



AVG 9 Anti-Virus plus Firewall

Manual do Utilizador

Revisão do documento 90.21 (3.2.2010)

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	7
2. Requisitos de Instalação do AVG	8
2.1 Sistemas Operativos Suportados	8
2.2 Requerimentos Mínimos e Recomendados de Hardware	8
3. Opções de Instalação do AVG	9
4. Gestor de Transferências do AVG	10
4.1 Selecção do Idioma	10
4.2 Verificação de Conectividade	11
4.3 Definições de Proxy	12
4.4 Transferir os Ficheiros a Instalar	13
5. Processo de Instalação do AVG	14
5.1 Execução da Instalação	14
5.2 Contrato de Licença	15
5.3 A verificar o Estado do Sistema	15
5.4 Seleccionar Tipo de Instalação	16
5.5 Activar a Licença do seu AVG	16
5.6 Instalação Personalizada - Pasta de Destino	18
5.7 Instalação Personalizada - Selecção de Componentes	19
5.8 Barra de Ferramentas de Segurança do AVG	20
5.9 Fechar aplicações abertas	21
5.10 A instalar o AVG	22
5.11 Agendar análises e actualizações regulares	23
5.12 Selecção de utilização do computador	23
5.13 A ligação à Internet do seu computador	24
5.14 A configuração da protecção do AVG está concluída	25
6. Após a Instalação	26
6.1 Optimização da análise	26
6.2 Registo do Produto	26
6.3 Aceder à Interface do Utilizador	26
6.4 Análise de todo o computador	27
6.5 Teste Eicar	27

6.6 Configuração Predefinida do AVG	28
7. Interface de Utilizador AVG	29
7.1 Menu de Sistema	30
7.1.1 Ficheiro	30
7.1.2 Componentes	30
7.1.3 Histórico	30
7.1.4 Ferramentas	30
7.1.5 Ajuda	30
7.2 Informação de Estado de Segurança	33
7.3 Links Rápidos	34
7.4 Síntese de Componentes	35
7.5 Estatísticas	36
7.6 Ícone da barra de tarefas	37
8. Componentes do AVG	38
8.1 Anti-Vírus	38
8.1.1 Anti-Vírus Princípios	38
8.1.2 Interface do Anti-vírus	38
8.2 Anti-Spyware	40
8.2.1 Anti-Spyware Princípios	40
8.2.2 Interface do Anti-Spyware	40
8.3 Anti-Rootkit	42
8.4 Firewall	42
8.4.1 Princípios da Firewall	42
8.4.2 Perfis da Firewall	42
8.4.3 Interface da Firewall	42
8.5 Verificador de E-mail	47
8.5.1 Princípios do Verificador de E-mail	47
8.5.2 Interface do Verificador de E-mail	47
8.5.3 Detecção de verificador de E-mail	47
8.6 Licença	52
8.7 Link Scanner	53
8.7.1 Princípios do Link Scanner	53
8.7.2 Interface do Link Scanner	53
8.7.3 AVG Search-Shield	53
8.7.4 AVG Active Surf-Shield	53
8.8 Protecção Online	57

8.8.1	<i>Princípios da Protecção Online</i>	57
8.8.2	<i>Interface da Protecção Online</i>	57
8.8.3	<i>Deteção da Protecção Online</i>	57
8.9	<i>Protecção Residente</i>	63
8.9.1	<i>Protecção Residente Princípios</i>	63
8.9.2	<i>Interface da Protecção Residente</i>	63
8.9.3	<i>Deteção da Protecção Residente</i>	63
8.10	<i>Actualizações</i>	68
8.10.1	<i>Princípios de Actualizações</i>	68
8.10.2	<i>Interface de Actualizações</i>	68
9.	Barra de Ferramentas de Segurança do AVG	71
9.1	<i>Interface da Barra de Ferramentas de Segurança do AVG</i>	71
9.2	<i>Opções da Barra de Ferramentas de Segurança do AVG</i>	73
9.2.1	<i>Separador Geral</i>	73
9.2.2	<i>Separador Botões Úteis</i>	73
9.2.3	<i>Separador Segurança</i>	73
9.2.4	<i>Separador Opções Avançadas</i>	73
10.	Definições Avançadas do AVG	78
10.1	<i>Aparência</i>	78
10.2	<i>Sons</i>	81
10.3	<i>Ignorar Condições de Erro</i>	82
10.4	<i>Quarentena de Vírus</i>	83
10.5	<i>Excepções PUP</i>	84
10.6	<i>Protecção Online</i>	87
10.6.1	<i>Protecção na Internet</i>	87
10.6.2	<i>Mensagens Instantâneas</i>	87
10.7	<i>Link Scanner</i>	91
10.8	<i>Análises</i>	92
10.8.1	<i>Analisar todo o computador</i>	92
10.8.2	<i>Análise em contexto</i>	92
10.8.3	<i>Analisar pastas ou ficheiros específicos</i>	92
10.8.4	<i>Análise de Dispositivo Amovível</i>	92
10.9	<i>Agendamentos</i>	99
10.9.1	<i>Análise agendada</i>	99
10.9.2	<i>Agendamento de actualização da base de dados de vírus</i>	99
10.10	<i>Verificador de E-mail</i>	111

10.10.1	Certificação	111
10.10.2	Filtro de Correio	111
10.10.3	Relatórios e Resultados	111
10.10.4	Servidores	111
10.11	Protecção Residente	121
10.11.1	Definições Avançadas	121
10.11.2	Exclusões de Directórios	121
10.11.3	Ficheiros Excluídos	121
10.12	Servidor de Memória Cache	126
10.13	Anti-Rootkit	128
10.14	Actualizar	129
10.14.1	Proxy	129
10.14.2	Acesso telefónico	129
10.14.3	URL	129
10.14.4	Gerir	129
10.15	Administração Remota	136
11.	Definições da Firewall	138
11.1	Geral	138
11.2	Segurança	139
11.3	Áreas e perfis de Adaptadores	140
11.4	Registos	141
11.5	Perfis	143
11.5.1	Informação do perfil	143
11.5.2	Redes definidas	143
11.5.3	Aplicações	143
11.5.4	Serviços do Sistema	143
12.	Análise do AVG	155
12.1	Interface de Análise	155
12.2	Análises Predefinidas	156
12.2.1	Analisar todo o computador	156
12.2.2	Analisar pastas ou ficheiros específicos	156
12.3	A analisar no Explorador do Windows	164
12.4	Análise da Linha de Comandos	165
12.4.1	Parâmetros da Análise CMD	165
12.5	Agendamento de Análise	168
12.5.1	Definições de agendamento	168

12.5.2 Como Analisar	168
12.5.3 O que Analisar	168
12.6 Resumo dos Resultados da Análise	179
12.7 Detalhes dos Resultados da Análise	181
12.7.1 Separador Resumo dos Resultados	181
12.7.2 Separador Infecções	181
12.7.3 Separador Spyware	181
12.7.4 Separador Avisos	181
12.7.5 Separador Rootkits	181
12.7.6 Separador Informações	181
12.8 Quarentena de Vírus	189
13. Actualizações do AVG	192
13.1 Níveis de Actualização	192
13.2 Tipos de Actualização	192
13.3 Processo de Actualização	193
14. Histórico de Eventos	194
15. FAQ e Suporte Técnico	196



1. Introdução

Este manual do utilizador disponibiliza informações compreensivas para o **AVG 9 Anti-Virus plus Firewall**.

Parabéns pela sua aquisição do AVG 9 Anti-Virus plus Firewall!

O **AVG 9 Anti-Virus plus Firewall** 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 9 Anti-Virus plus Firewall** 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 9 Anti-Virus plus Firewall** 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.



2. Requisitos de Instalação do AVG

2.1. Sistemas Operativos Suportados

O **AVG 9 Anti-Virus plus Firewall** destina-se a proteger estações de trabalho com os seguintes sistemas operativos:

- Windows 2000 Professional SP4 + Update Rollup 1
- 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)

2.2. Requerimentos Mínimos e Recomendados de Hardware

Requerimentos mínimos de hardware para o **AVG 9 Anti-Virus plus Firewall**:

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

Requerimentos recomendados de hardware para o **AVG 9 Anti-Virus plus Firewall**:

- Intel Pentium CPU 1,8 GHz
- 512 MB de memória RAM
- 510 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 9 Anti-Virus plus Firewall.

Recomendamos que experimente a nossa nova ferramenta, [Gestor de Transferências do AVG](#), que o ajudará a configurar o ficheiro de instalação no idioma pretendido!

Durante o processo de instalação, ser-lhe-á solicitado o número de licença/venda. Certifique-se de que 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 online, o número de licença foi-lhe enviado por e-mail.

4. Gestor de Transferências do AVG

O **Gestor de Transferências do AVG** é uma ferramenta simples que o ajuda a seleccionar o ficheiro de instalação adequado da versão de teste do produto AVG. Baseado nos dados introduzidos, o gestor irá seleccionar o produto específico, o tipo de licença, os componentes pretendidos, e o idioma. Por fim, o **Gestor de Transferências do AVG** prosseguirá para a transferência e iniciará o [processo de instalação](#) correspondente.

Aviso: Tenha em atenção que o Gestor de Transferências AVG não é adequado para a transferência das edições de rede e SBS, e só são suportados os seguintes sistemas operativos: Windows 2000 (SP4 + SRP roll-up), Windows XP, Windows Vista e Windows 7.

O **Gestor de Transferências do AVG** está disponível para transferência no website da AVG (<http://www.avg.com/>). De seguida é disponibilizada uma breve descrição de cada passo que deverá seguir no **Gestor de Transferências do AVG**:

4.1. Selecção do Idioma



No primeiro passo do **<%AVG_DOWNLOAD_MANAGER%** seleccione o idioma de instalação a partir do menu pendente. Tenha em atenção que a selecção do idioma se aplica apenas ao processo de instalação; após a instalação poderá alterar o idioma directamente nas definições do programa. Depois clique no botão **Seguinte** para

continuar.

