efectuadas nesta janela
- **Cancelar** - clique neste botão para retroceder para a [Interface do utilizador do AVG padrão \(síntese dos componentes\)](#)

7.11. Licença



Na interface do componente **Licença** encontrará um sucinto texto com a descrição da funcionalidade do componente, informação acerca do seu estado actual, e as seguintes informações:

- **Número de licença** - apresenta a versão resumida do seu número de licença (*por razões de segurança, os últimos quatro números estão ocultos*). Ao introduzir o seu número de licença, tem de ser absolutamente preciso e digitá-lo exactamente como este é apresentado. Como tal, recomendamos vivamente que utilize sempre o método "copiar e colar" para qualquer manuseamento do número de licença.
- **Tipo de licença** - especifica o tipo de produto instalado.
- **A licença expira** - esta data determina o período de validade da sua licença. Se quiser continuar a utilizar o **AVG Internet Security 2011** após esta data terá de renovar a sua licença. A renovação da licença pode ser efectuada on-line no [website da AVG](http://www.avg.com/).
- **Número de postos de trabalho** - quantos postos de trabalho nas quais pode instalar o seu **AVG Internet Security 2011**.

Botões de controlo

- **Registar** - 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.

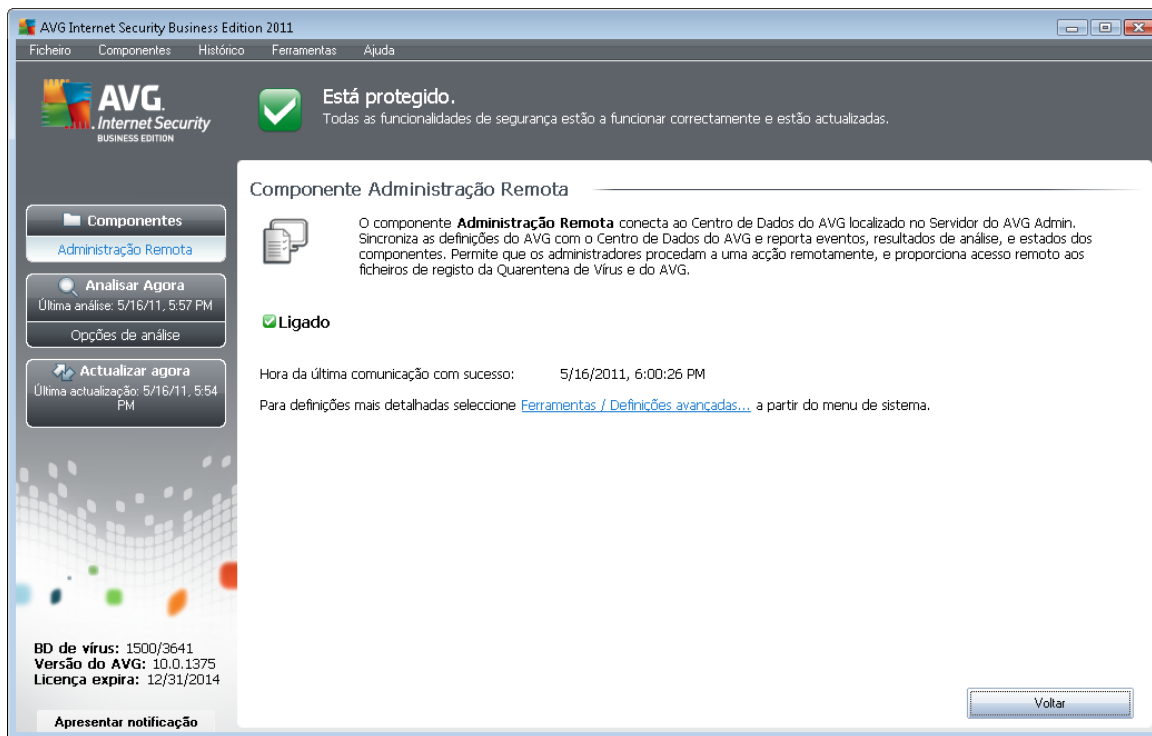


- **Reactivar** - abre a janela **Activar AVG** com os dados que introduziu na janela [Personalizar AVG](#) do processo de instalação. Nesta janela pode introduzir o seu número de licença para substituir o número de venda (o número com o qual instalou o AVG), ou para substituir o número de licença antigo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

Nota: Se estiver a utilizar a versão de teste do **AVG Internet Security 2011**, os botões aparecem como **Comprar agora** e **Activar**, permitindo-lhe comprar a versão completa do programa imediatamente. Para produtos **AVG Internet Security 2011** instalados com um número de venda, os botões são apresentados como **Registar** e **Activar**.

- **Retroceder** - prima este botão para retroceder para a [Interface do utilizador do AVG](#) padrão (síntese dos componentes).

7.12. Administração Remota



O componente **Administração Remota** só é apresentado na interface do utilizador do **AVG Internet Security 2011** caso tenha instalado a edição Business do seu produto (consulte o componente [Licença](#)). Na janela **Administração Remota** encontra as informações relativas ao estado do componente (se está activo e conectado ao servidor). Todas as definições do componente **Administração Remota** devem ser configuradas nas **Definições Avançadas / Administração Remota**.

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 \(www.avg.com\)](http://www.avg.com), na secção **Centro de Suporte / Transferência / Documentação**.



Botões de controlo

- **Retroceder** - prima este botão para retroceder para a [Interface do utilizador do AVG](#) padrão (*síntese dos componentes*).

7.13. Protecção Online

7.13.1. Princípios da Protecção Online

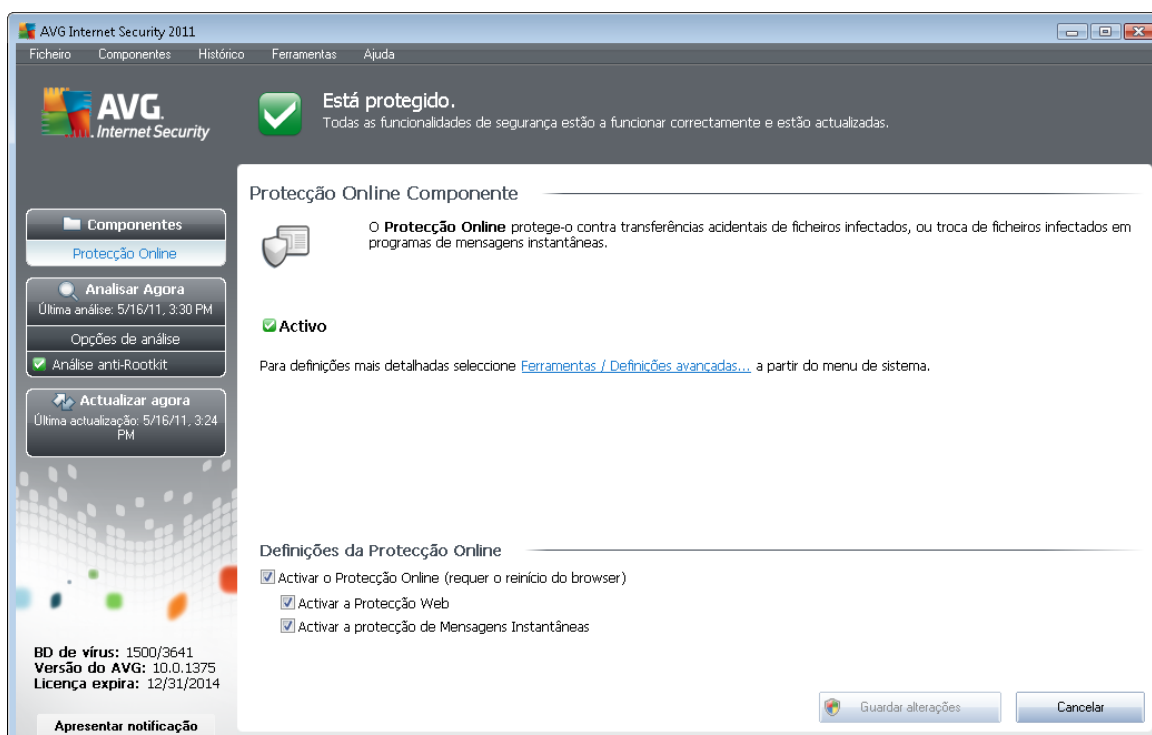
A **Protecção Online** é um tipo de protecção residente em tempo real; analisa o conteúdo da páginas Web visitadas (*e possíveis ficheiros incluídos nestas*) mesmo antes destas serem apresentadas no seu browser ou serem transferidas para o seu computador.

A **Protecção Online** detecta que a página que está prestes a visitar inclui algum javascript perigoso e evita que a página seja apresentada. Além disso, reconhece malware contido na página e pára a sua transferência imediatamente para que este nunca aceda ao seu computador.

Nota: A Protecção Online AVG não se destina a plataformas de servidores!

7.13.2. Interface da Protecção Online

A interface do componente **Protecção Online** descreve o comportamento deste tipo de protecção. Pode ainda consultar informações relativas ao estado actual do componente. Na parte inferior da janela encontrará então as opções de edição elementares desta funcionalidade do componente:





Definições da Protecção Online

Antes de mais, tem a opção para activar/desactivar imediatamente a **Protecção Online** ao marcar o item **Activar Protecção Online**. Esta opção está activada por predefinição e o componente **Protecção Online** está activo. No entanto, se não tiver uma boa razão para alterar esta definição, recomendamos que mantenha o componente activado. Se o item estiver marcado e a **Protecção Online** estiver em execução, são activadas duas opções de configuração:

- **Activar a Protecção na Internet** - esta opção confirma que a **Protecção Online** deve analisar o conteúdo do website.
- **Activar a protecção de Mensagens Instantâneas** - marque este item se quiser que a **Protecção Online** verifique se a comunicação de mensagens instantâneas (ex. ICQ, MSN Messenger, ...) está isenta de vírus.

Por favor tenha em atenção: 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.

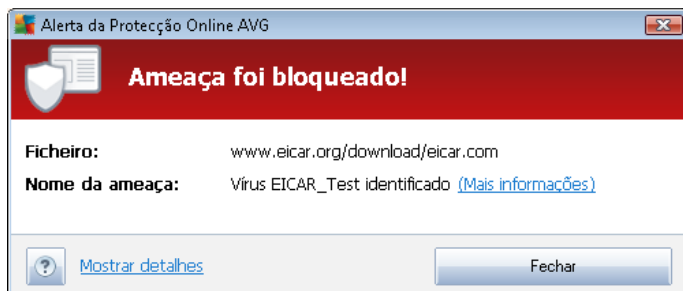
Botões de controlo

Os botões de controlo disponíveis na interface da **Protecção Online** 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 [Interface do utilizador do AVG padrão](#) (síntese dos componentes)

7.13.3. Detecção 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:

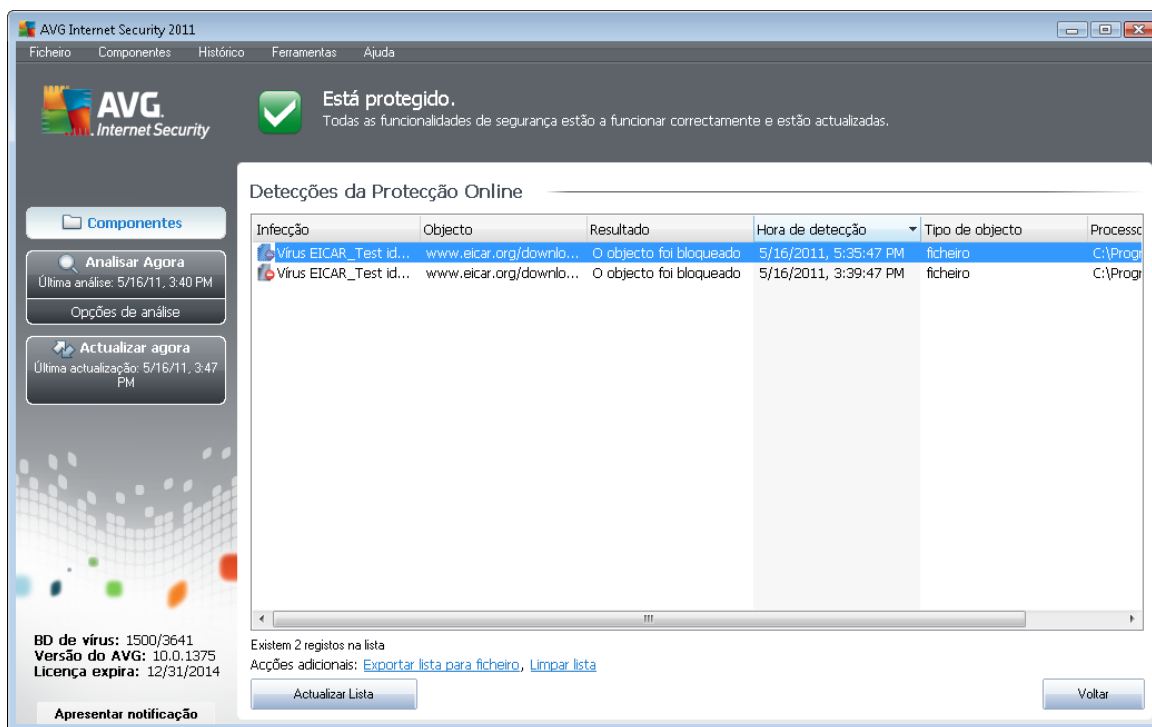




Nesta janela de aviso encontra dados sobre o ficheiro que foi detectado e considerado infectado (*Nome do ficheiro*), o nome da infecção detectada (*Nome da ameaça*) e um link para a [Enciclopédia de vírus](#) onde pode aceder a informações detalhadas sobre a infecção detectada (se esta for conhecida). 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**). O botão **Actualizar lista** procederá à actualização da lista de detecções da **Protecção Online**. O botão **Retroceder** leva-o de volta à [Interface do utilizador do AVG](#) padrão (síntese de componentes).

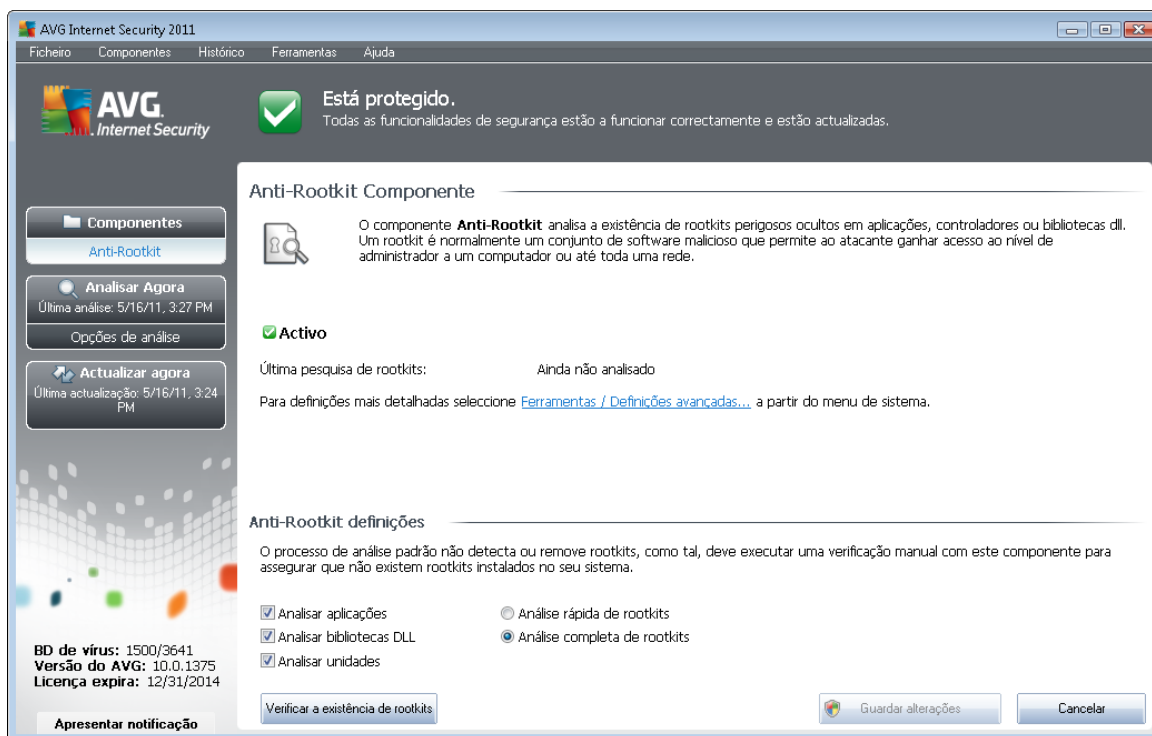
7.14. Anti-Rootkit

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.

7.14.1. Princípios do Anti-Rootkit

O **componente AVG 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 **AVG 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 **AVG 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.

7.14.2. Interface do Anti-Rootkit



A interface do utilizador do **Anti-Rootkit** disponibiliza uma breve descrição da funcionalidade do componente, informa o estado actual do componente e reporta a última vez que o teste **Anti-Rootkit** foi executado (**última verificação de rootkits**). A janela **Anti-Rootkit** apresenta ainda o link [Ferramentas/Definições Avançadas](#). Use o link para aceder à configuração avançada do componente **Anti-Rootkit**.

Por favor tenha em atenção: 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 do componente Anti-Rootkit

Na parte inferior da janela pode encontrar a secção **Definições do Anti-Rootkit** onde pode configurar algumas funções elementares da análise de presença de rootkits. Primeiro, seleccione as caixas respectivas para especificar os objectos que devem ser analisados:

- **Analisar aplicações**
- **Analisar bibliotecas DLL**
- **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** - prima este botão para guardar todas as alterações efectuadas nesta interface e para regressar à [Interface do utilizador do AVG](#) (*síntese de componentes*)
- **Cancelar** - prima este botão para regressar à [Interface do utilizador do AVG](#) (*síntese de componentes*) sem ter guardado quaisquer alterações efectuadas

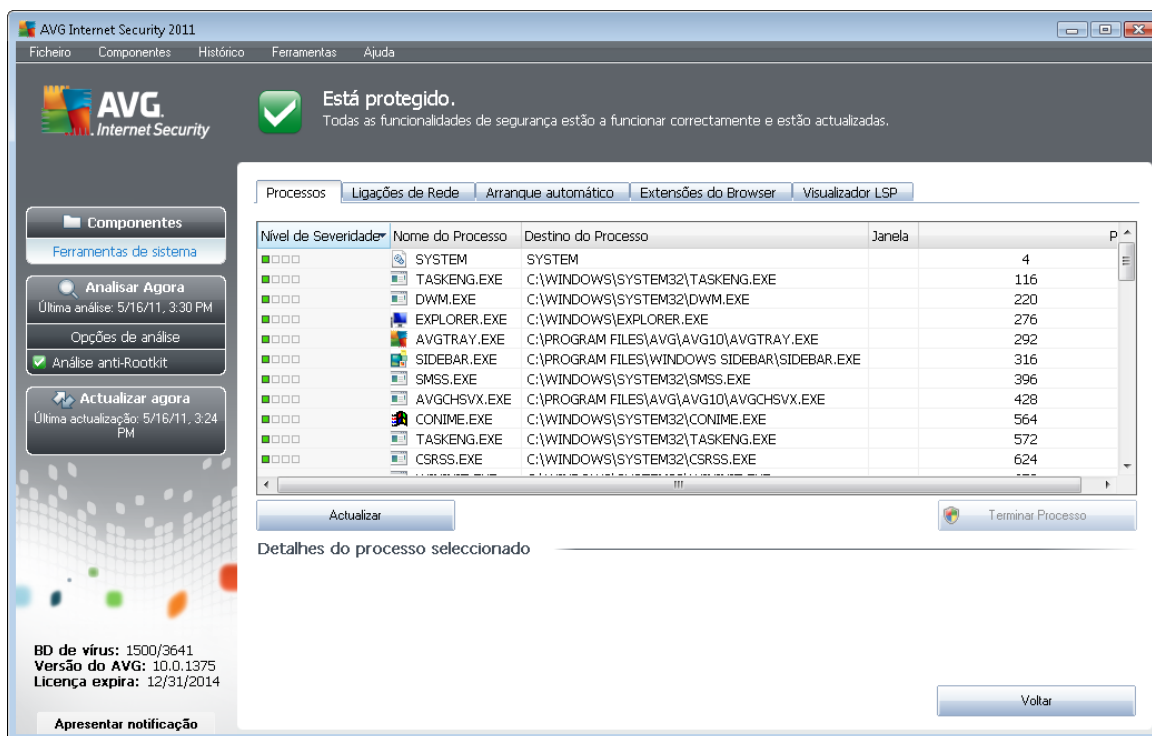
7.15. Ferramentas

As **Ferramentas de sistema** são referentes a ferramentas que disponibilizam um resumo detalhado do ambiente e sistema operativo do **AVG Internet Security 2011** . 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!

7.15.1. 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

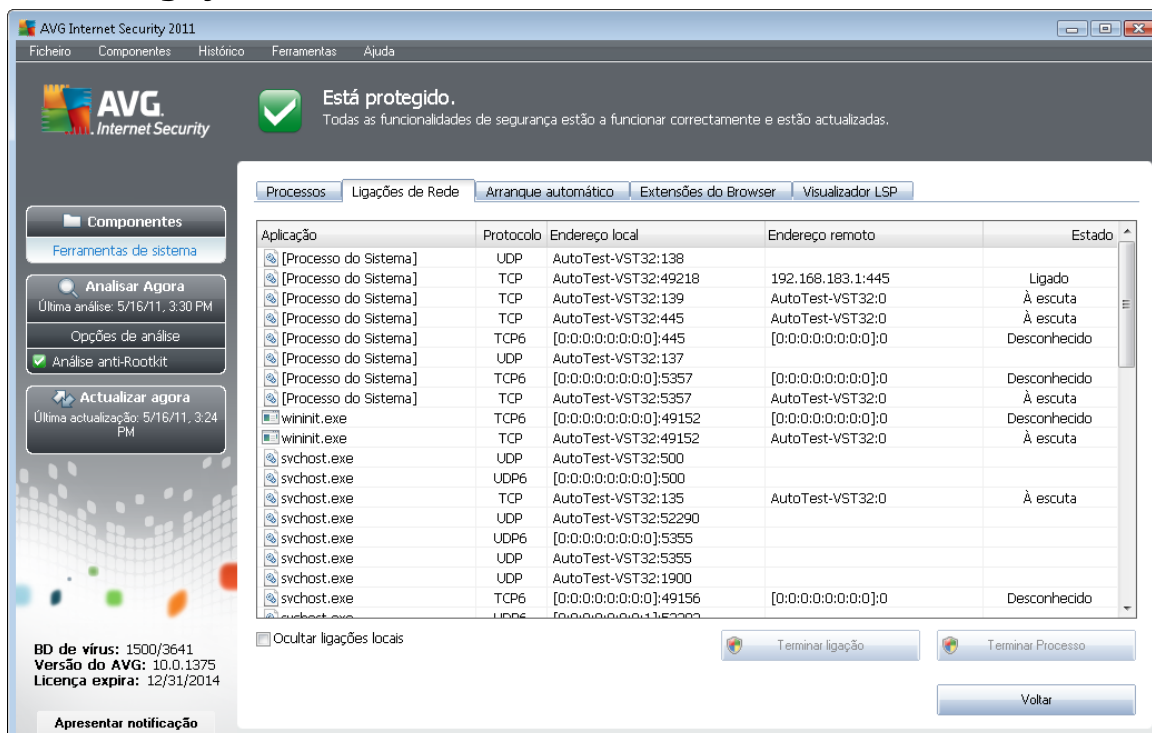
Os botões de controlo disponíveis na interface das **Ferramentas do Sistema** são os seguintes:

- **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 [Interface do utilizador do AVG](#) padrão (síntese de componentes)

7.15.2. 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:
 - o TCP – protocolo utilizado em conjunto com o Protocolo de Internet (IP) para transmitir informações através da Internet
 - o 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.

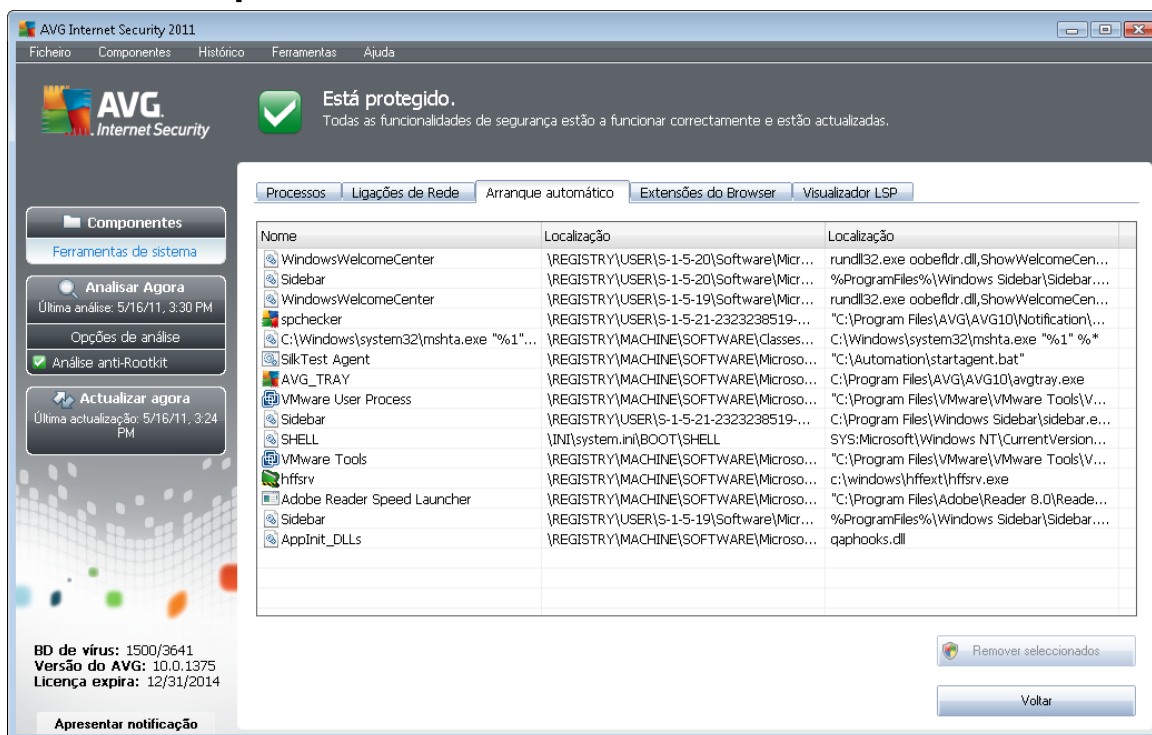
Botões de controlo

Os botões de controlo disponíveis são:

- **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!

7.15.3. Arranque automático



A janela **Iniciação com o arranque do Windows** 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.

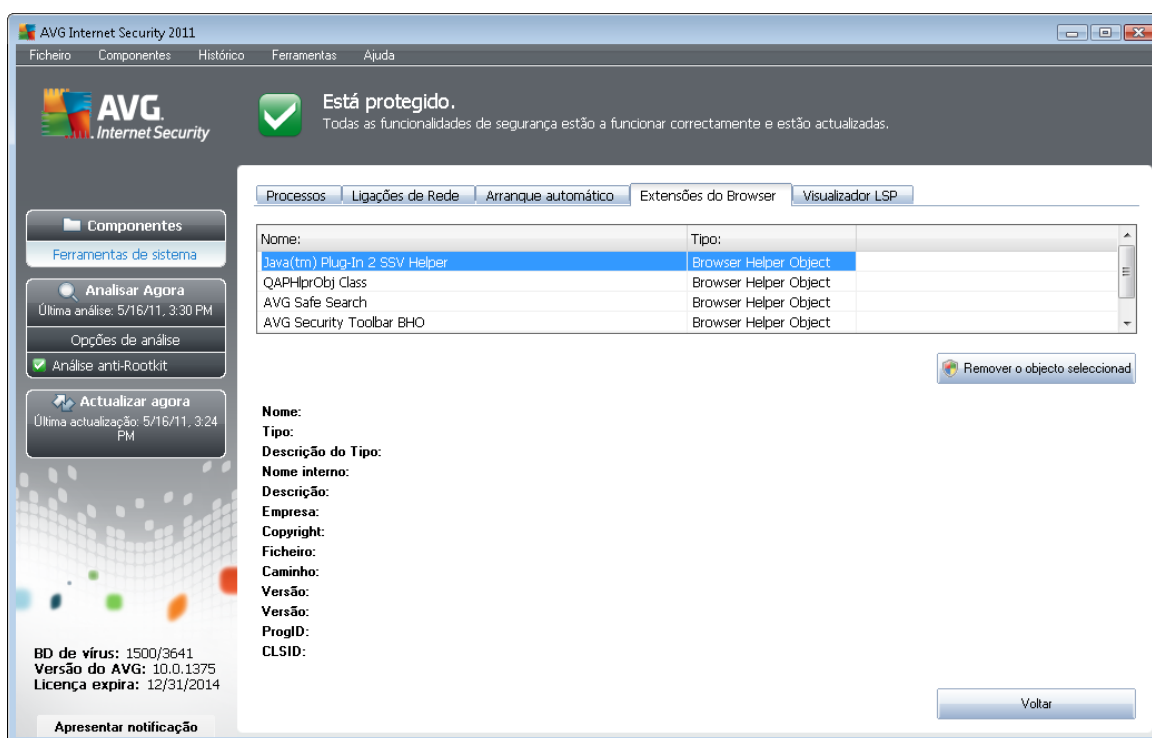
Pode eliminar uma ou mais entradas, seleccionando-as e premindo o botão **Eliminar itens seleccionados**. O botão **Retroceder** leva-o de volta à [Interface do utilizador do AVG](#) padrão (síntese



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!

7.15.4. Extensões do Browser



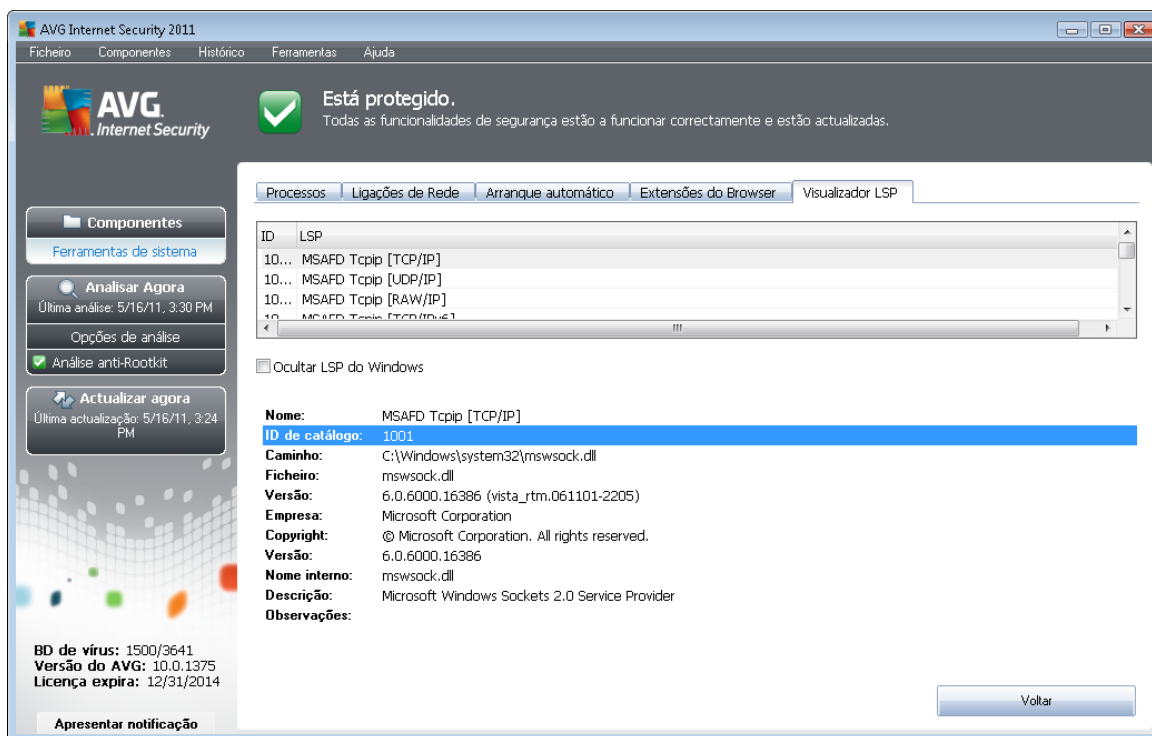
A janela **Extensões do Browser** contém uma lista de plug-ins (*ou seja, aplicações*) que estão instaladas no ser browser da Internet. Esta lista pode conter plug-ins de aplicações normais e programas potenciais de malware. Clique num objecto na lista para obter informações detalhadas sobre o plug-in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

Botões de controlo

Os botões de controlo disponíveis no separador **Extensão do Browser** são:

- **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 [Interface do utilizador do AVG](#) padrão (síntese de componentes)

7.15.5. Visualizador LSP



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

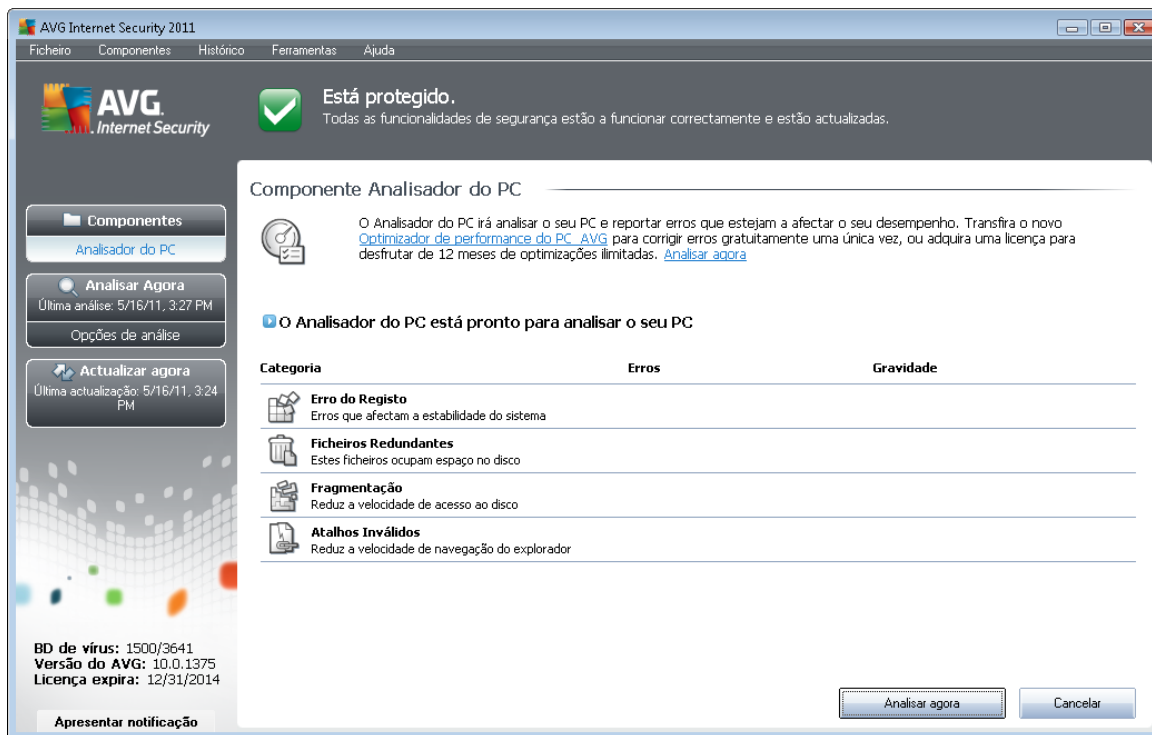
Um **Layered Service Provider (LSP)** é um controlador do sistema ligado aos serviços de rede do sistema operativo Windows. Tem acesso a todos os dados que entram e saem do computador, incluindo a capacidade de os modificar. Alguns LSPs são necessários para permitir que o Windows estabeleça ligação a 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.

Para incluir LSP do Windows na lista, demarque a caixa de verificação **Ocultar LSP do Windows**. O botão **Retroceder** leva-o de volta à [Interface do utilizador do AVG](#) padrão (*síntese de componentes*).

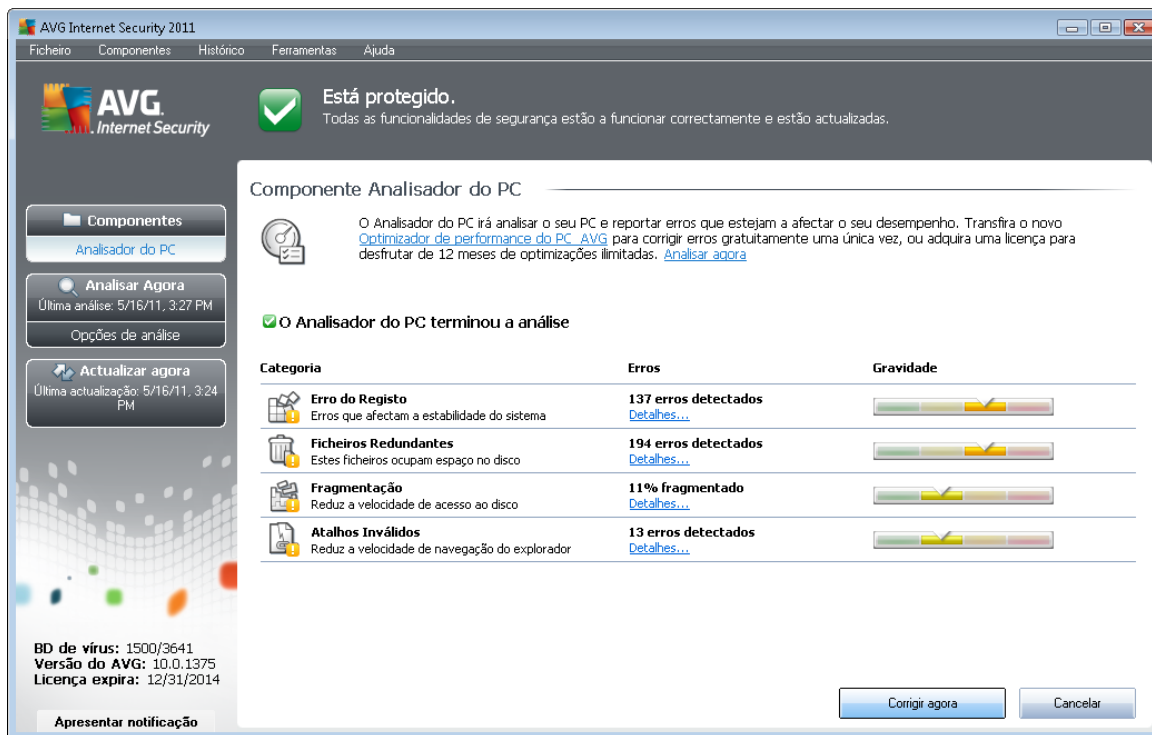
7.16. Analisador do PC

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 atualizadas 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

7.17. Protecção de Identidade

Protecção de Identidade do AVG é um produto anti-malware que se destina 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. Garante que todos os programas em execução no seu PC estão a funcionar devidamente. A **Protecção de Identidade do AVG** identifica e bloqueia continuamente comportamentos suspeitos e protege o seu computador contra todo o novo malware.

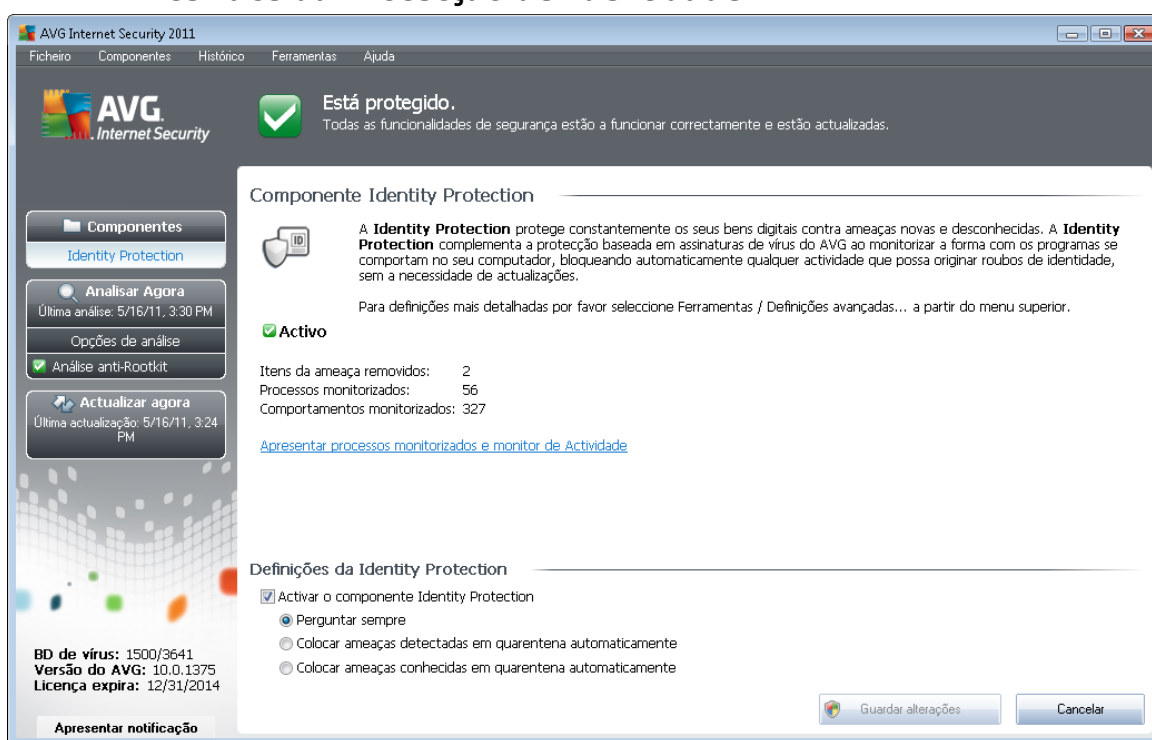


7.17.1. Princípios da Protecção de Identidade

Protecção de Identidade do AVG 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. À medida que o malware evolui e surge na forma de programas normais que podem permitir o acesso ao seu computador pelo atacante remoto para roubos de identidade, a **Protecção de Identidade do AVG** protege-o deste tipo de malware com novas formas de execução. É uma protecção complementar do [Anti-Vírus AVG](#) que o protege de vírus baseados em ficheiros e vírus conhecidos por meio de um mecanismo de assinaturas e análise.