4.2. Verificação de Conectividade

No passo seguinte, o **Gestor de Transferências do AVG** tentará estabelecer uma ligação à Internet para localizar quaisquer eventuais actualizações. Não lhe será permitido continuar o processo de transferência até o **Gestor de Transferências do AVG** conseguir completar o teste de conectividade.

- Se o teste não apresentar qualquer conectividade, certifique-se de que está efectivamente conectado à Internet. Depois clique no botão **Tentar de novo**.



- Se estiver a utilizar uma ligação Proxy à Internet, clique no botão **Definições de Proxy** para especificar as suas [informações de proxy](#):
- Se a verificação for sucedida, clique no botão **Seguinte** para continuar.

4.3. Definições de Proxy



Se o **Gestor de Transferências do AVG** não conseguir identificar as suas Definições de proxy será necessário especificá-las manualmente. Preencha os seguintes dados por favor:

- **Servidor** - introduza um nome de servidor proxy válido ou endereço IP
- **Porta** - faculte o número de porta respectivo
- **Utilizar proxy de autenticação** - se o seu servidor proxy necessitar de autenticação, seleccione esta caixa.
- **Seleccionar autenticação** - a partir do menu pendente seleccione o tipo de autenticação. Recomendamos vivamente que mantenha o valor predefinido (*o servidor proxy facultará automaticamente os requisitos*). No entanto, se for um utilizador avançado, também pode seleccionar a opção Basic (*exigida por alguns servidores*) ou a opção NTLM (*exigida por todos os Servidores ISA*). Depois, introduza um **Nome de utilizador** e **Palavra-passe** válidos (opcional).

Confirme as suas definições ao premir o botão **Aplicar** para seguir para o próximo passo do **Gestor de Transferências do AVG**.

4.4. Transferir os Ficheiros a Instalar



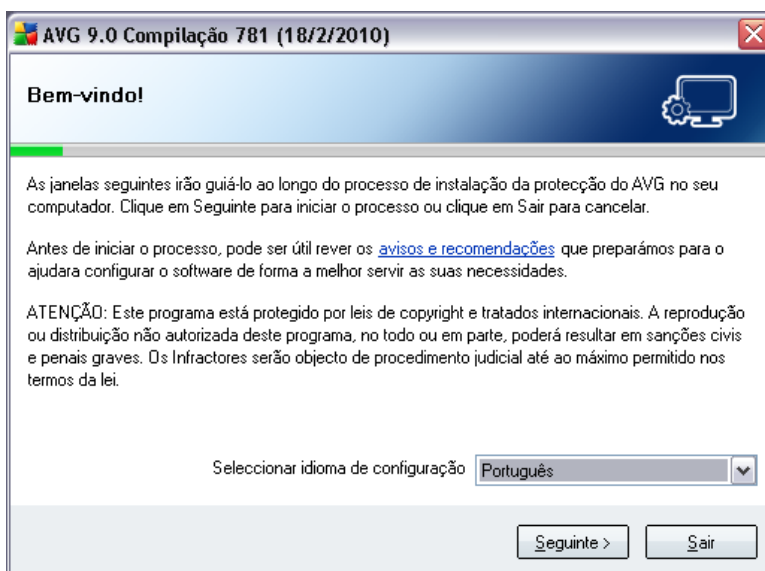
Agora, facultou todas as informações necessárias para que o **Gestor de Transferências do AVG** inicie a transferência do pacote de instalação e inicie o processo de instalação. De seguida, continue para o [Processo de Instalação do AVG](#).

5. Processo de Instalação do AVG

Para instalar o **AVG 9 Anti-Virus plus Firewall** 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 on-line. Pode transferir o ficheiro a partir do website da AVG (<http://www.avg.com/>), na secção **Centro de Suporte / Transferências**. Ou, pode utilizar a nossa nova ferramenta **Gestor de Transferências AVG** que o ajuda a criar e a transferir o pacote de instalação de que necessita, e iniciar o processo de instalação.

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

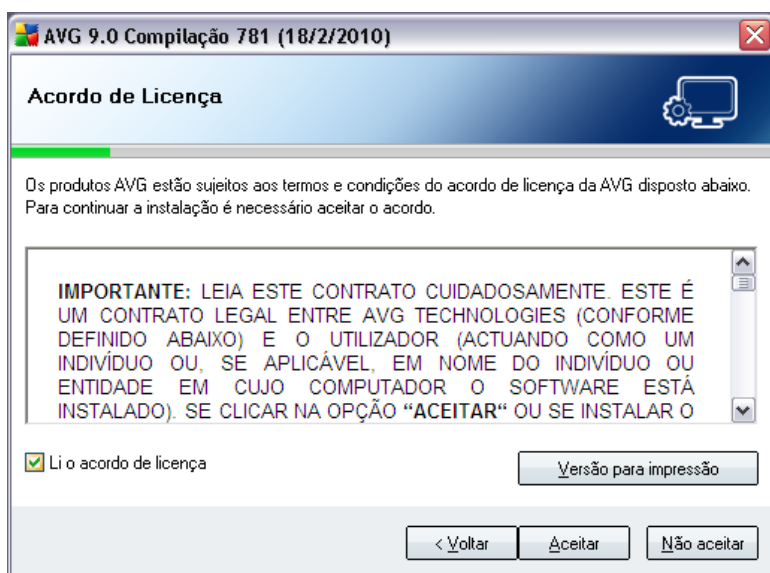
5.1. Execução da Instalação



O processo de instalação inicia com a janela **Bem-vindo ao Programa de Configuração do AVG**. Aqui pode seleccionar o idioma utilizado para o processo de instalação. Na parte inferior da janela encontra o item **Escolher idioma de configuração**, e seleccione o idioma pretendido a partir da Lista de Opções. Depois clique no botão **Seguinte** para confirmar e continue para a janela seguinte.

Atenção: Aqui pode escolher o idioma exclusivamente para o processo de instalação. Não está a seleccionar o idioma para a aplicação AVG - isso pode ser especificado mais tarde durante o processo de instalação!

5.2. Contrato de Licença



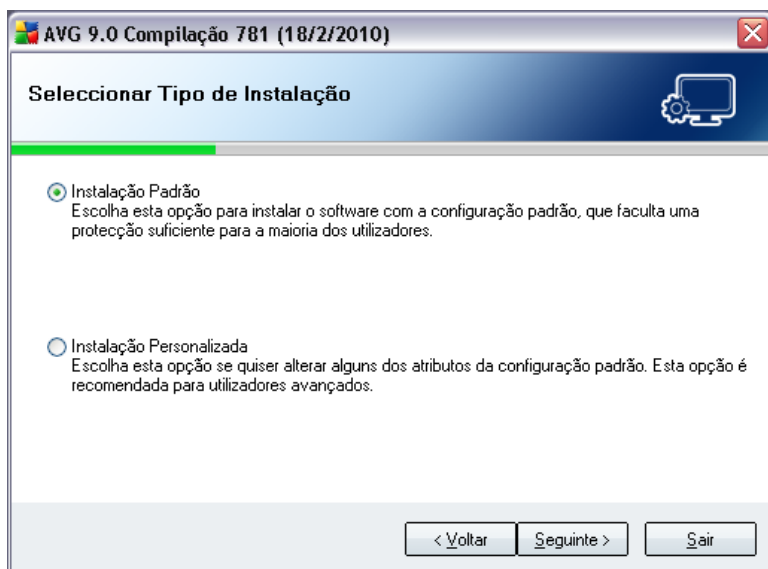
A janela **Acordo de Licenciamento** faculta o texto integral do acordo de Licenciamento do AVG. Leia-o atentamente e confirme que leu, compreendeu e aceita o acordo ao marcar a caixa ***Eu li o acordo de licença*** e clicando no botão **Aceito**.

Se não concordar com o acordo de licença clique no botão **Não aceito**, e o processo de instalação será abortado imediatamente.

5.3. A verificar o Estado do Sistema

Uma vez confirmado o acordo de licença, será reencaminhado para a janela **A Verificar o Estado do Sistema**. Esta janela não necessita de qualquer intervenção; o seu sistema está a ser verificado antes de a instalação do AVG iniciar. Por favor aguarde até que o processo esteja concluído, depois continue automaticamente para a janela seguinte.

5.4. Seleccionar Tipo de Instalação



A janela **Seleccionar Tipo de Instalação** oferece a possibilidade de escolher entre duas opções de instalação: instalação **padrão** e **personalizada**.

Para a maioria dos utilizadores, é recomendável a **instalação 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 optimizada. Futuramente, se houver necessidade de alterar a configuração, tem sempre a possibilidade de o fazer directamente na aplicação AVG.

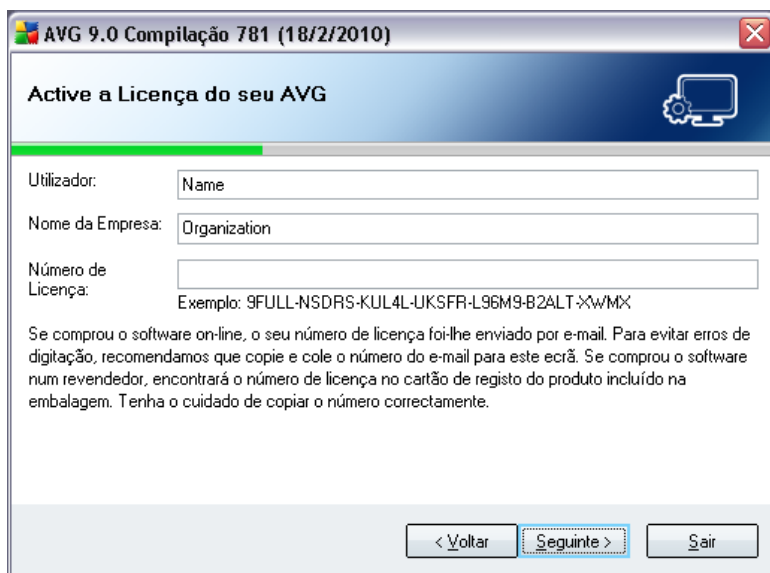
A **instalação personalizada** só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o AVG com definições que não as padrão. Ex. para corresponder a requisitos de sistema específicos.

5.5. Activar a Licença do seu AVG

Na janela **Activar a sua licença do AVG** tem de preencher os dados de registo. Digite o seu nome (**Campo Nome de Utilizador**) e o nome da sua organização (**Campo Nome da Empresa**).

Depois introduza o seu número de licença/venda no campo de texto **Número de Licença**. O número de venda pode ser encontrado na caixa do CD do seu **AVG 9 Anti-Virus plus Firewall**. O número de licença estará na mensagem de e-mail de confirmação que recebeu após comprar o seu **AVG 9 Anti-Virus plus Firewall** 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.



AVG 9.0 Compilação 781 (18/2/2010)

Active a Licença do seu AVG

Utilizador:

Nome da Empresa:

Número de Licença:

Exemplo: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2<-XwMX

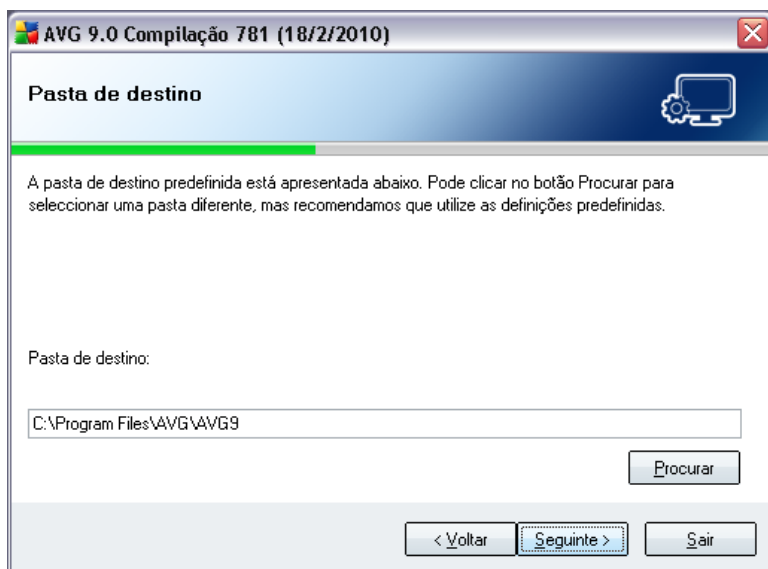
Se comprou o software on-line, o seu número de licença foi-lhe enviado por e-mail. Para evitar erros de digitação, recomendamos que copie e cole o número do e-mail para este ecrã. Se comprou o software num revendedor, encontrará o número de licença no cartão de registo do produto incluído na embalagem. Tenha o cuidado de copiar o número correctamente.

< Voltar **Seguinte >** Sair

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

Se tiver seleccionado instalação padrão no passo anterior, será reencaminhado directamente para a janela **Barra de Ferramentas de Segurança do AVG**. Se tiver seleccionado a instalação personalizada continuará com a janela **Pasta de Destino**.

5.6. Instalação Personalizada - Pasta de Destino

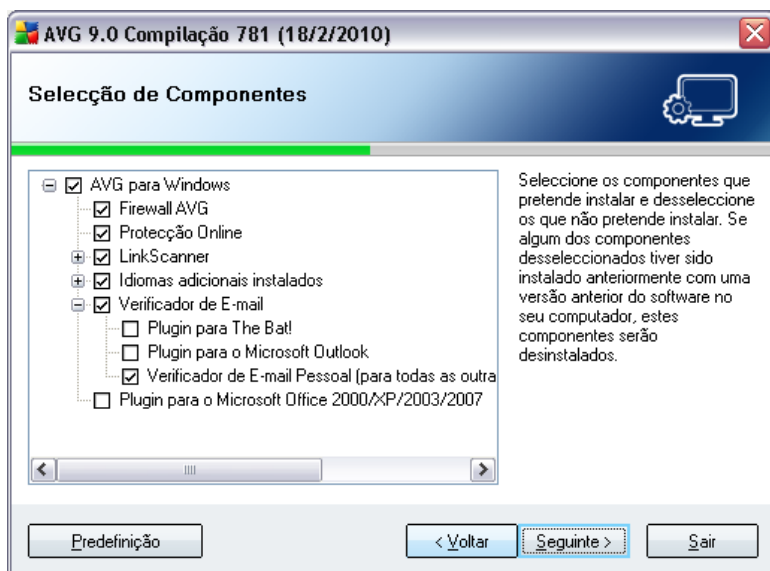


A janela **Pasta de Destino** permite-lhe especificar a localização onde o **AVG 9 Anti-Virus plus Firewall** deve ser instalado. O AVG será instalado por predefinição na pasta de ficheiros de programas localizada na unidade C:. Na eventualidade de a pasta não existir ainda, ser-lhe-á solicitado numa nova janela que confirme que concorda com a criação desta pasta por parte do AVG agora.

Se quiser alterar esta localização, utilize o botão **Procurar** para visualizar a estrutura da unidade, e seleccione a respectiva pasta.

Prima o botão **Seguinte** para confirmar.

5.7. Instalação Personalizada - Selecção de Componentes



A janela **Seleção de Componentes** apresenta uma síntese de todos os componentes do **AVG 9 Anti-Virus plus Firewall** que podem ser instalados. Se as definições predefinidas não forem da sua conveniência, pode remover/adicionar componentes específicos.

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

- **Seleção do Idioma**

Na lista de componentes a serem instalados é possível definir qual o idioma(s) com que o AVG deve ser instalado. Marque o item **Idiomas adicionais instalados** e depois seleccione os idiomas pretendidos a partir do respectivo menu.

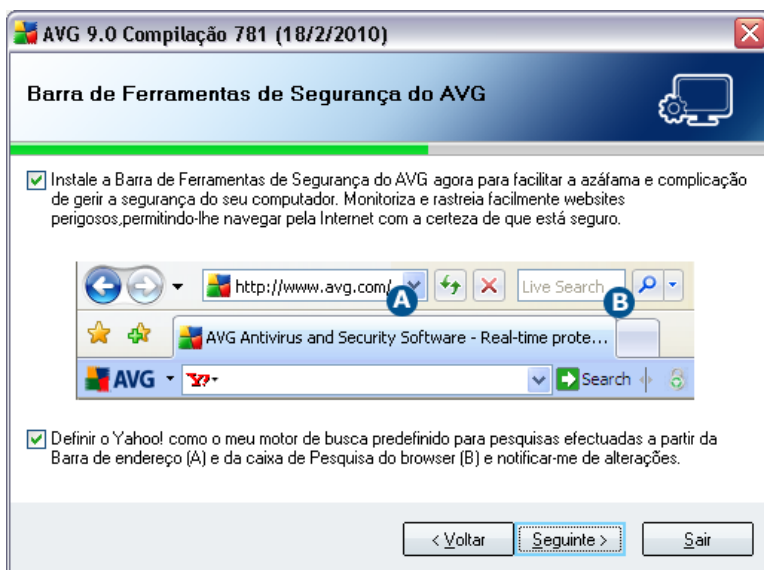
- **Plug-ins do Verificador de E-mail**

Clique no item **Verificador de E-mail** para abrir e decidir em que plug-in este deve ser instalado para garantir a segurança do seu correio electrónico. Por predefinição, será instalado o **Plugin para o Microsoft Outlook**. Outra opção específica é o **Plugin para o The Bat!** Se utilizar outro cliente de correio electrónico (*Ms Exchange, Qualcomm Eudora, ...*), seleccione a opção **Verificador de E-mail Pessoal** para activar automaticamente a protecção das

suas comunicações de correio electrónico independentemente do programa de correio electrónico que utilizar.

Continue clicando no botão **Seguinte**.

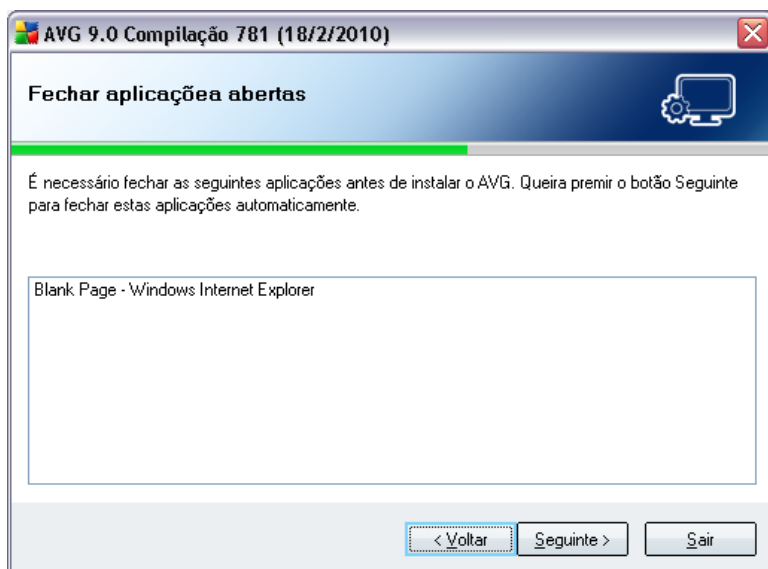
5.8. Barra de Ferramentas de Segurança do AVG



Na janela **Barra de Ferramentas de Segurança do AVG**, decida se quer instalar a **Barra de Ferramentas de Segurança do AVG** (verificação dos resultados de procura dos motores de busca da Internet suportados). Se não alterar as definições predefinidas, 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. 2.0 ou superior) para lhe proporcionar protecção compreensiva on-line enquanto navega na Internet.

Além disso, tem a opção de decidir se quer optar pelo Yahoo! como o motor de busca predefinido. Se assim for, queira marcar a caixa correspondente.