Recomendamos vivamente que tenha ambos os componentes ([Anti-Vírus AVG](#) e **Protecção de Identidade do AVG) instalados para desfrutar de protecção completa para o seu PC.**

7.17.2. Interface da Protecção de Identidade



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

- **Itens de malware 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 da Protecção de Identidade

Na parte inferior da janela encontra a secção **Definições da Protecção de Identidade**, onde pode editar algumas características básicas da funcionalidade 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:

- o **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*)
- o **Colocar ameaças detectadas em quarentena automaticamente** - todas as aplicações detectadas como sendo malware serão bloqueadas automaticamente
- o **Colocar ameaças conhecidas em quarentena automaticamente** - só as aplicações que são indubitavelmente reconhecidas como malware serão bloqueadas

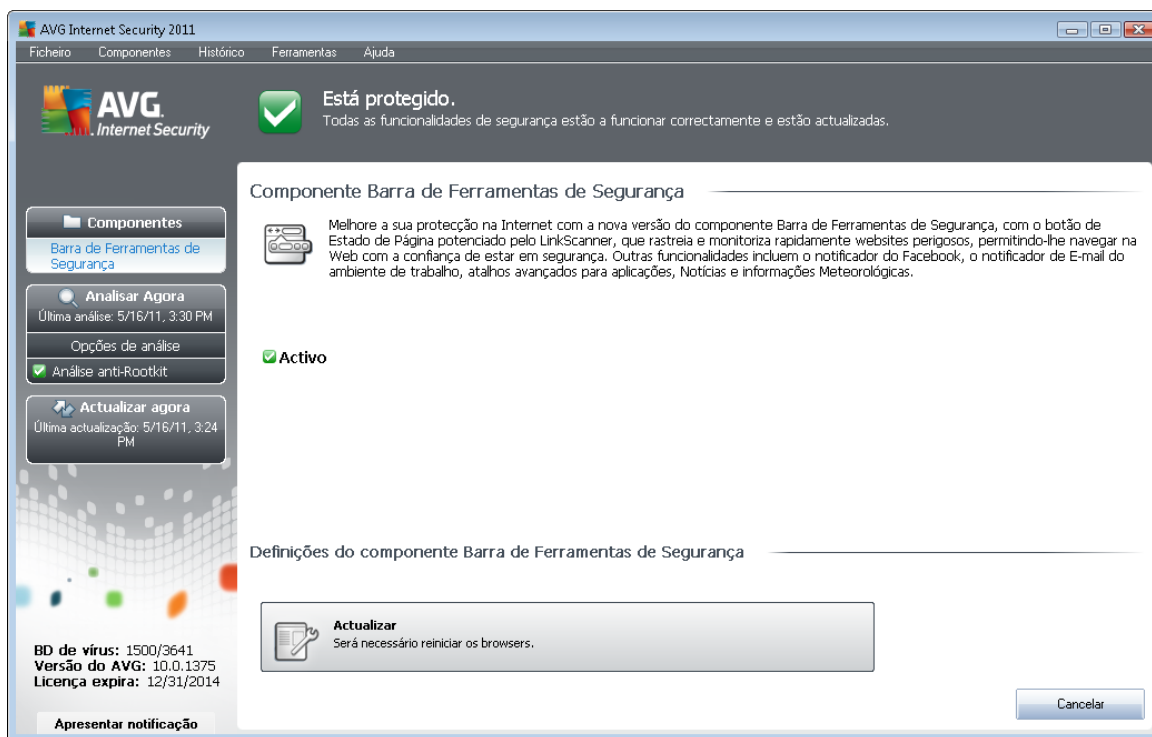
Botões de controlo

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 [Interface do utilizador do AVG padrão](#) (*síntese dos componentes*)

7.18. Barra de Ferramentas de Segurança

A **Barra de Ferramentas de Segurança** é uma barra de ferramentas opcional do browser que disponibiliza uma protecção avançada do AVG e várias funcionalidades e ferramentas facilmente acessíveis quando navega na Internet. A **Barra de Ferramentas de Segurança** é actualmente suportada pelos browsers Internet Explorer (6.0 ou superior), e Mozilla Firefox (3.0 ou superior):



Todas as definições do componente **Barra de Ferramentas de Segurança** são acessíveis directamente na [Barra de Ferramentas de Segurança](#) no seu browser.



8. Barra de Ferramentas de Segurança AVG

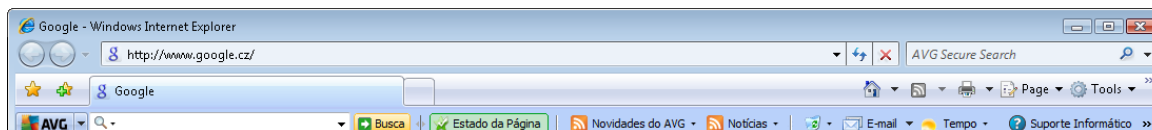
A **Barra de Ferramentas de Segurança AVG** é uma nova ferramenta que trabalha em conjunto com o componente [LinkScanner](#). A **Barra de Ferramentas de Segurança AVG** pode ser usada para controlar as funções do componente [LinkScanner](#) e para ajustar o seu comportamento.

Se optar pela instalação da barra de ferramentas durante a instalação do **AVG Internet Security 2011**, esta será adicionada ao seu browser (*Internet Explorer 6.0 ou superior e Mozilla Firefox 3.0 ou superior*) automaticamente. Actualmente, não são suportados outros browsers.

Nota: Na eventualidade de utilizar um browser alternativo (ex. Avant Browser) pode ocorrer um comportamento inesperado.

8.1. Interface da Barra de Ferramentas de Segurança AVG

A **Barra de Ferramentas de Segurança AVG** foi concebida para funcionar com o **MS Internet Explorer**(versão 6.0 ou superior) e o **Mozilla Firefox** (versão 3.0 ou superior). Uma vez decidido pela instalação da **Barra de Ferramentas de Segurança AVG** (durante o [processo de instalação do AVG](#) foi inquirido sobre se pretendia ou não instalar o componente), o componente ficará localizado no seu browser mesmo abaixo da barra de endereços:



A **Barra de Ferramentas de Segurança AVG** consiste no seguinte:

8.1.1. Botão de logótipo do AVG

Este botão proporciona acesso a itens gerais da barra de ferramentas. Clique no botão de logótipo para ser redireccionado para o [website da AVG](#). Clicar com o cursor junto ao ícone AVG abrirá as seguintes opções:

- **Informações da Barra de Ferramentas** - link para a página inicial da **Barra de Ferramentas de Segurança AVG com informações detalhadas relativas à protecção da barra de ferramentas**
- **Iniciar o AVG** - abre a [interface do utilizador](#) do **AVG Internet Security 2011**
- **Informações do AVG** - abre um menu de contexto com os seguintes links para importantes informações de segurança relativas ao **AVG Internet Security 2011**:
 - o *Acerca de Ameaças* - abre o [website da AVG](#) numa página que disponibiliza dados importantes sobre as principais ameaças, recomendações para a remoção de vírus, informações sobre a actualização do AVG, acesso à [base de dados de vírus](#) e outras informações relevantes
 - o *Notícias da AVG* - abre a página que disponibiliza os mais recentes comunicados de imprensa relativos à AVG



o *Nível de Ameaça Actual* - abre a página do laboratório de vírus com uma apresentação gráfica do nível de ameaças actual na Internet

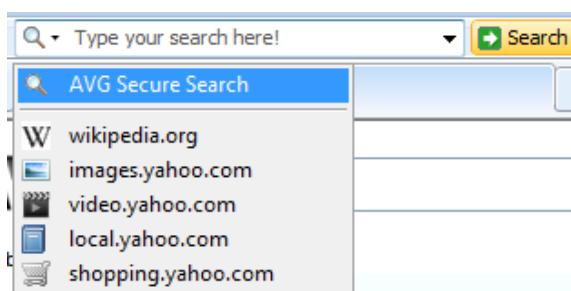
o *Laboratório de Ameaças AVG* - abre o website [Relatórios de Sites AVG](#) onde pode pesquisar ameaças específicas por nome e obter informações detalhadas sobre cada uma delas

- **Opções** - abre uma janela de configuração onde pode ajustar as definições da **Barra de Ferramentas de Segurança AVG** conforme as suas necessidades - consulte o seguinte capítulo [Opções da Barra de Ferramentas de Segurança AVG](#)
- **Eliminar Histórico** - permite-lhe eliminar, **na Barra de Ferramentas de Segurança AVG**, o histórico completo, ou eliminar separadamente o histórico de pesquisa, o histórico do browser, o histórico de transferências e eliminar cookies.
- **Actualizar** - verifica a existência de novas actualizações para a sua **Barra de Ferramentas de Segurança AVG**
- **Ajuda** - faculta opções para abrir o ficheiro de ajuda, contactar o [suporte técnico da AVG](#), enviar o seu feedback em relação ao produto, ou visualizar os detalhes da versão actual da barra de ferramentas

8.1.2. Caixa de pesquisa do AVG Secure Search (powered by Google)

A caixa **AVG Secure Search (powered by Google)** é uma forma fácil e segura de pesquisar na Web usando o AVG Secure Search (powered by Google). Digite uma palavra ou frase na caixa de pesquisa e clique no botão **Procurar**, ou na tecla **Enter**, para iniciar a pesquisa directamente no servidor AVG Secure Search (powered by Google), independentemente da página que está actualmente apresentada. A caixa de pesquisa também lista o seu histórico de pesquisa. As pesquisas efectuadas via a caixa de pesquisa são analisadas pela protecção [Search-Shield](#).

Em alternativa, no campo de pesquisa, pode mudar para a Wikipédia ou outro serviço de pesquisa específico - consulte a imagem:



8.1.3. Estado da Página

Directamente na barra de ferramentas, este botão apresenta a avaliação da página Web actualmente apresentada com base nos critérios do componente [Surf-Shield](#) :

-  - A página de destino é segura

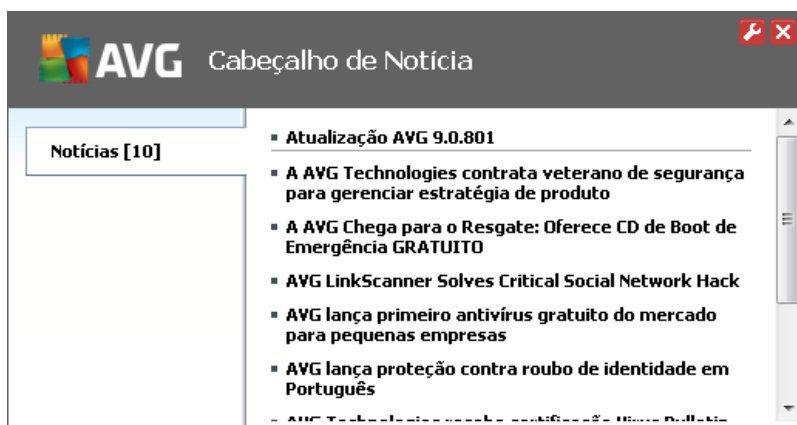


-  - A página é algo suspeita.
-  - A página contém ligações para páginas identificadas como perigosas.
-  - A página de destino contém ameaças activas! Para sua segurança, não lhe será permitido visitar esta página.
-  - A página de destino não está acessível, e, como tal, não pôde ser analisada.

Clique no botão para abrir um painel informativo com dados detalhados sobre a página específica.

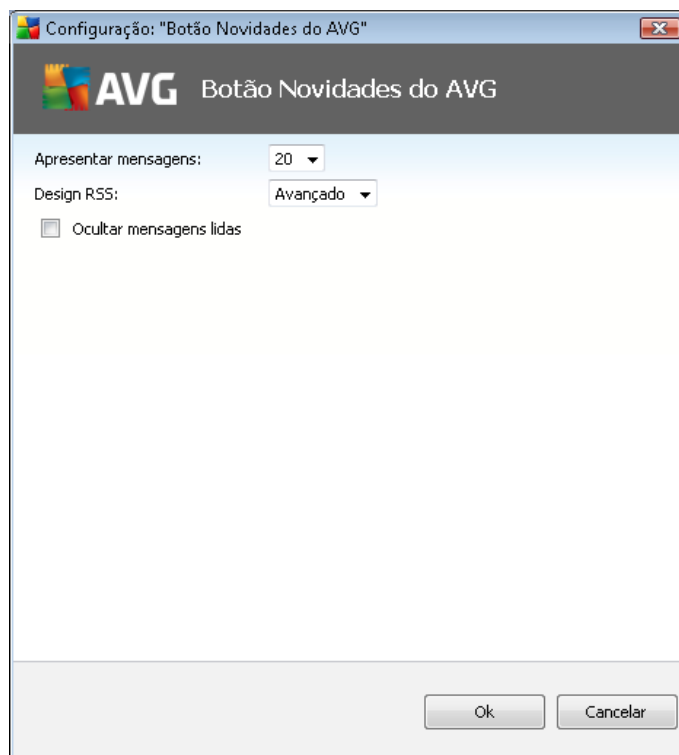
8.1.4. Notícias do AVG

Directamente na **Barra de Ferramentas de Segurança AVG**, este botão abre uma síntese dos últimos **Cabeçalhos de notícias** relativos ao AVG, seja notícias da imprensa ou comunicados da empresa:



No canto superior direito estão disponíveis dois botões de controlo vermelhos:

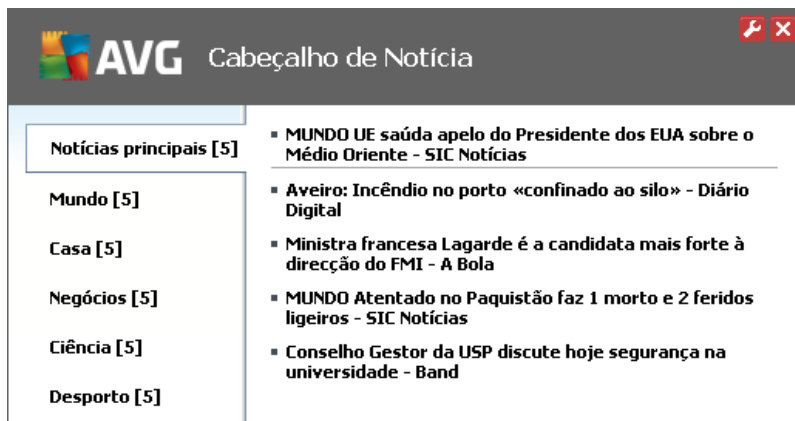
-  - o botão abre a janela de edição onde pode especificar os parâmetros do botão **Notícias do AVG** apresentado na **Barra de Ferramentas de Segurança AVG**:



- o **Apresentar mensagens** - altere o número de mensagens que pretende que sejam apresentadas simultaneamente
 - o **Design RSS** - seleccione entre o modo Avançado/Básico da visualização actual da síntese de notícias (*por predefinição, está seleccionado o modo Avançado - consulte a imagem acima*)
 - o **Ocultar mensagens lidas** - marque este item para confirmar que as mensagens que já tiver lido já não serão apresentadas novamente, para que possam ser apresentadas mensagens novas
-  - clique neste botão para fechar a síntese de notícias aberta

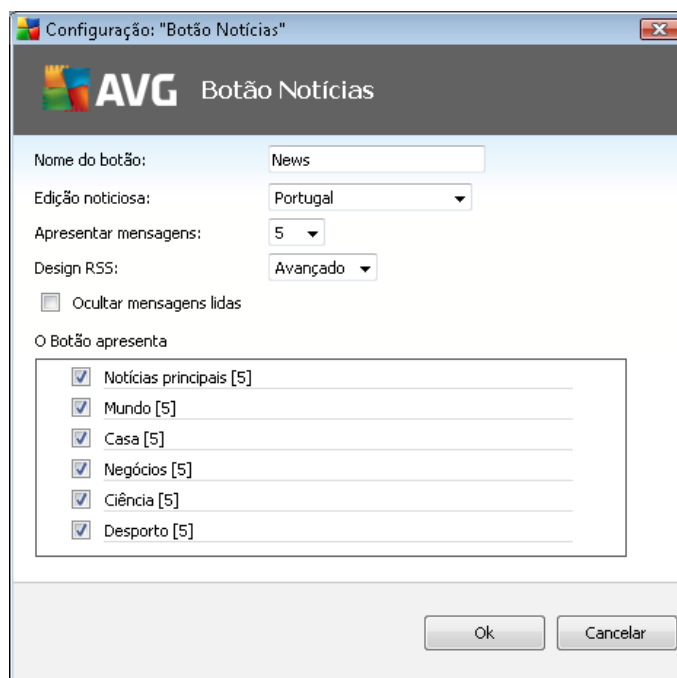
8.1.5. Notícias

Similarmente, directamente a partir da **Barra de Ferramentas de Segurança AVG**, este botão abre uma síntese das últimas notícias de canais de comunicação social seleccionados e divididos em várias secções:



No canto superior direito estão disponíveis dois botões de controlo vermelhos:

-  - o botão abre a janela de edição onde pode especificar os parâmetros do botão **Notícias** apresentado na **Barra de Ferramentas de Segurança AVG**:



- o **Nome do botão** - pode alterar o nome com que o botão é apresentado na **Barra de Ferramentas de Segurança AVG**
- o **Edição de notícias** - escolha um país da lista para consultar notícias da região seleccionada
- o **Apresentar mensagens** - especifique o número de mensagens que pretende que sejam apresentadas simultaneamente
- o **Design RSS** - alterne entre modo Básico/Avançado para seleccionar o design da síntese de notícias (**o design avançado está seleccionado por predefinição, consulte a imagem acima**)
- o **Ocultar mensagens lidas** - marque este item para confirmar que as mensagens que já tiver lido não deverão ser apresentadas novamente na síntese de notícias e deverão ser substituídas por um novo cabeçalho



o **O botão apresenta** - neste campo pode atribuir o tipo de notícias que deve ser apresentado na síntese de notícias da **Barra de Ferramentas AVG**

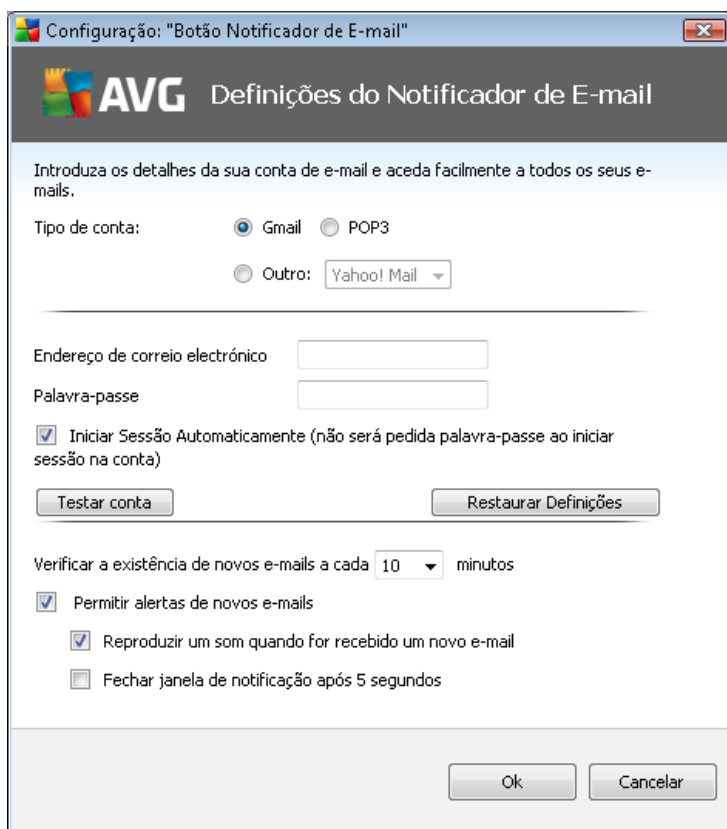
-  - clique neste botão para fechar a síntese de notícias aberta

8.1.6. Eliminar histórico

Com este botão pode eliminar o histórico do seu browser, exactamente como na opção **Logótipo AVG -> Eliminar histórico**.

8.1.7. Notificador de E-mail

O botão **Notificador de E-mail** permite-lhe activar a opção de informação sobre novas mensagens de e-mail directamente na interface da [Barra de Ferramentas de Segurança AVG](#). O botão abre a seguinte janela de edição, onde pode definir os parâmetros da sua conta de e-mail e as regras de apresentação de e-mail. Siga as instruções apresentadas na janela:



- **Tipo de conta** - Especifique o tipo de protocolo que a sua conta de e-mail usa. Pode seleccionar entre as seguintes alternativas: *Gmail*, *POP3*, ou seleccionar o nome do servidor a partir do menu de contexto no item *Outro* (actualmente, pode usar esta opção se a sua conta for do *Yahoo! JP Mail* ou *Hotmail*). Se não tiver a certeza do tipo de servidor de e-mail que a sua conta usa, tente obter essa informação junto do seu fornecedor de e-mail, ou do seu fornecedor de serviços de Internet.
- **Início de sessão** - Na secção abaixo, introduza a forma exacta do seu *endereço de e-mail* e a respectiva *palavra-passe*. Mantenha a opção de *Início de sessão automático* marcada

para não ter de preencher estes dados constantemente.

- **Testar conta** - Use este botão para testar as informações introduzidas.
- **Restaurar Definições** - Remove rapidamente as informações de endereço de e-mail introduzidas acima.
- **Verificar a existência de novos e-mails a cada ... minutos** - Defina o intervalo de tempo a ser usado para verificar a existência de novas mensagens de e-mail (*no intervalo de 5-120 minutos*) e especifique se, e como, pretende ser informado sobre a recepção da nova mensagem.
- **Permitir alertas de novos e-mails** - Desmarque esta caixa para desactivar as notificações visuais da recepção de novas mensagens de e-mail.
 - o **Reproduzir um som quando for recebido um novo e-mail** - Desmarque esta caixa para desactivar as notificações sonoras de recepção de novas mensagens de e-mail.
 - o **Fechar janela de notificação após 5 segundos** - Marque esta caixa para fechar automaticamente a janela de notificação visual de recepção de novas mensagens de e-mail decorridos 5 segundos.

8.1.8. Informação Meteorológica

O botão **Tempo** apresenta as informações relativas à temperatura actual (*actualizada a cada 3-6 horas*) na localização seleccionada directamente na interface da **Barra de Ferramentas de Segurança AVG**. Clique no botão para abrir um novo painel informativo com uma síntese detalhada do tempo:



Brno, CZ [[alterar localização](#)]

 **26° C** Velocidade do vento 19,31 km/h
Nascer do sol: 05:04
Pôr do Sol: 20:34

 SEX Máxima: 24 °C Mínima: 14 °C	 SÁB Máxima: 25 °C Mínima: 14 °C
--	--

Actualizado 05/20/2011 14:38:10 **YAHOO! NEWS** [Previsão Completa >](#)

De seguida são apresentadas as opções de edição:

- **Alterar localização** - clique no texto **Alterar localização** para abrir uma nova janela com o



nome **Procurar a sua localização**. Introduza o nome da localização pretendida no campo de texto e confirme clicando no botão **Procurar**. De seguida, na lista de todas as localizações com nomes correspondentes, seleccione a localização que pretende. Finalmente, o painel informativo será apresentado novamente com a informação meteorológica da localização seleccionada.

- **Conversor Fahrenheit / Centígrados**- no canto superior direito do painel informativo, pode escolher entre as escalas de graus Fahrenheit ou Centígrados. Consoante a sua selecção, a informação da temperatura será apresentada na escala seleccionada.
- **Previsão Completa** - se quiser uma previsão completa e detalhada, use o link **Previsão Completa** para aceder ao website especializado em meteorologia.

8.1.9. Facebook

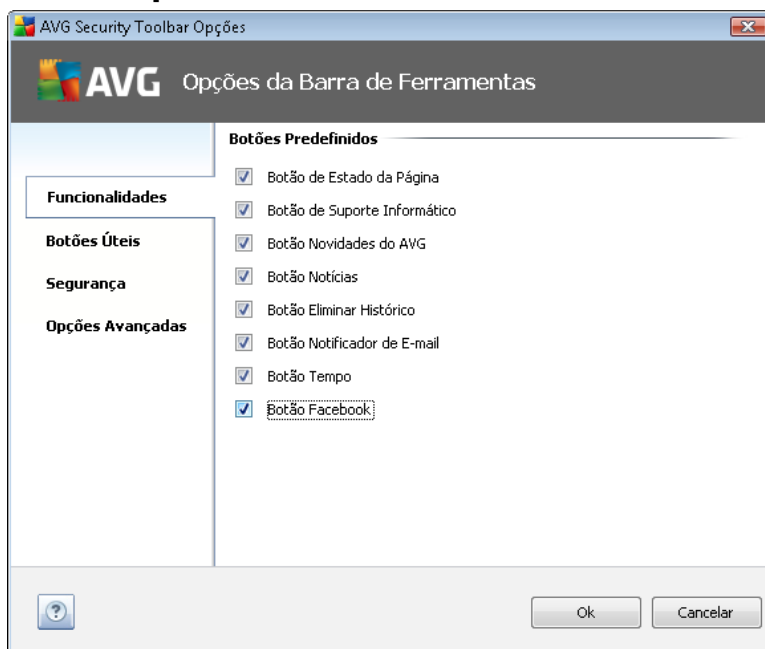
O botão **Facebook** permite-lhe conectar-se à rede social [Facebook](#) directamente a partir da **Barra de Ferramentas de Segurança AVG**. Clique no botão e será apresentada a janela de início de sessão; clique novamente para abrir a janela de **início de sessão no Facebook**. Introduza os seus dados de acesso e prima o botão **Conectar**. Se ainda não tiver uma conta no [Facebook](#), pode criar uma directamente através do link **Registar no Facebook**.

Uma vez concluído o processo de registo no [Facebook](#), será convidado a permitir a aplicação **Extensão Social do AVG**. A funcionalidade desta aplicação é essencial para a ligação barra de ferramentas - [Facebook](#), como tal, é recomendável que permita o seu funcionamento. A ligação ao [Facebook](#) será então activada e o botão do **Facebook** na **Barra de Segurança AVG** passará a disponibilizar o menu de opções padrão do [Facebook](#).

8.2. Opções da Barra de Ferramentas de Segurança AVG

A configuração dos parâmetros da **Barra de Ferramentas de Segurança do AVG** pode ser acedida directamente a partir do painel da **Barra de Ferramentas de Segurança do AVG**. A interface de edição abre a partir do item **AVG / Opções** do menu da barra de ferramentas numa nova janela com a identificação **Opções da Barra de Ferramentas** que está dividida em quatro secções:

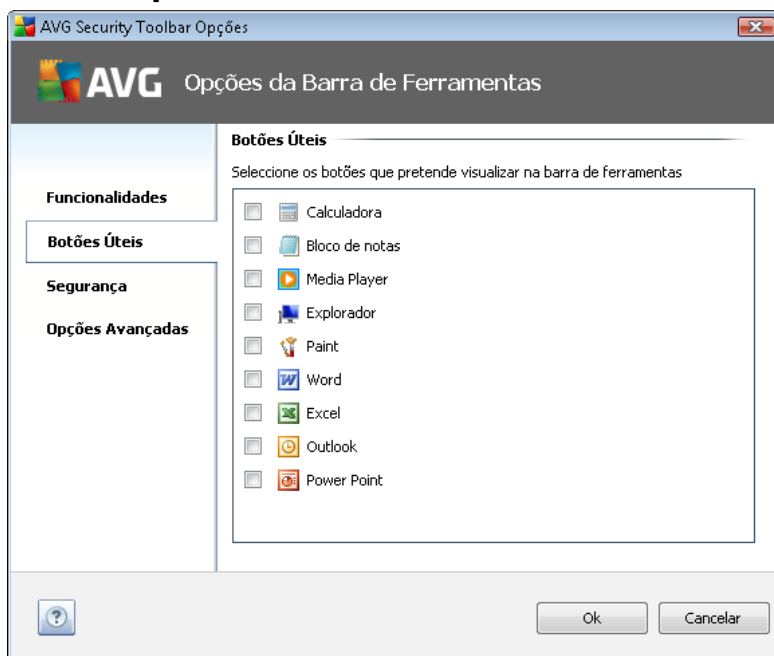
8.2.1. Separador Geral



Neste separador, pode especificar os botões de controlo da barra de ferramentas que devem ser apresentados ou ocultos no painel da **Barra de Ferramentas de Segurança AVG**. Marque uma opção na eventualidade de pretender que o botão respectivo seja apresentado. Consulte mais adiante uma descrição de cada botão da barra de ferramentas:

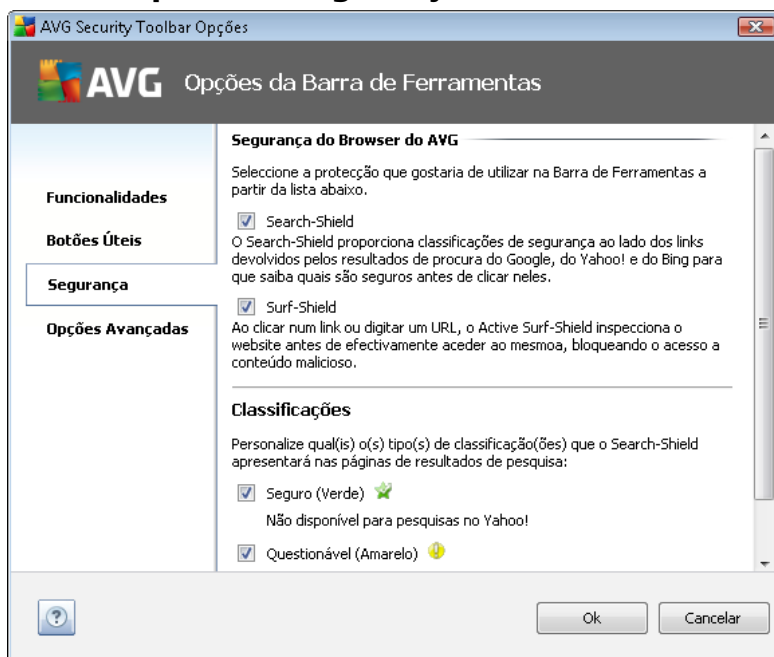
- **Botão de Estado da Página** - o botão oferece a possibilidade de apresentação das informações relativas ao estado de segurança da página actualmente aberta na **Barra de Ferramentas de Segurança AVG**
- **Botão Notícias da AVG** - o botão abre a página que disponibiliza os mais recentes comunicados de imprensa relativos à AVG
- **Botão Notícias** - o botão disponibiliza uma síntese estruturada das notícias actuais da imprensa diária
- **Botão Eliminar Histórico** - este botão permite-lhe Eliminar todo o histórico, ou Eliminar o histórico de pesquisa, Eliminar o histórico de transferências, ou Eliminar cookies directamente a partir do painel da Barra de Ferramentas de Segurança AVG
- **Botão Notificador de E-mail** - o botão permite-lhe ser informado sobre a recepção de novas mensagens de e-mail na interface da **Barra de Ferramentas de Segurança AVG**
- **Botão Tempo** - o botão disponibiliza informações imediatas sobre a situação meteorológica numa localização seleccionada
- **Botão facebook** - o botão oferece acesso directo à rede social [Facebook](https://www.facebook.com/AVG)

8.2.2. Separador Botões Úteis



O separador **Botões Úteis** permite-lhe seleccionar aplicações de uma lista e apresentar os seus ícones na interface da barra de ferramentas. O ícone serve então como atalho para a inicialização imediata da respectiva aplicação.

8.2.3. Separador Segurança



O separador **Segurança** está dividido em duas secções, **Segurança do Browser do AVG** e

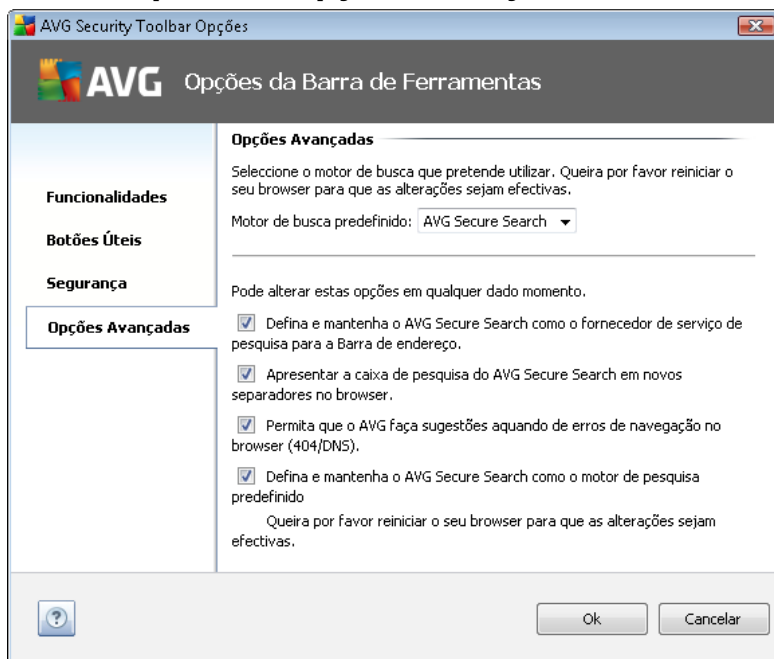


Classificações, onde pode marcar caixas específicas para atribuir à **Barra de Ferramentas de Segurança do AVG** funcionalidades que queira usar:

- **Segurança do Browser do** - seleccione este item para activar ou desactivar o serviço [AVG Search-Shield](#) e/ou [Surf-Shield](#)
- **Classificações** - seleccione os símbolos gráficos usados para a classificação de cada resultado pelo componente [Search-Shield](#) que pretende utilizar:
 - o  a página é segura
 - o  a página é algo suspeita
 - o  a página contém ligações para páginas identificadas como perigosas
 - o  a página contém ameaças activas
 - o  a página não está acessível, e não pôde ser analisada

Marque a opção respectiva para confirmar que pretende ser informado acerca deste nível de ameaça específico. No entanto, não é possível desactivar a apresentação da marca vermelha atribuída para páginas que contenham ameaças activas e perigosas. ***Mais uma vez, é recomendável que mantenha a configuração predefinida pelo fornecedor do programa a menos que tenha uma razão válida para a alterar.***

8.2.4. Separador Opções Avançadas





No separador **Opções Avançadas** seleccione primeiro o motor de busca que pretende utilizar por predefinição. Tem a opção de *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* e *Yahoo! JP*. Uma vez alterado o motor de busca predefinido, queira reiniciar o seu browser para que a alteração produza efeito.

Pode ainda activar ou desactivar outras definições específicas da **Barra de Ferramentas de Segurança AVG** (a legenda listada é referente às predefinições do *AVG Secure Search (powered by Google)*):

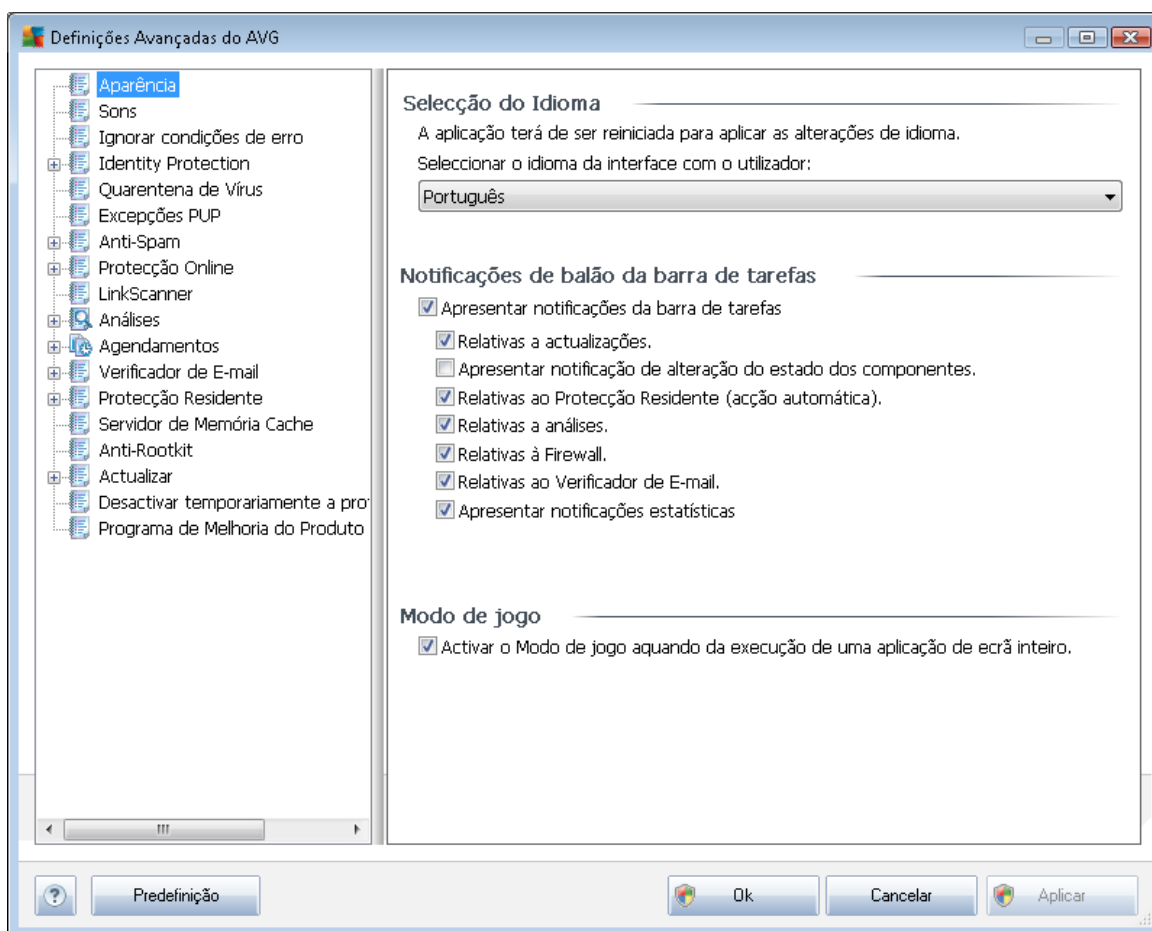
- **Defina e mantenha o AVG Secure Search (powered by Google) como o fornecedor de serviço de pesquisa para a Barra de endereço** - se marcada, esta opção permite-lhe digitar uma palavra-chave de pesquisa directamente na barra de endereço do seu browser e o serviço do Google será usado automaticamente para procurar websites relevantes.
- **Permitir que o AVG faça sugestões aquando de erros de navegação (404/DNS)** - se for parar a uma página inexistente durante a navegação Web, ou a uma página que não pode ser apresentada (erro 404), será automaticamente redireccionado para uma página Web que lhe disponibiliza opções de selecção entre páginas alternativas com associação temática.
- **Defina e mantenha o AVG Secure Search (powered by Google) como o motor de pesquisa predefinido** - o Google é o motor de pesquisa predefinido para pesquisas na Internet feitas a partir da **Barra de Ferramentas de Segurança AVG** e, com a activação desta opção, pode ainda tornar-se o motor de pesquisa predefinido do seu browser.

9. Definições Avançadas do AVG

A janela de configuração avançada do **AVG Internet Security 2011** 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. Selecciona o componente ao qual pretende alterar a configuração (*ou a parte específica deste*) para abrir a janela de edição na janela na secção do lado direito.

9.1. Aparência

O primeiro item da árvore de navegação, **Aparência**, refere-se às definições gerais da [Interface do utilizador do AVG](#) e a algumas opções elementares do comportamento da aplicação:

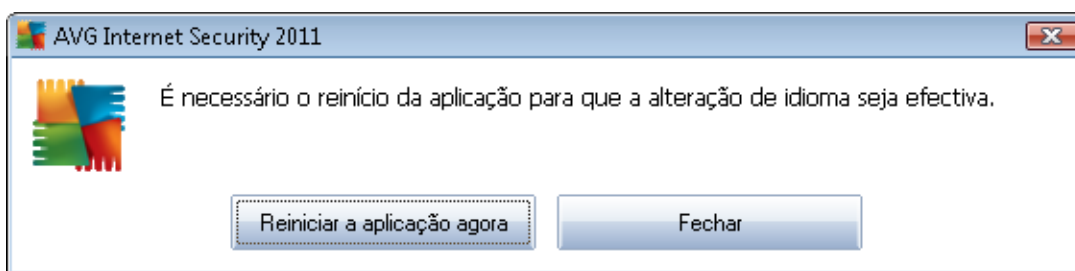


Seleção do Idioma

Na secção **Seleção de Idioma** pode escolher o idioma que pretende a partir do menu de opções; o idioma será então utilizado para toda a [Interface do Utilizador do AVG](#). 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 instalado por predefinição*). No entanto, para concluir a alteração de idioma da aplicação terá de

reiniciar a interface do utilizador; siga os passos seguintes:

- Selecciona o idioma da aplicação pretendido e confirme a selecção clicando no botão **Aplicar** (canto inferior direito)
- Prima o botão **OK** para confirmar
- É apresentada uma nova janela a informá-lo de que a alteração do idioma da interface do utilizador do AVG requer a reinicialização da aplicação:



Notificações de balão da barra de tarefas

Nesta secção pode suprimir a apresentação de balões de notificação relativos ao estado da aplicação na barra de notificação. Os balões de notificação serão apresentados por predefinição e é recomendável que mantenha esta configuração! Os balões de notificação normalmente informam acerca de alguma alteração de estado dos componentes do AVG, e deve ter atenção aos mesmos!

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), pode definir e especificar as suas preferências marcando/desmarcando as seguintes opções:

- **Apresentar notificações da barra de notificações do sistema** - este item está seleccionado por predefinição (*activado*), e as notificações são apresentadas. Desmarque este item para desactivar por completo a apresentação de balões de notificação. Quando activado, pode ainda especificar quais as notificações específicas que devem ser apresentadas.
 - o **Apresentar notificações da barra de notificação relativas a actualizações** - decida se as informações relativas ao início, progresso e finalização da actualização do AVG deverão ser apresentadas;
 - o **Apresentar notificações relativas a alterações de estado dos componentes** - decida se as informações relativas à actividade/inactividade dos componentes, ou os seus possíveis problemas deverão ser apresentadas. Ao notificar de um estado de erro de um componente, esta opção é equivalente à função informativa do [ícone da barra de notificação do sistema](#) (mudança de cor) que notifica de problemas em qualquer componente do AVG.
 - o **Apresentar notificações da barra de notificação relativas à Protecção Residente (acção automática)** - 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 [Restauração automática](#) da Protecção Residente estiver activada);

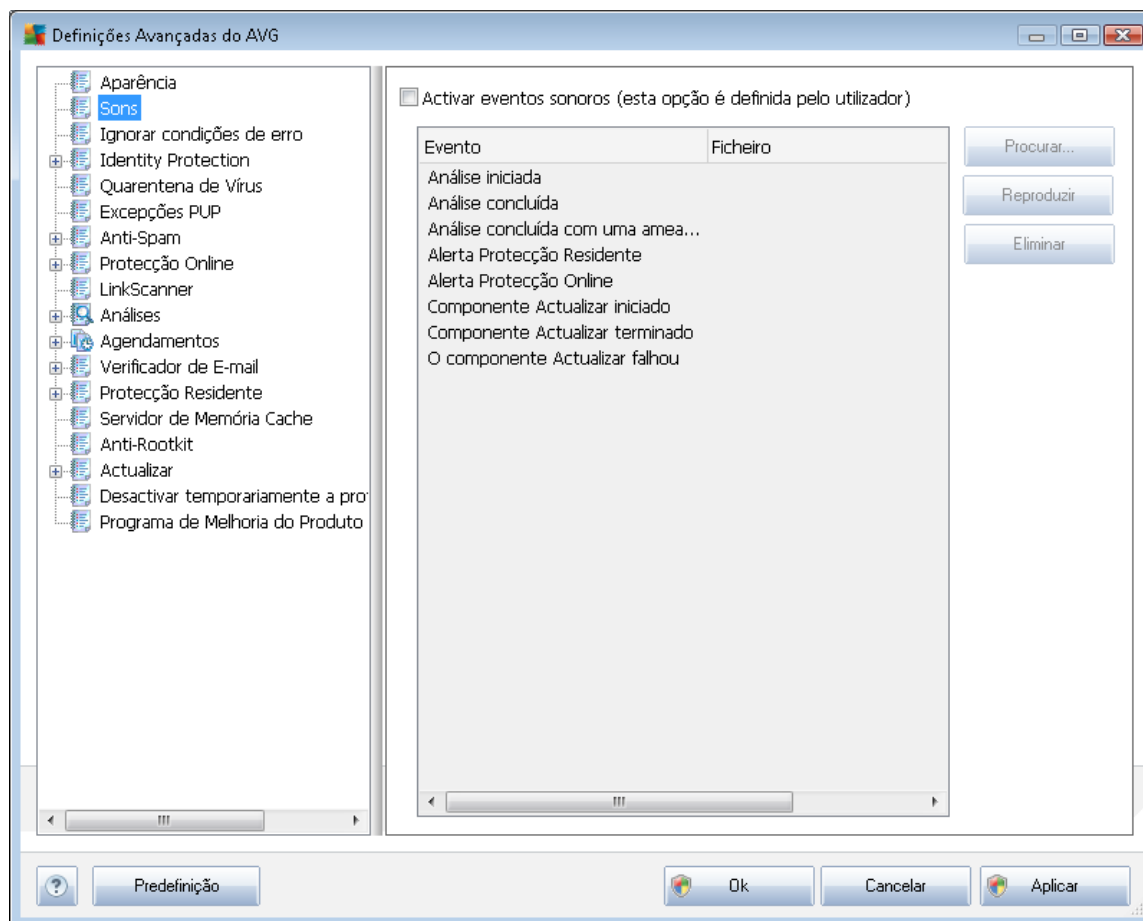
- o **Apresentar notificações da barra de notificação relativas a [análises](#)** - decida se as informações relativas ao início automático da análise agendada, o seu progresso e resultados deverão ser apresentadas;
- o **Apresentar notificações da barra de notificação relativas à [Firewall](#)** - decida 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;
- o **Apresentar notificações da barra de notificação relativas ao [Verificador de E-mail](#)** - decida se as informações aquando da análise de todas as mensagens de e-mail a receber e a enviar deverão ser apresentadas.
- o **Apresentar notificações estatísticas** - mantenha a opção marcada para permitir a apresentação de notificações estatísticas na barra de tarefas.