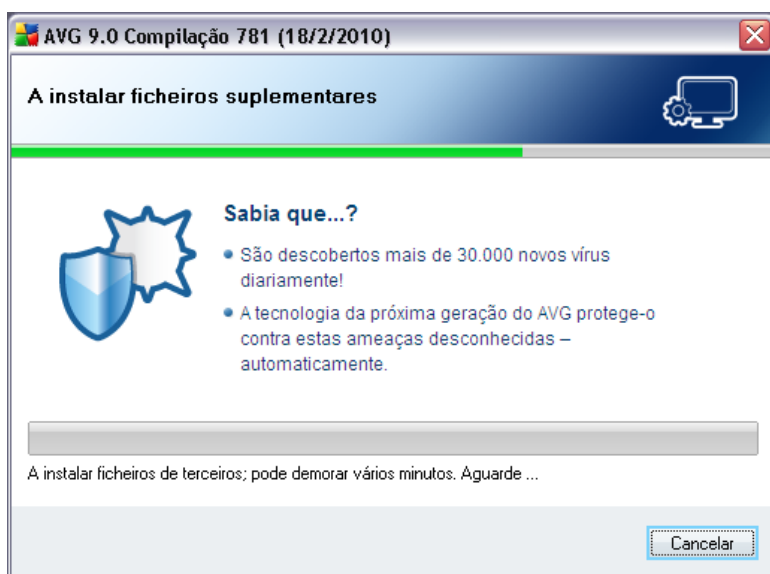
5.9. Fechar aplicações abertas



A janela **Fechar aplicações abertas** é apresentada durante o processo de instalação se houver programas incompatíveis em execução no computador no momento. Nessa altura, é apresentada a lista dos programas que é necessário fechar para concluir o processo de instalação com sucesso. Clique no botão **Seguinte** para confirmar que concorda em fechar as aplicações respeitantes e continuar para o próximo passo.

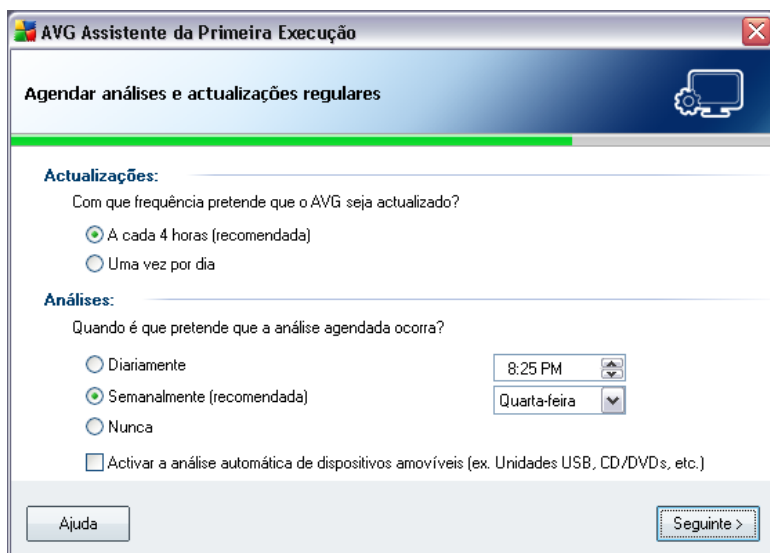
5.10. A instalar o AVG

A janela **A instalar o AVG** 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.

5.1.1. Agendar análises e actualizações regulares



Na janela **Agendamento de análises e actualizações regulares** defina o intervalo para verificação de acessibilidade de novos ficheiros de actualização, e defina a hora em que a [análise agendada](#) deve ser iniciada. É recomendável que mantenha os valores predefinidos. Clique no botão **Seguinte** para continuar.

5.1.2. Selecção de utilização do computador



Nesta janela, o **Assistente de Configuração da Firewall** pergunta que tipo de computador utiliza. Por exemplo, o seu portátil, que estabelece ligação à Internet a partir de muitos locais diferentes (*aeroportos, quartos de hotel, etc.*) requer regras de segurança mais restritas do que as de um computador num domínio (*rede da empresa, etc.*).). Com base no tipo de utilização do computador seleccionada, as regras predefinidas da **Firewall** serão definidas com um nível de segurança diferente.

Existem duas opções alternativas que pode seleccionar:

- **Computador de secretária**
- **Computador portátil**

Confirme a selecção premindo o botão **Seguinte** e continue para a próxima janela de diálogo.

5.13. A ligação à Internet do seu computador



Nesta janela de diálogo, o **Assistente de Configuração da Firewall** pergunta como é que o computador está ligado à Internet. Com base no tipo de ligação seleccionado, as regras predefinidas da **Firewall** serão definidas com um nível de segurança diferente.

Existem três opções alternativas que pode seleccionar:

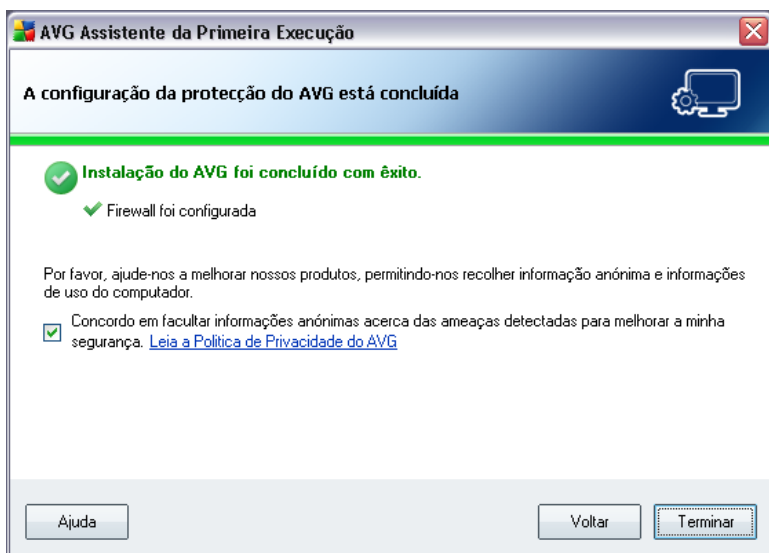
- **Directamente através de um modem**

- **Directamente através de um router com ou sem fios**
- **O computador pertence a um domínio**

Selecção o tipo de ligação que melhor descreve a ligação do seu computador à Internet.

Confirme a selecção premindo o botão **Seguinte** e continue para a próxima janela de diálogo.

5.14. A configuração da protecção do AVG está concluída



Agora, o seu **AVG 9 Anti-Virus plus Firewall** está configurado.

Nesta janela pode decidir se quer activar a opção de reportação anónima de exploits e websites perigosos ao laboratório de vírus da AVG. Se assim for, marque a opção **Concordo em facultar informações ANÓNIMAS acerca das ameaças detectadas para melhorar a minha segurança**.

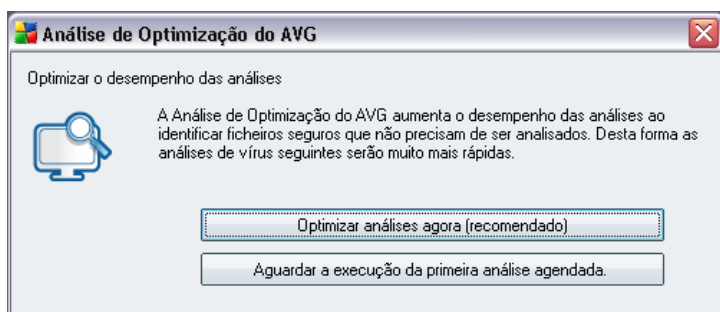
Finalmente, prima o botão **Concluir**. Pode ser necessário reiniciar o computador para poder começar a utilizar o AVG.

6. Após a Instalação

6.1. Optimização da análise

A funcionalidade de análise de optimização verifica as pastas *Windows* e *Ficheiros de programas* onde detecta ficheiros específicos (*actualmente são os ficheiros *.exe, *.dll e *.sys*) e guarda a informação relativa a estes ficheiros. No próximo acesso estes ficheiros não serão analisados novamente e, desta forma, o tempo de análise é reduzido significativamente.

Uma vez concluído o processo de instalação será convidado a executar a análise de optimização:



Recomendamos que use esta opção e execute o processo de análise de optimização clicando no botão **Optimizar análise agora**.

6.2. Registo do Produto

Estando terminada a instalação do **AVG 9 Anti-Virus plus Firewall**, 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.

6.3. Aceder à Interface do Utilizador

A **Interface do Utilizador do AVG** pode ser acedida de várias formas:

- fazendo duplo clique no ícone do AVG na barra de notificação
- fazendo duplo clique no ícone do AVG no ambiente de trabalho



- a partir do menu **Iniciar/Todos os Programas/AVG 9.0/Interface do Utilizador do AVG**

6.4. 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 9 Anti-Virus plus Firewall**. Por este motivo deve executar uma análise [Analisar todo o computador](#) para se certificar de que não existem infecções no seu PC.

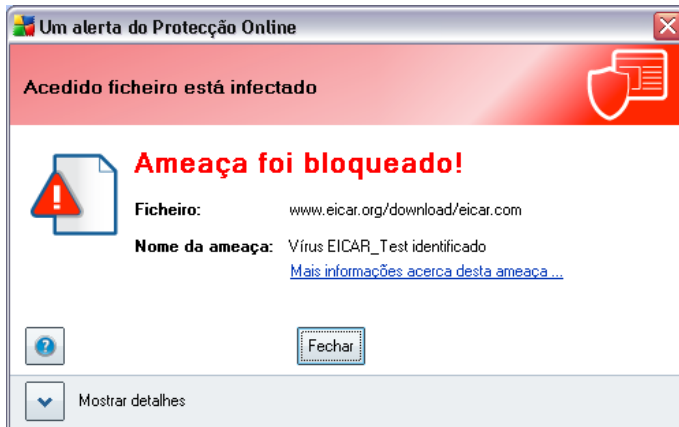
Para instruções relativas à execução de [Analisar todo o computador](#) por favor consulte o capítulo [Análise do AVG](#).

6.5. Teste Eicar

Para confirmar que o **AVG 9 Anti-Virus plus Firewall** 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 da Protecção on-line 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!**

6.6. Configuração Predefinida do AVG

A configuração predefinida (ou seja, a forma como a aplicação está configurada imediatamente após a instalação) do **AVG 9 Anti-Virus plus Firewall** 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.