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*).

9.2. Sons

Na janela **Sons** pode especificar se quer ser informado de acções específicas do AVG por meio de uma notificação sonora. Se assim for, marque a opção **Activar eventos sonoros** (*desactivado por predefinição*) para activar a lista de acções do AVG:

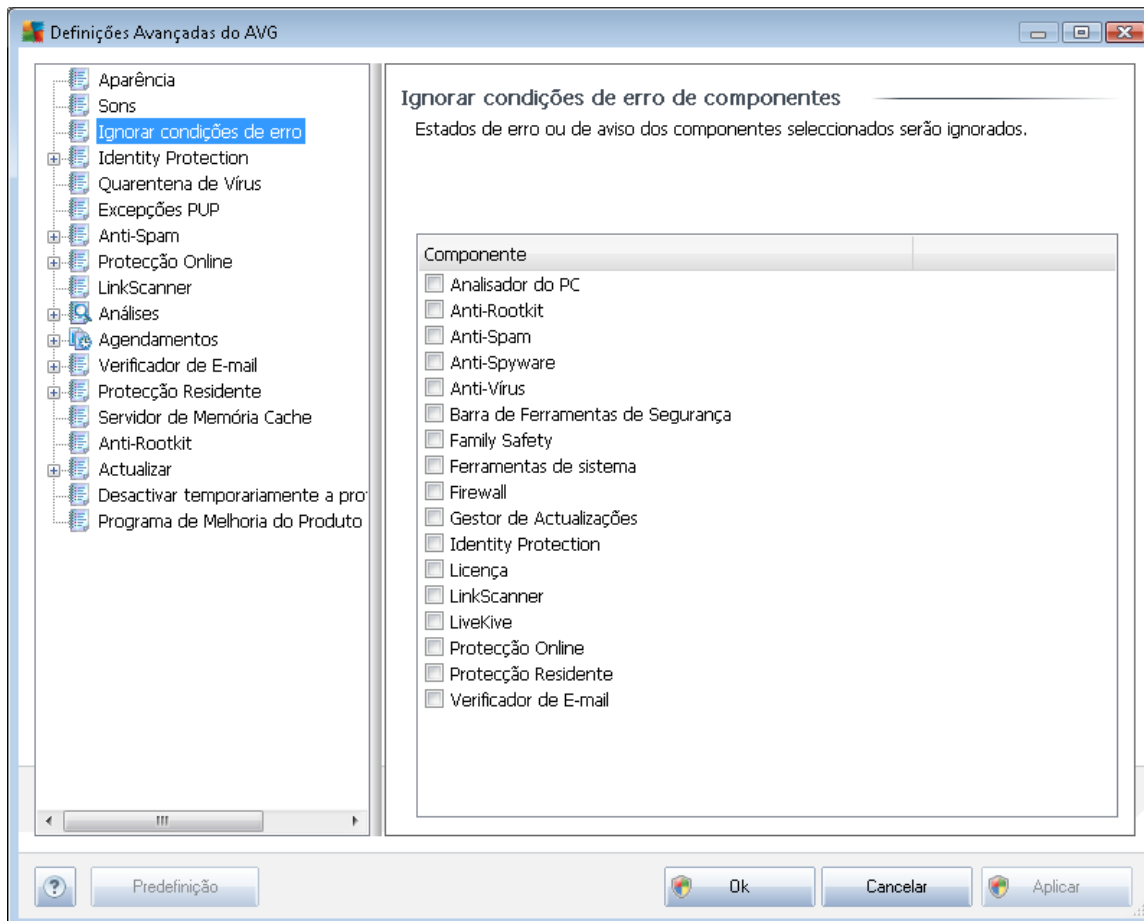


Depois, seleccione o evento respectivo a partir da lista procure (**Procurar**) no seu disco um som adequado que pretenda atribuir a este evento. Para ouvir o som seleccionado, realce o evento na lista e prima o botão **Reproduzir** . Use o botão **Eliminar** para remover o som atribuído a um evento específico.

Nota: Só são suportados sons *.wav!

9.3. Ignorar Condições de Erro

Na janela ***Ignorar condições de erro de componentes*** pode seleccionar todos 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 notificação** - 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 notificação 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

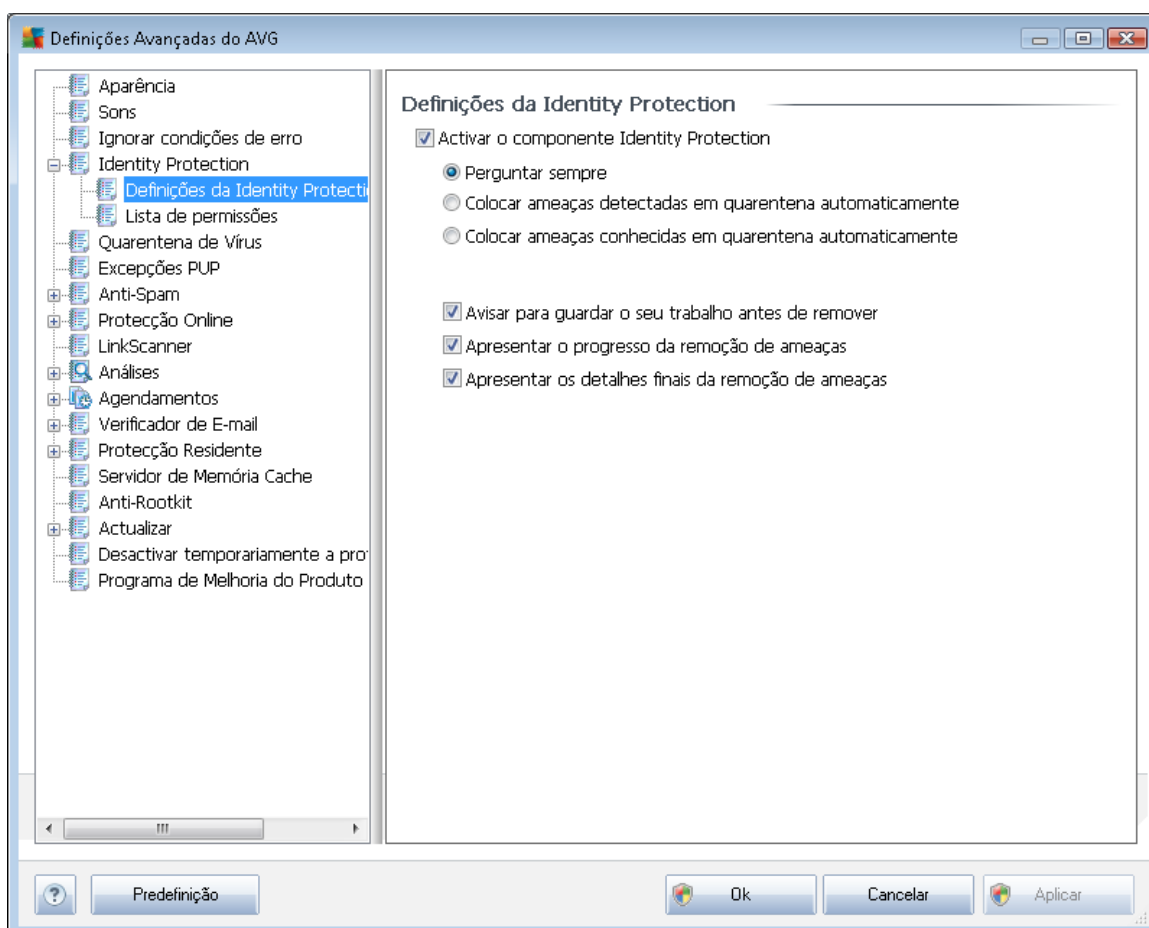
deliberadamente, e tem consciência do risco potencial. Em simultâneo, uma vez apresentado a cinzento, o ícone não poderá apresentar quaisquer outros erros que possam surgir.

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 de **Ignorar estado do componente** também está disponível para componentes específicos directamente a partir da [síntese dos componentes na janela principal do AVG](#).

9.4. Protecção de Identidade

9.4.1. 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:

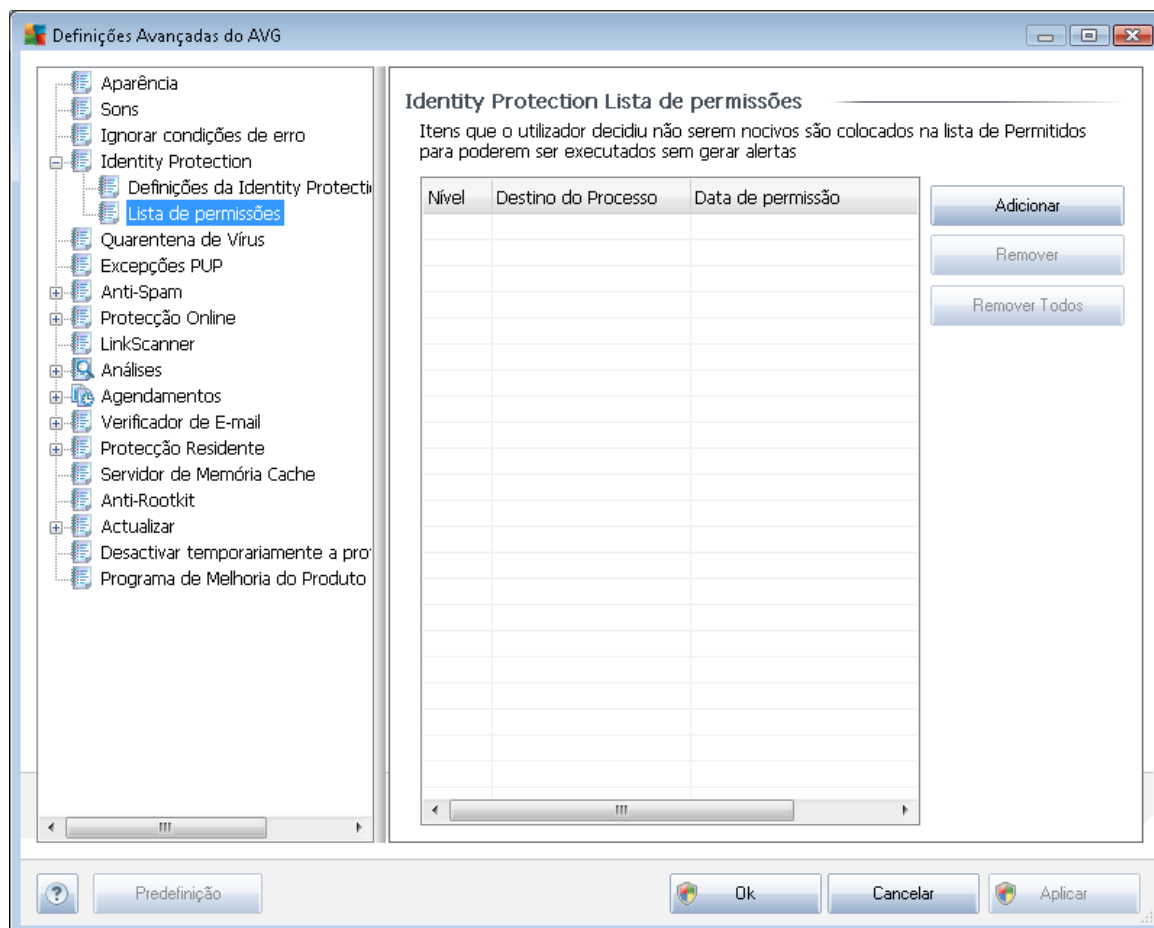
- **Perguntar sempre** (activado por predefinição) - quando uma ameaça for detectada, ser-lhe-á solicitado que decida se a mesma deve ser movida para a quarentena para garantir que não são removidas aplicações que pretende ter em execução.
- **Colocar ameaças detectadas em quarentena automaticamente** - marque esta caixa para definir que pretende que todas as ameaças eventualmente detectadas sejam movidas para o espaço seguro da [Quarentena de Vírus do AVG](#) 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 AVG](#).

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.
- **Mostrar o progresso de remoção de malware** - (activado como 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 detalhes finais da remoção de malware** - (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.*).

9.4.2. 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:



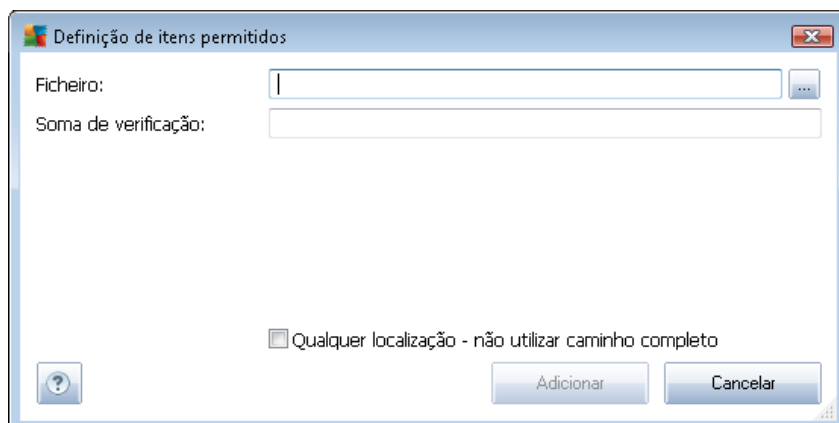
A **Lista de permissões da Protecção de Identidade** disponibiliza as seguintes informações sobre cada aplicação:

- **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:



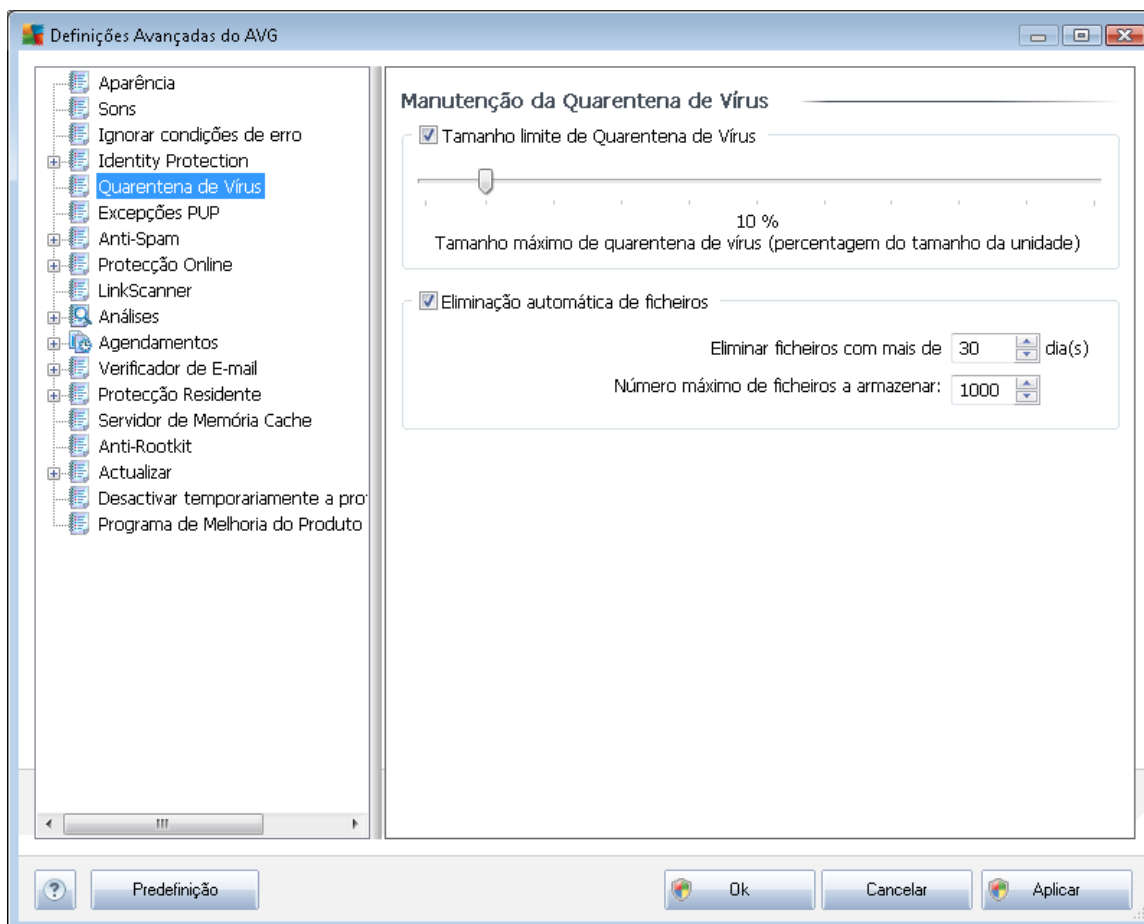
o **Ficheiro** - digite o caminho completo do ficheiro (*aplicação*) que pretende marcar como excepção

o **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.

o **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

9.5. Quarentena de Vírus



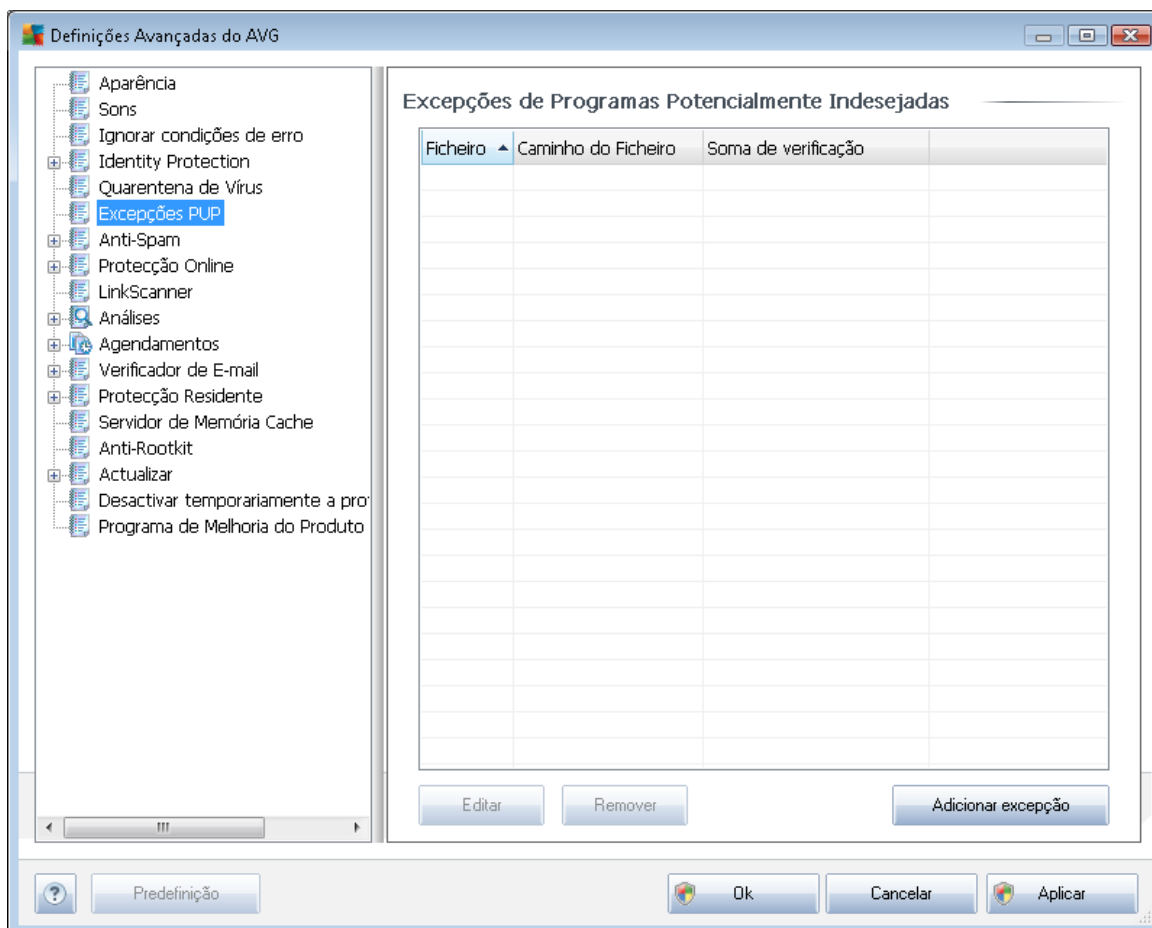
A janela **Manutenção da Quarentena de Vírus** permite-lhe definir vários parâmetros em relação à administração dos objectos armazenados na [Quarentena de Vírus](#):

- **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**)

9.6. Excepções PUP

O **AVG Internet Security 2011** 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 comunicado pelo AVG 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 **Exceções 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:

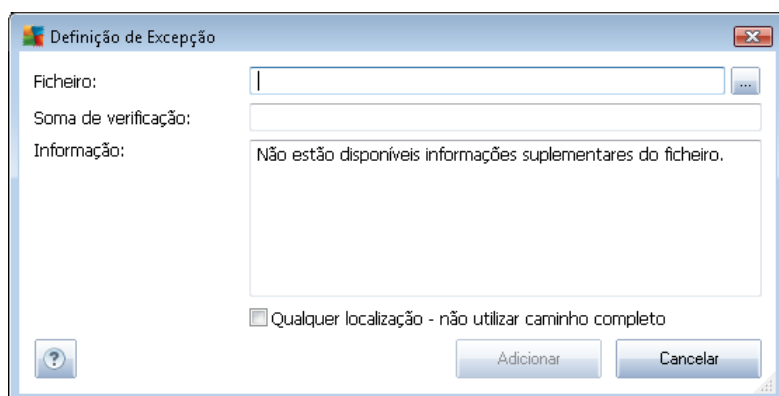
- **Ficheiro** - faculta o nome da aplicação respectiva
- **Localização do Ficheiro** - apresenta a localização da aplicação
- **Soma de verificação** - apresenta a 'assinatura' única do ficheiro seleccionado. Esta soma de verificação é uma cadeia de caracteres gerada automaticamente, que permite ao 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

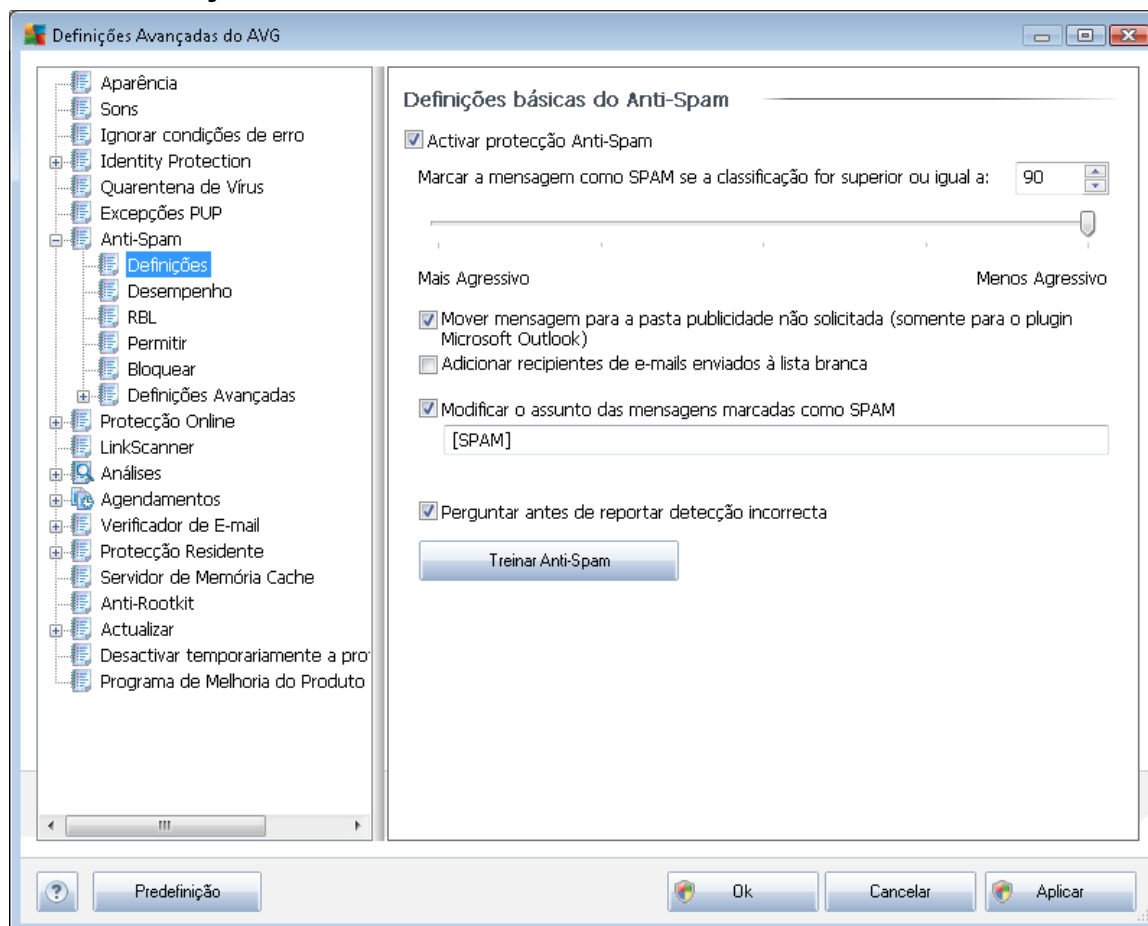
- **Remover** - elimina o item seleccionado da lista de excepções
- **Adicionar excepção** - abre uma janela de edição onde pode definir os parâmetros da nova excepção a ser criada:



- o **Ficheiro**- digite o caminho completo do ficheiro que pretende marcar como excepção
- o **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.
- o **Informação do ficheiro** - apresenta qualquer informação adicional disponível acerca do ficheiro (*informações de licença/versão, etc.*)
- o **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*).

9.7. Anti-Spam

9.7.1. Definições



Na janela **Definições básicas 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.

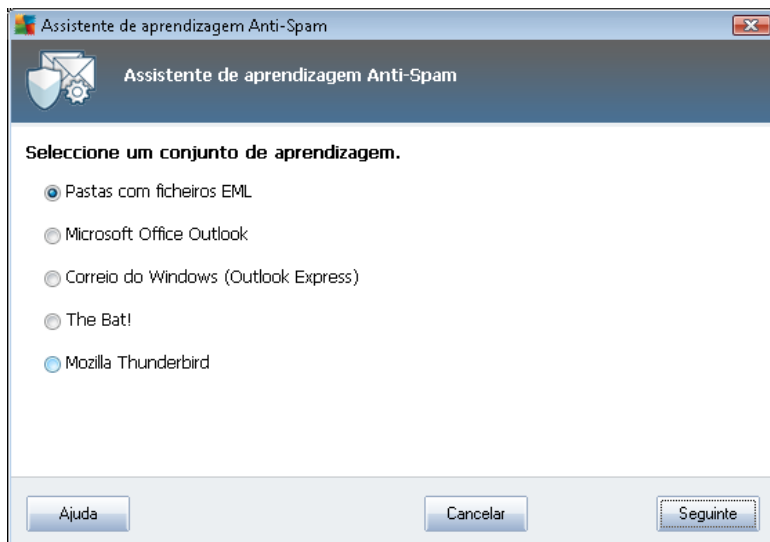
Na janela **Definições básicas do componente Anti-Spam** pode definir a forma como os e-mails detectados como [spam](#) deverão ser tratados:

- **Mover mensagem para a pasta publicidade não solicitada** - seleccionar 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;
- **Adicionar remetentes de e-mail à [lista branca](#)** - seleccione esta caixa para confirmar que todos os remetentes de mensagens de e-mail são de confiança, e que todas as mensagens de e-mail enviadas das suas contas de e-mail podem ser entregues;
- **Modificar o assunto das mensagens marcadas como SPAM** - seleccione 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 concordado em 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:

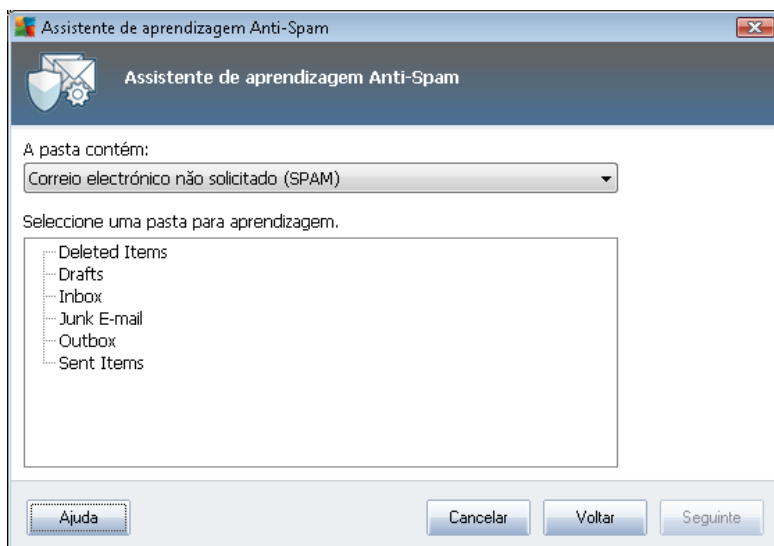
- **Um cliente de e-mail específico** - se usar um dos clientes de e-mail listados (*MS Outlook, Outlook Express, The Bat!*), basta seleccionar a opção respectiva
- **Pasta com ficheiros EML** - Se utilizar outro programa de e-mail, deverá primeiro guardar as mensagens para uma pasta específica (no *formato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

Selecione 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



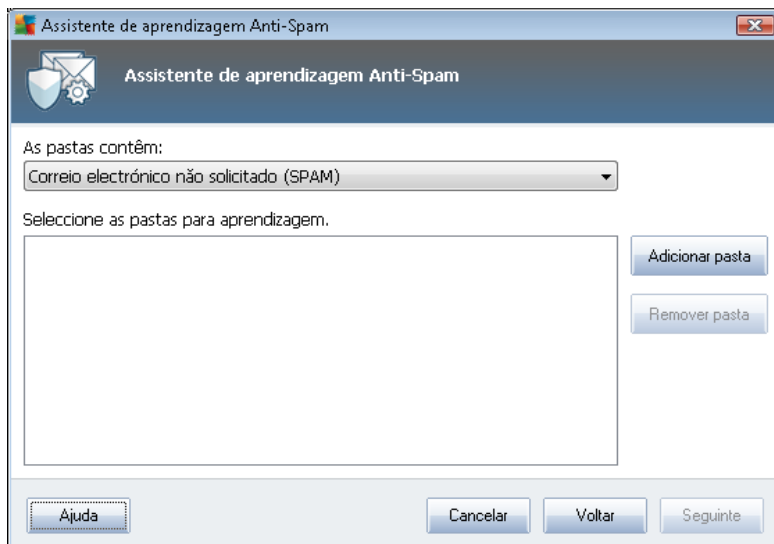
Nesta janela, por favor selecione a pasta que contém as mensagens que pretende utilizar para a aprendizagem. Clique no botão **Adicionar pasta** para localizar a pasta com os ficheiros .eml (*mensagens de e-mail guardadas*). A pasta seleccionada será então apresentada na janela.

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

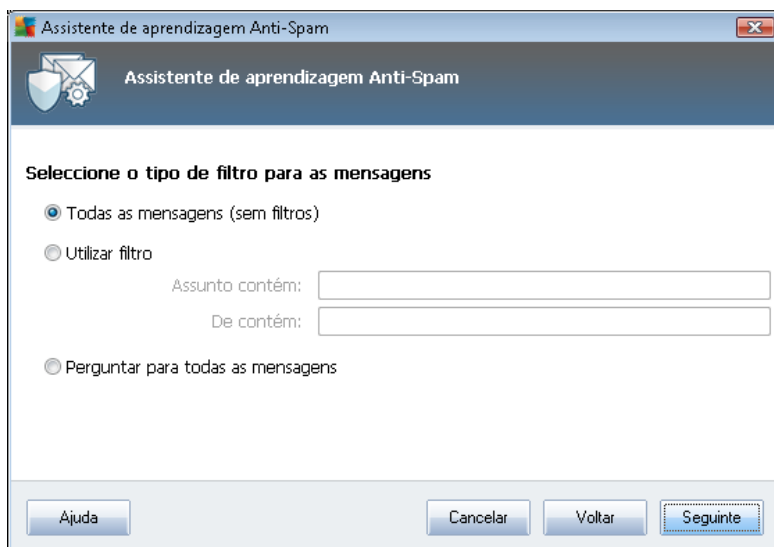
Assim que confirmar uma das opções, é apresentada uma nova janela.



Atenção: No caso do Microsoft Office Outlook, será solicitado que selecione 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 selecione-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.



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)**.

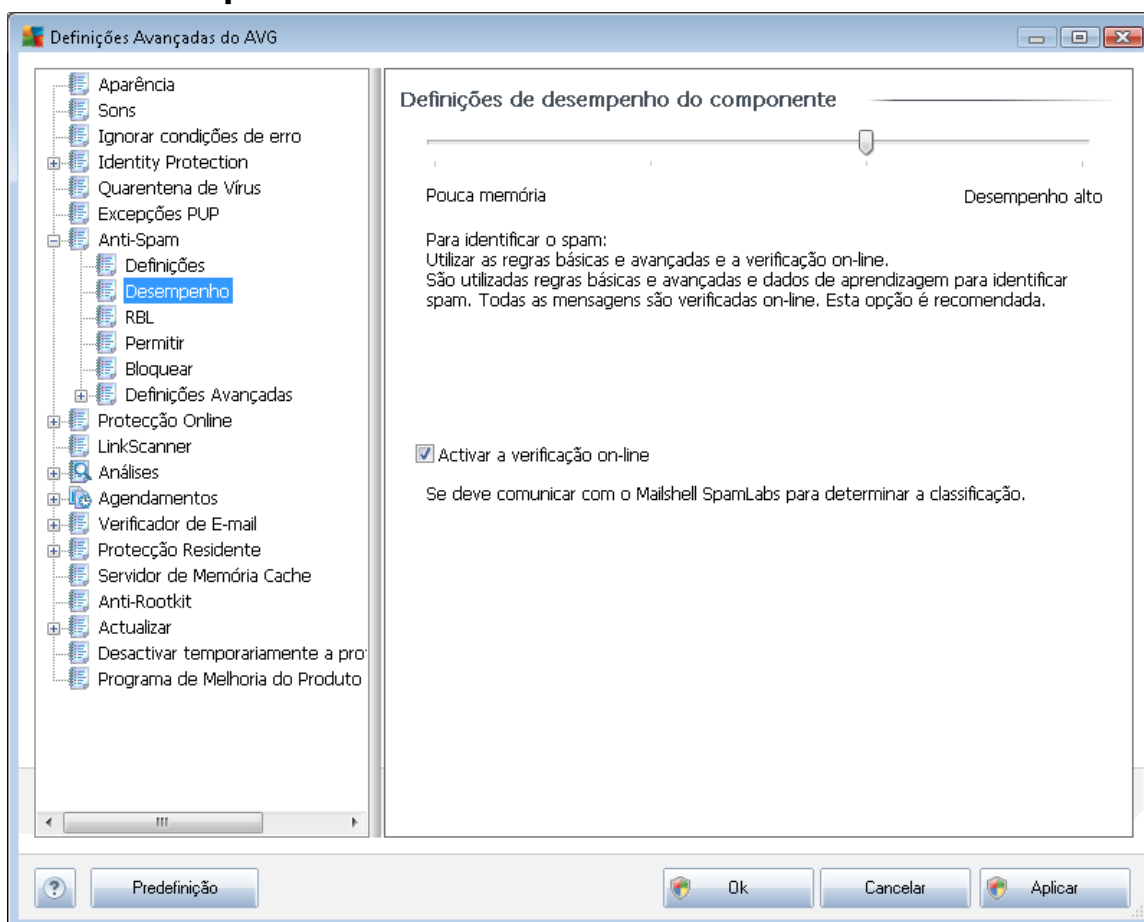
Se não tiver a certeza em relação às mensagens contidas na pasta, e se quiser que o Assistente o inquiria em relação a cada mensagem (para que possa determinar se a mensagem deve ser utilizada para aprendizagem ou não), seleccione a opção **Perguntar para cada mensagem**.

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 exactamente aos critérios introduzidos serão usadas para a aprendizagem, sem mais qualquer solicitações.

Atenção!: Quando preenche ambos os campos de texto, os endereços que correspondam a apenas uma das duas condições serão igualmente utilizados.

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.

9.7.2. Desempenho





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

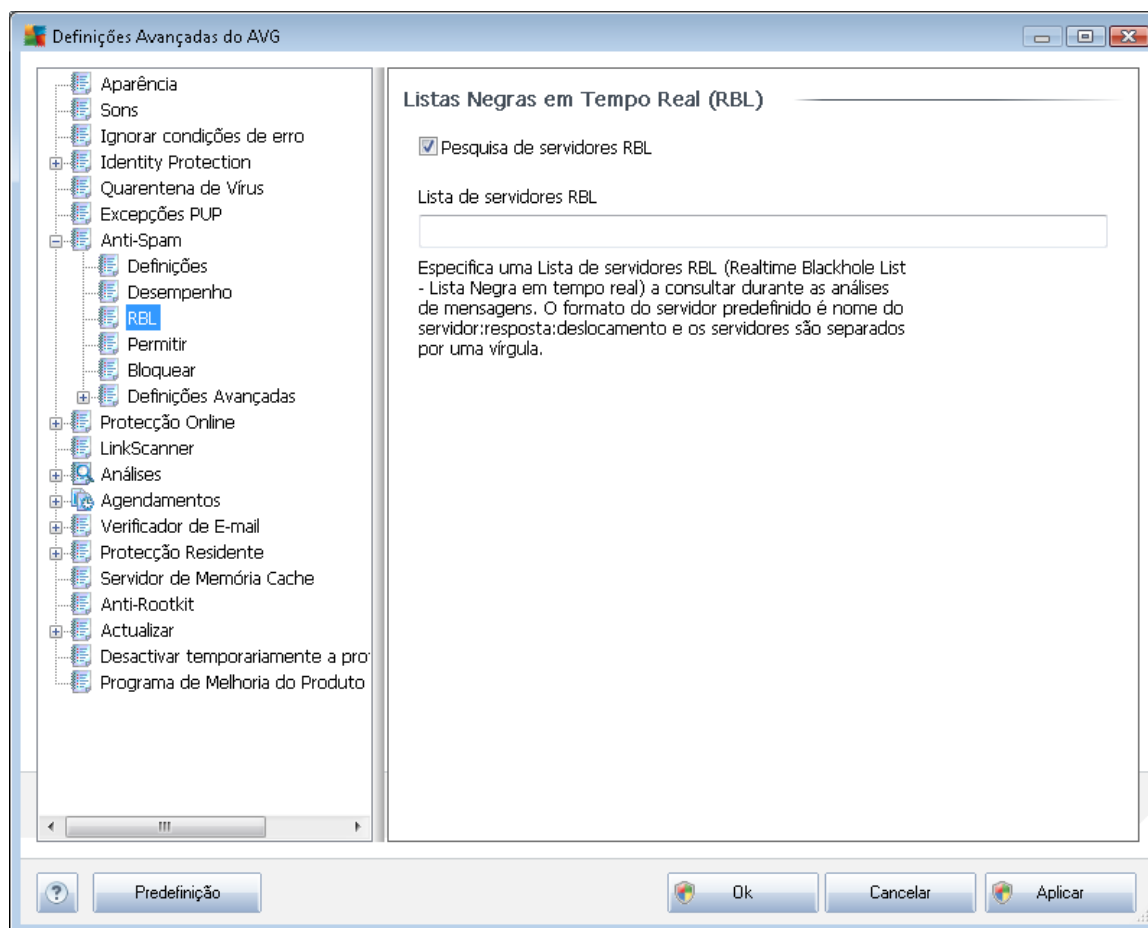
- **Memória baixa** - não serão utilizadas quaisquer regras durante o processo de análise para identificar [spam](#). Serão utilizados apenas dados de aprendizagem para identificação. Este modo não é recomendado para uso comum, a não ser que o hardware do computador seja muito fraco.
- **Alto desempenho** - este modo requer uma grande quantidade de memória. Durante o processo de análise para identificar [spam](#), serão utilizadas as seguintes características: regras e cache de base de dados 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!

9.7.3. RBL

O item **RBL** abre uma janela de edição apelidada **Realtime Blackhole Lists**:



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

O servidor RBL (*Real-time Blackhole List*) é um servidor DNS com uma base de dados extensiva de remetentes de spam conhecidos. Quando esta funcionalidade está ligada, todas as mensagens de e-mail serão verificadas de acordo com a base de dados do servidor RBL e serão assinaladas como [spam](#) se forem idênticas a qualquer uma das entradas da base de dados. As bases de dados dos servidores RBL contêm identificadores de [spam](#) actualizados ao minuto, para garantir a melhor e mais rigorosa detecção de spam. Esta funcionalidade é particularmente útil para utilizadores que recebem grandes quantidades de spam que o componente [Anti-Spam](#) normalmente não consegue detectar.

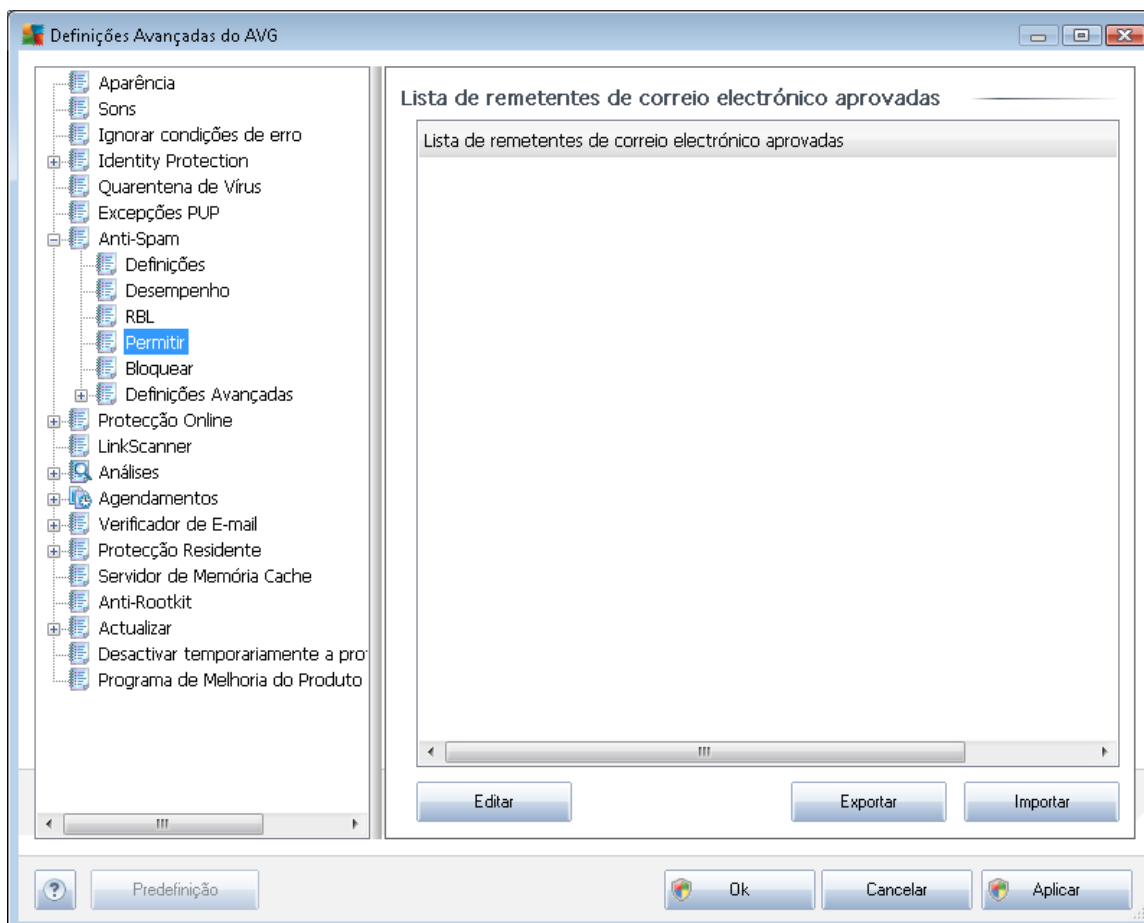
A **lista de servidores RBL** permite-lhe definir localizações específicas de servidores RBL.