7. Interface de Utilizador AVG

O **AVG 9 Anti-Virus plus Firewall** 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) facultar-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 >>](#)

7.1. 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 9 Anti-Virus plus Firewall**. 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:

7.1.1. Ficheiro

- **Sair** - fecha a interface do utilizador do **AVG 9 Anti-Virus plus Firewall**. No entanto, a aplicação AVG continuará a ser executada em segundo plano e o seu computador continuará protegido!

7.1.2. 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** - abre a página predefinida do componente [Anti-vírus](#)
- **Anti-Rootkit** - abre a página predefinida do componente [Anti-Rootkit](#)
- **Anti-Spyware** - abre a página predefinida do componente [Anti-Spyware](#)
- **Firewall** - abre a página predefinida do componente [Firewall](#)
- **Link Scanner** - abre a página predefinida do componente [Link Scanner](#)

- **Verificador de E-mail** - abre a página predefinida do componente [Verificador de E-mail](#)
- **Licença** - abre a página predefinida do componente [Licença](#)
- **Protecção Online** - abre a página predefinida do componente [Protecção Online](#)
- **Protecção Residente** - abre a página predefinida do componente [Protecção Residente](#)
- **Actualizações** - abre a página predefinida do componente [Actualizações](#)

7.1.3. 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 detectadas 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 registadas **AVG 9 Anti-Virus plus Firewall**.
- [Firewall](#) - abre a interface das definições da Firewall no separador [Registos](#) com uma síntese detalhada de todas as acções da Firewall

7.1.4. 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 um teste manual de um único ficheiro seleccionado da estrutura em árvore do seu disco
- **Actualizar** inicia automaticamente o processo de actualização do **AVG 9 Anti-Virus plus Firewall**
- **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 9 Anti-Virus plus Firewall**. 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 avançadas do componente **Firewall**

7.1.5. 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 9 Anti-Virus plus Firewall**, os dois últimos itens aparecem como **Comprar agora** e **Activar**, permitindo-lhe comprar a versão completa do programa imediatamente. Para produtos **AVG 9 Anti-Virus plus Firewall** 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**.

7.2. 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 9 Anti-Virus plus Firewall**. 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.



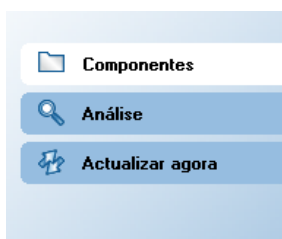
O ícone vermelho indica que o AVG está em estado crítico! Um ou mais componentes não estão a funcionar devidamente e o AVG não consegue proteger o seu computador. Preste atenção imediata à resolução do problema referenciado. Se não conseguir resolver o problema sozinho, contacte a equipa de [suporte técnico da AVG](#).

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](#).

7.3. 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 >>](#)
- **Verificador do computador** - utilize este link para abrir a interface de análise do AVG onde pode executar testes directamente, agendar análises ou editar os seus parâmetros - consulte o capítulo [Análises do AVG >>](#)

- **Actualizar agora** - este link abre a interface de actualização, e inicia o processo de actualização do AVG - 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.

7.4. 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 9 Anti-Virus plus Firewall**, 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** analisa as suas aplicações em segundo plano à medida que as executa - [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 da Internet - [detalhes >>](#)
- **Anti-Rootkit** detecta programas e tecnologias que tentam camuflar malware - [detalhes >>](#)
- **Verificador de E-mail** verifica todo o e-mail a receber e a enviar pela existência de vírus - [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 >>](#)
- **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 >>](#)

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**. Seleccionar 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](#).

7.5. 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:

- **Última análise**- faculta a data em que a última análise foi efectuada
- **Última actualização**- faculta a data em que a última actualização foi executada
- **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 9.0.xx, em que 9.0 é a versão da linha do produto, e xx representa o número de compilação)
- **A licença expira** - faculta a data de expiração da licença do seu AVG

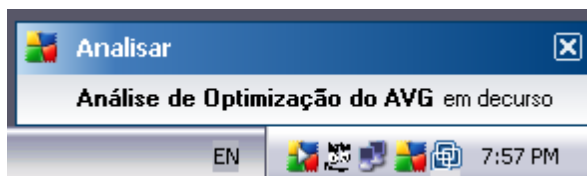
7.6. Ícone da barra de tarefas

Ícone da Barra de Notificação (na barra de tarefas do Windows) indica o estado actual do seu **AVG 9 Anti-Virus plus Firewall**. 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](#)
- **Actualizar** - inicia imediatamente uma [actualização](#)

8. Componentes do AVG

8.1. Anti-Vírus

8.1.1. Anti-Vírus Princípios

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.

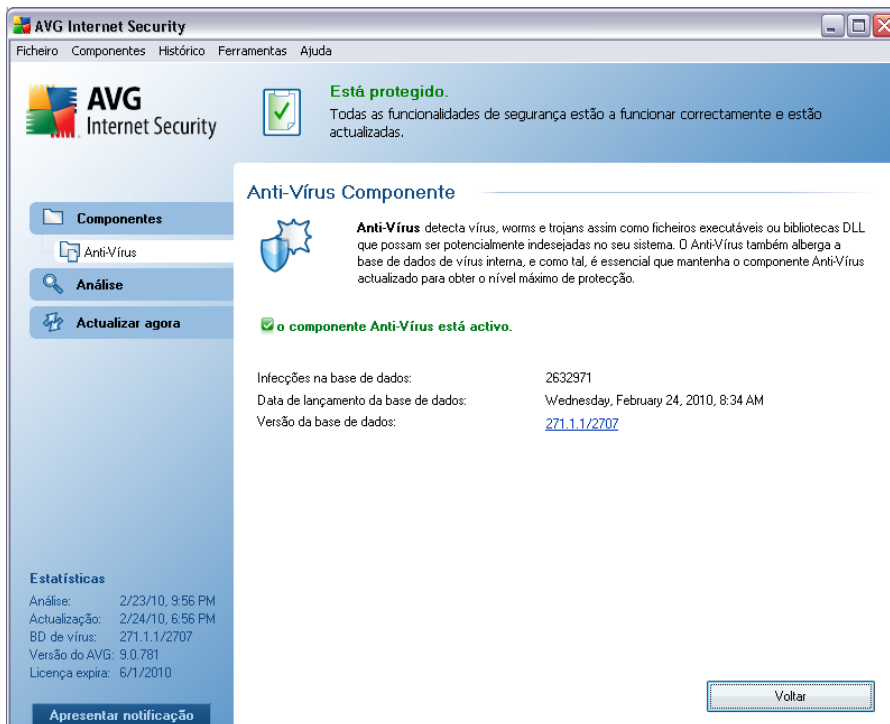
A característica mais importante da protecção anti-vírus é que nenhum vírus conhecido pode ser executado no computador!

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.

8.1.2. 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** :

- **Definições de Infecções** - o número faculta a contagem de definições de vírus na versão actualizada da base de dados de vírus
- **Última actualização da base de dados**- especifica quando e a que horas a base de dados de vírus foi actualizada pela última vez
- **Versão da base de dados** - define o número da versão da 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).

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.

8.2. Anti-Spyware

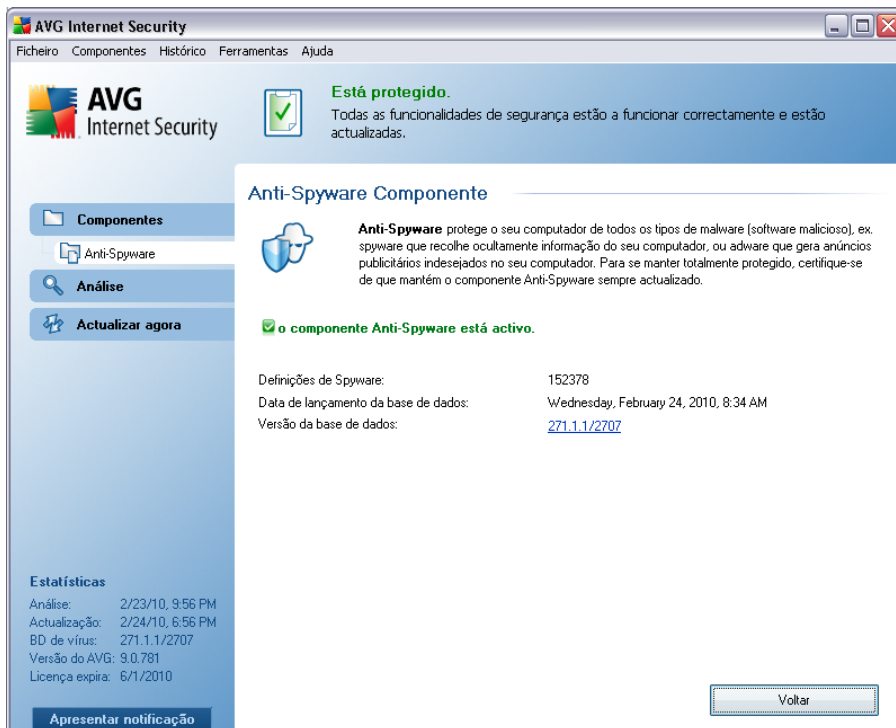
8.2.1. Anti-Spyware Princípios

Spyware é normalmente definido como um tipo de malware, isto é, software que recolhe informações do computador do utilizador sem o seu conhecimento ou consentimento. Algumas aplicações de spyware podem ser instaladas propositadamente e, na maior parte dos casos, incluem anúncios, janelas de pop-ups ou outros tipos de software desagradável.

Actualmente, a maior fonte de infecções são os websites com conteúdos potencialmente perigosos. Outros métodos de transmissão como, por exemplo, através de e-mail ou de worms e vírus, são igualmente predominantes. A protecção mais importante consiste na utilização de um analisador permanente em segundo plano, **Anti-Spyware**, que funciona como uma protecção residente e analisa as aplicações em segundo plano à medida que estas são executadas.

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 9 Anti-Virus plus Firewall** 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.

8.2.2. Interface do Anti-Spyware



O interface do componente **Anti-Spyware** faculta uma sucinta síntese da funcionalidade do componente, informação acerca do estado actual do componente (O componente *Anti-Spyware está activo.*), e algumas estatísticas do componente **Anti-Spyware** :

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

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.

8.3. 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 pressupõe a assunção do 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 standard dos sistemas operativos. Acontece que estes são também frequentemente trojans, como tal enganam os utilizadores para que estes pensem que os mesmos podem ser executados com 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.

8.4. 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.

8.4.1. 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

8.4.2. 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. Selecciona esta opção se se ligar à Internet a partir de casa, ou se estiver numa pequena rede empresarial sem controlo central. Além disso, selecciona 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

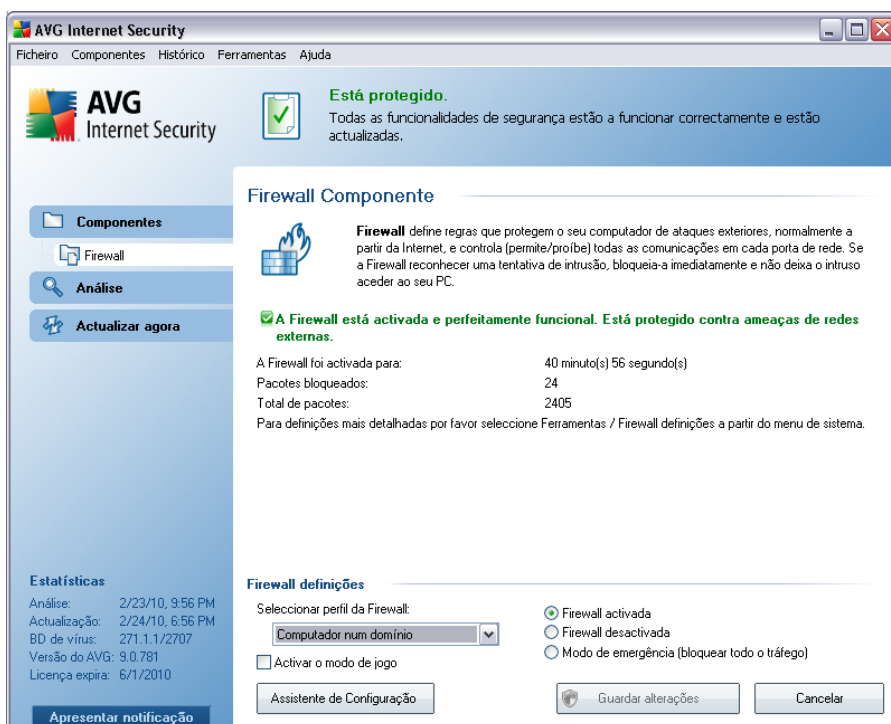
A funcionalidade de mudança de perfil permite à [Firewall](#) mudar automaticamente

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.

8.4.3. Interface da Firewall



A interface do componente **Firewall** faculta alguma informação básica acerca da funcionalidade do componente, 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

Configuração básica do componente

- **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 assegurar que durante a execução de aplicações de ecrã inteiro (jogos, apresentações Power Point, etc.), a [Firewall](#) não apresentará janelas a inquirir se quer 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.
- **Estado da Firewall:**
 - o **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
 - 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)** - selecione 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,

selecione 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

- **[Assistente de configuração](#)** - prima o botão para mudar para a janela correspondente (*usada durante o processo de instalação*) apelidada **[Seleção de Utilização do Computador](#)** onde pode especificar a configuração do componente **[Firewall](#)**
- **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*)

8.5. 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.

8.5.1. Princípios do Verificador de E-mail

O componente **Verificador de E-mail** analisa as mensagens de e-mail a receber/a enviar automaticamente. Pode utilizá-lo com clientes de e-mail que não tenham o seu próprio plug-in no AVG (ex. *Outlook Express, Mozilla, 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.

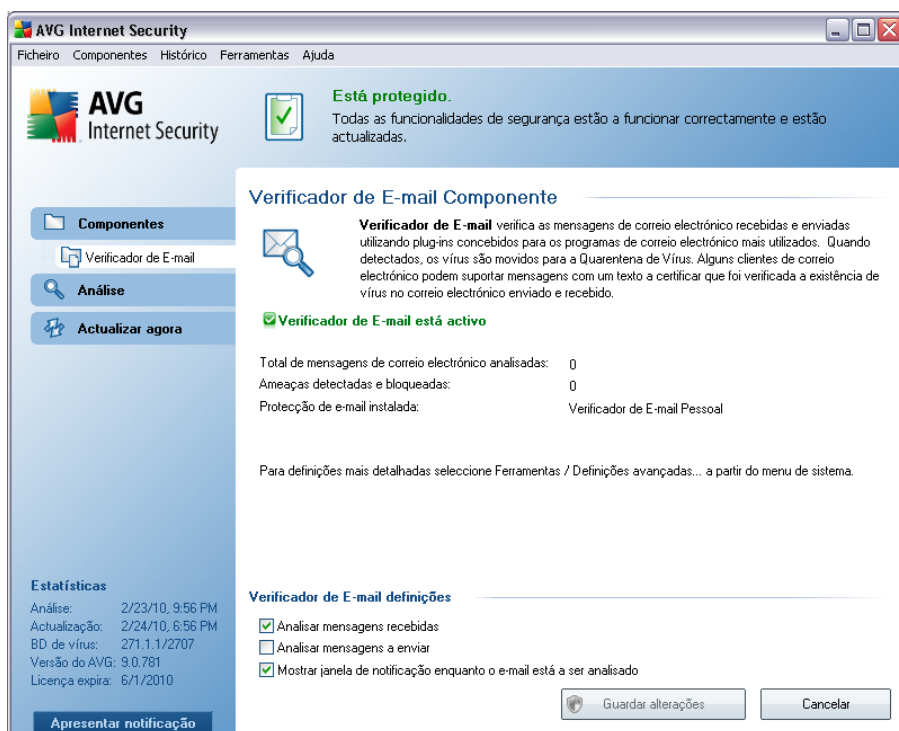
- **Correio a receber:** Durante a recepção de uma mensagem do servidor, o

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!

8.5.2. Interface do Verificador de E-mail



No janela do componente **Verificador de E-mail** pode encontrar um pequeno texto com a descrição da funcionalidade do componente, e informações relativas ao seu estado actual (*O Verificador de E-mail está activo.*), e as seguintes estatísticas:

- **Total de mensagens de E-mail analisadas** - quantas mensagens de correio electrónico 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 e-mail desde a última execução do **Verificador de E-mail**
- **Protecção de correio electrónico instalada** - informações acerca de um plug-in específico de protecção de correio electrónico respeitante ao seu cliente de correio electrónico predefinido instalado

Configuração básica do componente

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 de e-mail 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 enquanto as mensagens de E-mail estão a ser analisadas** - marque este item para confirmar que pretende ser avisado através de uma janela de notificação acima do ícone do AVG na barra de notificação durante a análise ao seu correio electrónico 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



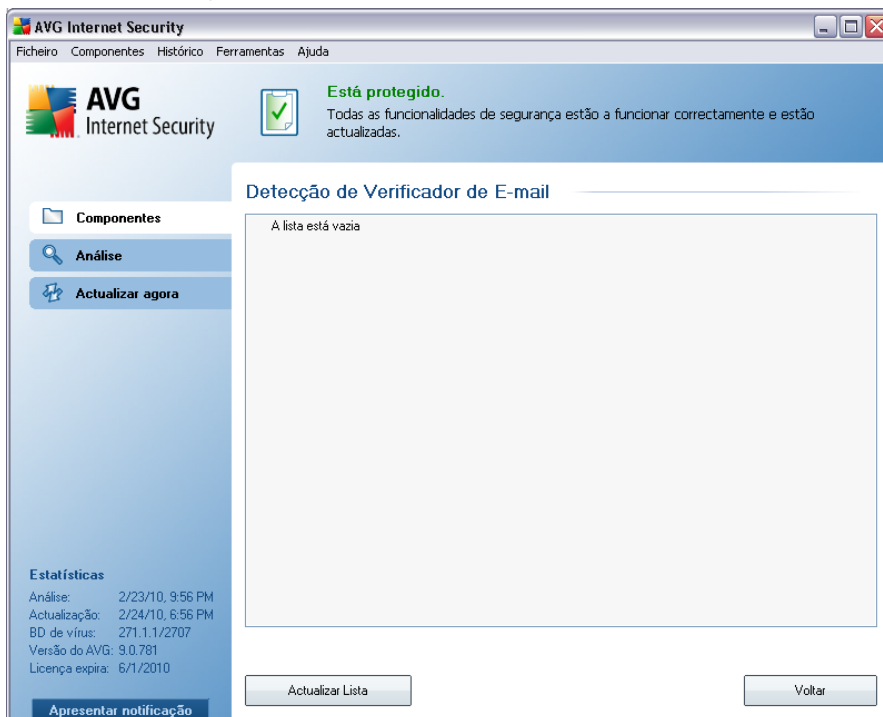
configuração do AVG na janela [Definições Avançadas do AVG](#) que lhe é apresentada.