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

Não são enviados dados pessoais para o servidor!

9.7.4. Lista Branca

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 como [spam](#).



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

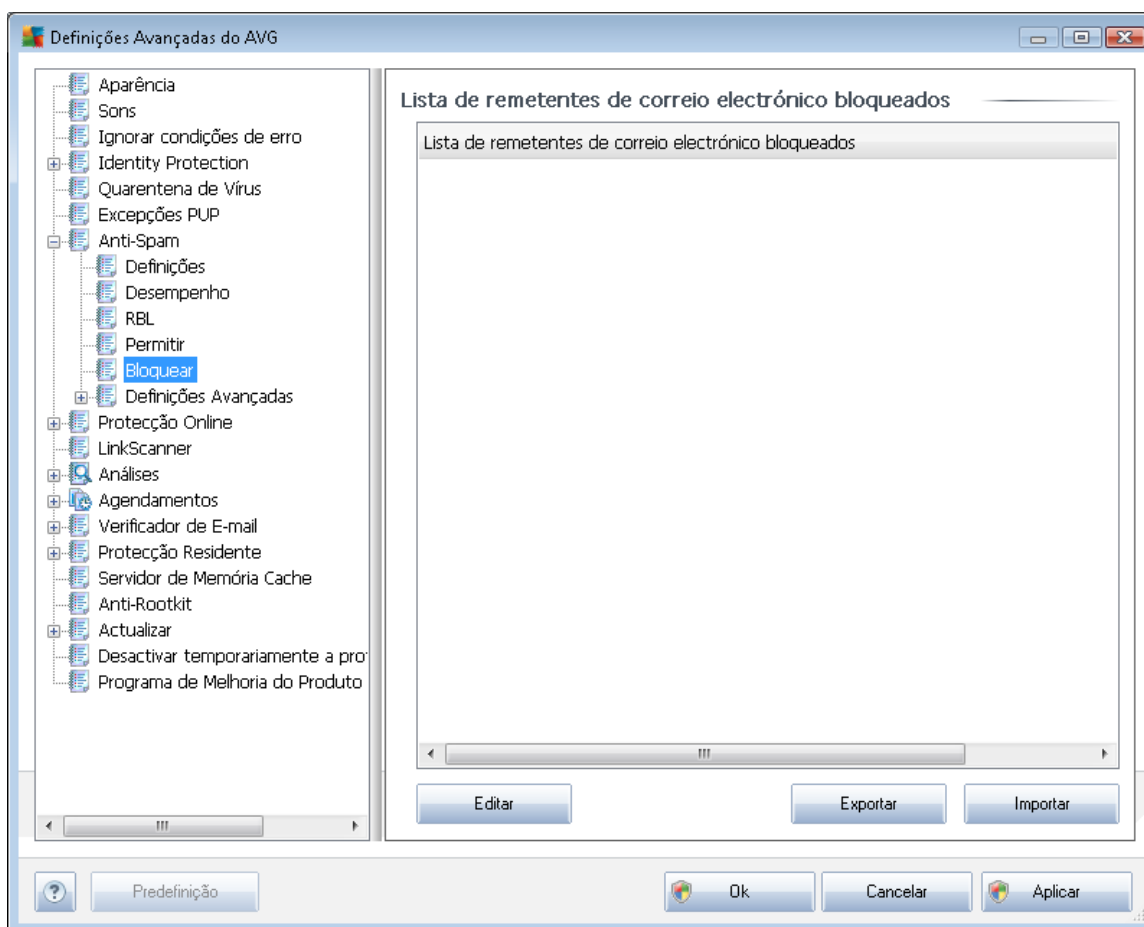
Quando já tiver uma lista de remetentes/ou nomes de domínio preparada, pode introduzi-los por meio de um dos seguintes métodos: via introdução directa de cada endereço de correio electrónico ou importando toda a lista de endereços de uma vez. Estão disponíveis os seguintes botões de controlo:

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

9.7.5. Lista Negra

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

9.7.6. Definições Avançadas

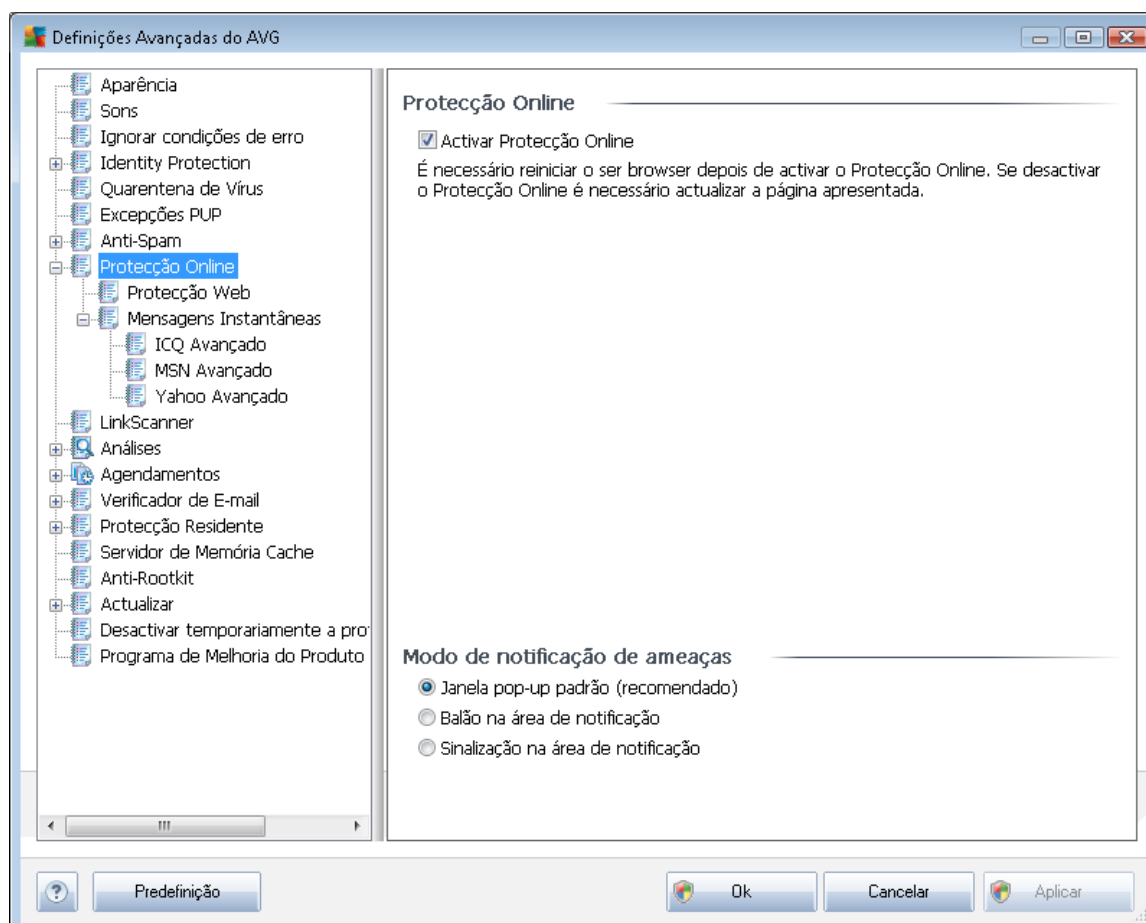
O separador Definições Avançadas contém opções de definições suplementares para o componente Anti-Spam. Estas definições são destinadas a utilizadores experientes, regra geral administradores de redes que precisem de configurar detalhadamente a protecção anti-spam para uma protecção superior dos servidores 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 específica 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

9.8. Protecção Online



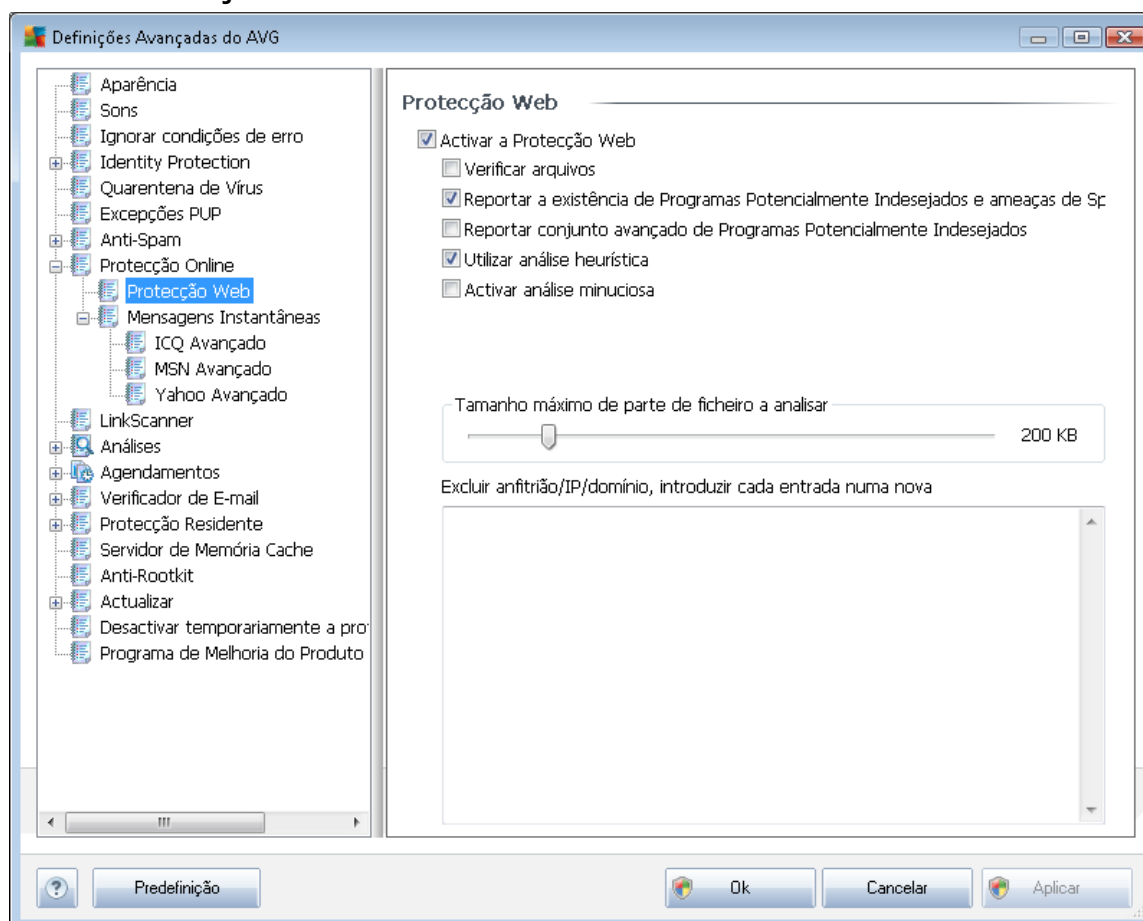
A janela **Protecção Online** permite-lhe activar/desactivar na íntegra o componente **Protecção Online** através da opção **Activar a Protecção Online** (activada por predefinição). Para mais definições avançadas deste componente por favor continue para as janelas subsequentes conforme listado na árvore de navegação:

- [Protecção na Internet](#)
- [Mensagens Instantâneas](#)

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 notificação.

9.8.1. Protecção na Internet



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:
 - o **Verificar arquivos** - (desactivado por predefinição): analisar o conteúdo de arquivos possivelmente incluídos na página www a ser apresentada.
 - o **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.
 - o **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.

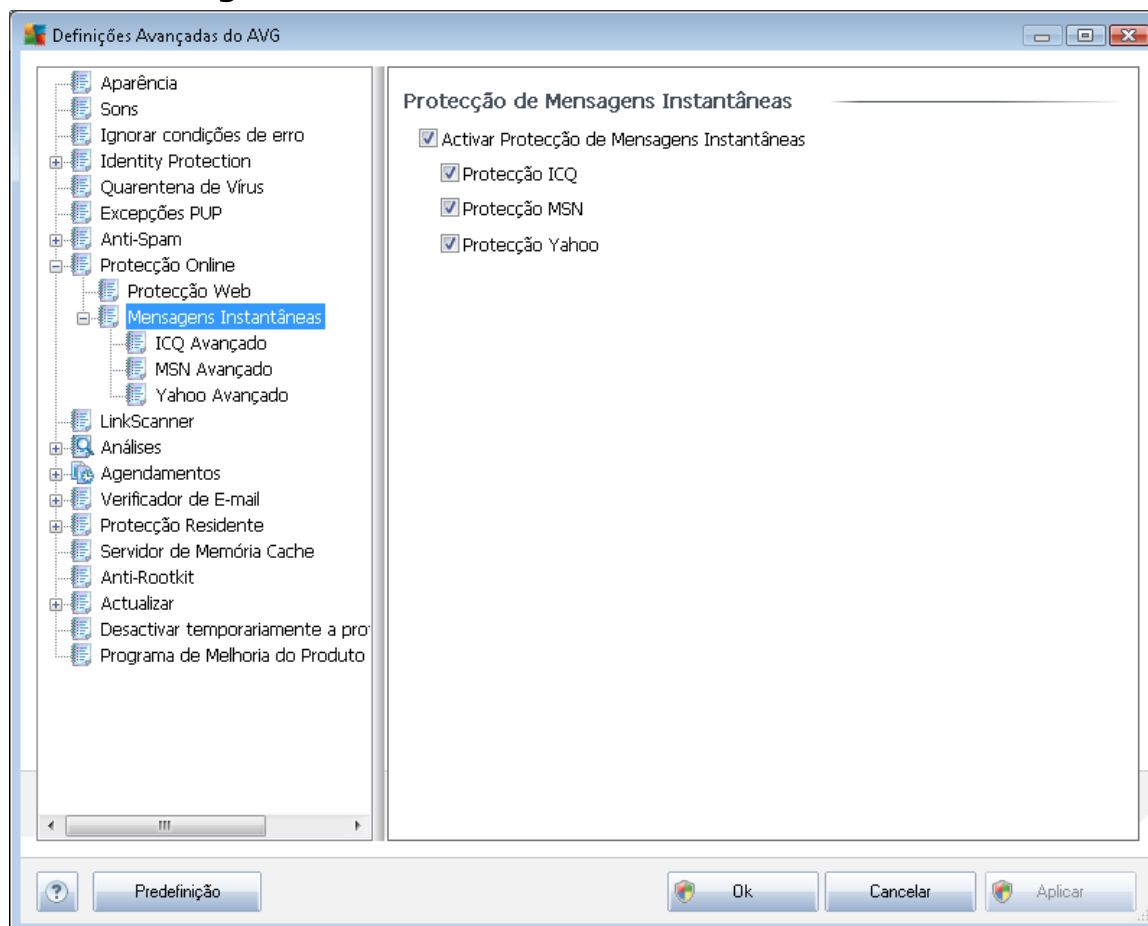
o **Utilizar a análise heurística**- (*activado por predefinição*): analisar o conteúdo da página a ser apresentada utilizando o método [análise heurística](#)(*emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual*).

o **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.

o **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.

o **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.

9.8.2. Mensagens Instantâneas

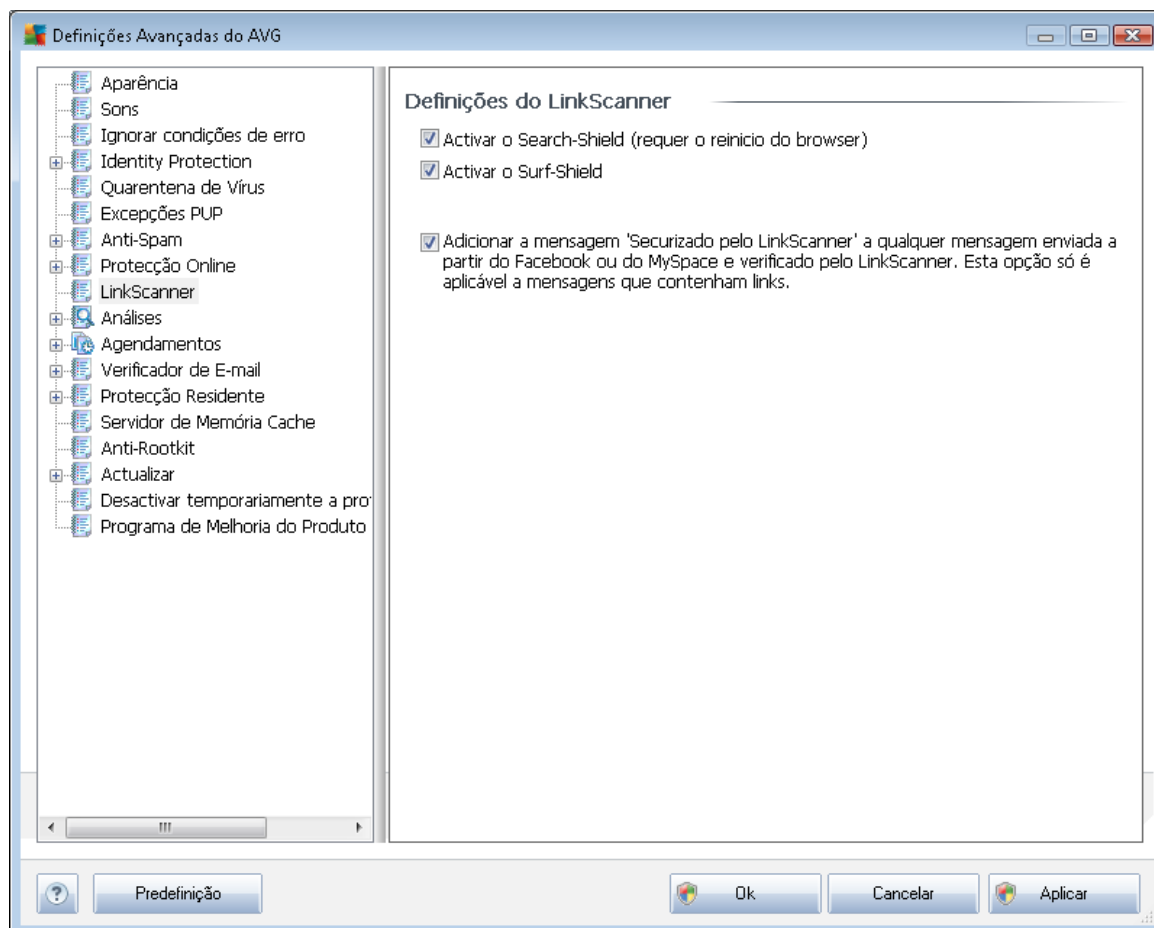


Na janela **Protecção de Mensagens Instantâneas** pode editar as definições dos componentes da **Protecção Online** relativos à análise de mensagens instantâneas. São actualmente suportados os três programas de mensagens instantâneas seguintes: **ICQ**, **MSN** e **Yahoo** - marque o item respectivo para cada um deles se pretender que a **Protecção Online** verifique as comunicações on-line pela existência de vírus.

Para mais especificações de utilizadores permitidos/bloqueados pode visualizar e editar a janela respectiva (**ICQ Avançado**, **MSN Avançado**, **Yahoo Avançado**) e especificar a **Lista Branca** (lista de utilizadores que poderão comunicar consigo) e **Lista Negra** (utilizadores que deverão ser bloqueados).

9.9. 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*).
- **Adicionar 'Analisado pelo LinkScanner'...** - marque este item para confirmar que pretende introduzir o aviso de certificação sobre a verificação do **LinkScanner** em todas as mensagens que contenham hiperligações e sejam enviadas a partir das redes sociais Facebook e MySpace.

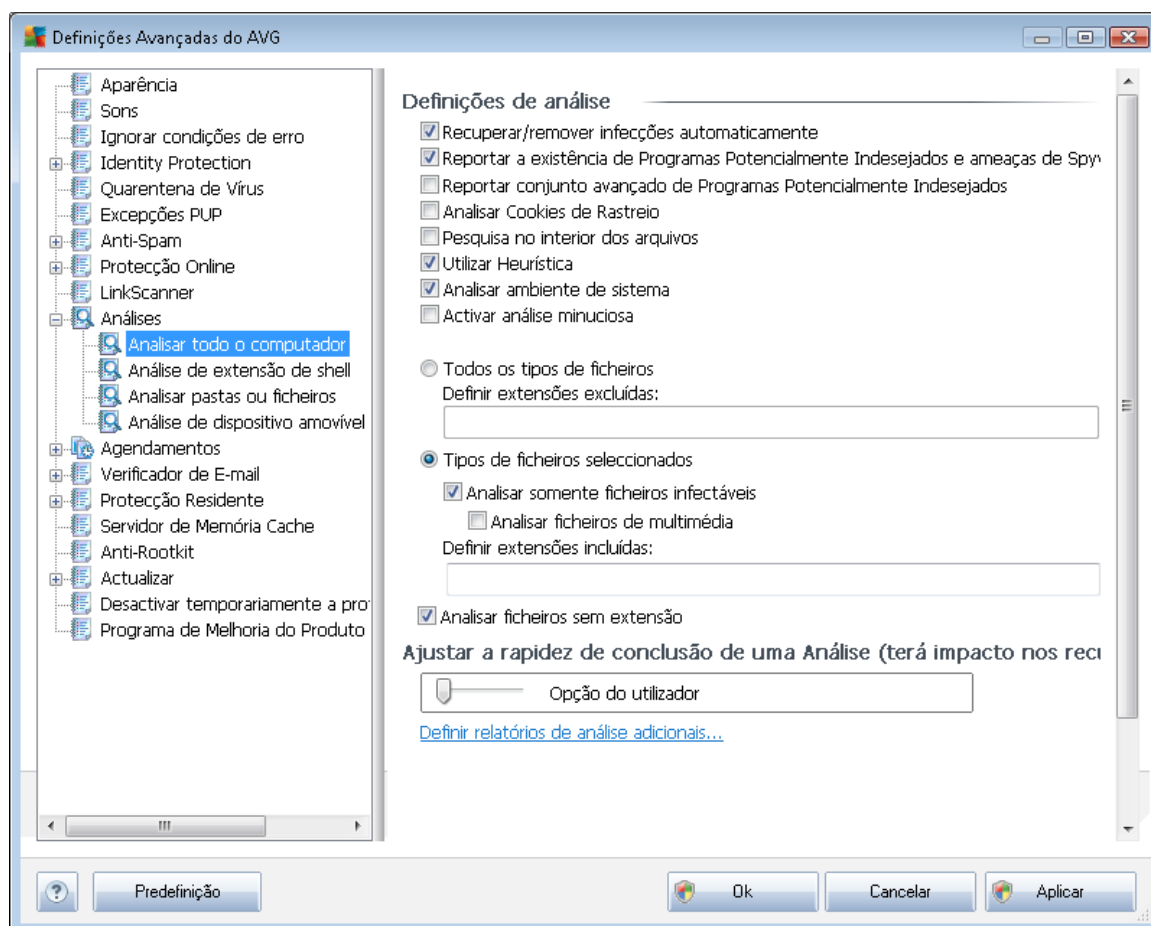
9.10. Análises

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
- [Analisar Ficheiros e Pastas Específicos](#) - análise padrão predefinida de áreas seleccionadas do seu computador
- [Análise de Dispositivo Amovível](#) - análise específica de dispositivos amovíveis conectados ao seu computador

9.10.1. Analisar 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 infecção automaticamente** (activado por predefinição) - se for detectado um vírus durante a análise, o ficheiro 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 Rastreo** (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, rastreo, e manutenção de informação específica 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.

Além disso deve decidir se pretende que sejam analisados

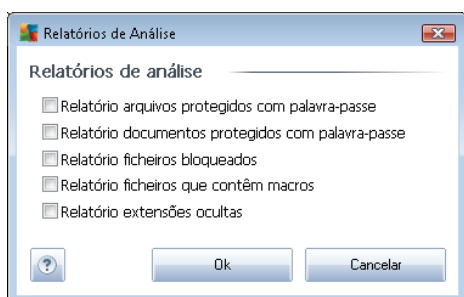
- **Todos os tipos de ficheiros** com a possibilidade de definir excepções para a análise ao providenciar uma listagem extensões de ficheiro separadas por vírgula (*uma vez guardada, as vírgulas mudam para ponto e vírgula*) que não devem ser analisadas;
- **Tipos de ficheiros seleccionados** - pode especificar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

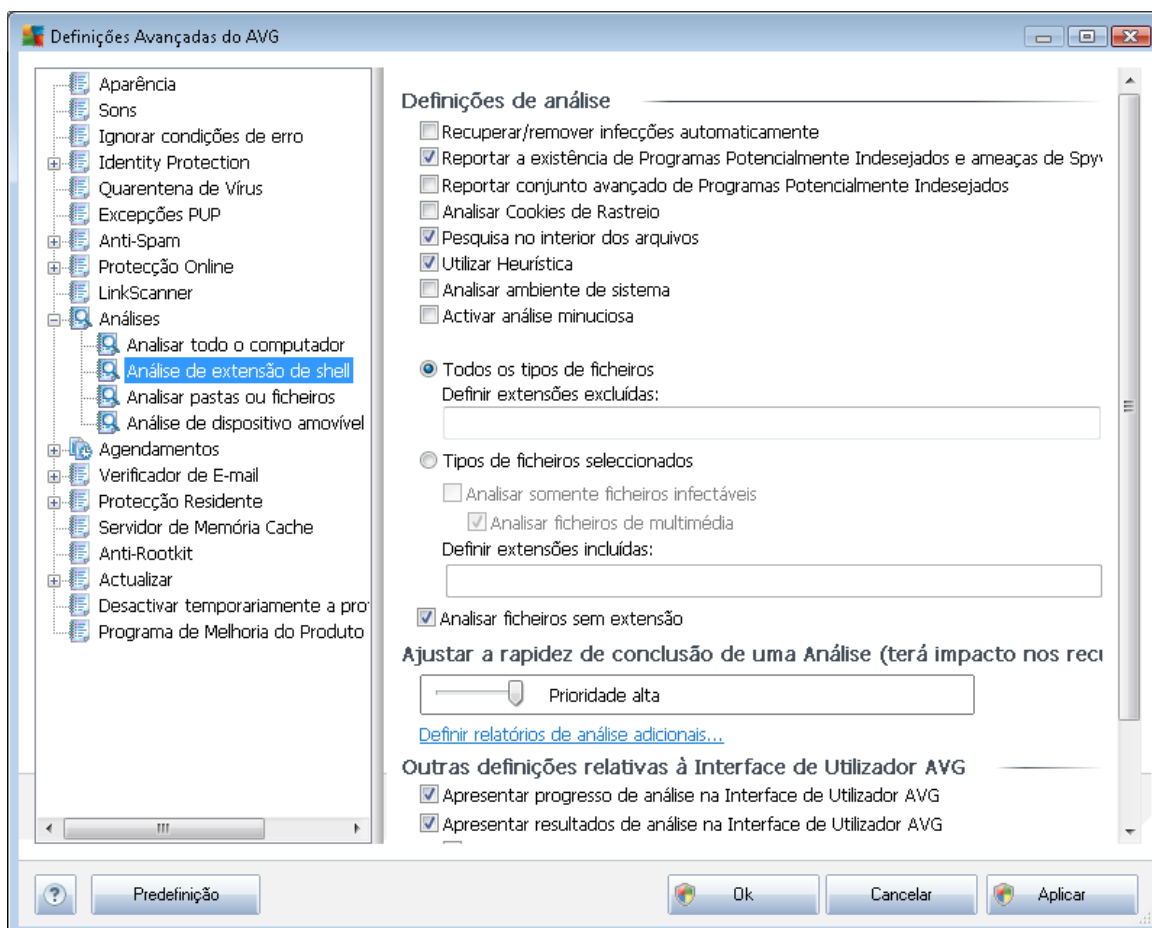
Clique no link **Configurar relatórios de análise adicionais ...** para abrir uma janela independente apelidada **Relatórios de análise** onde pode seleccionar vários itens para definir quais as detecções que deverão ser reportadas:



9.10.2. 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](#):



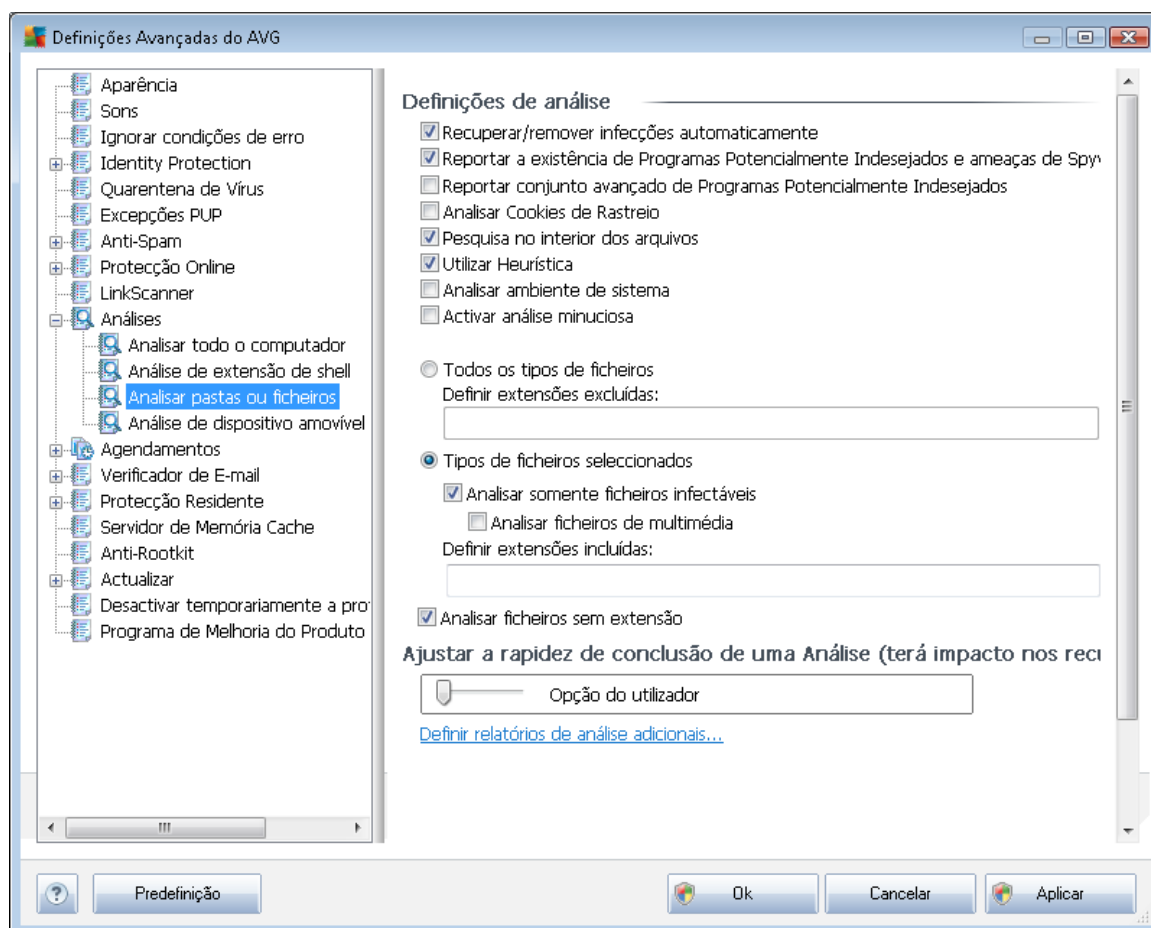
A lista de parâmetros é idêntica aos disponíveis para a análise [Analisar todo o computador](#). No entanto, as predefinições diferem (por exemplo, a *Análise de todo o computador* não verifica os arquivos por predefinição, mas verifica o ambiente do sistema; a *Análise em contexto* é o oposto).

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.

9.10.3. Analisar pastas ou ficheiros específicos

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](#):

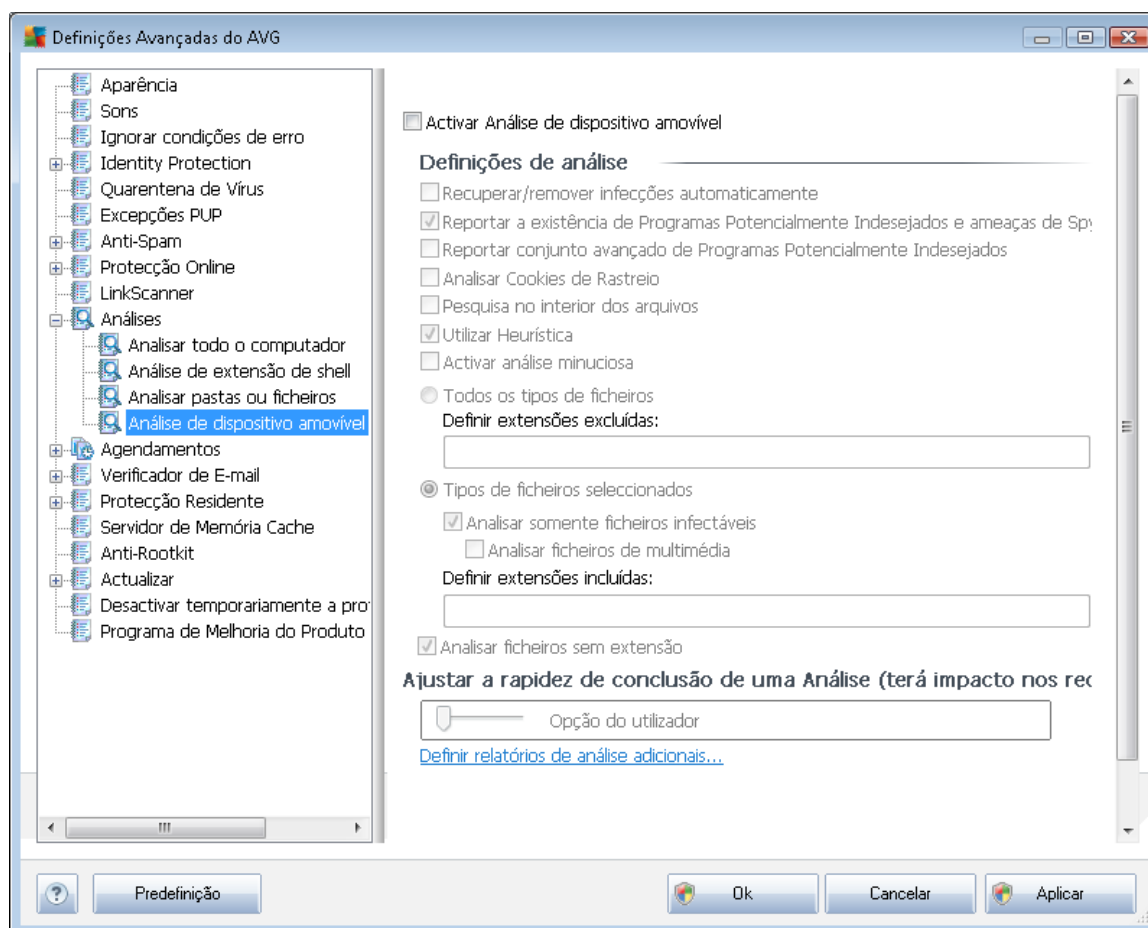


Todos os parâmetros definidos nesta janela de configuração aplicam-se apenas às áreas seleccionadas para análise com a [Análise de ficheiros e pastas específicos](#)!

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

9.10.4. 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](#).

9.11. Agendamentos

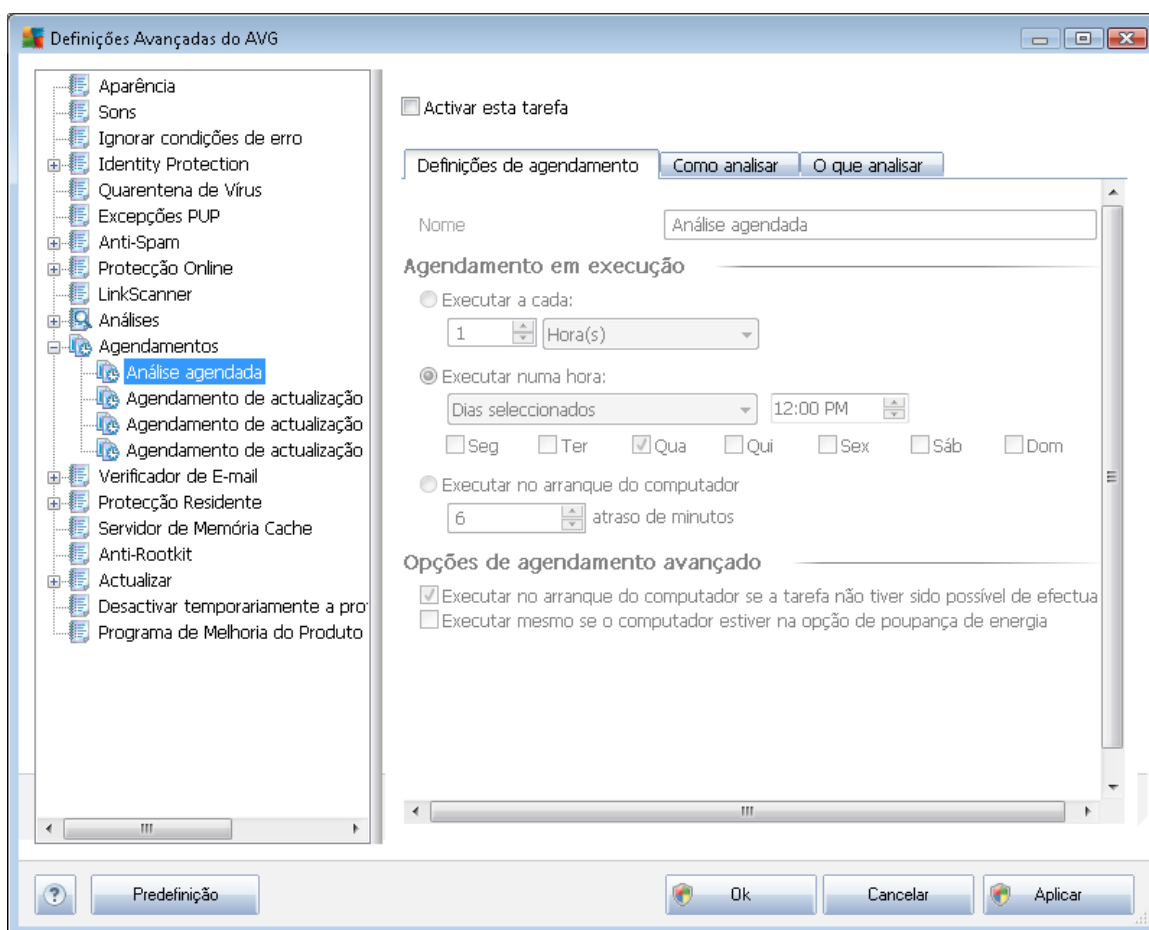
Na secção **Agendamentos** pode editar as definições predefinidas do:

- [Análise agendada](#)

- [Agendamento de actualização da base de dados de vírus](#)
- [Agendamento de actualização do programa](#)
- [Agendamento de Actualização do Anti-Spam](#)

9.11.1. 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:

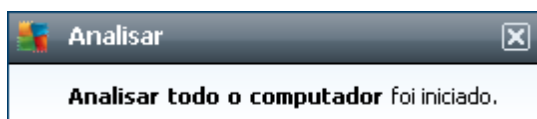
Agendamento em execução

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 (**Acção baseada no arranque do computador**).

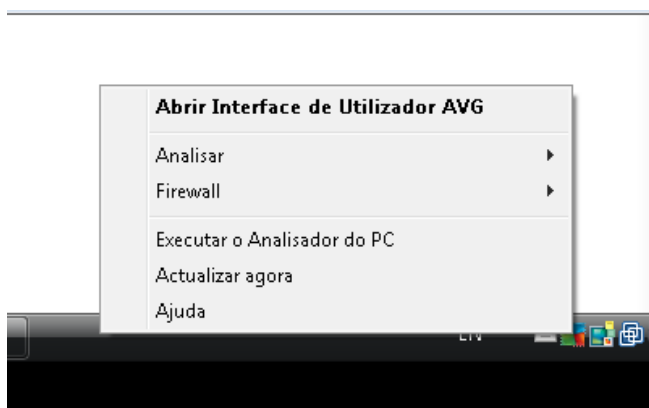
Opções de agendamento avançado

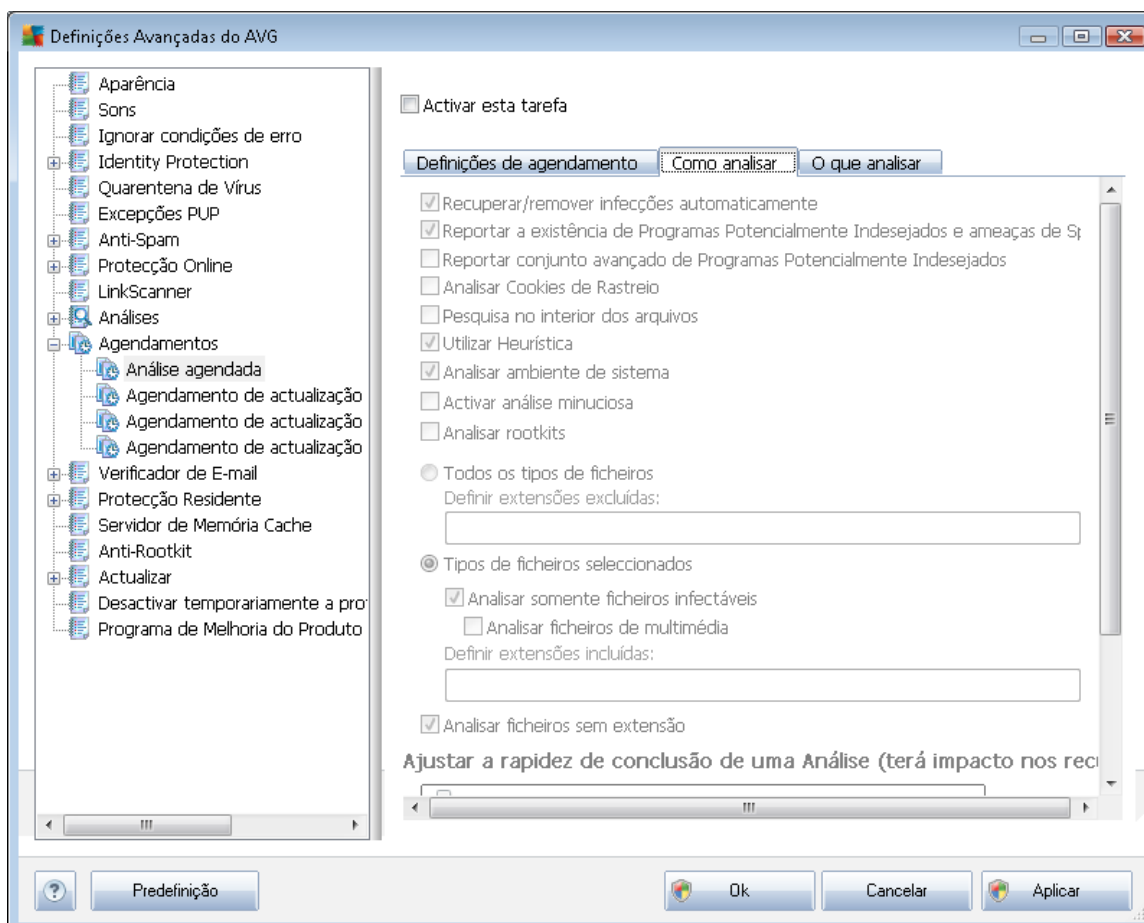
Esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

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 notificação 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 infecção automaticamente** (activado por predefinição): se for detectado um vírus durante a análise, o ficheiro 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 Rastreo** (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, rastreo, e manutenção de informação específica 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**(desactivado por predefinição): seleccione este item se pretender incluir a detecção de rootkits na análise de todo o computador. A detecção apenas de rootkits está disponível no componente [Anti-Rootkit](#);

Além disso deve decidir se pretende que sejam analisados

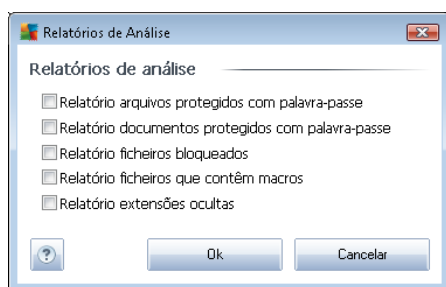
- **Todos os tipos de ficheiros** com a possibilidade de definir excepções para a análise ao providenciar uma listagem extensões de ficheiro separadas por vírgula (*uma vez guardada, as vírgulas mudam para ponto e vírgula*) que não devem ser analisadas;
- **Tipos de ficheiros seleccionados** - pode especificar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

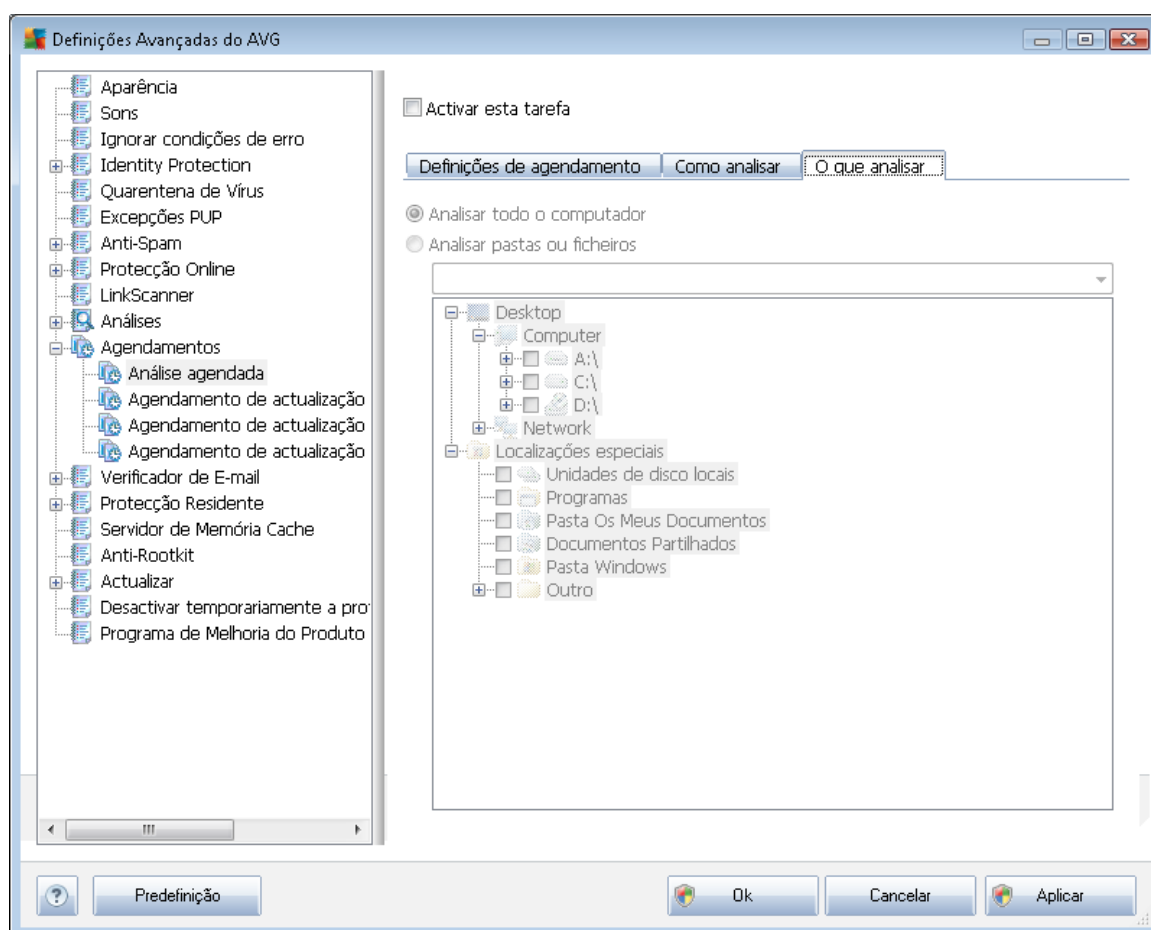
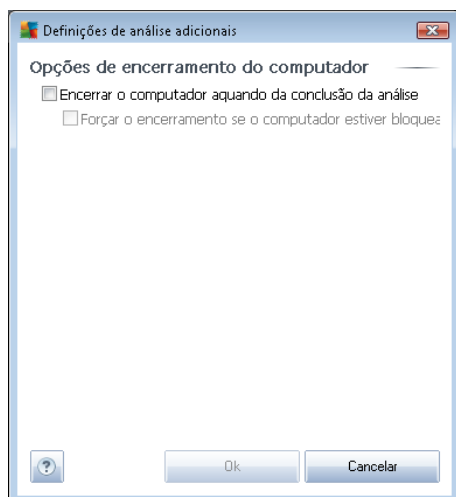
Definir relatórios de análise adicionais

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**).

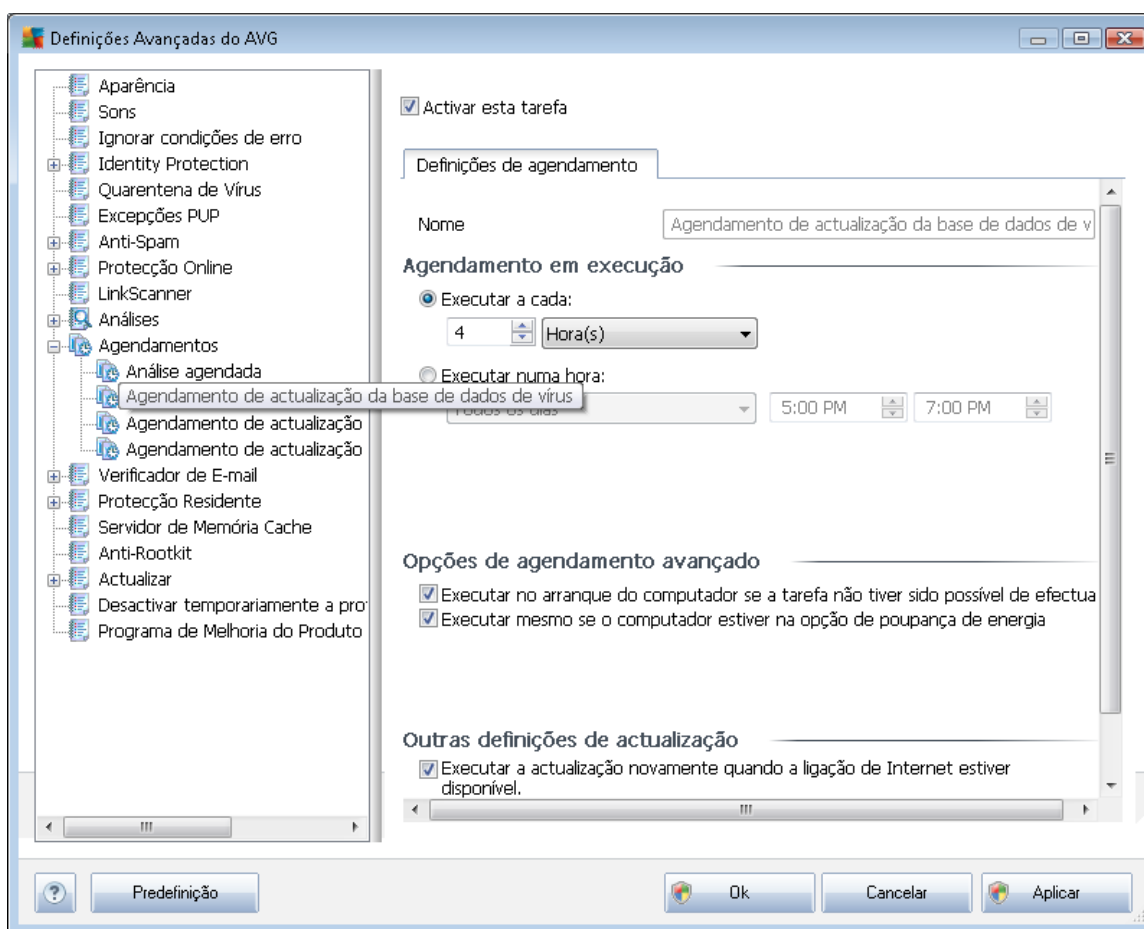


No separador **O que analisar** pode definir se pretende agendar uma [análise a todo o computador](#) ou [analisar ficheiros e pastas específicos](#). Na eventualidade de seleccionar a análise de ficheiros e pastas específicos, na parte inferior desta janela é activada a estrutura da árvore apresentada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

pode especificar pastas a serem analisadas.

9.11.2. Agendamento de actualização da base de dados de vírus

Se for *realmente necessário*, pode desmarcar o item **Activar esta tarefa** para desactivar temporariamente a actualização da base de dados de vírus agendada e activá-la posteriormente:



O agendamento de actualização da base de dados de vírus básico está previsto no componente [Gestor de Actualizações](#). Nesta janela pode configurar alguns parâmetros detalhados do agendamento de actualização da base de dados de vírus. 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 da base de dados de vírus. 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 análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca ou desligado.

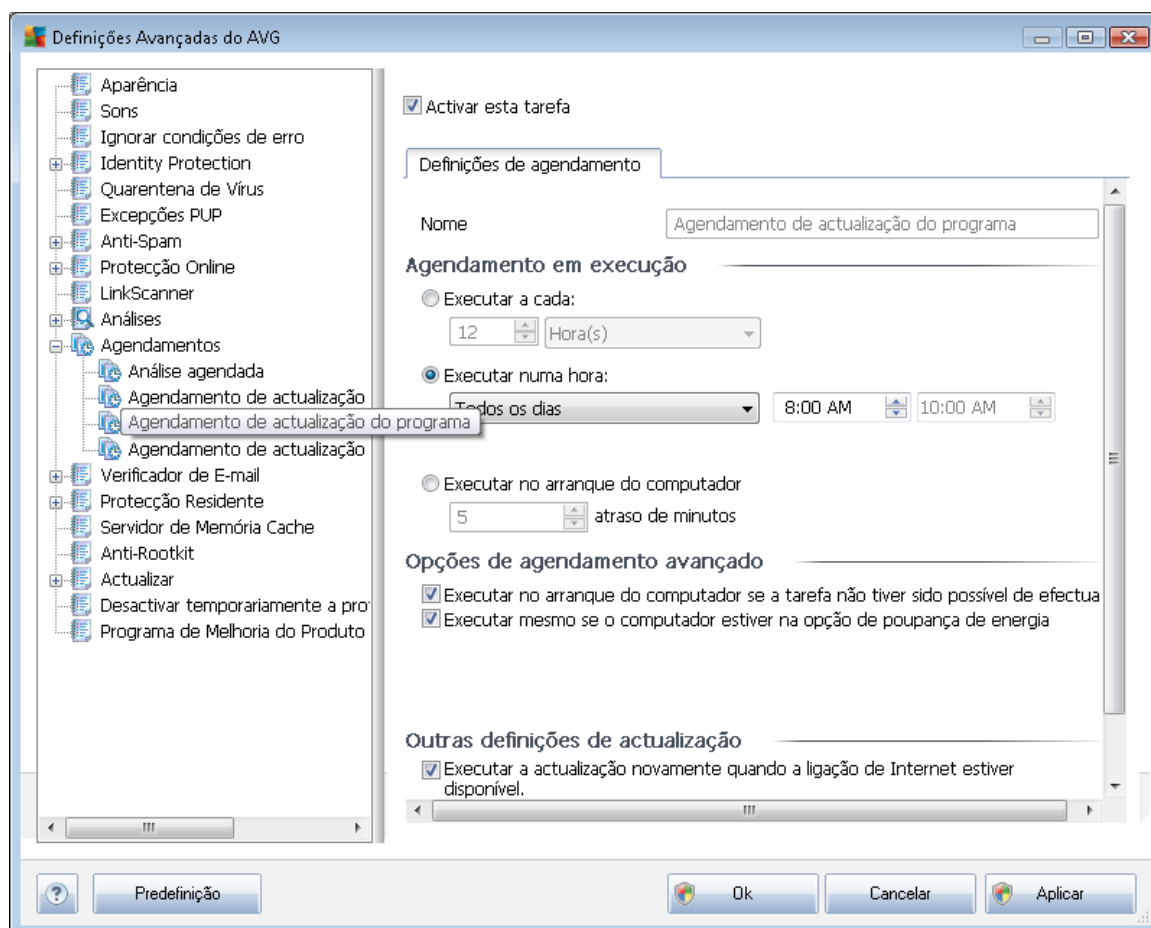
Outras definições de actualização

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 notificação](#) considerando que tenha mantido a configuração predefinida da janela [Definições Avançadas/Aparência](#).

9.11.3. 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 (**Ação 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

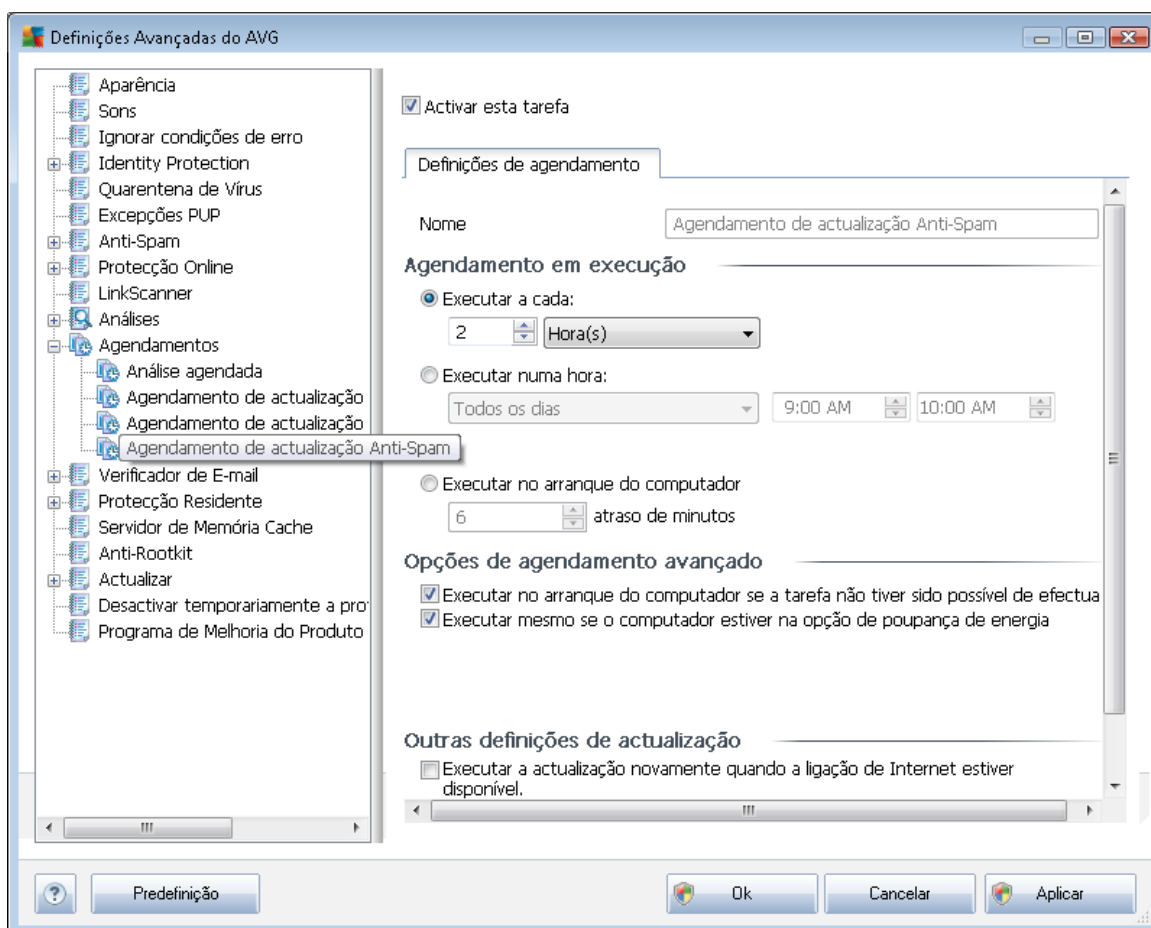
Marque a opção ***Executar a actualização novamente assim que a ligação Internet estiver disponível*** para certificar-se de que se o processo de actualização ou a ligação à Internet falharem, a actualização será executada de novo imediatamente após o restabelecimento da ligação à Internet.

Uma vez iniciado o agendamento à hora especificada, será avisado deste facto através de uma janela de pop-up aberta no [ícone do AVG na barra de notificação](#) 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.

9.11.4. Agendamento de Actualização do Anti-Spam

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



O agendamento de actualizações básicas do componente **Anti-Spam** está previsto no componente **Gestor de Actualizações**. 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 (**Ação 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.

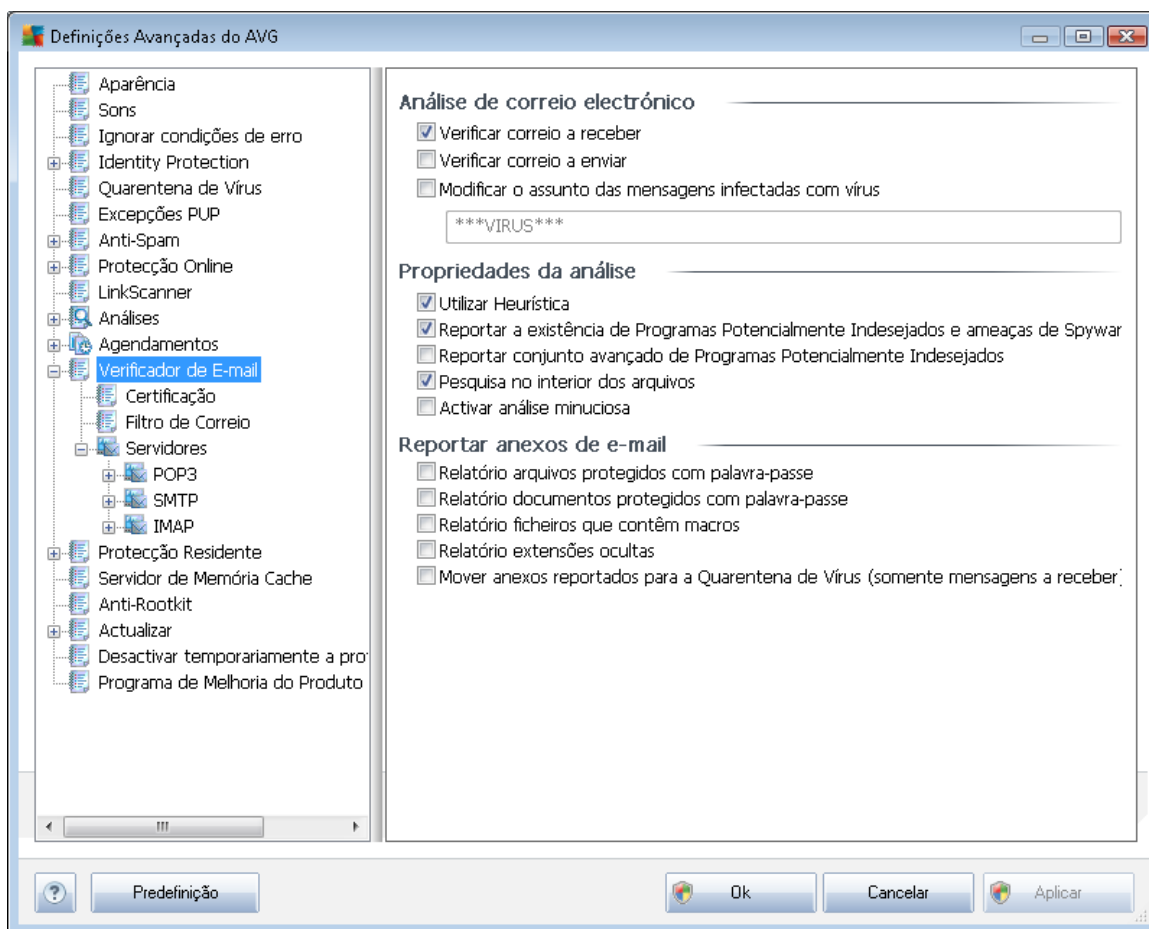
Outras definições de actualização

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 notificação](#) (considerando que tenha mantido a configuração predefinida da janela [Definições Avançadas/Aparência](#)).

9.12. 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.



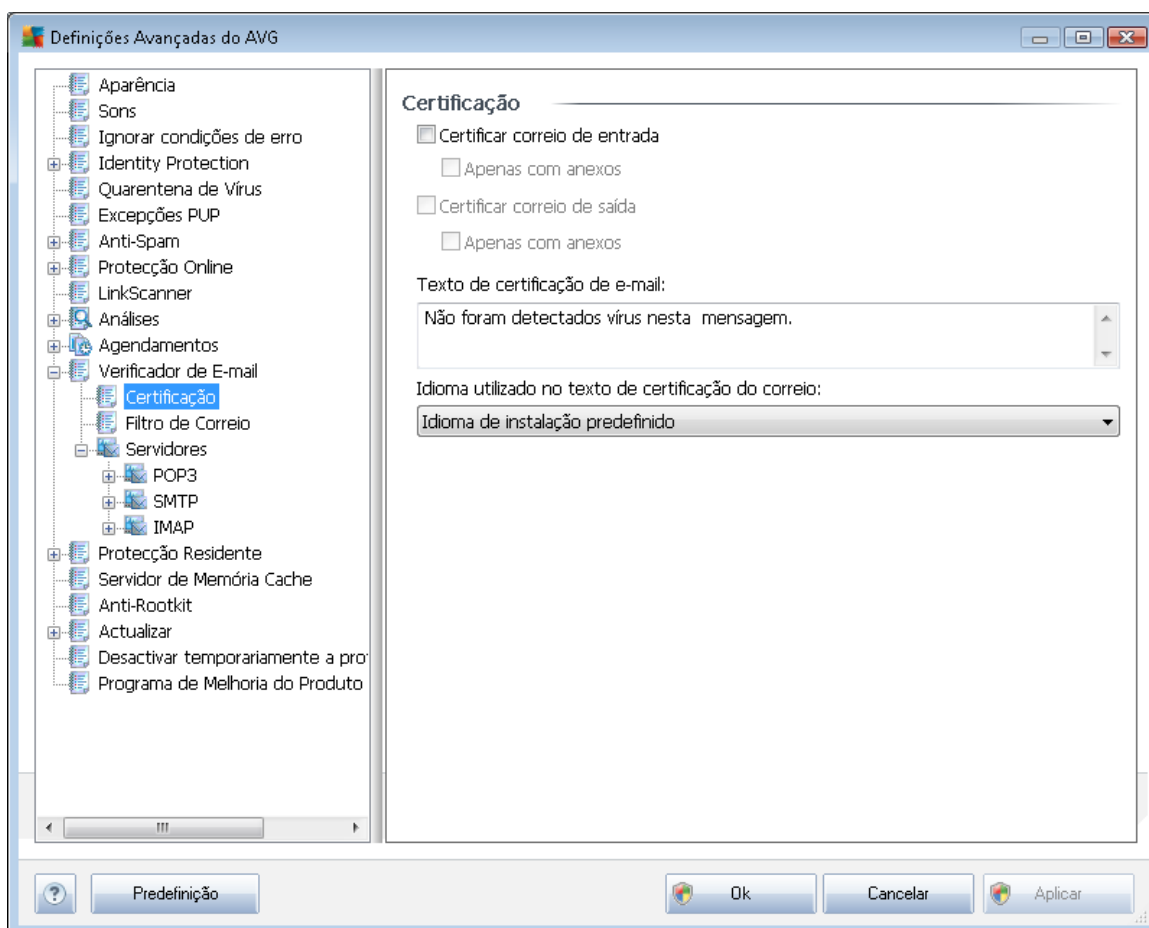
Reportar anexos de e-mail

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](#).

9.12.1. Certificação

Na janela **Certificação** pode especificar o texto e idioma da certificação para o correio a receber e a enviar:



O texto de certificação consiste em duas partes, a parte do utilizador e a parte do sistema - consulte o seguinte exemplo: a primeira linha representa a parte do utilizador, o resto é gerado automaticamente pelo sistema:

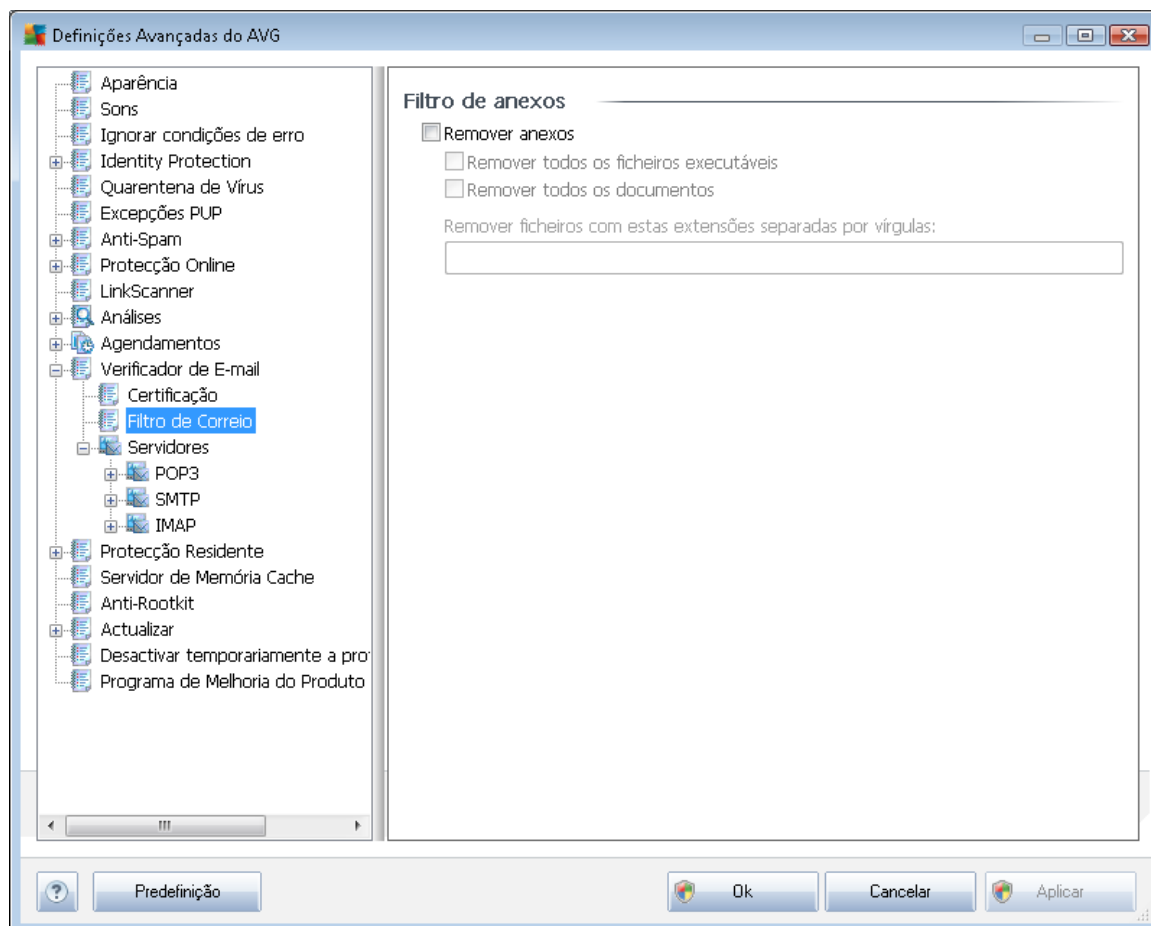
Não foram detectados vírus nesta mensagem.

Verificado pelo AVG.

Versão: x.y.zz / Base de Dados de Vírus: xx.y.z – Data de lançamento: 12/9/2010

Se decidir usar a certificação para mensagens de correio a receber ou a enviar, pode especificar mais à frente o texto exacto da parte do utilizador do texto de certificação (**texto de certificação de e-mail**), e escolher o idioma que deve ser usado para a parte da certificação gerada automaticamente pelo sistema (**Idioma utilizado no texto de certificação do correio**)

9.12.2. Filtro de Correio

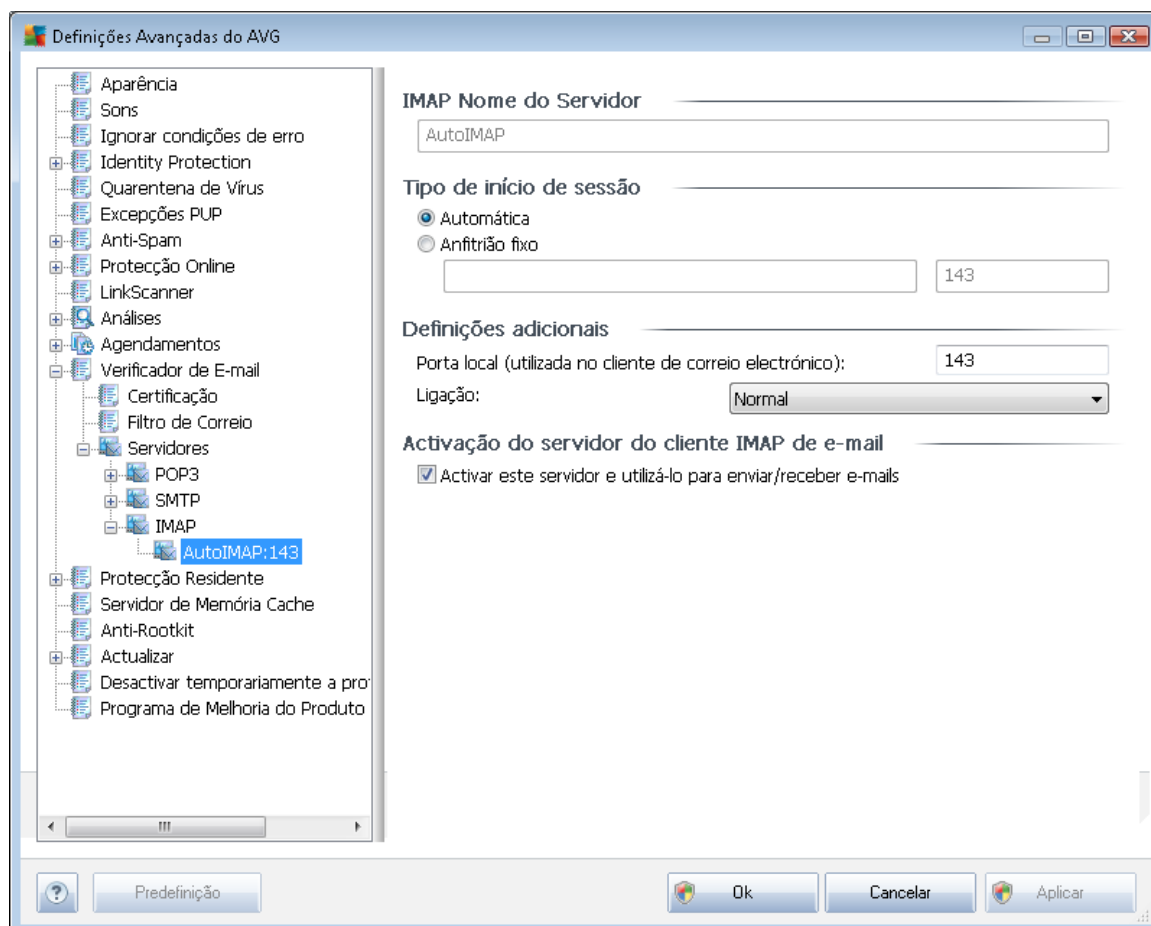


A janela **Filtro de anexos** permite-lhe configurar parâmetros para a análise de anexos do e-mail. A opção **Remover anexos** está desactivada por predefinição. Se decidir activá-la, todos os anexos do e-mail detectados como infecciosos ou potencialmente perigosos serão removidos automaticamente. Se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

9.12.3. Servidores

Na secção **Servidores** pode editar parâmetros dos servidores do componente [Verificador de Correio Electrónico](#), ou configurar um novo servidor usando o botão **Adicionar novo servidor**.

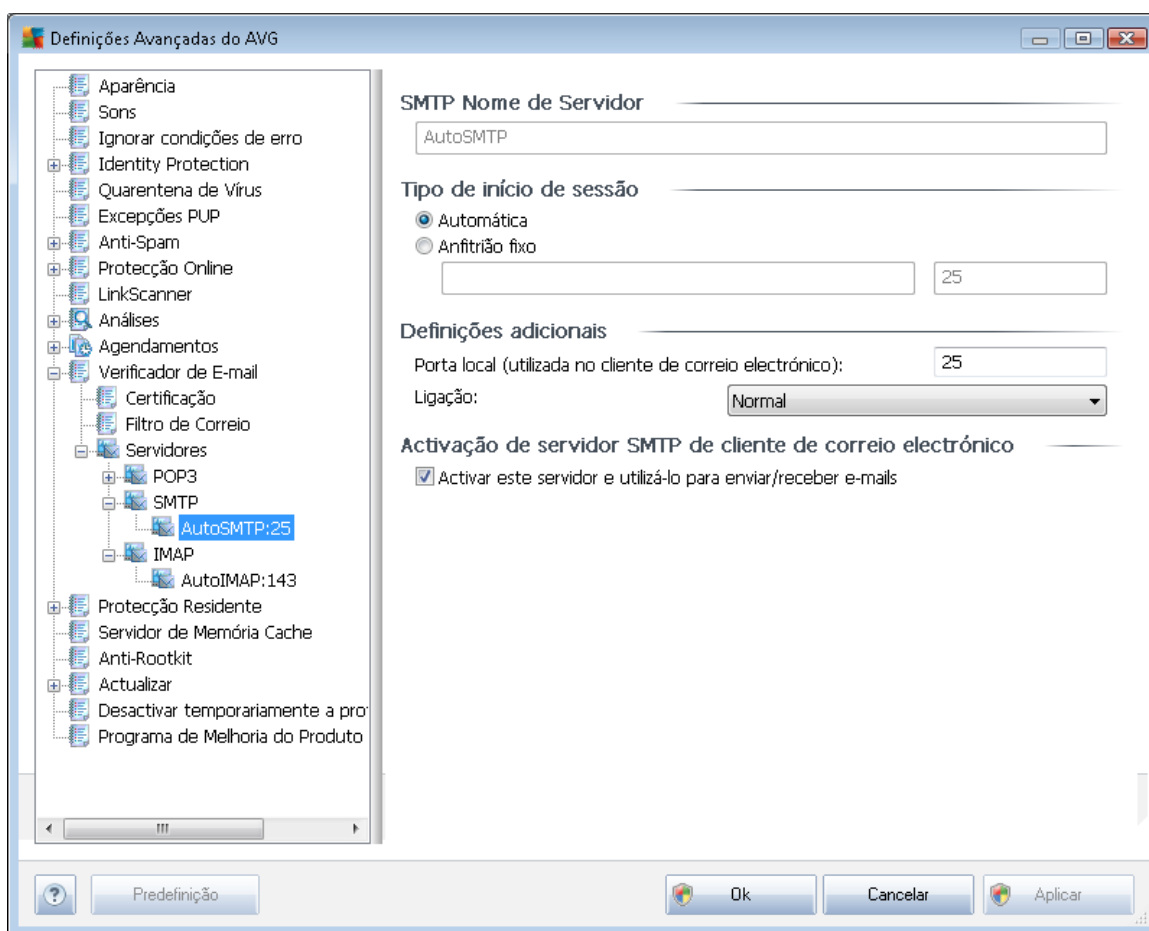


Nesta janela (acessível via **Servidores / POP3**) pode configurar um novo servidor do [Verificador de E-mail](#) utilizando o protocolo POP3 para e-mail a receber:

- **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 início de sessão** - define o método para determinar o servidor de e-mail utilizado para e-mail a receber:
 - o **Automático** - O início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de correio electrónico.
 - o **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,*

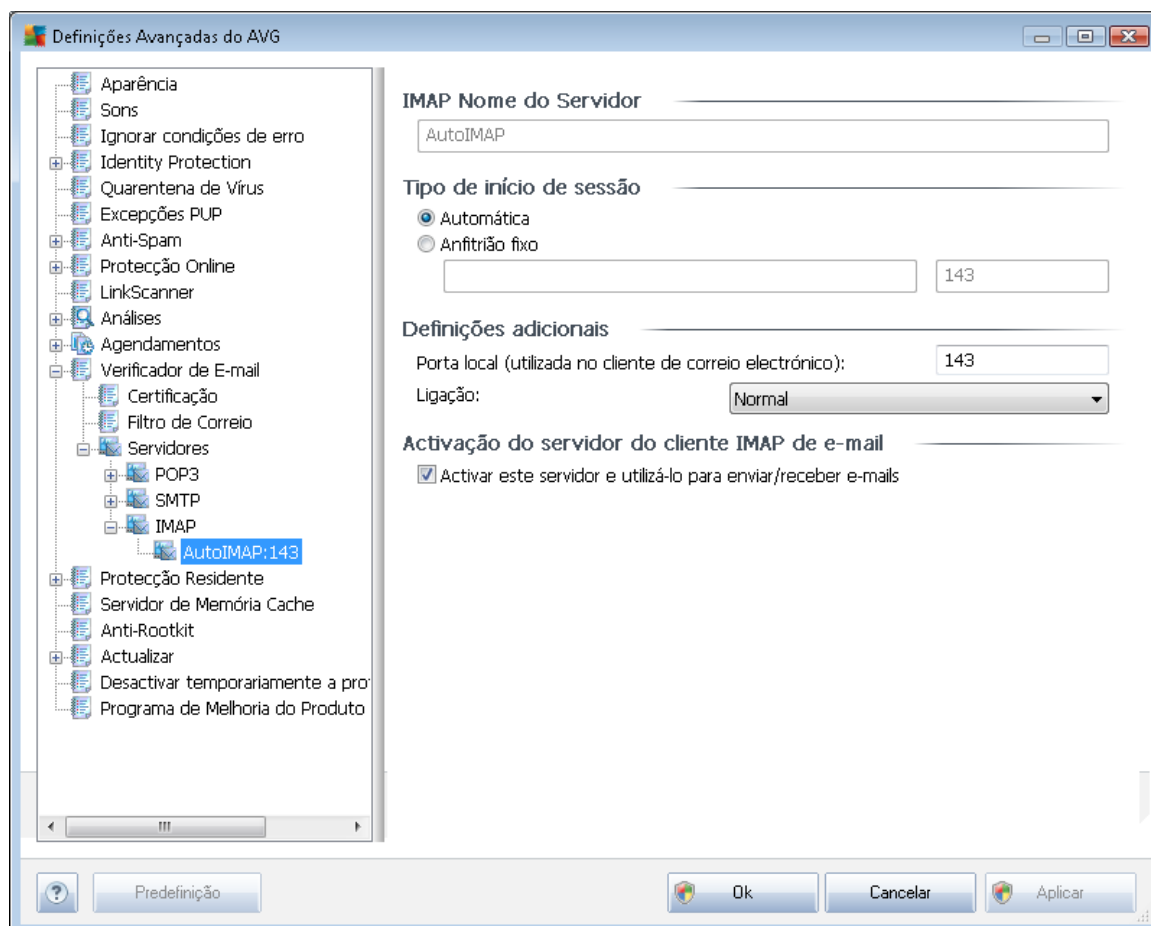
acme.com:8200). A porta padrão para comunicação POP3 é 110.