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)

8.5.3. 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

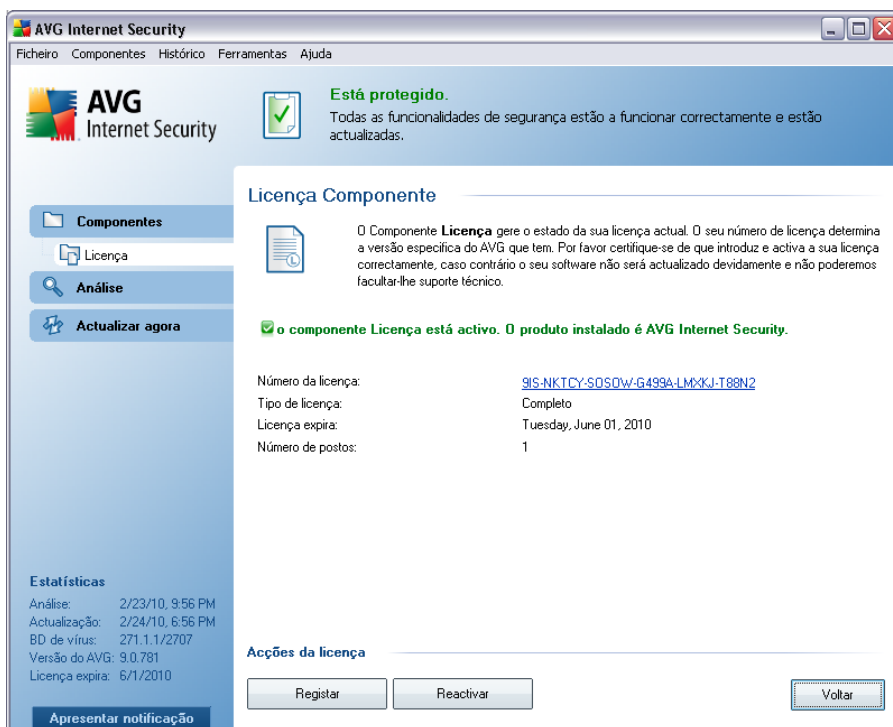
Na parte inferior da janela, abaixo da lista, encontrará informações sobre o número total de objectos detectados listados acima. Pode ainda exportar toda a lista dos objectos detectados num ficheiro (**Exportar lista para ficheiro**) e eliminar todas as entradas sobre objectos detectados (**Lista vazia**).

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** - leva-o de volta à [Interface do utilizador do AVG](#) padrão (síntese de componentes)

8.6. Licença



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

- **Número de licença** - faculta a forma exacta do seu número de licença. 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 9 Anti-Virus plus Firewall** após esta data terá de renovar a sua licença. A [renovação da licença pode ser efectuada on-line](http://www.avg.com/) no website da AVG (<http://www.avg.com/>).
- **Número de postos de trabalho** - quantos postos de trabalho nas quais pode instalar o seu **AVG 9 Anti-Virus plus Firewall**.

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 9 Anti-Virus plus Firewall**, os botões aparecem como **Comprar agora** e **Activar**, permitindo-lhe comprar a versão completa do programa imediatamente. Para produtos **AVG 9 Anti-Virus plus Firewall** 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).

8.7. Link Scanner

8.7.1. Princípios do Link Scanner

O componente **LinkScanner** proporciona protecção contra websites que são criados para instalar malware no seu computador através do browser ou dos seus plug-ins. A tecnologia do **LinkScanner** consiste em duas funcionalidades, o [AVG Search-Shield](#) e o [AVG Active Surf-Shield](#):

- O [AVG Search-Shield](#) contém uma lista de websites (*endereços URL*) que são conhecidos como sendo perigosos. Ao utilizar o Google, Yahoo!, Bing, Baidu, Altavista ou Yandex, todos os resultados de pesquisa são verificados em conformidade com esta lista e é apresentado um ícone de veredicto (no Yahoo! só é apresentado o ícone de "Website com exploits" nos resultados de busca). Se digitar um endereço directamente no seu browser e clicar numa ligação para qualquer website ou por exemplo no seu e-mail, esta é verificada automaticamente e bloqueada se necessário.
- O [AVG Active Surf-Shield](#) analisa o conteúdo dos websites que visita, independentemente do endereço do website. Mesmo que um website não seja

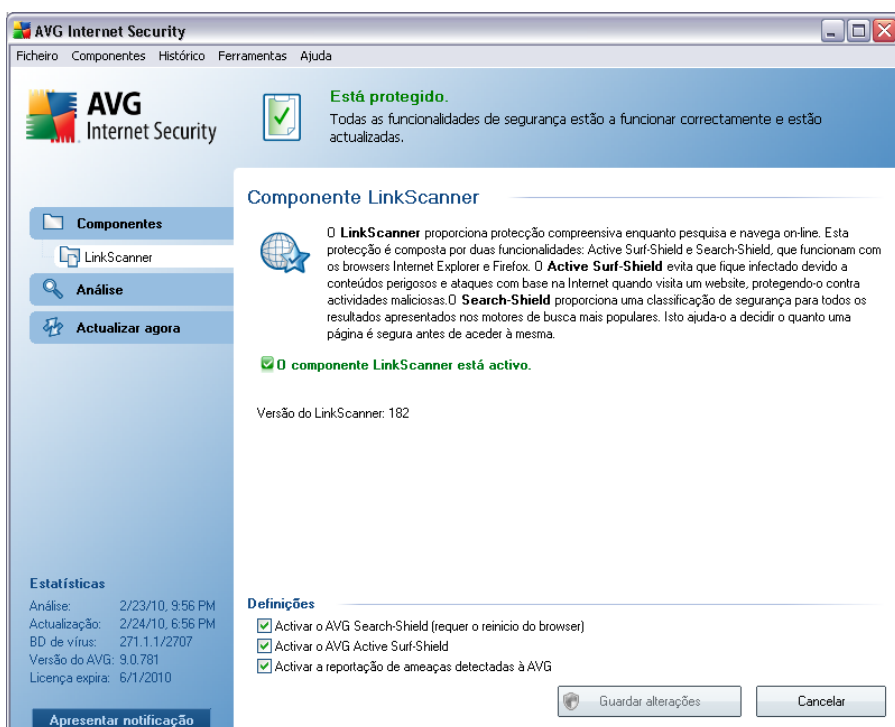
detectado pelo [AVG Search Shield](#) (ex. quando um novo website malicioso é criado, ou quando um website anteriormente seguro passa a conter malware), será detectado e bloqueado pelo [AVG Active Surf-Shield](#) assim que tentar visitar o website.

Nota: O AVG LinkScanner não se destina a plataformas de servidores!

8.7.2. Interface do Link Scanner

O componente **LinkScanner** consiste em duas partes que pode activar/desactivar na interface do **componente LinkScanner**:

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



Na parte inferior da janela pode editar várias opções:

- **Activar o [AVG Search-Shield](#)**- (activado por predefinição): ícones de

notificação de aviso em procuras efectuadas no Google, Yahoo! Bing, Baidu, Yandex ou Altavista: tendo verificado antecipadamente o conteúdo dos websites facultados pelo motor de busca.

- **Activar o AVG Active 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*).
- **Activar a reportagem de ameaças detectadas à AVG** - seleccione este item para permitir a reportagem de exploits e websites maliciosos encontrados pelos utilizadores seja através do **Safe Surf** ou do **Safe Search** para juntar à base de dados de recolha de informação relativa a actividade maliciosa na Web.

8.7.3. AVG Search-Shield

Ao pesquisar na Internet com o **AVG Search-Shield** activado, todos os resultados de pesquisa devolvidos pelos motores de busca mais populares como o Yahoo!, Google, Bing, Altavista, Yandex, etc. serão 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 de destino é segura (*com o motor de busca do Yahoo! este ícone não será apresentado na Barra de Ferramentas de Segurança do AVG!*).



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.

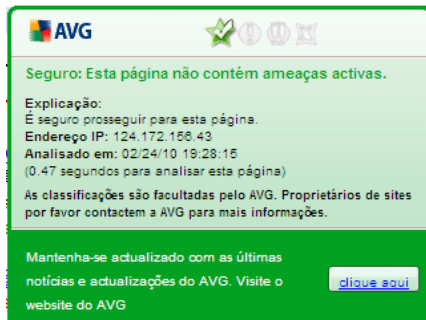


A página de destino contém ameaças activas! Para sua segurança, não lhe será permitido visitar esta página.



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

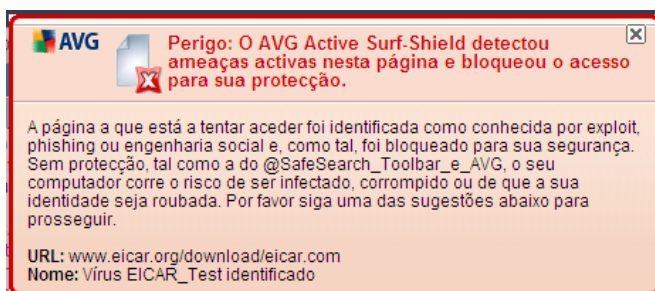
Colocar o cursor sobre um ícone de classificação individual apresentará detalhes acerca do link em questão. As informações incluem detalhes adicionais da ameaça, (se for o caso), o endereço IP do link e quando a página foi analisada pelo AVG:



8.7.4. AVG Active 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!

8.8. Protecção Online

8.8.1. Princípios da Protecção Online

A Protecção Online é um tipo de protecção residente em tempo real; analisa o conteúdo das 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!

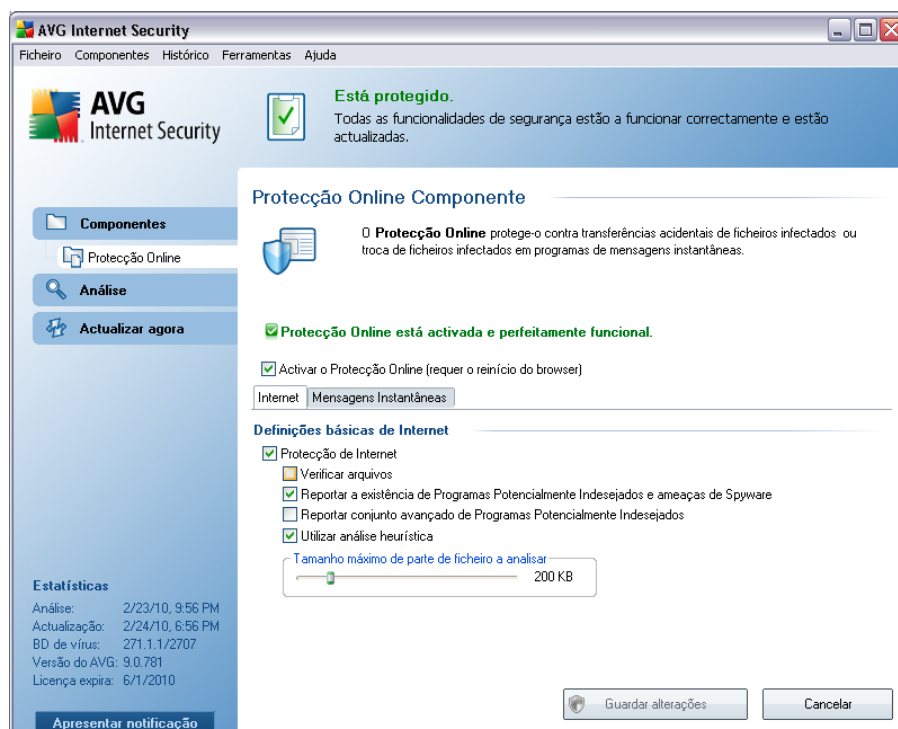
8.8.2. Interface da Protecção Online

A interface do componente **Protecção Online** descreve o comportamento deste tipo de protecção. Pode encontrar mais à frente informações relativas ao estado actual do componente (*A Protecção Online está activa e completamente funcional.*). Na parte inferior da janela encontrará então as opções de edição elementares desta funcionalidade do componente.