- **Definições adicionais** - especifica parâmetros mais detalhados:
 - o **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.
 - o **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 início de sessão** - define o método para determinar o servidor de e-mail utilizado para e-mail a enviar:
 - o **Automático** - o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
 - o **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:
 - o **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.
 - o **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:

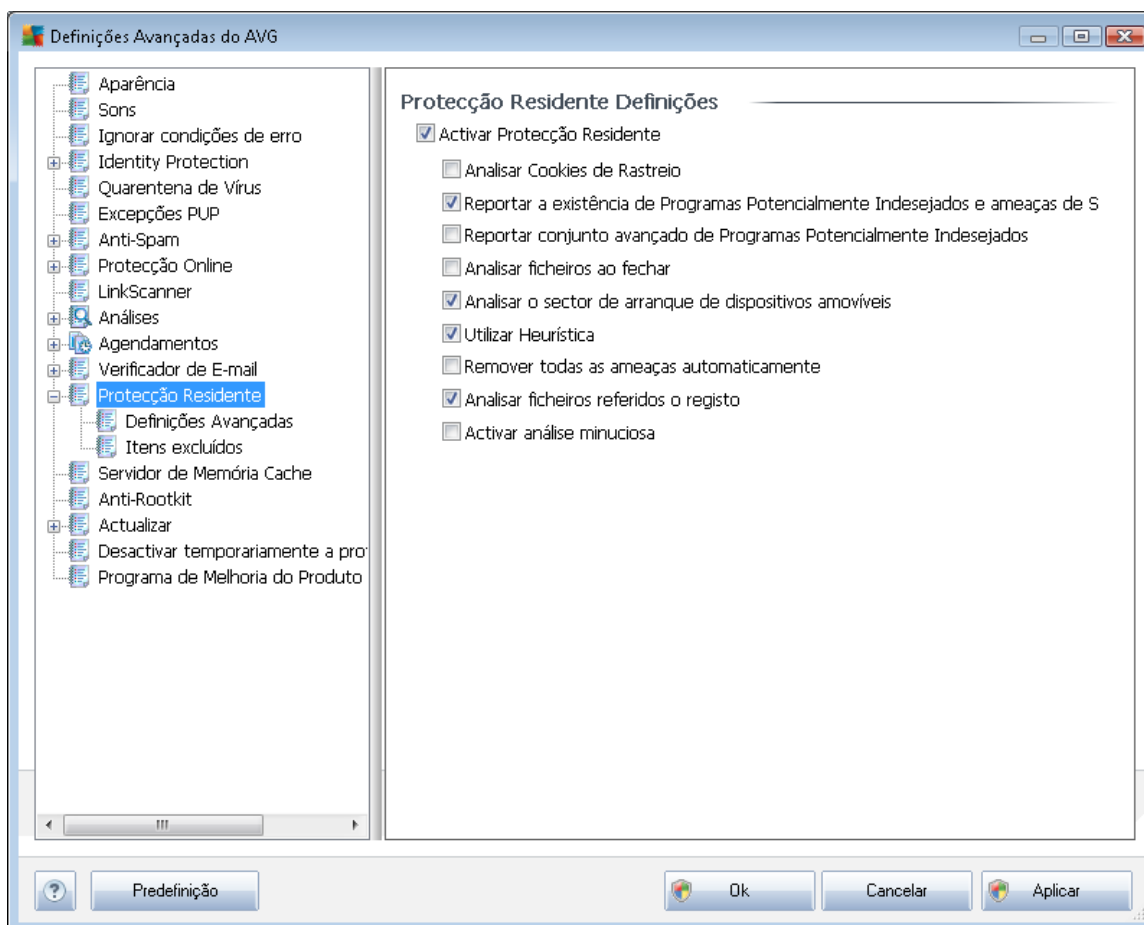
- **Nome do Servidor IMAP** - neste campo pode especificar o nome de servidores adicionados recentemente (*para adicionar um servidor IMAP, clique com o botão direito do rato sobre o item IMAP do menu de navegação à esquerda*). Este campo estará desactivado para servidores "AutoIMAP" criados automaticamente.
- **Tipo de início de sessão** - define o método para determinar o servidor de e-mail utilizado para e-mail a enviar:
 - o **Automático** - o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
 - o **Anfitrião Fixo** - 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:
 - o **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.
 - o **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

9.13. Protecção Residente

O componente **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 **Protecção**



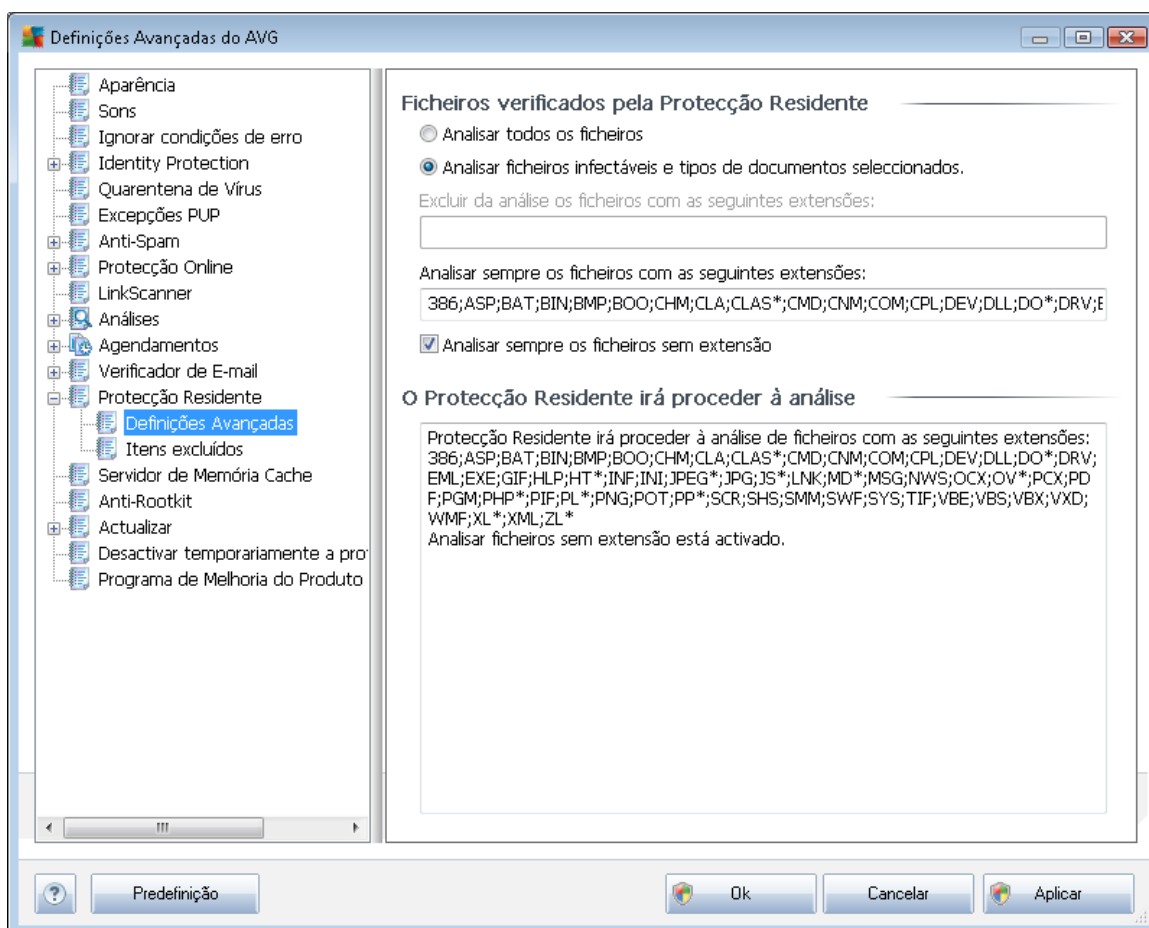
Residente completamente ao seleccionar/desmarcar o item **Activar Protecção Residente** (esta opção está activada por predefinição). Adicionalmente, pode seleccionar quais as funcionalidades da **Protecção Residente** que deverão ser activadas:

- **Analisar a Existência de Cookies de Rastreamento** (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 websites 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)
- **Remover todas as ameaças automaticamente** (desactivado por predefinição) - qualquer infecção detectada será recuperada automaticamente se houver uma cura disponível, e todas as infecções que não puderem ser recuperadas serão removidas.
- **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.



9.13.1. Definições Avançadas

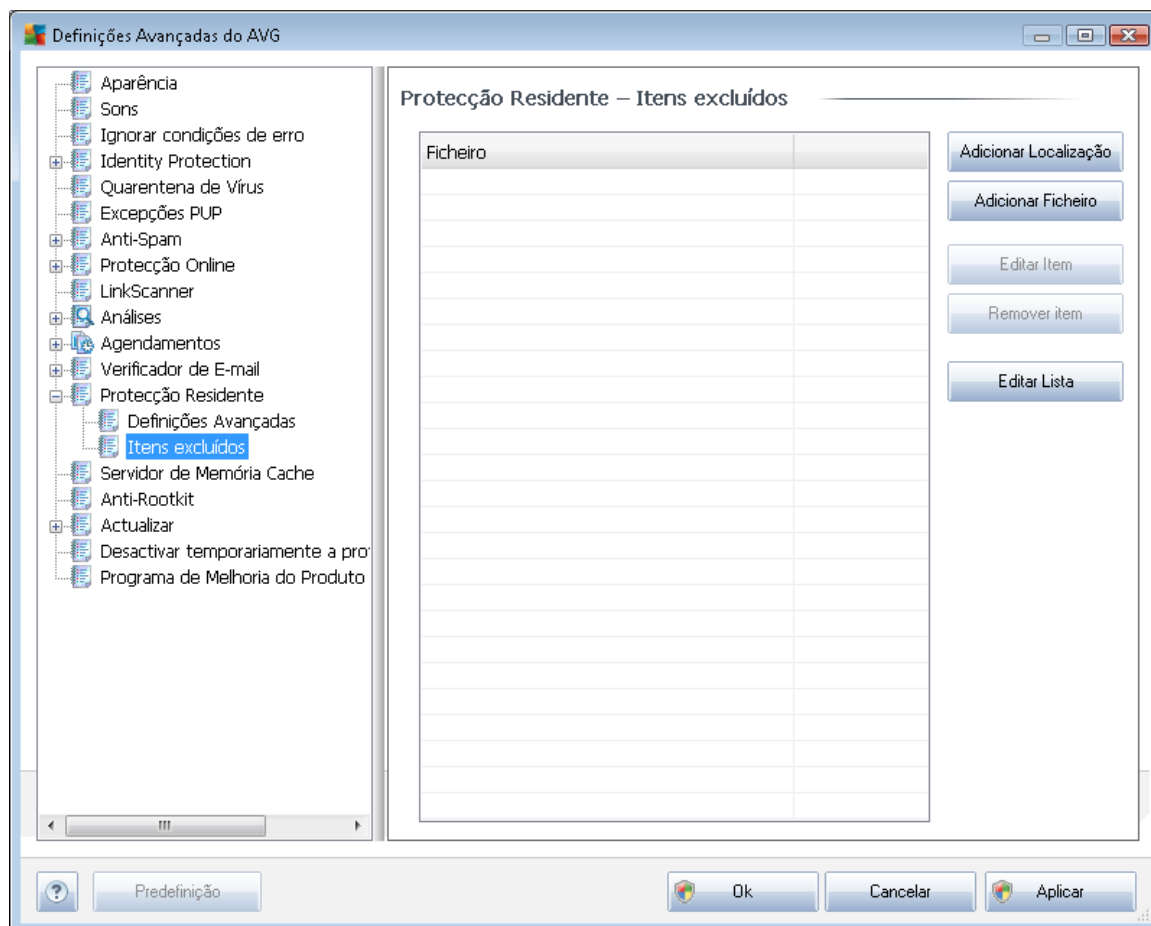
Na janela **Ficheiros verificados pela Protecção Residente** é possível configurar os ficheiros a analisar (por extensões):



Decida se pretende que todos os ficheiros sejam analisados, ou somente os ficheiros infectáveis - se assim for, pode ainda especificar uma lista de extensões de modo a definir ficheiros que devam ser excluídos da análise, assim como uma lista de extensões de ficheiros que defina ficheiros que deverão ser analisados em qualquer circunstância.

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.

9.13.2. Itens excluídos



A janela **Protecção Residente - Itens excluídos** oferece a possibilidade de definir ficheiros e/ou pastas que devem ser excluídos da análise da [Protecção Residente](#).

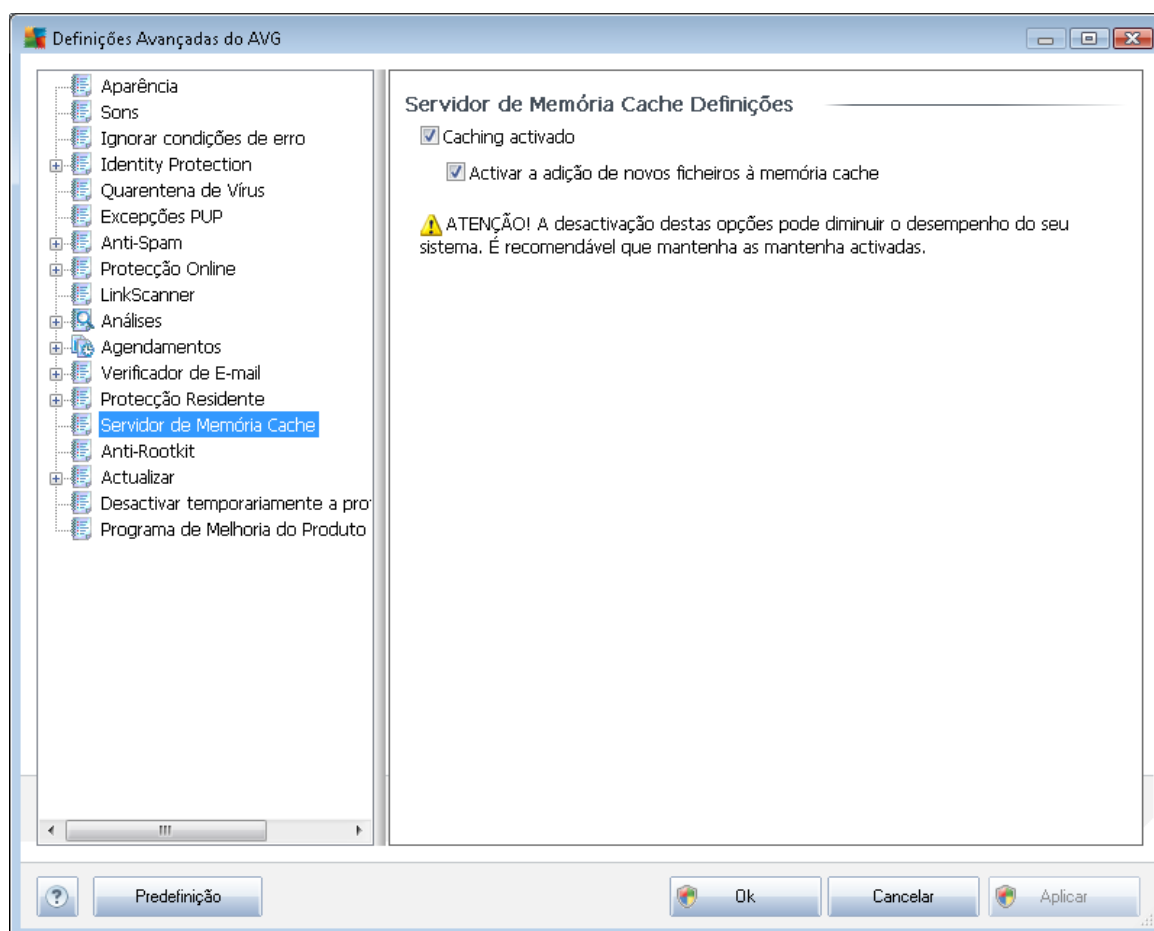
Se não for estritamente necessário, recomenda-se vivamente que não exclua quaisquer itens!

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

9.14. Servidor de Memória Cache

O **Servidor de Memória Cache** é um processo destinado a acelerar qualquer análise (*análise manual, análise de todo o computador agendada, análise da [Protecção Residente](#)*). Recolhe e mantém as informações relativas a ficheiros seguros (*ficheiros de sistema com assinatura digital, etc.*): Estes ficheiros são então considerados seguros e são ignorados durante a análise.

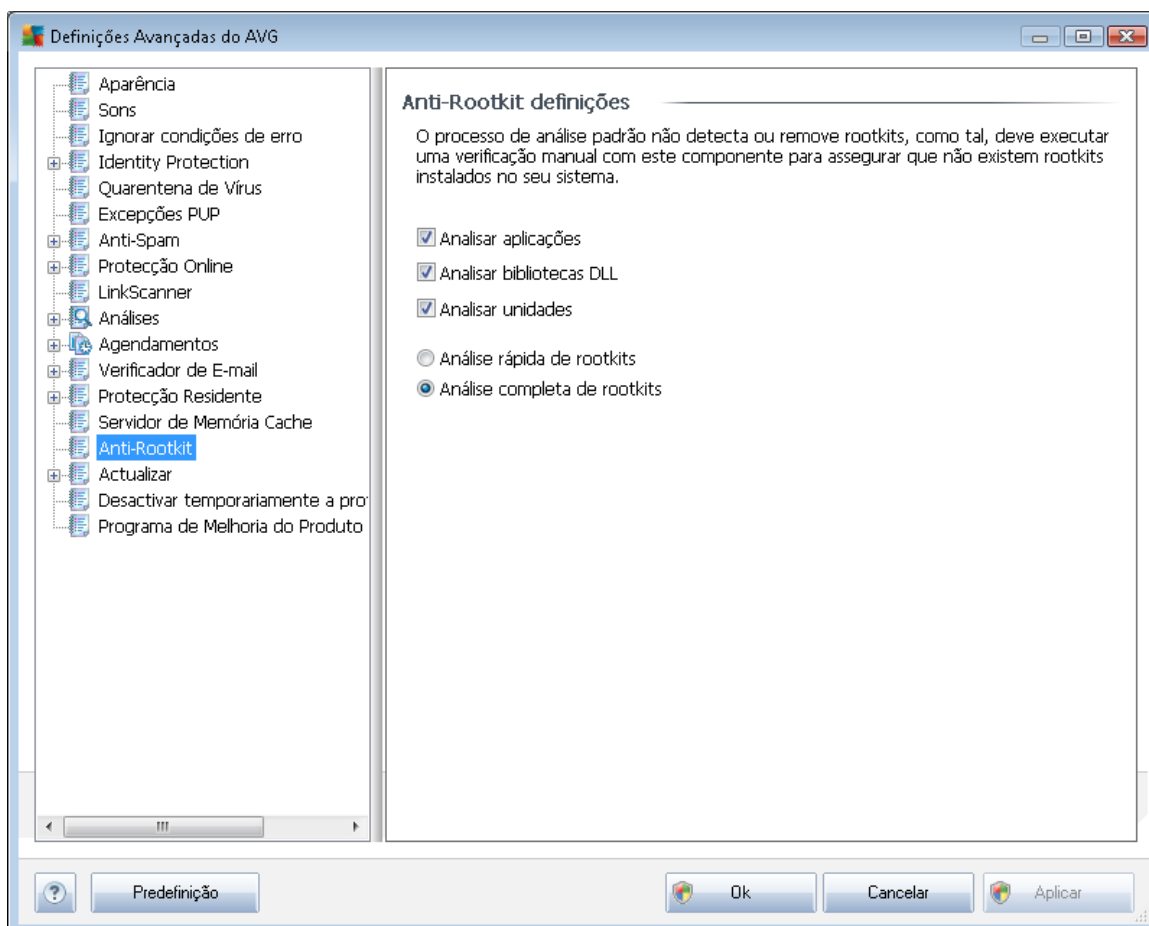


A janela de definições disponibiliza duas opções:

- **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.

9.15. Anti-Rootkit

Nesta janela pode editar a configuração do componente [Anti-Rootkit](#):



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](#)*.

Primeiro, seleccione as caixas de verificação respectivas para especificar objectos que devem ser analisados:

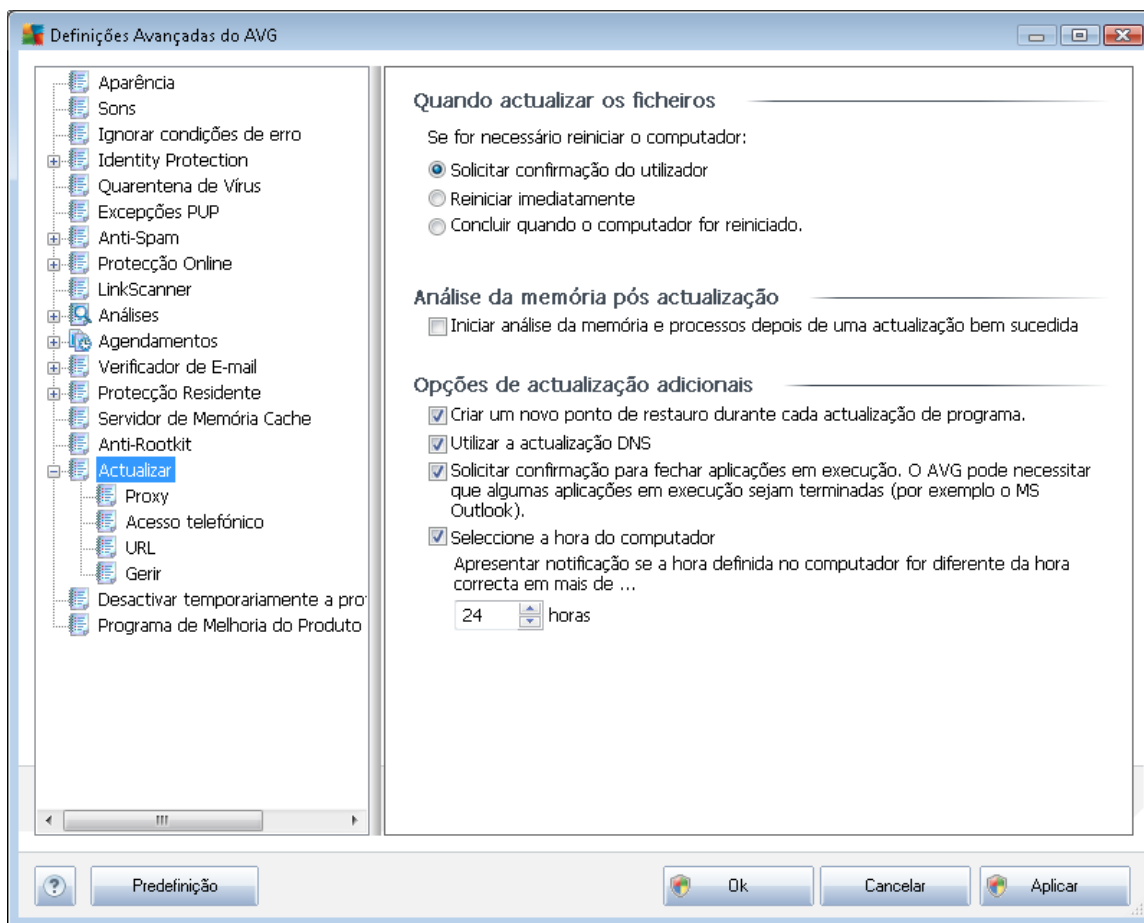
- **Analisar aplicações**
- **Analisar bibliotecas DLL**
- **Analisar unidades**

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*)

9.16. 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 requiera 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 aprobe um reinício 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!

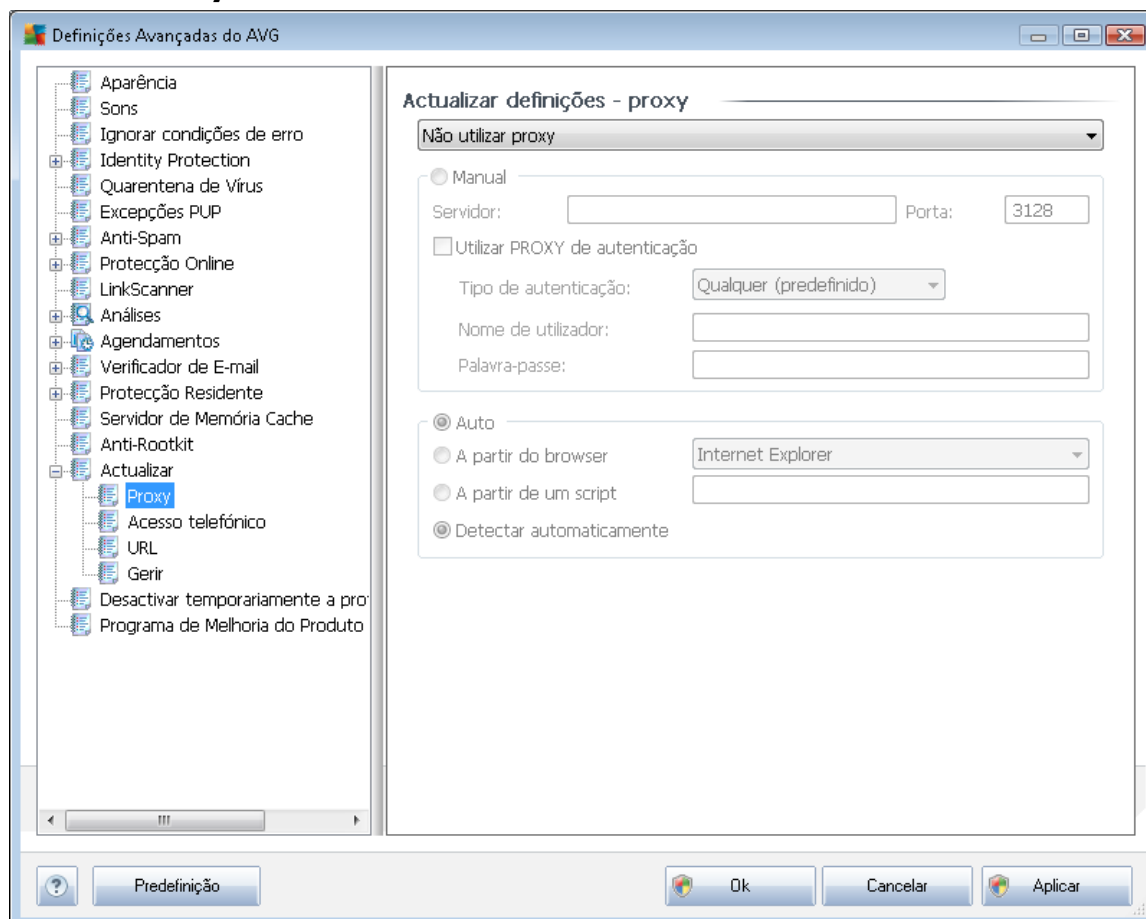
Análise da memória pós actualização

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 2011** 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.

9.16.1. 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 o servidor proxy**- definições predefinidas
- **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*)

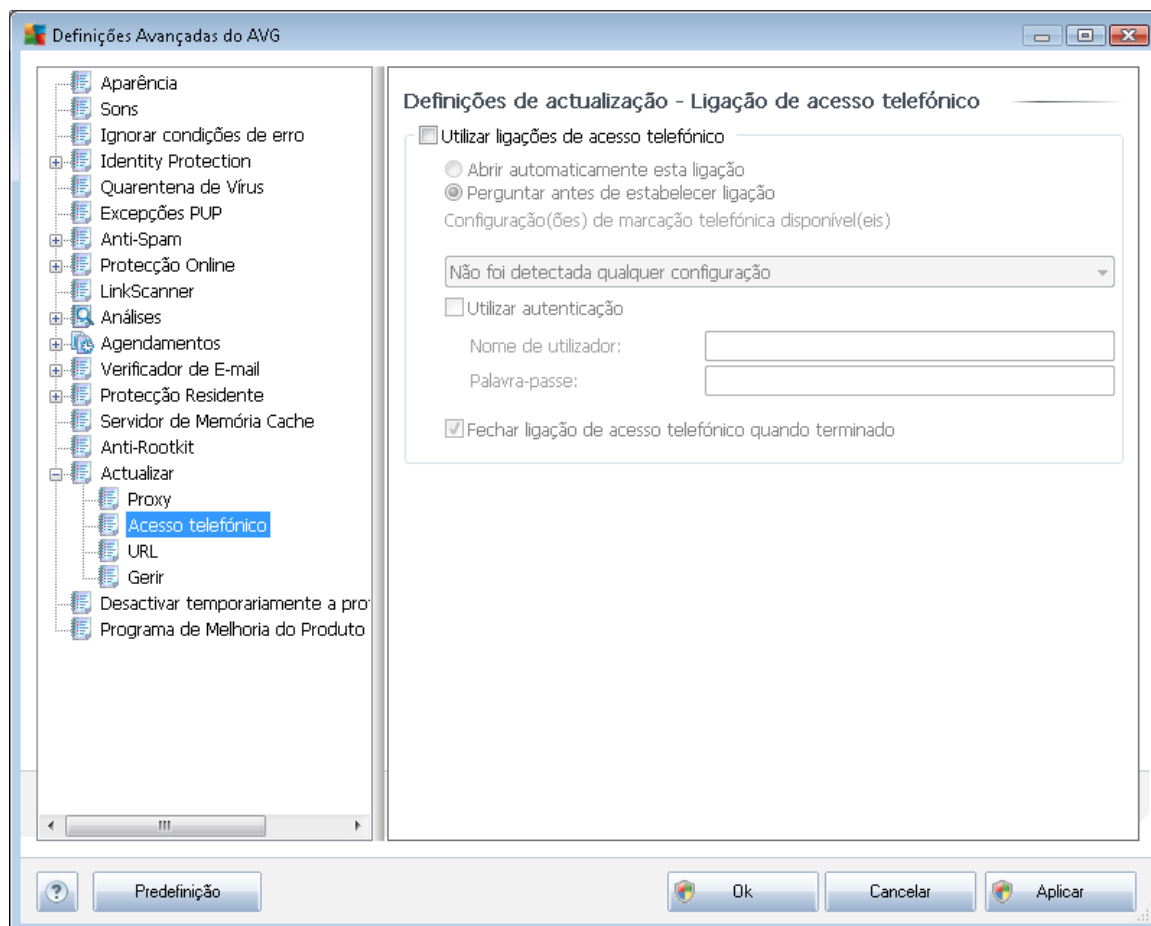
O servidor proxy também pode ter regras específicas configuradas para cada utilizador. Se o seu servidor proxy estiver configurado desta forma, seleccione a opção **Utilizar PROXY de autenticação** para verificar se o seu nome de utilizador e palavra-passe são válidos para estabelecer ligação à Internet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

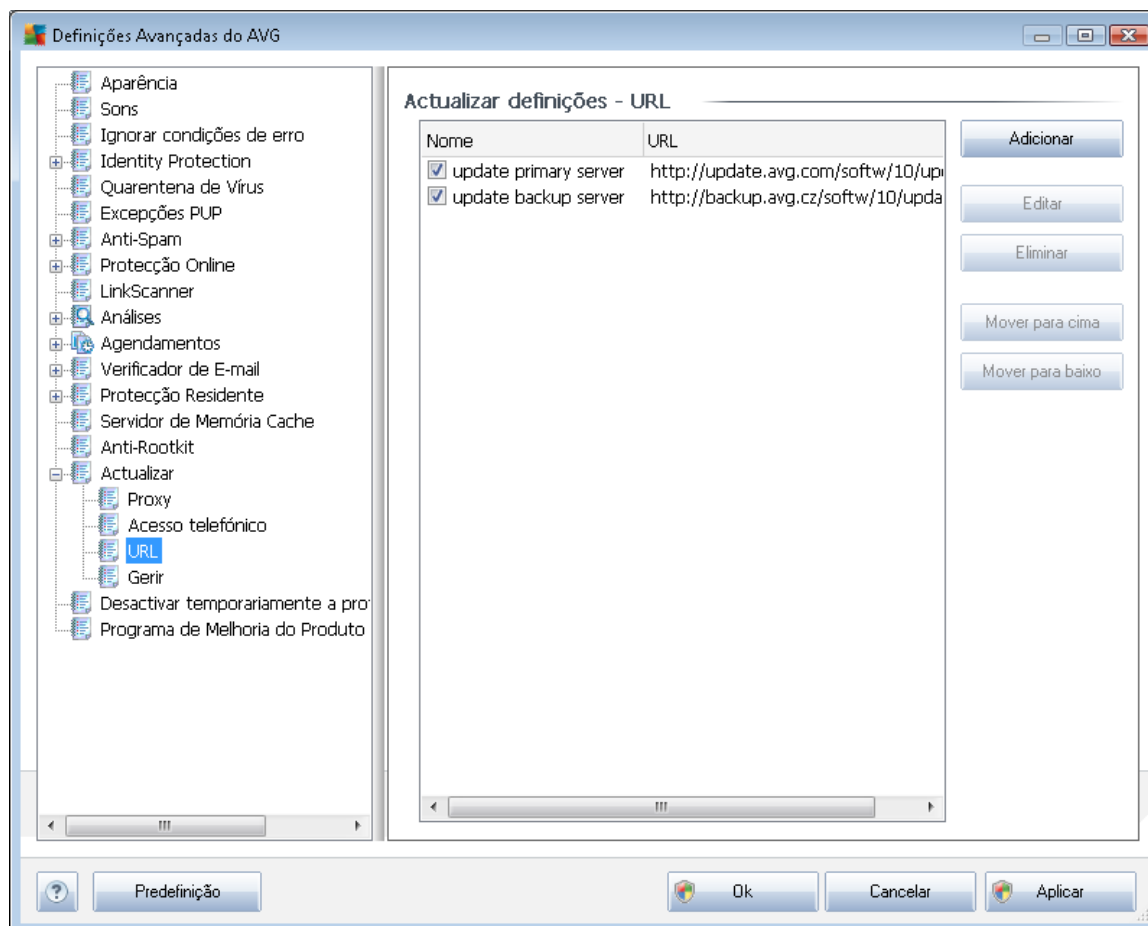
9.16.2. Acesso telefónico



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**).

9.16.3. URL

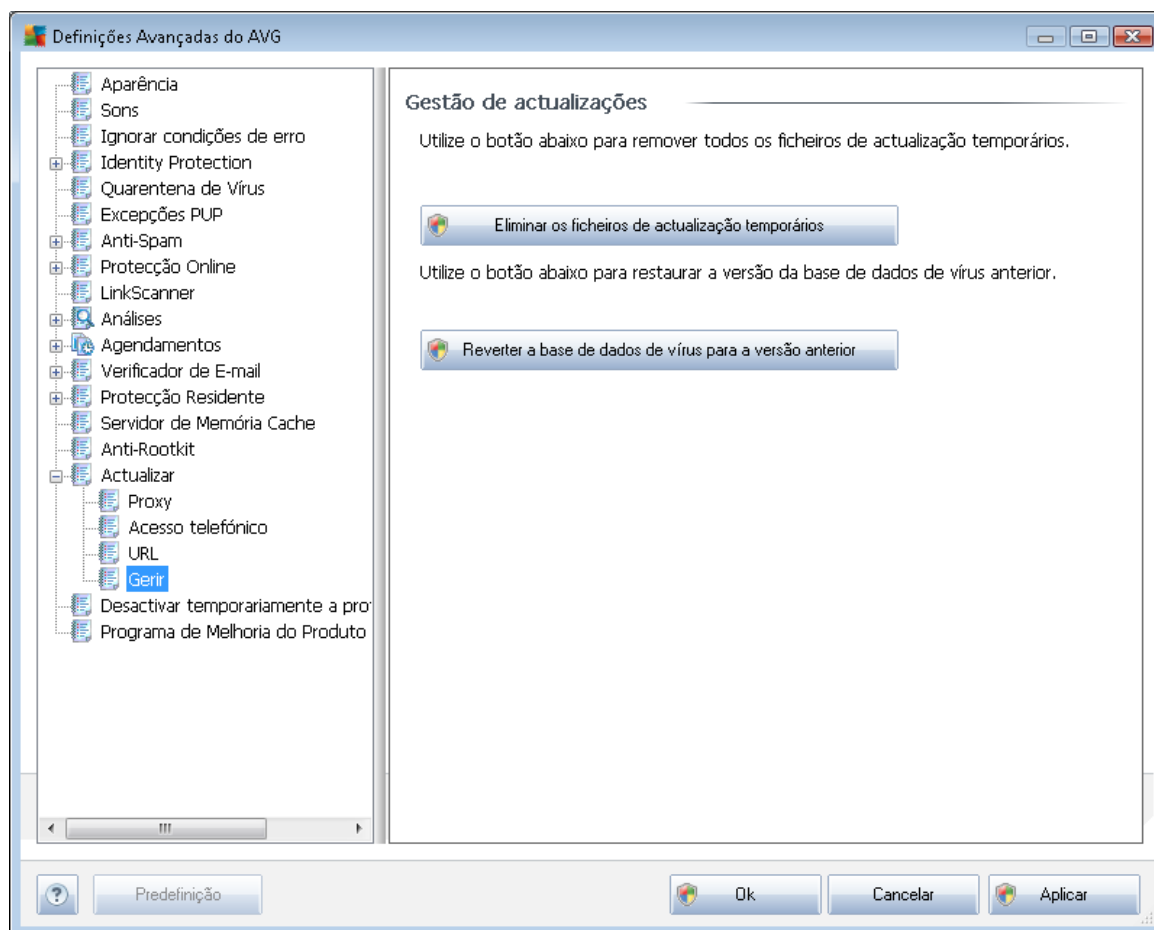


A janela **URL** apresenta uma lista de endereços da Internet a partir dos quais pode transferir os ficheiros de actualização. A lista e os respectivos itens podem ser modificados, utilizando os botões de controlos seguintes:

- **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

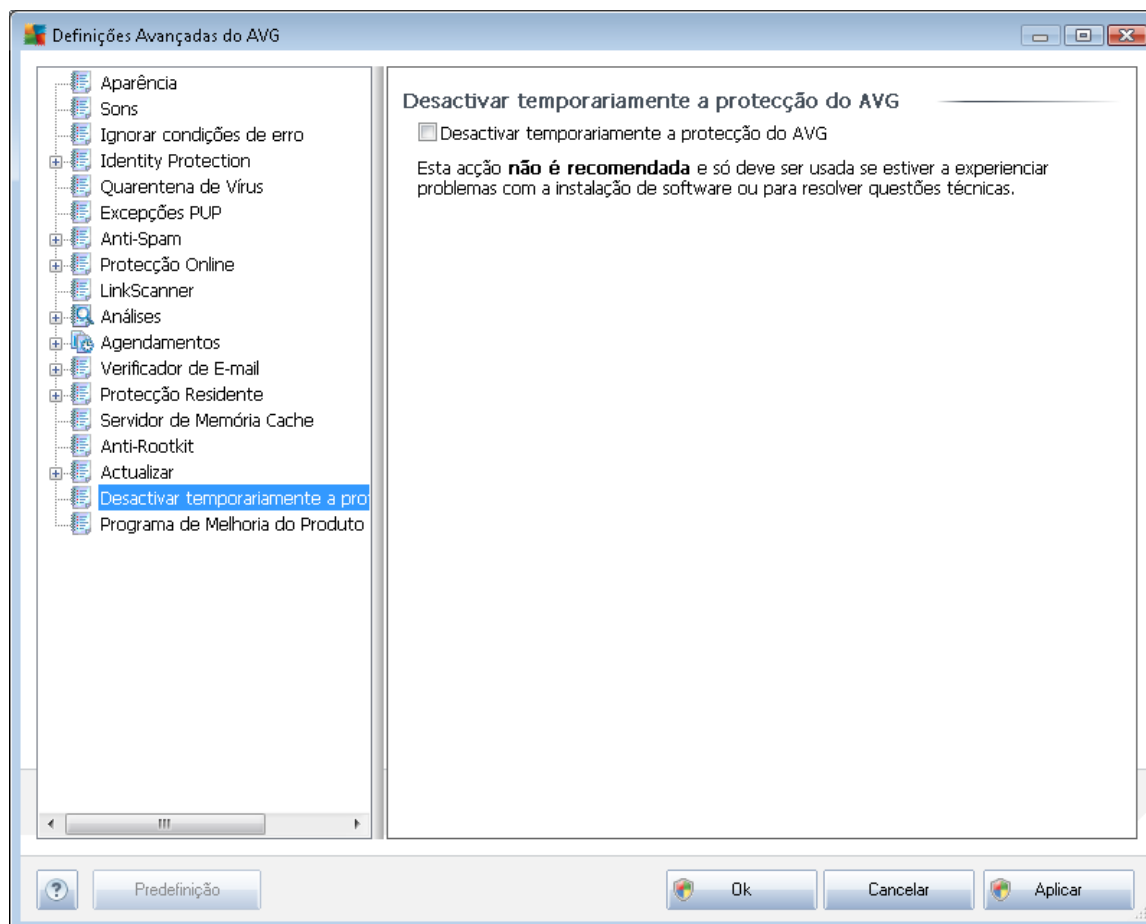
9.16.4. Gerir

A janela **Gerir** 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*)

9.17. 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 2011** de uma só vez.

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

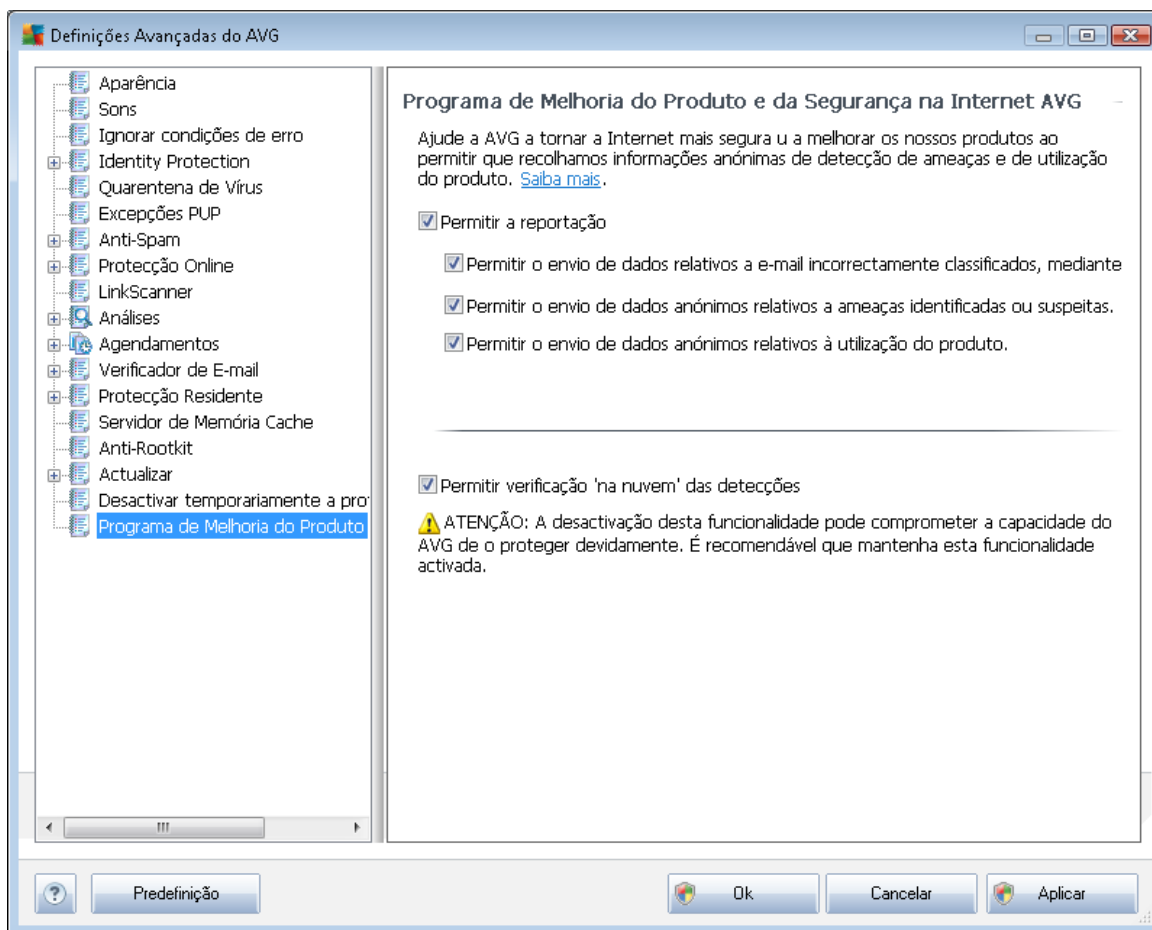
Na maioria dos casos, **não é necessário** desactivar o AVG antes de instalar novo software ou controladores, mesmo que o instalador ou o assistente do software sugiram que os programas e aplicações em execução devam ser encerrados primeiro para garantir que não ocorrem interrupções durante o processo de instalação. Caso enfrente problemas durante a instalação, experimente desactivar o componente **Protecção Residente** primeiro. Se efectivamente tiver de desactivar o AVG temporariamente, deverá reactivá-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.



9.18. 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. Marque a opção **Permitir a reportação** para permitir a reportação de ameaças detectadas à 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, e não são incluídos nos relatórios quaisquer dados de identificação pessoal. A reportação de ameaças detectadas é opcional, no entanto, pedimos-lhe que também active esta funcionalidade, uma vez que nos ajuda a melhorar a protecção da navegação on-line tanto para si como para outros utilizadores do AVG.



Hoje em dia, existem muitas mais ameaças do que os 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:

- **Um 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.

- **Um worm** é uma subcategoria de vírus que, ao contrário dos vírus, não precisa de um objecto "hospedeiro" para se juntar; envia-se a 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 um 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 das 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 de todos estes tipos diferentes de ameaças, o AVG inclui estes componentes especializados:

- **[Anti-Vírus](#)** para proteger o seu computador de vírus,
- **[Anti-Spyware](#)** para proteger o seu computador de spyware,



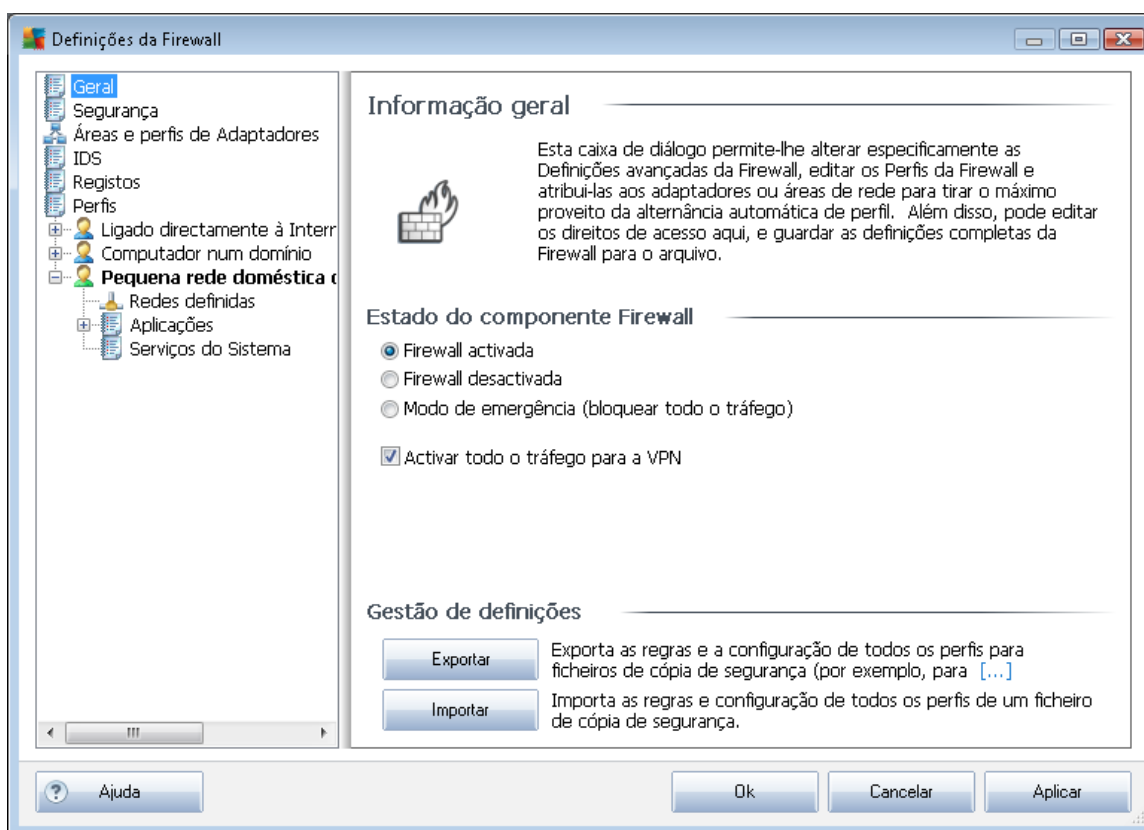
- [Protecção Online](#) para o proteger tanto de vírus como de spyware quando navega na Internet,
- [LinkScanner](#) para o proteger de outras ameaças on-line mencionadas neste capítulo.

10. Definições da Firewall

A configuração da [Firewall](#) abre numa nova janela onde pode configurar através de várias janelas parâmetros muito avançados do componente. **No entanto, a edição de configuração avançada é destinada apenas a utilizadores especialistas e experientes.**

10.1. 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

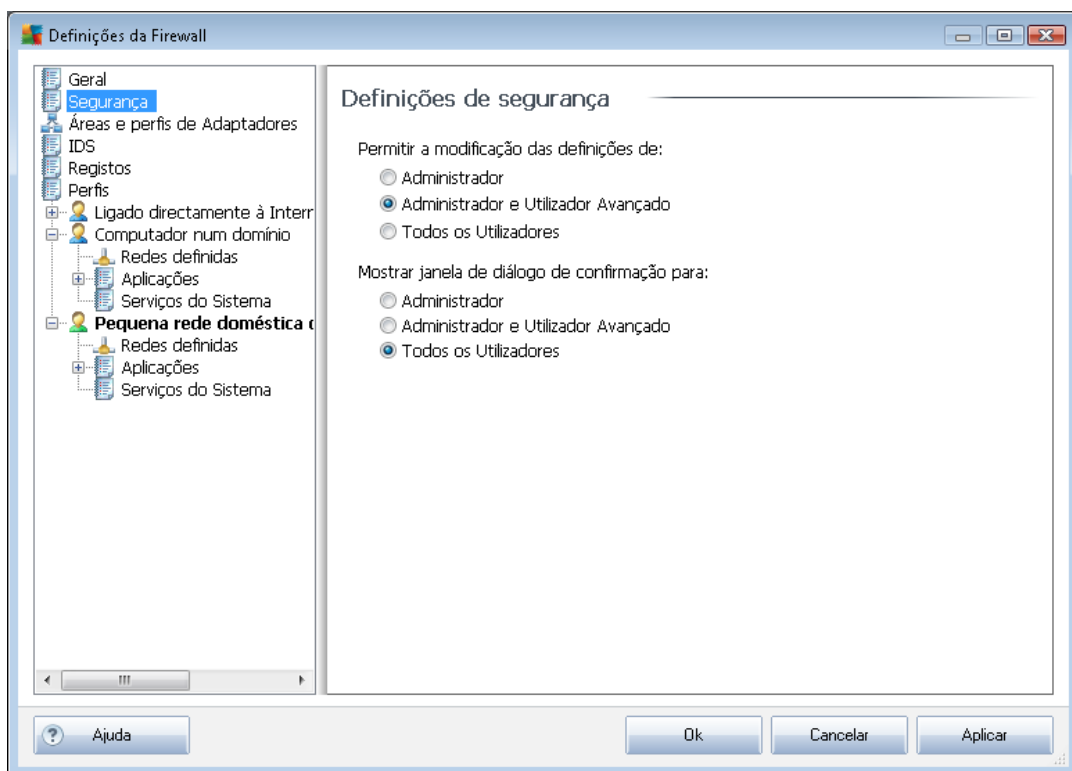
- **Activar todo o tráfego para a VPN** - se usar uma ligação VPN (Virtual Private Network - Rede Privada Virtual), ex. para se ligar ao escritório a partir de casa, recomendamos que marque a caixa. A **Firewall AVG** procurará automaticamente pelos adaptadores de rede, detectará os que são usados para 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 / 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.

10.2. Segurança



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

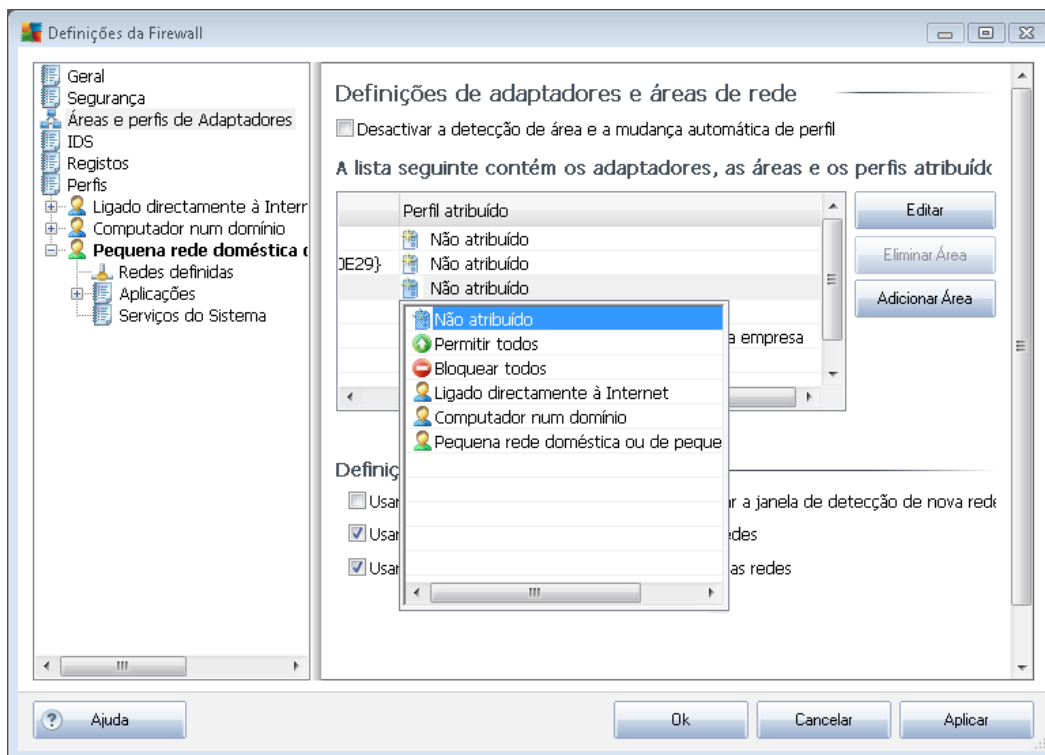
- **Permitir modificação de definições para** . especifique a quem é permitido alterar a configuração da [Firewall](#)
- **Apresentar janela de confirmação para**- especifique a quem a janela de confirmação (*janela a solicitar uma decisão numa situação que não está prevista por uma regra da [Firewall](#)*) 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

10.3. 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:





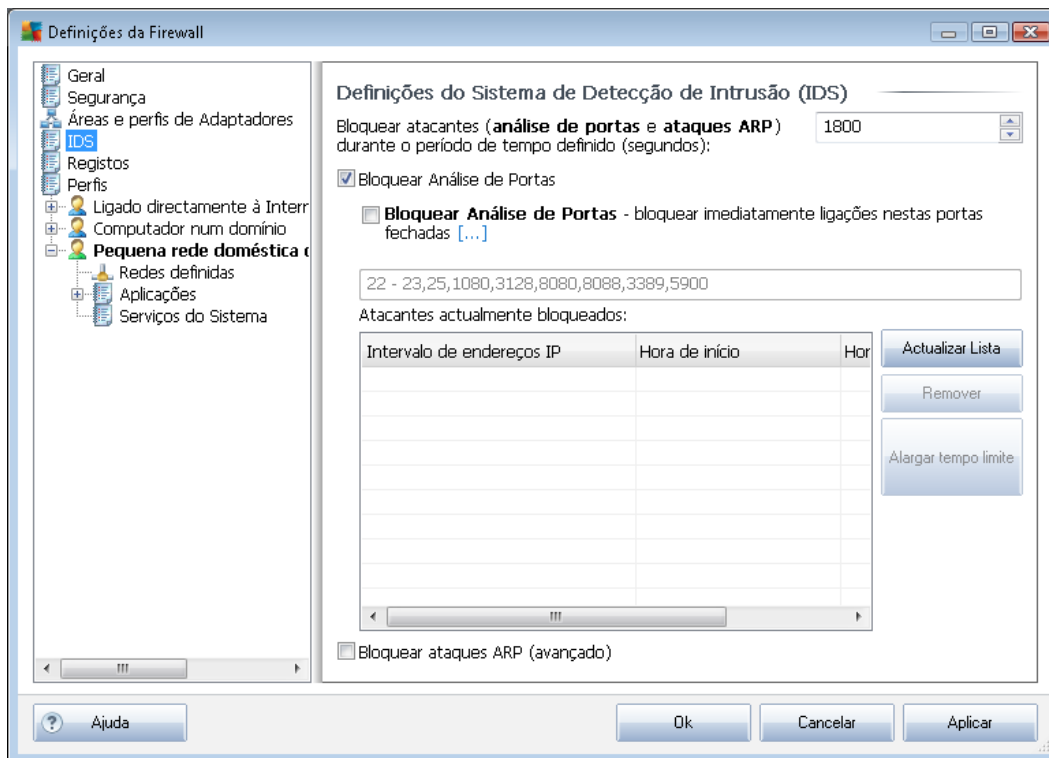
- **Desactivar a detecção de área e a mudança automática de perfil** - pode ser atribuído um dos perfis definidos a cada tipo de interface de rede, respectivamente a cada área. Se não quiser definir perfis específicos, será usado um perfil comum. No entanto, se decidir distinguir perfis e atribuí-los 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 no item respectivo na lista de adaptadores e seleccione o perfil.

Definições avançadas

- o **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.
- o **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).
- o **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).

10.4. IDS

O **Sistema de Detecção de Intrusão** 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 seguinte interface:



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

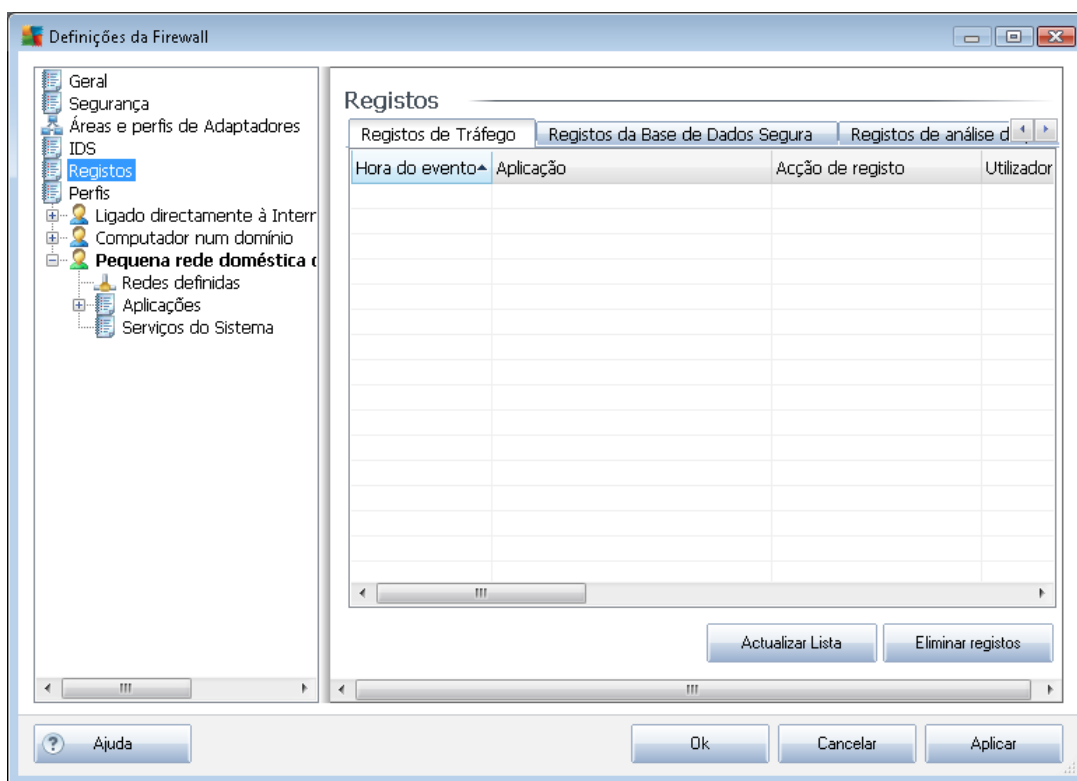
- **Bloquear os atacantes durante um período de tempo definido** - aqui pode especificar durante quantos segundos deverá a porta ser bloqueada sempre que for detectada uma tentativa de comunicação suspeita na mesma. Por predefinição, o tempo de intervalo está definido para 1800 segundos (30 minutos).
- **Bloquear Análise de Portas** - 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 **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.
 - o **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** activa o bloqueio de tipos especiais de tentativas de comunicação numa 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.

10.5. 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.

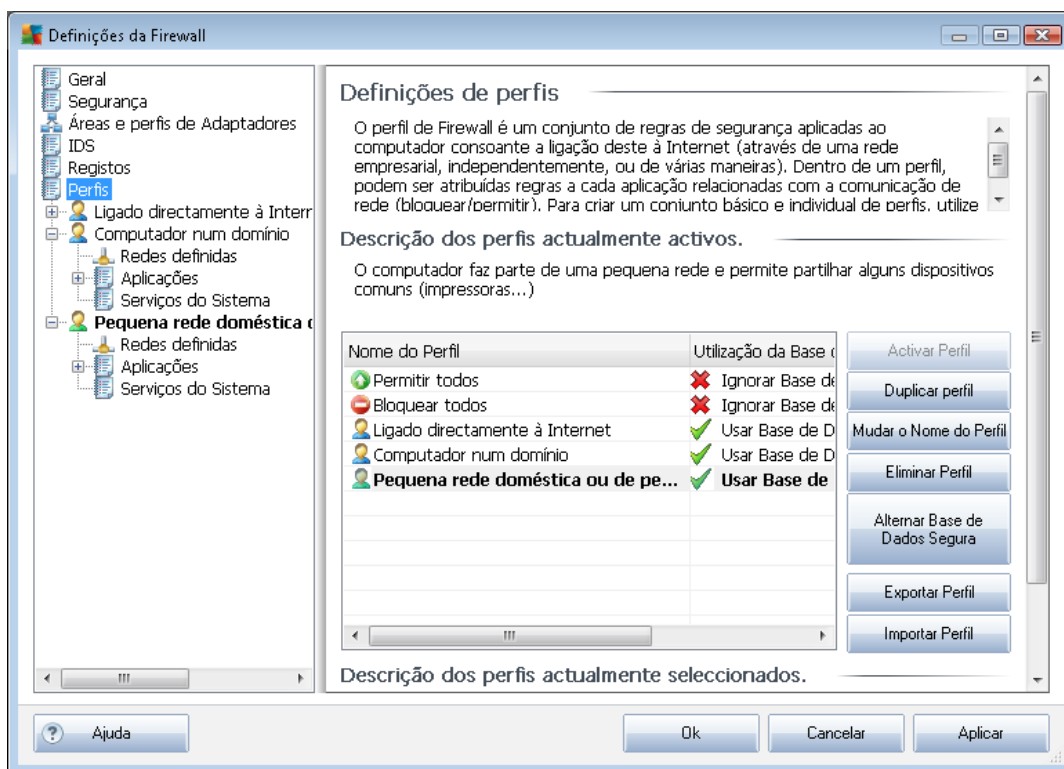
- **Registos de análise de portas** - providencia registo de todas as actividades do [Sistema de Detecção de Intrusão](#).
- **Registos ARP** - registo de informações sobre o bloqueio de tipos especiais de tentativas de comunicação numa rede local (opção [Bloquear ataques ARP](#)) detectadas pelo [Sistema 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.
- **Lista vazia** - eliminar todas as entradas na tabela.

10.6. Perfis

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



Todos os outros [perfis](#) de sistema podem então ser editados directamente nesta janela usando os seguintes 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.

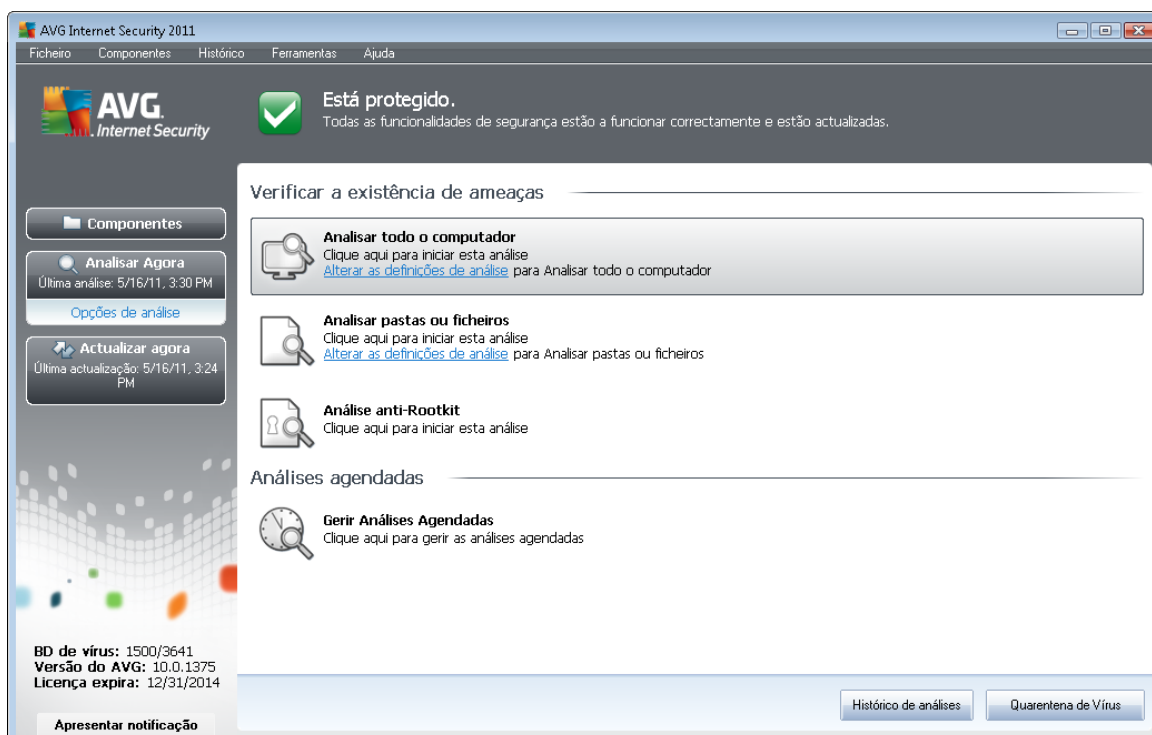
Consoante o número de perfis definidos que são mencionados na lista na janela **Perfil**, a estrutura do menu de navegação à esquerda será alterada em conformidade. Cada perfil definido cria uma secção específica no item **Perfil**. Podem ser editados perfis específicos nas seguintes janelas (*que são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



11. Análise do AVG

A análise é uma parte crucial do funcionamento do **AVG Internet Security 2011**. Pode executar testes a pedido ou [agendá-los para serem executados periodicamente](#) em alturas convenientes.

11.1. 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:
 - o [Análise de todo o computador](#)
 - o [Analisar pastas ou ficheiros específicos](#)
 - o [Análise anti-Rootkit](#)
- [secção agendamento de análise](#) - 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

11.2. Análises Predefinidas

Uma das principais funcionalidades do **AVG Internet Security 2011** 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.

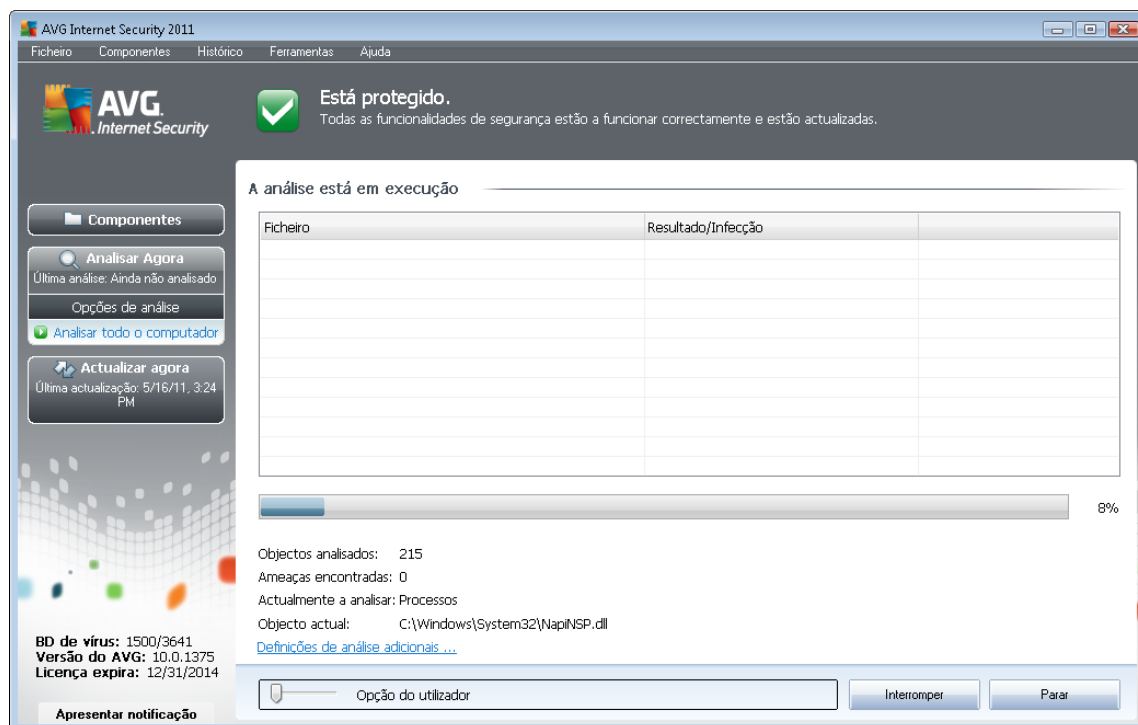
No **AVG Internet Security 2011** encontrará os seguintes tipos de análises predefinidas pelo fornecedor do software:

11.2.1. 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.

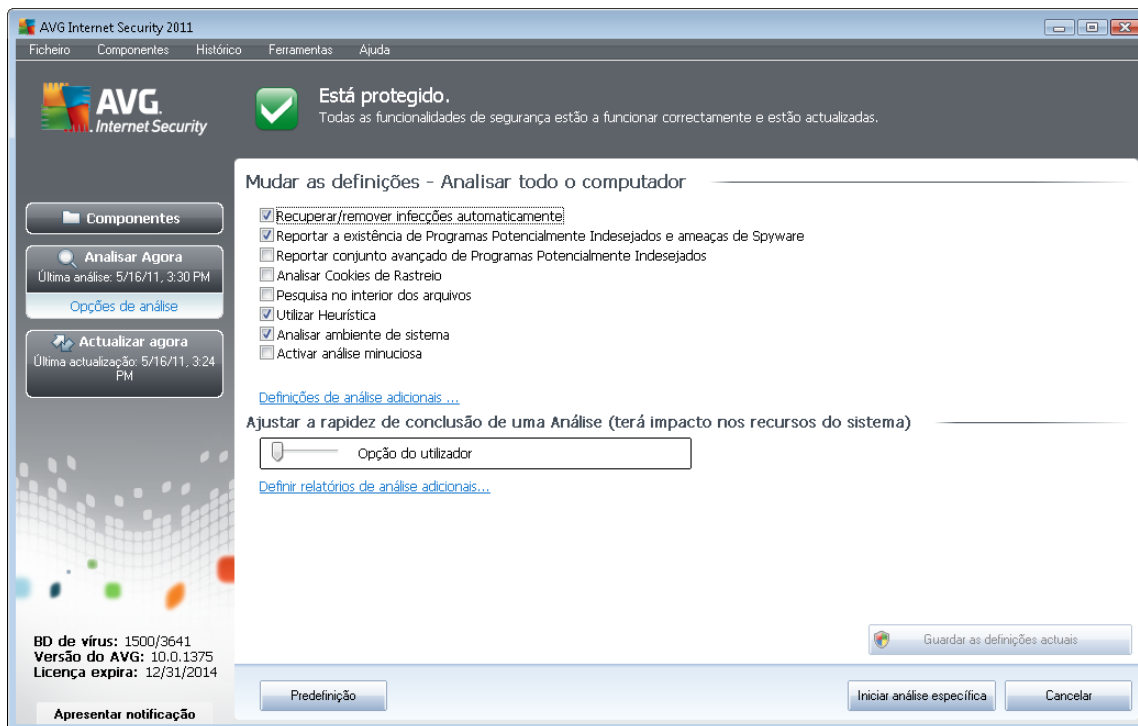
Início de análise

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

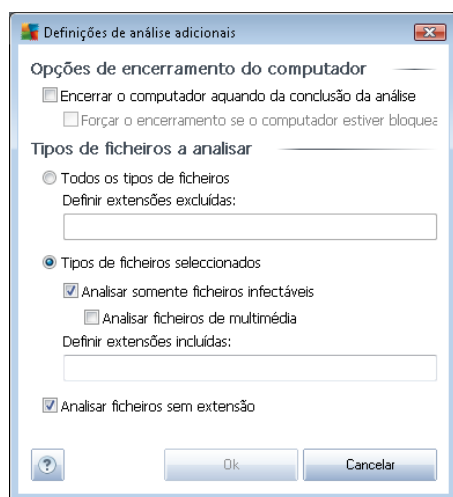
Tem a opção de editar as predefinições da análise da **Análise de todo o computador**. Clique no link **Alterar as definições de análise** para aceder à janela **Alterar as definições de análise da Análise de todo o computador** (acessível a partir da [interface de análise](#) através do link **Alterar 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:
 - o **Recuperar/remover infecção automaticamente** (activado por predefinição) - se for detectado um vírus durante a análise, o ficheiro 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](#).
 - o **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.
 - o **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.
 - o **Analisar a existência de Cookies de Rastreio** (desactivado por predefinição) - este parâmetro do componente [Anti-Spyware](#) define que as cookies deverão ser

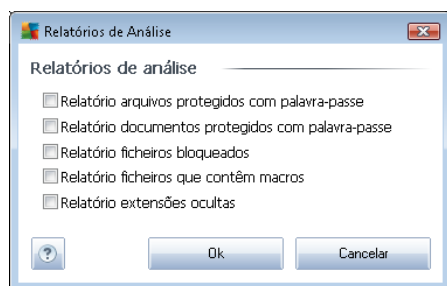
detectadas durante a análise; (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação específica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos*).

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



- o **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**).
- o **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.

11.2.2. 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



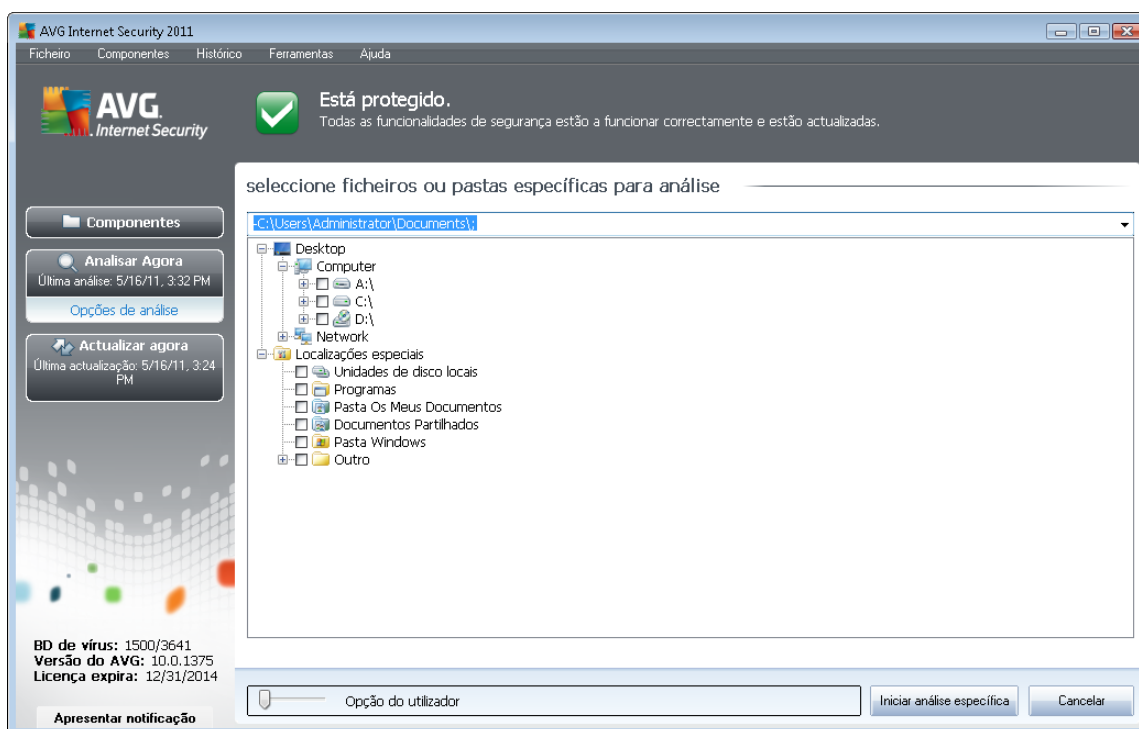
utilizada para configurar os seus próprios testes e os seus agendamentos consoante as suas necessidades.

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.

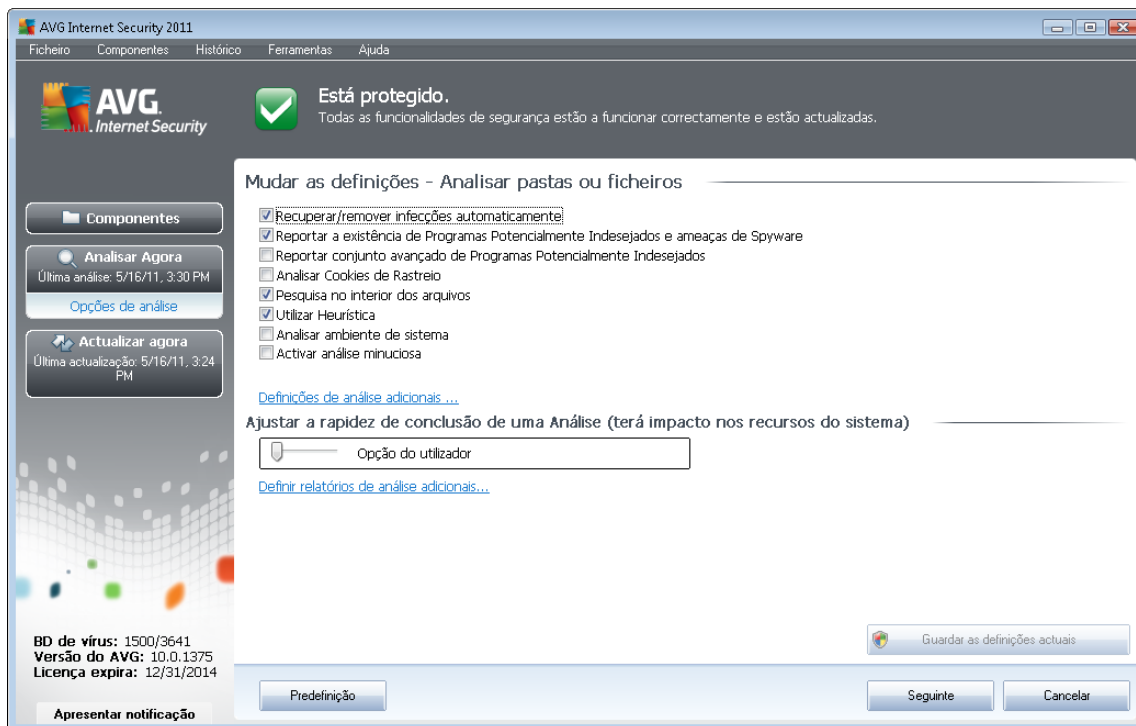
Também existe a possibilidade de analisar uma pasta específica excluindo todas as sub-pastas desta da análise; para isso deverá escrever um sinal de menos "-" à frente do caminho gerado automaticamente (veja a *captura de ecrã*). Para excluir toda a pasta da análise utilize o "!" parâmetro.

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

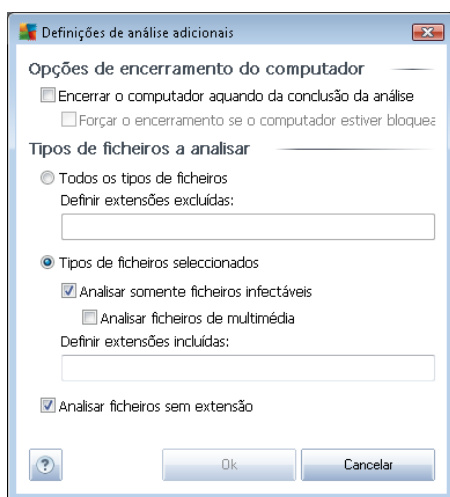
Tem a opção de editar as definições padrão predefinidas da análise **Analisar ficheiros e pastas específicos**. Clique no link **Alterar definições de análise** para ir para a janela **alterar definições de análise para a Análise de ficheiros e pastas específicos**. **É recomendável que mantenha das 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:
 - o **Recuperar/remover infecção automaticamente** (activado por predefinição) - se for detectado um vírus durante a análise, o ficheiro 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](#).
 - o **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.
 - o **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.
 - o **Analisar a existência de Cookies de Rastreio** (desactivado por predefinição) - este parâmetro do componente [Anti-Spyware](#) define que as cookies deverão ser

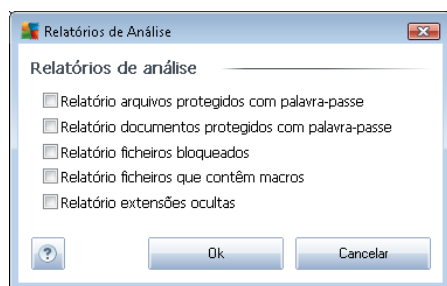
detectadas durante a análise (cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação específica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos).

- o **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,...
- o **Utilizar Heurística** (desactivado 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.
- o **Analisar o ambiente do sistema** (desactivado por predefinição) - a análise verificará também as áreas de sistema do seu computador.
- o **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:



- o **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**).
- o **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.
- **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](#)).

11.2.3. Análise Anti-Rootkit

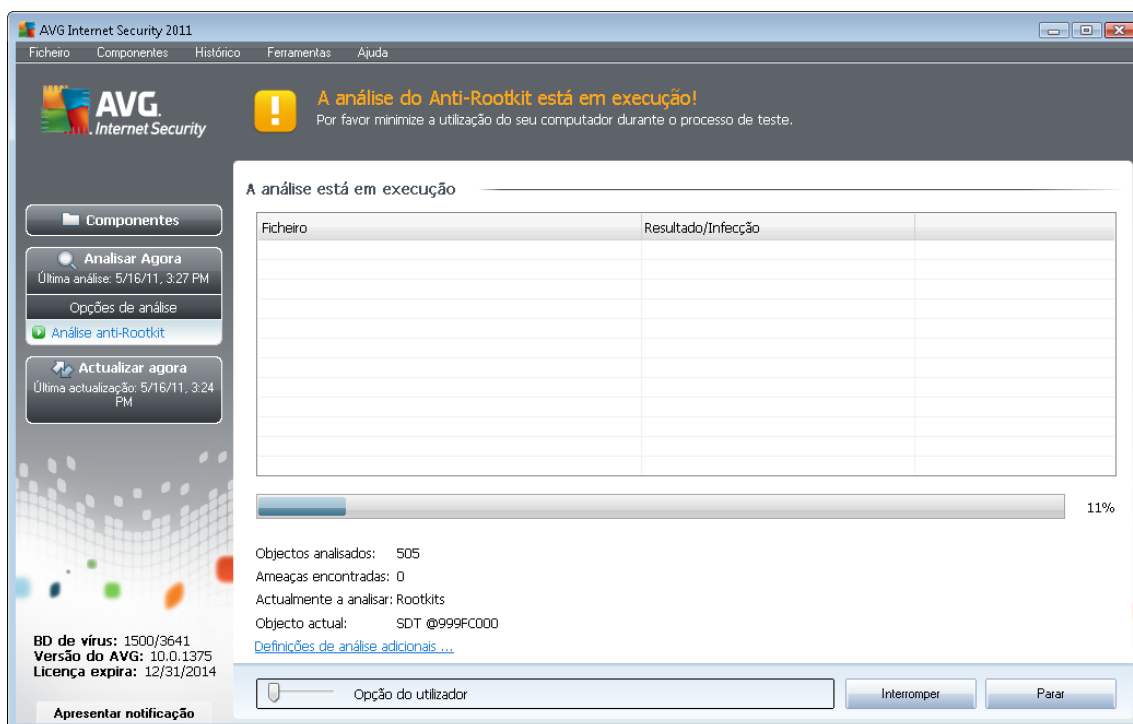
A **análise Anti-Rootkit** analisa o seu computador pela existência de eventuais rootkits (*programas e tecnologias que podem ocultar actividade de malware no seu computador*). Se for detectado um rootkit, isto não significa necessariamente que o computador esteja infectado. Em alguns casos,



podem ser erroneamente detectados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Início de análise

A **análise Anti-Rootkit** pode ser iniciada directamente a partir da [interface de análise](#) clicando no ícone de 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 (**Pausar**) ou cancelada (**Cancelar**) se necessário.

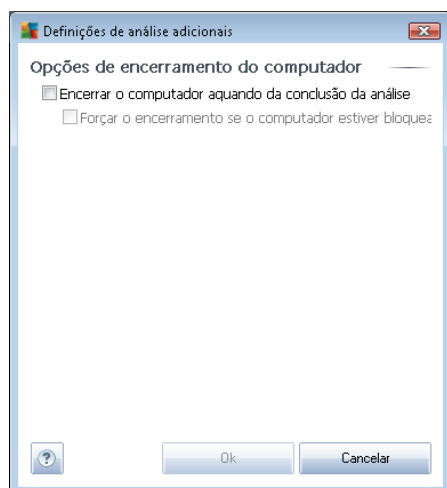


Edição da configuração de análise

A **análise Anti-Rootkit** é sempre iniciada a partir das predefinições e a edição dos parâmetros de análise só é acessível na janela [Definições Avançadas do AVG / Anti-Rootkit](#). A seguinte configuração está disponível na interface de análise, mas apenas durante a execução da análise:

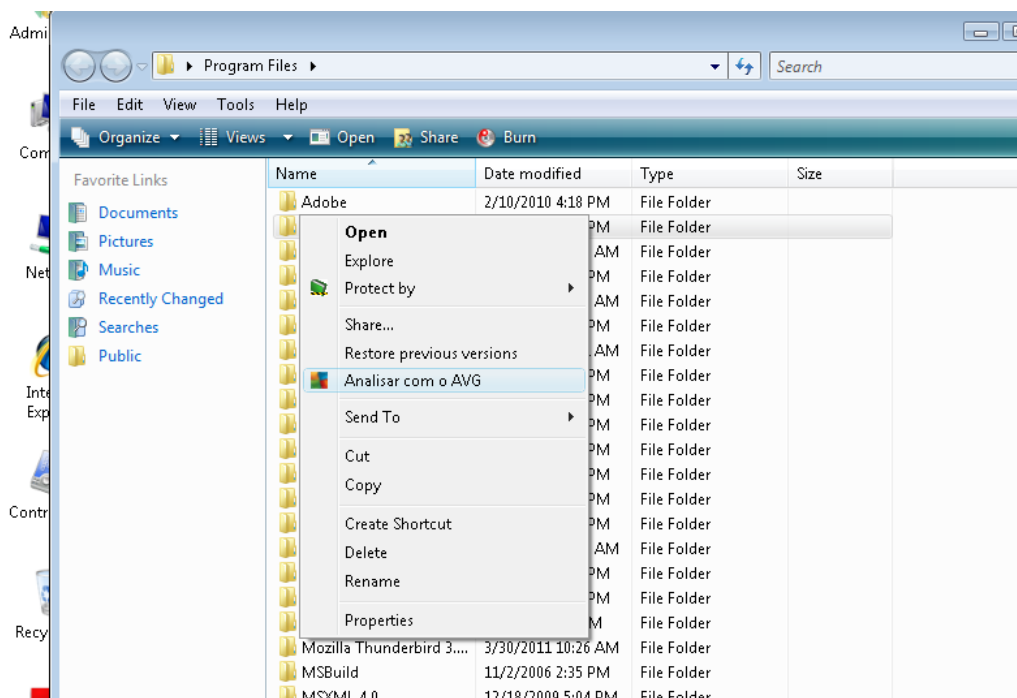
- **Análise automática** - pode usar o cursor para alterar a prioridade do processo de análise. O valor desta opção está, por predefinição, definido para o nível *Definida pelo utilizador* de utilização automática de recursos. Em alternativa, pode executar o processo de análise mais lentamente, o que 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*).

- **Definições de análise adicionais** - este link abre uma janela de **Definições de análise adicionais** onde pode definir possíveis condições de encerramento do computador relativas à **Análise Anti-Rootkit** (**Encerrar o computador aquando da conclusão da análise**, ou possivelmente **Forçar encerramento do computador se bloqueado**):



11.3. 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 2011** 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 verificar
- Clique com o botão direito do rato sobre o objecto para abrir o menu de contexto
- Seleccione a opção **Analisar com o AVG** para proceder à análise do ficheiro com o AVG

11.4. Análise da Linha de Comandos

No **AVG Internet Security 2011** 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.

11.4.1. 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
- **/MACROW** Reportar macros
- **/PWDW** Reportar ficheiros protegidos por palavra-passe
- **/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



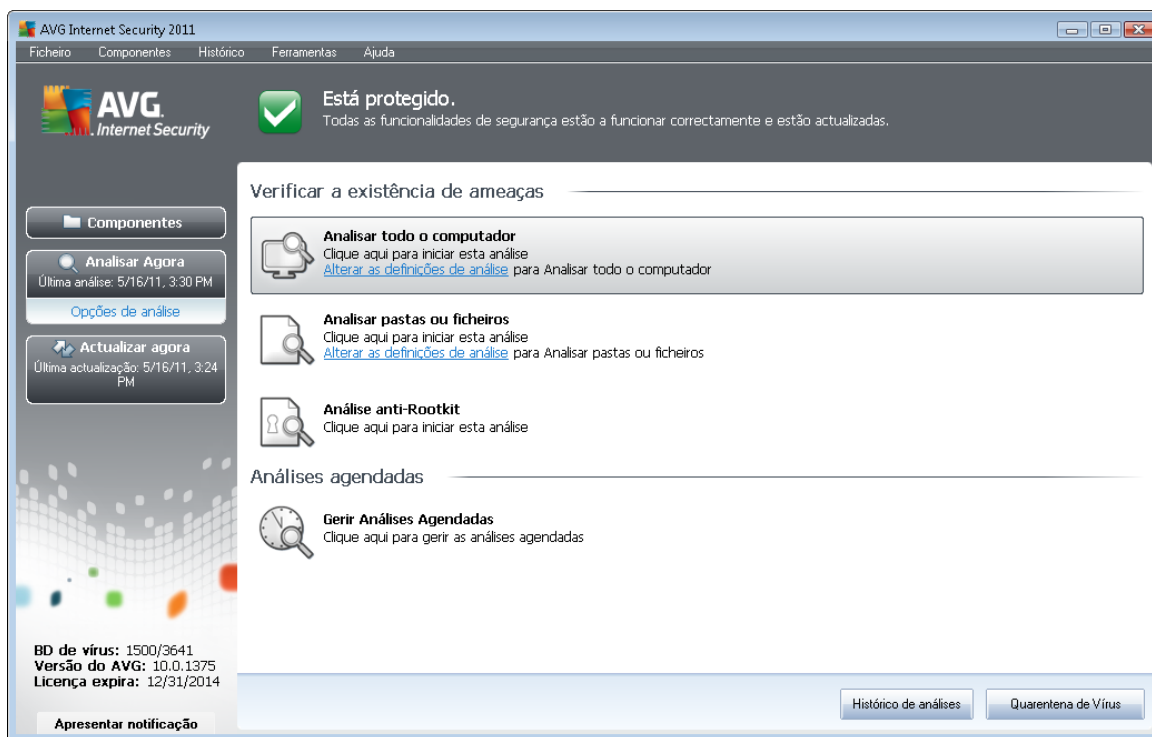
- **/PROC** Analisar processos activos
- **/PUP** Reportar ["Programas potencialmente indesejados"](#)
- **/REG** Analisar registo
- **/COO** Analisar cookies
- **/?** Apresentar ajuda neste tópico
- **/HELP** Apresentar ajuda acerca deste tópico
- **/PRIORITY** Defina a prioridade de análise /Baixa, 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)
- **/ARCBOMBSW** Reportar ficheiros de arquivo recomprimidos

11.5. Agendamento de Análise

Com o **AVG Internet Security 2011** 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.

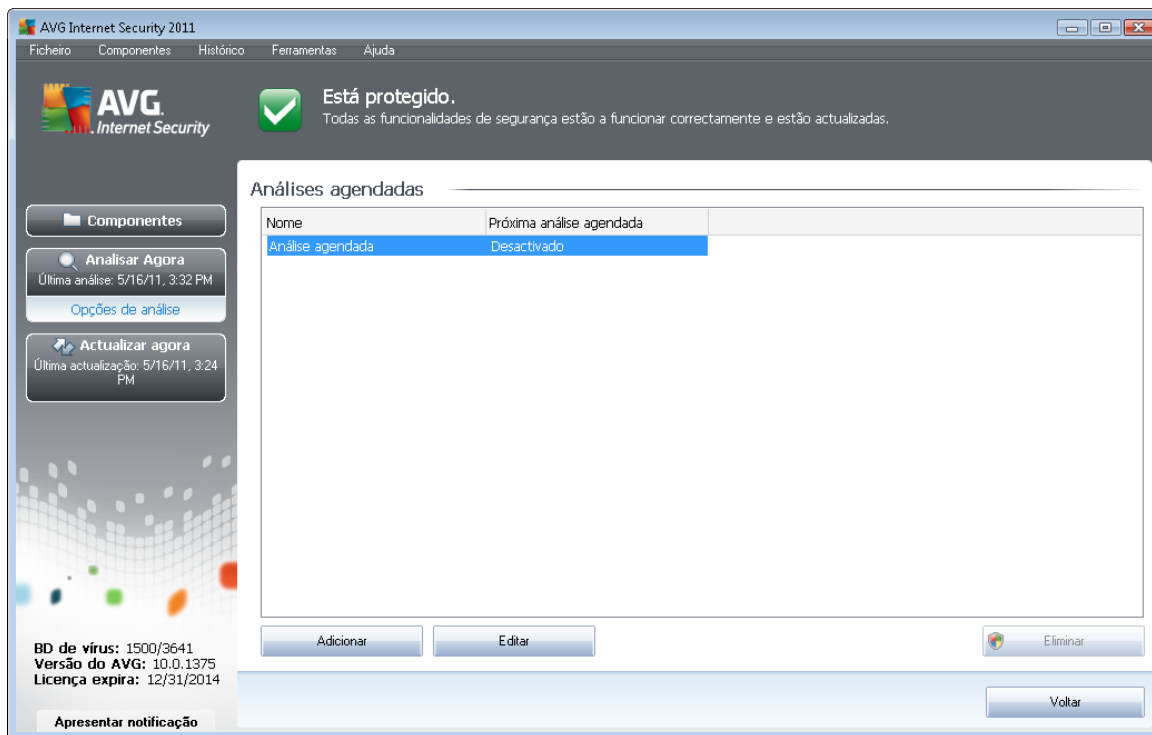
Deve executar a [Análise de todo o computador](#) regularmente, pelo menos uma vez por semana. No entanto, se possível, execute a análise de todo computador diariamente - conforme configurado na configuração de agendamento de análise predefinida. Se o computador estiver "sempre ligado" então pode agendar 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:

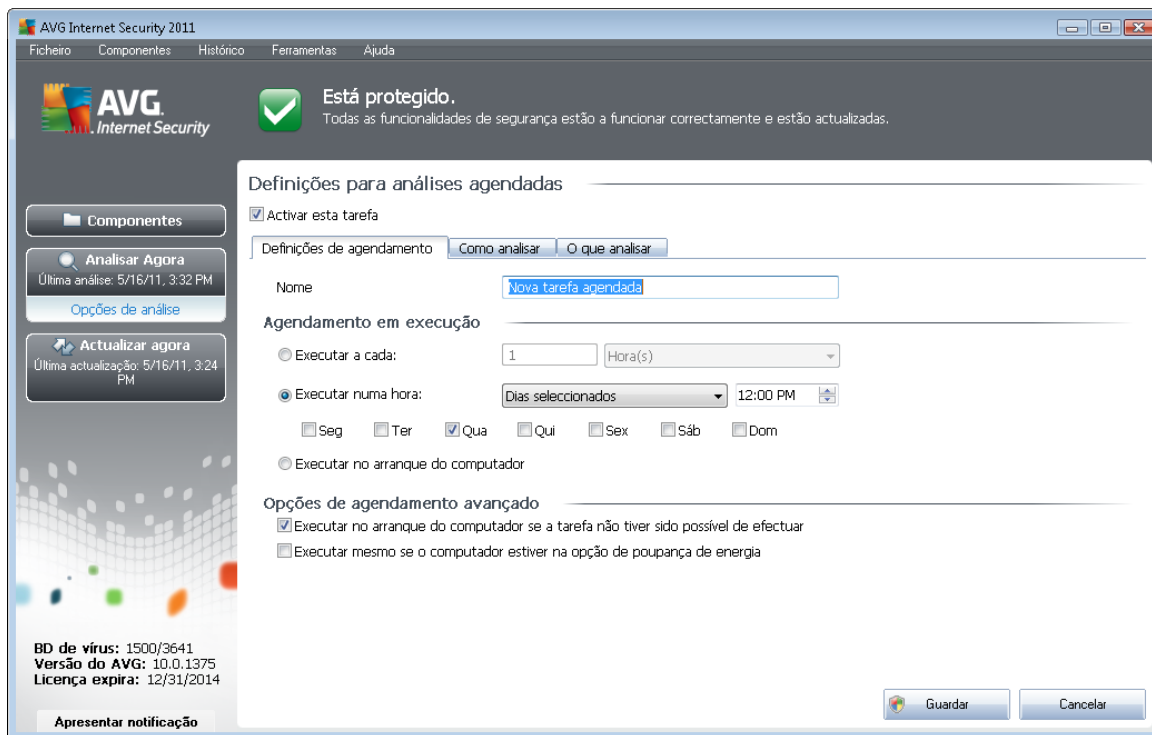


Pode editar / adicionar análises por meio dos seguintes botões de controlo:

- **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](#)

11.5.1. 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:

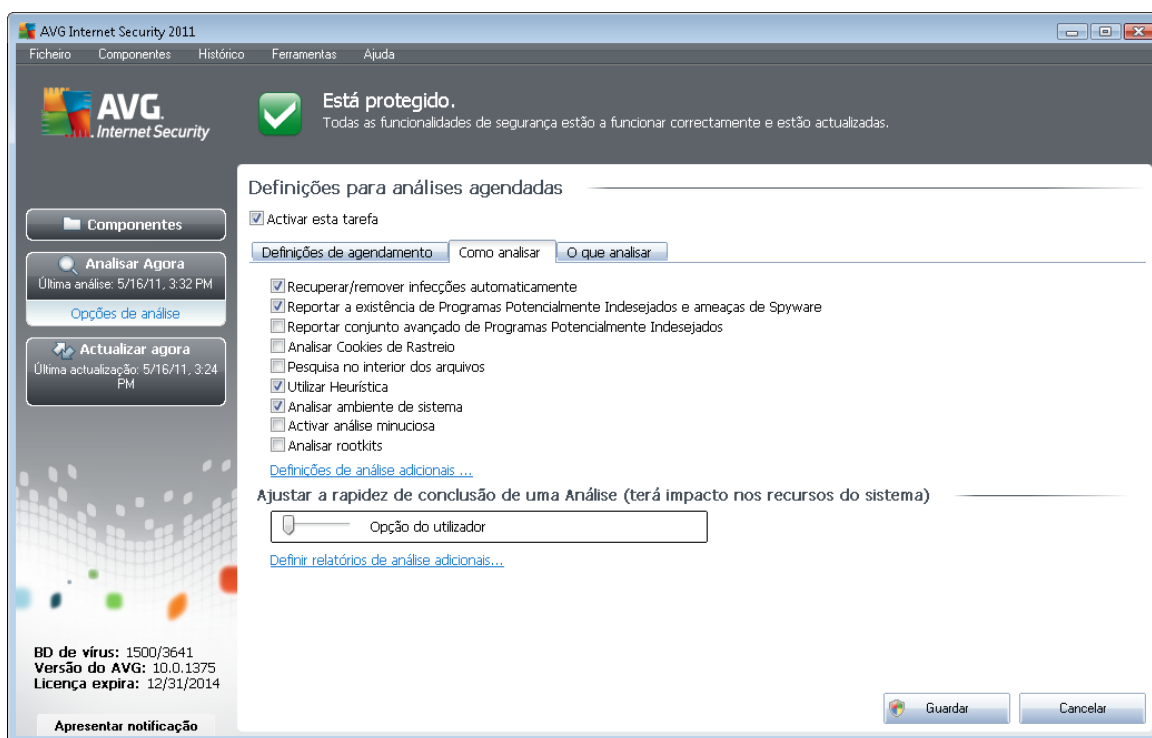
- **Agendamento em execução** - especifique os intervalos de tempo para a execução do novo agendamento de análise. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (**Executar a cada ...** ou definindo uma data e hora precisas (**Executar a uma hora específica ...**), ou ainda definindo um evento ao qual a execução da actualização esteja associada (**Ação 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](#).

11.5.2. 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:

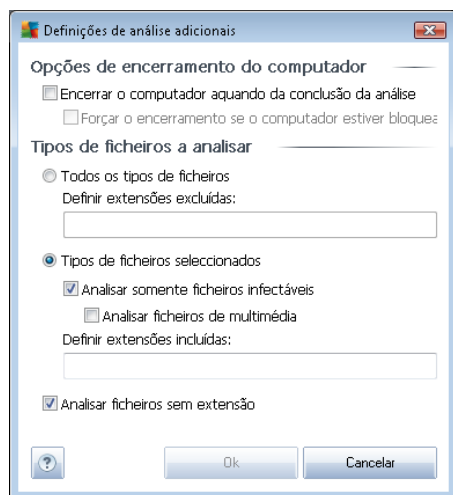
- **Recuperar/remover infecção automaticamente** (activado por predefinição): se for detectado um vírus durante a análise, o ficheiro pode ser recuperado automaticamente se houver uma cura disponível. Na eventualidade de o ficheiro infectado não poder ser recuperado automaticamente, ou se decidir desactivar 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 Rastreo** (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, rastreo, e manutenção de informação específica 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.

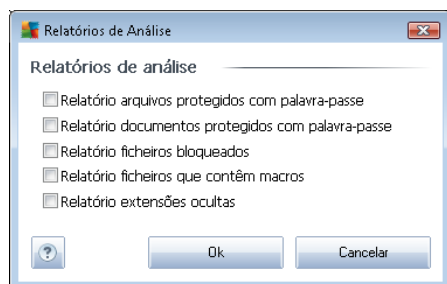
Depois, pode alterar a configuração de análise da seguinte forma:

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



- o **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**).
- o **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:



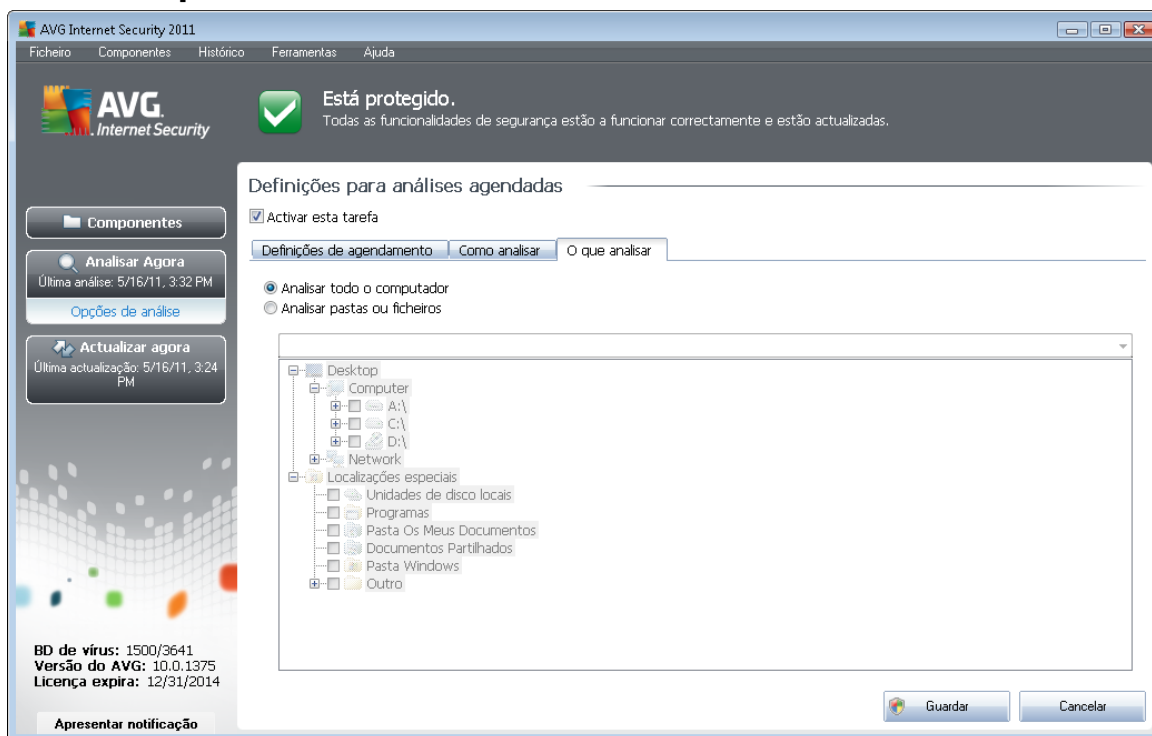
Nota: A configuração de análise está predefinida para um desempenho ideal. A menos que tenha uma razão válida para alterar as definições de análise, é recomendável que mantenha a configuração predefinida. Quaisquer alterações à configuração deverão ser efectuadas exclusivamente por utilizadores avançados. Para mais opções de configuração de análise consulte a janela [Definições avançadas](#) acessível via o item **Ficheiro / Definições Avançadas** do menu de sistema.

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](#).

11.5.3. 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**
 - o C:\Ficheiros de Programas\
 - o na versão de 64 bits C:\Ficheiros de Programas (x86)
- **Pasta Os Meus Documentos**



o para o Win XP: C:\Documents and Settings\Default User\Os Meus Documentos\

o para o Windows Vista/7: C:\Users\utilizador\Documentos\

- **Documentos Partilhados**

o para o Win XP: C:\Documents and Settings\All Users\Documentos\

o para o Windows Vista/7: C:\Users\Public\Documentos\

- **Pasta Windows - C:\Windows**

- **Outra**

o *Unidade de sistema* - a unidade de disco rígido na qual o sistema operativo está instalado (normalmente C:)

o *Pasta de sistema* - C:\Windows\System32\

o *Pasta dos Ficheiros Temporários* - C:\Documents and Settings\User\Local\ (Windows XP); ou C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)

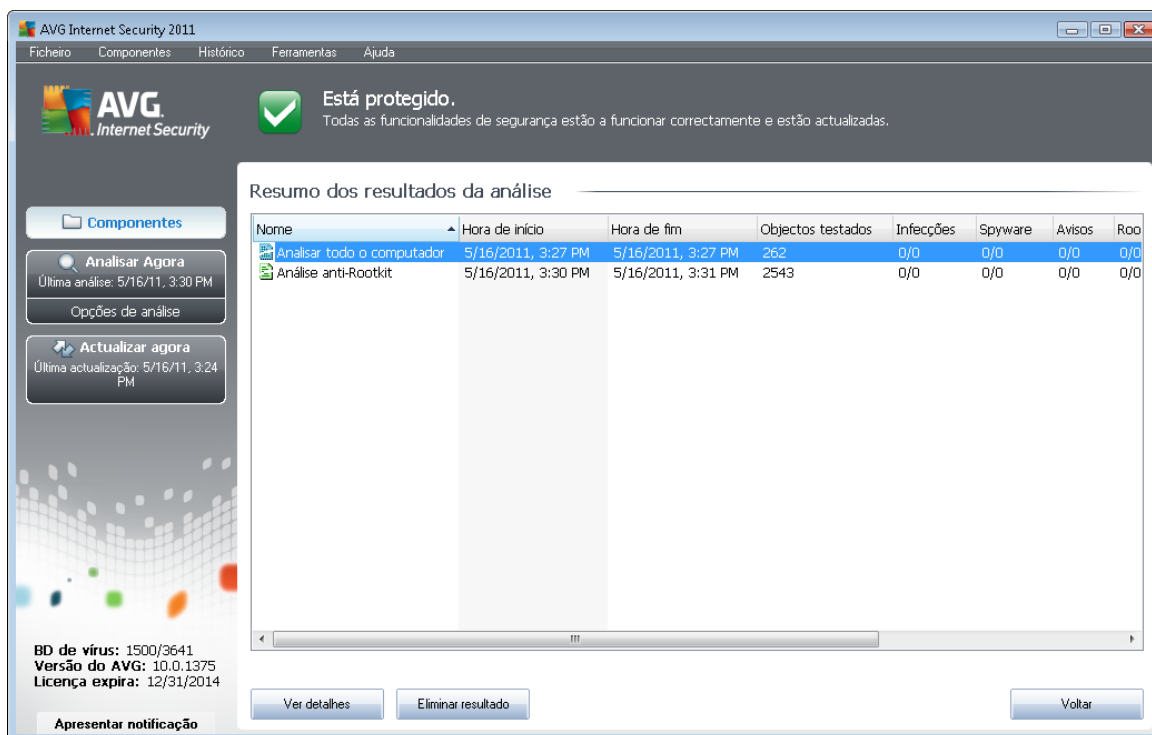
o *Ficheiros Temporários da Internet* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); ou C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Botões de controlo 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](#).

11.6. 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 facultava 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 botão **Ver detalhes** (na parte inferior desta janela).



- **Hora de início** - 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
- **Infeções** - número de [infeções 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](#)

11.7. 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:

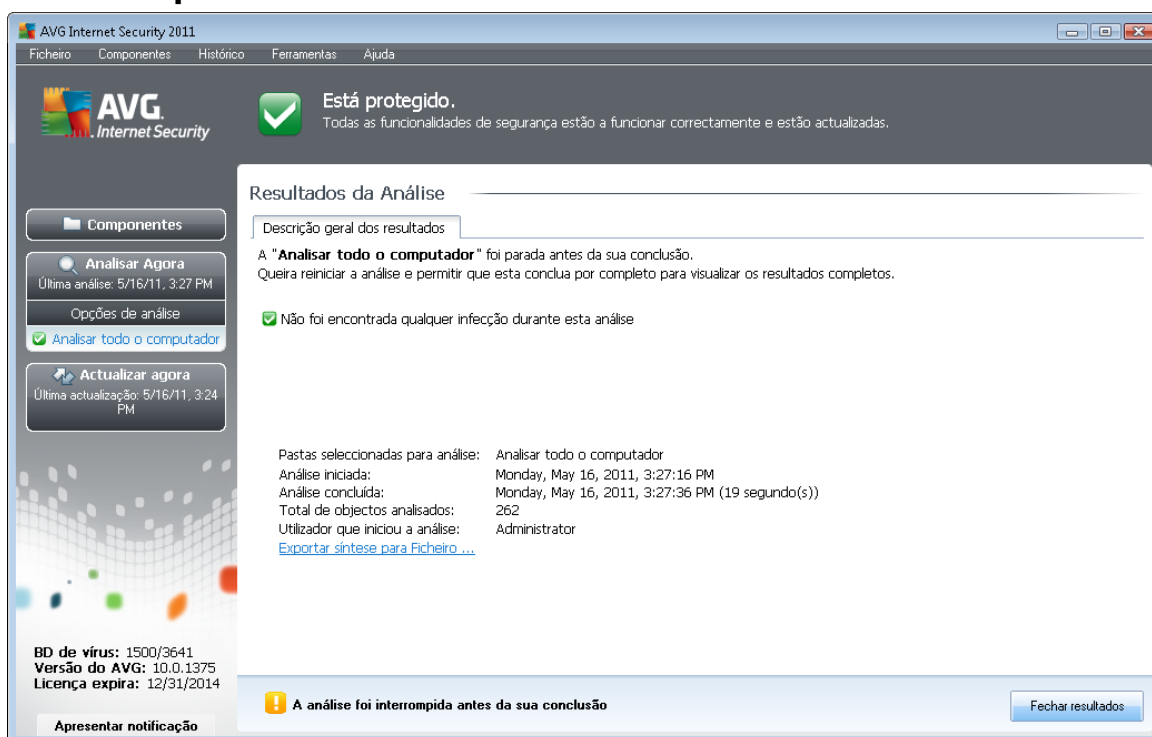
- **Síntese de Resultados** - este separador é apresentado constantemente e faculta dados estatísticos que descrevem o progresso da análise
- **Infeções** - este separador só é apresentado se tiver sido detectada alguma [infeção de vírus](#) durante a análise
- **Spyware** - este separador só é apresentado 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 facultava mensagem de aviso aquando da detecção. Além disso, encontrará aqui informações sobre objectos que não foi possível analisar (ex. arquivos protegidos por palavra-passe).

11.7.1. 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 início da análise, ao número total de objectos analisados, à duração da análise e ao número de erros que tenham ocorrido durante a análise.

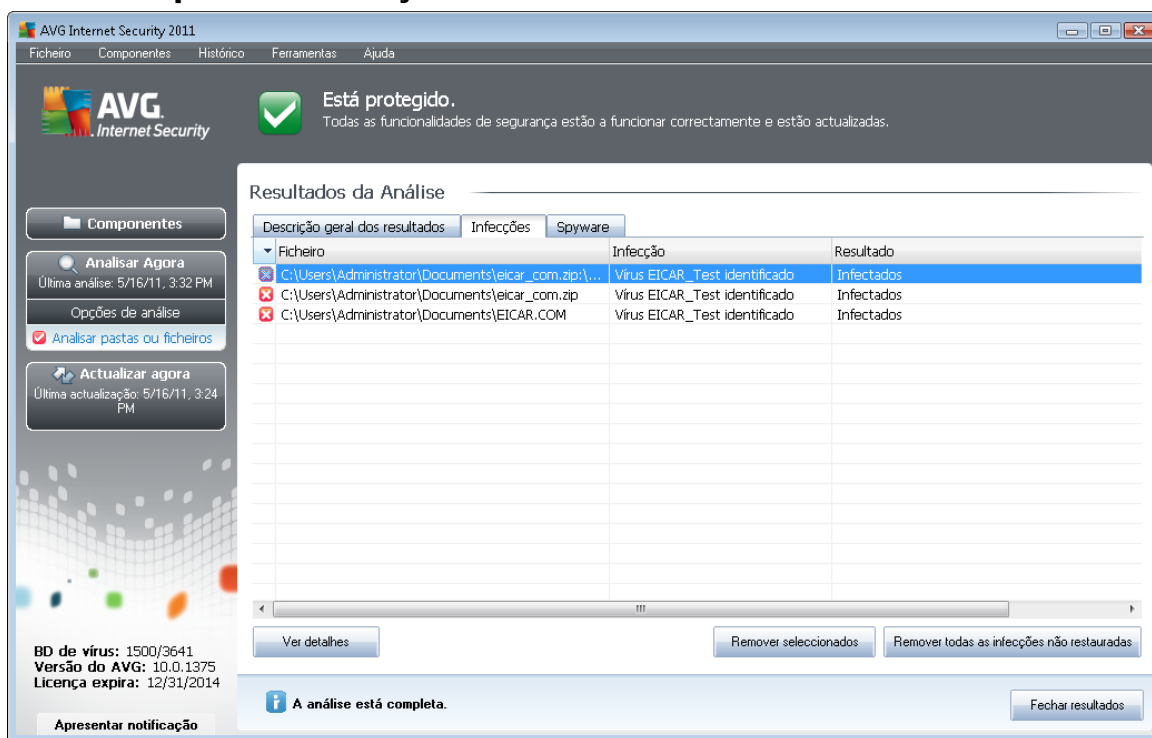
Botões de controlo

Existe um botão de controlo disponível nesta janela. O botão **Fechar resultados** remete para a



janela [Resumo dos resultados da análise](#).

11.7.2. Separador Infecções



O separador **Infecções** só é apresentado na janela **Resultados da Análise** se [tiver sido detectada alguma infecção](#) durante a análise. O separador está dividido em três secções que facultam a seguinte informação:

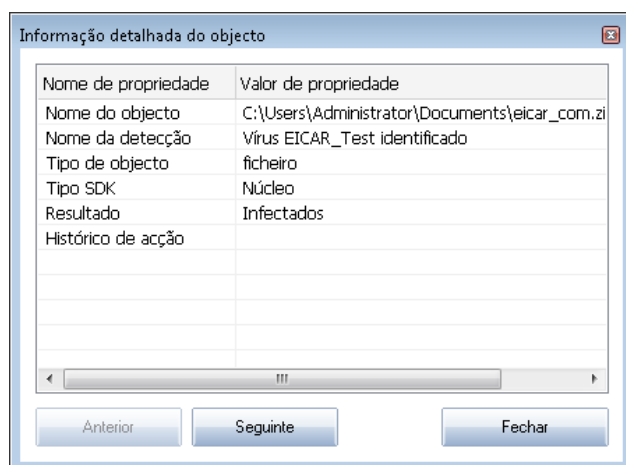
- **Ficheiro** - localização original completa do objecto infectado
- **Infecções** - nome do [vírus detectado](#) (para detalhes específicos relativos a vírus por favor consulte a [Enciclopédia de vírus](#) on-line)
- **Resultado** - define o estado actual do objecto infectado que foi detectado durante a análise:
 - o **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)
 - o **Recuperado** - o objecto infectado foi recuperado automaticamente e mantido na sua localização original
 - o **Movido para a Quarentena de Vírus** - o objecto infectado foi movido para a [Quarentena de Vírus](#)
 - o **Eliminado** - o objecto infectado foi eliminado

- o **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](#))
- o **Ficheiro bloqueado - não testado** - o objecto detectado está bloqueado e o AVG não o consegue analisar
- o **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
- o **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** :

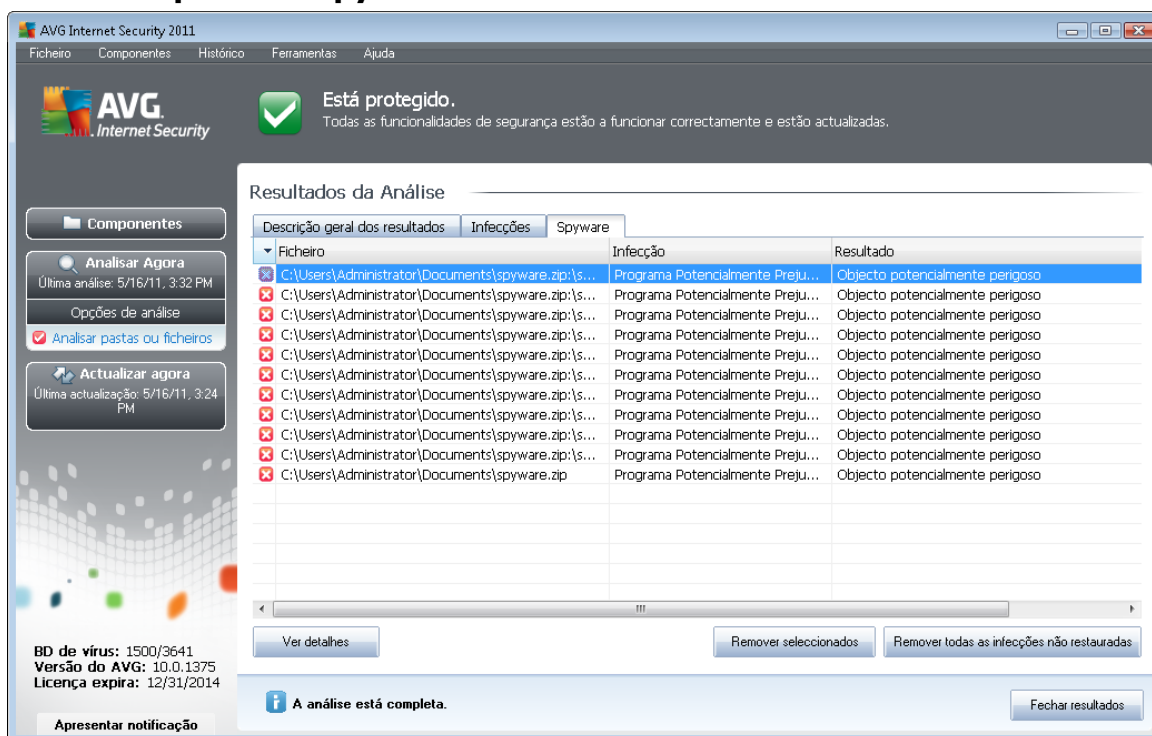


Nesta janela pode encontrar informações detalhadas sobre o objecto infeccioso detectado (ex. nome e localização do objecto infectado, tipo de objecto, tipo SDK, resultado da detecção e histórico das acções associadas ao objecto detectado). Ao utilizar os botões **Anterior/ Seguinte** pode visualizar informações relativas a detecções específicas. 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

11.7.3. 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:

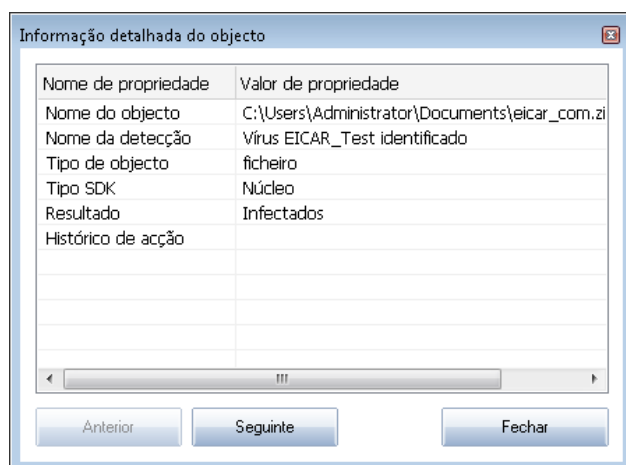
- **Ficheiro** - localização original completa do objecto infectado
- **Infecções** - nome do spyware detectado (para detalhes relativos a vírus específicos por favor consulte a Enciclopédia de vírus on-line)
- **Resultado** - define o estado actual do objecto infectado que foi detectado durante a análise:
 - o **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)
 - o **Recuperado** - o objecto infectado foi recuperado automaticamente e mantido na sua localização original
 - o **Movido para a Quarentena de Vírus** - o objecto infectado foi movido para a Quarentena de Vírus
 - o **Eliminado** - o objecto infectado foi eliminado

- o **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)
- o **Ficheiro bloqueado - não testado** - o objecto detectado está bloqueado e o AVG não o consegue analisar
- o **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
- o **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 específicas. 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

11.7.4. 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 for detectado apenas um Aviso durante um teste do AVG, 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 AVG 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.

11.7.5. Separador Rootkits

O separador **Rootkits** apresenta informações sobre os rootkits detectados durante a análise se tiver iniciado a [Análise Anti-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.

A estrutura deste separador é basicamente a mesma do [separador Infecções](#) ou do [separador Spyware](#).

11.7.6. 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 pode detectar ficheiros que podem não estar infectados, mas que são suspeitos. Estes ficheiros são reportados como [Aviso](#).

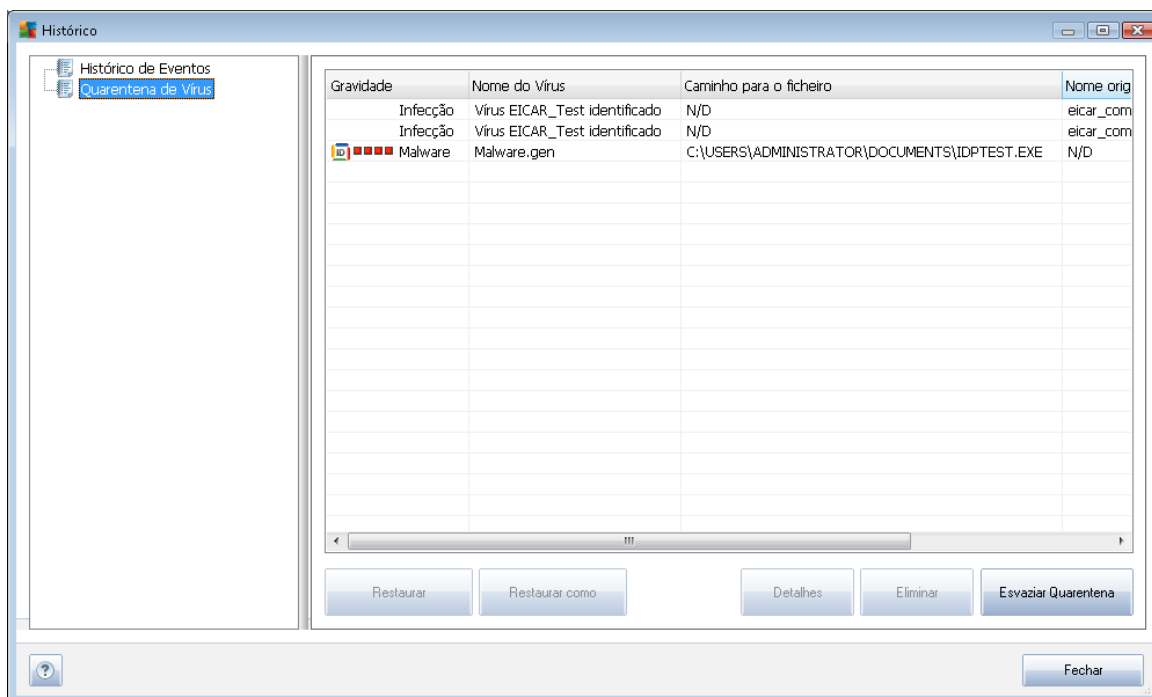


ou como **Informação**.

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 (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 reporta esses ficheiros para evitar a abertura accidental 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 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. Isto normalmente significa que existe um ficheiro que está constantemente a ser usado pelo sistema (ex. *ficheiro swap*).

11.8. 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 2011**, 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

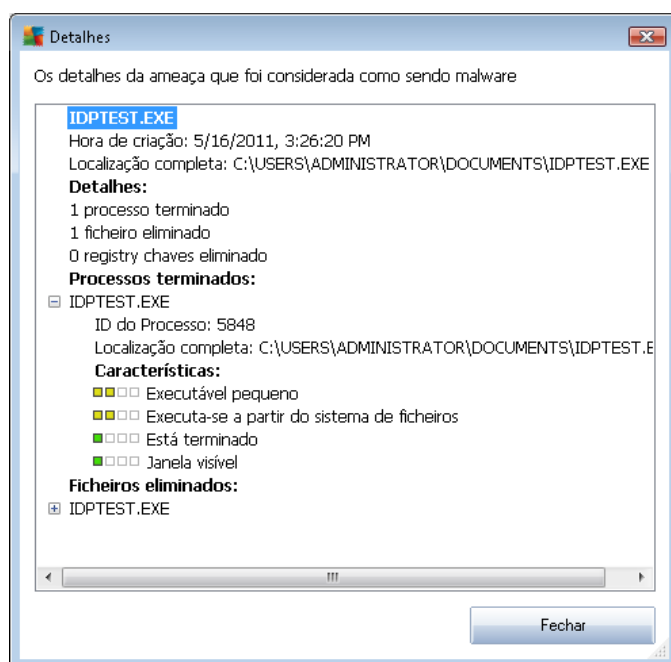
eventualidade de o objecto ter um nome específico que seja conhecido (ex. o nome de um anexo de e-mail que não corresponde ao conteúdo efectivo do anexo), este será facultado nesta coluna.

- **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).



12. Actualizações do AVG

Manter o seu AVG actualizado é essencial para assegurar que todos os vírus recém descobertos serão detectados assim que possível.

Uma vez que as actualizações do AVG não são lançadas em conformidade com qualquer período pré-determinado, mas antes em função da quantidade e gravidade das novas ameaças, é recomendável que verifique a existência de novas actualizações pelo menos uma vez por dia ou com maior frequência. Só desta forma terá a certeza de que o seu **AVG Internet Security 2011** também é mantido actualizado durante o dia.

12.1. Níveis de Actualização

O AVG faculta dois níveis de actualização dos quais pode escolher:

- **Definições de actualização** contém alterações necessárias para uma protecção anti-vírus 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 seleccionar o nível de prioridade que deve ser transferido e aplicado.

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.

12.2. Tipos de Actualização

É possível distinguir dois tipos de actualização:

- **A actualização manual** consiste numa actualização imediata do AVG que pode ser executada sempre que for necessário.
- **Actualização agendada** - no AVG, também é possível [predefinir um plano de actualização](#). A actualização programada é então executada periodicamente, de acordo com a configuração definida. Sempre que existem novos ficheiros de actualização na localização especificada, são transferidos directamente a partir da Internet ou de um directório da rede. Quando não existem novas actualizações disponíveis, nada acontece.

12.3. Processo de Actualização

O processo de actualização pode ser executado imediatamente à medida que a necessidade surge via o [link rápido Actualizar agora](#). Este link está constantemente disponível a partir de qualquer janela da [Interface do utilizador do AVG](#). No entanto, ainda é altamente recomendável efectuar actualizações regularmente conforme expresso no agendamento de actualizações editável no componente [Actualizações](#).

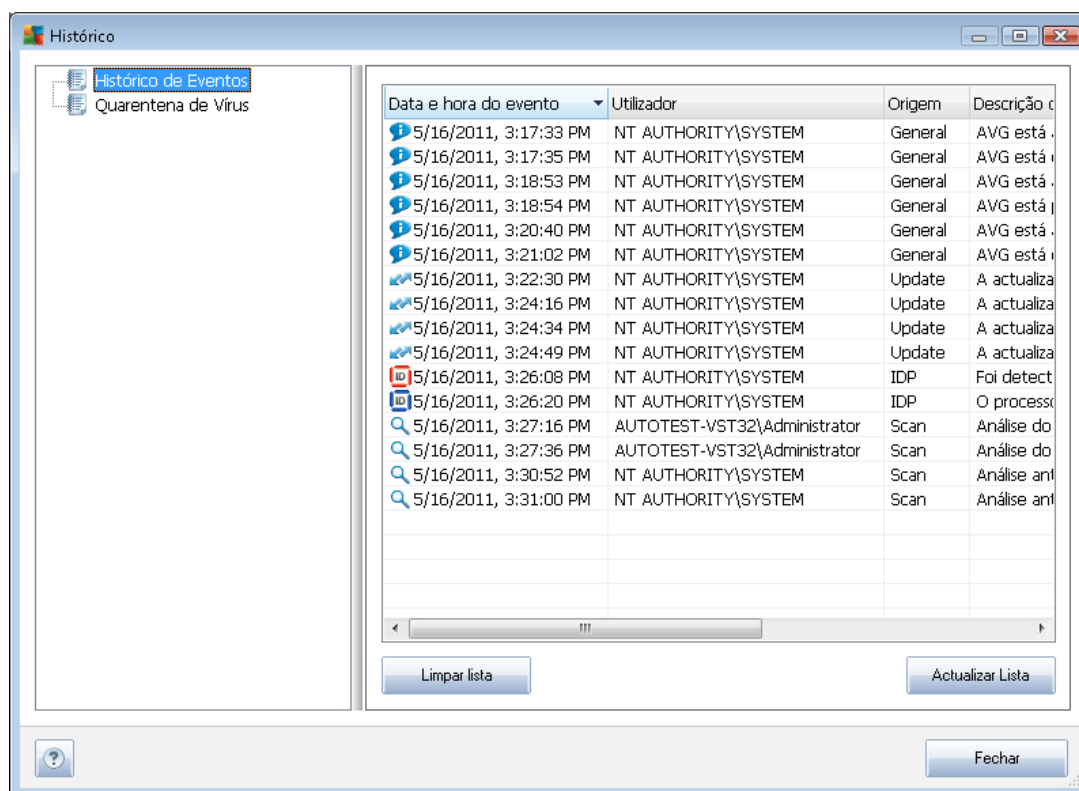
Assim que inicia a actualização, o AVG verifica a existência de novos ficheiros de actualização disponíveis. Se assim for, o AVG inicia a transferência e executa o processo de actualização



autonomamente. 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, ...*).

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 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. Recomendado apenas a utilizadores avançados!*

13. 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 2011**. O **Histórico** regista os seguintes tipos de eventos:

- Informações acerca das actualizações da aplicação do AVG
- Início, conclusão ou interrupção de análises (*incluindo as análises executadas automaticamente*)
- Eventos relacionados com a detecção de vírus (*pela [Protecção Residente](#) ou 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** apresenta quem iniciou o evento
- **Origem** apresenta o 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

- **Limpar Lista** - eliminar todas as entradas na lista de eventos
- **Actualizar Lista** - actualizar todas as entradas na lista de eventos



14. FAQ e Suporte Técnico

Se tiver qualquer tipo de problemas com o seu AVG, de natureza comercial ou técnica, consulte a secção [Perguntas Frequentes](http://www.avg.com/) no website do AVG (<http://www.avg.com/>).

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