Configuração básica do componente

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 seleccionado, e a **Protecção Online** estiver em execução, estão mais opções de configuração disponíveis e editáveis em dois separadores:

- **Web** - pode editar a configuração do componente em relação à análise do conteúdo do website. A interface de edição permite-lhe configurar as seguintes opções elementares:

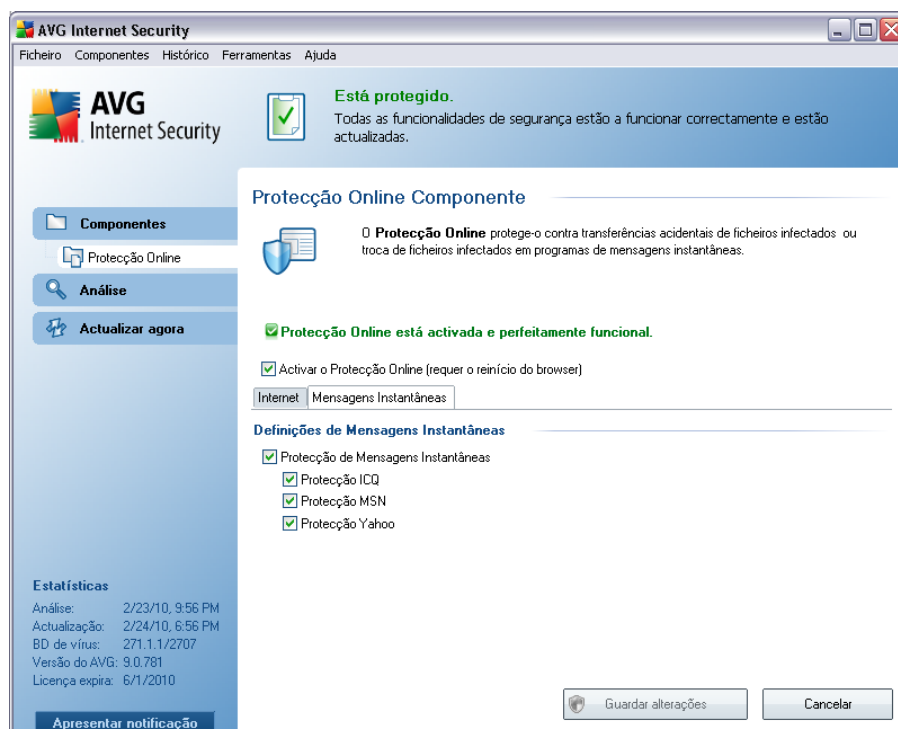


o **Protecção na Internet** - esta opção confirma que a **Protecção Online** deve analisar o conteúdo das páginas www. Uma vez que esta opção está activada (*por predefinição*), pode ainda activar/desactivar estes itens:

- **Verificar arquivos** - analisar o conteúdo de arquivos possivelmente incluídos na página www a ser apresentada
- **Reportar Programas Potencialmente Indesejados e ameaças de Spyware** - (*activado por predefinição*): marque para activar o componente **Anti-Spyware** e analisar a existência de spyware assim como de vírus. **O Spyware** representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador
- **Reportar conjunto avançado de Programas Potencialmente Indesejados** - se a opção anterior estiver activada, também pode marcar esta caixa para detectar pacotes expandidos de **spyware**: programas que são perfeitamente fidedignos e inofensivos quando

adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.

- **Utilizar a análise heurística** - analisar o conteúdo da página a ser apresentada utilizando o método de análise heurística, ou seja, emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual. Como tal, pode inclusivamente detectar códigos maliciosos ainda não descritos na base de dados de vírus (consulte [Princípios Anti-vírus](#)).
- **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.
- **Mensagens Instantâneas** - permite-lhe editar as definições do componente referente à análise de mensagens instantâneas (ex. ICQ, MSN Messenger, . Yahoo ..) .



o Protecção de Mensagens Instantâneas - marque este item se pretender que a Protecção Online verifique se a comunicação on-line está livre de vírus. Considerando que esta opção está activada, pode ainda especificar qual a aplicação de mensagens instantâneas que pretende controlar - actualmente **AVG 9 Anti-Virus plus Firewall** suporta as aplicações ICQ, MSN, e Yahoo.

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, selecione 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:

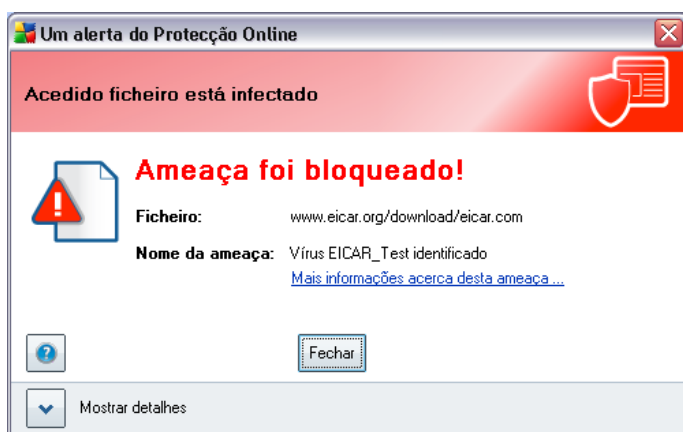
- **Guardar alterações** - clique neste botão para guardar e aplicar quaisquer

alterações efectuadas nesta janela

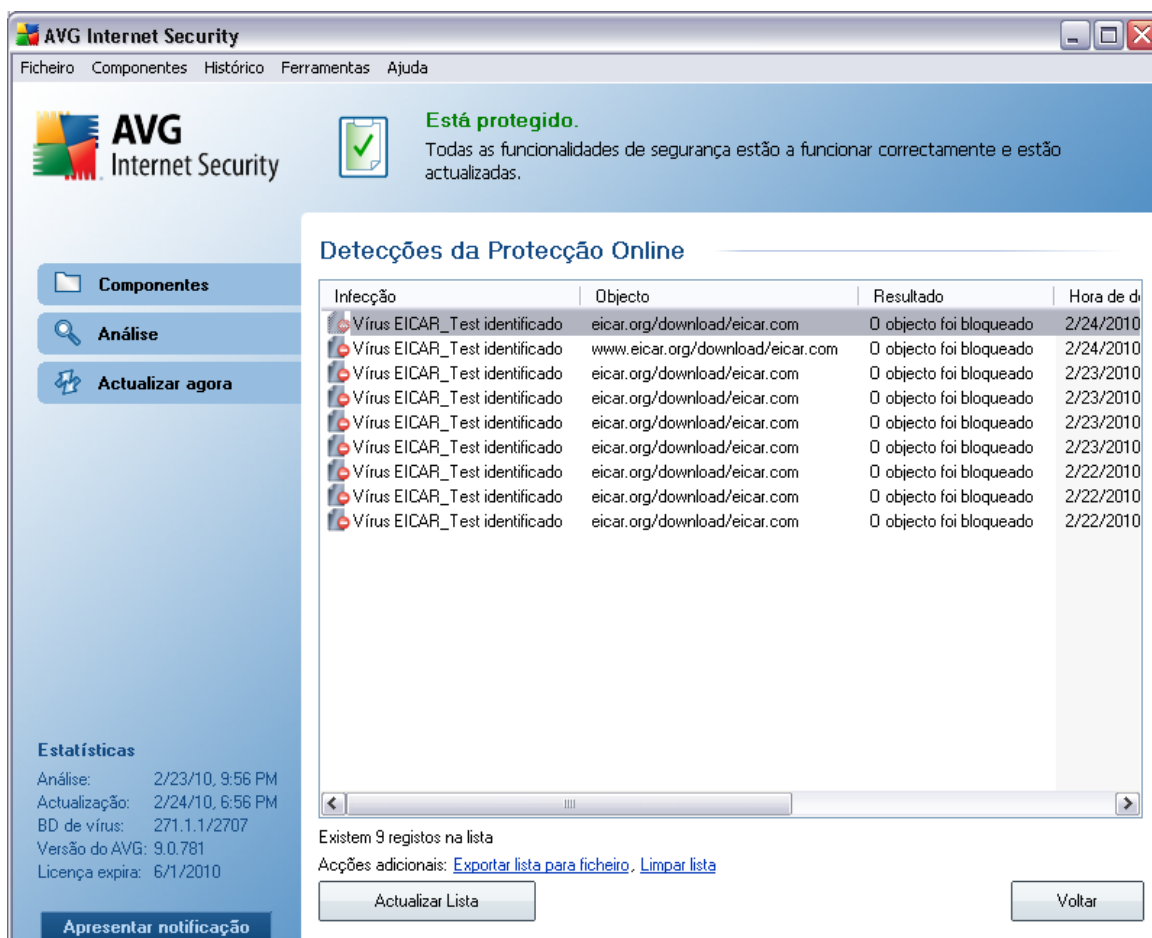
- **Cancelar** - clique neste botão para retroceder para a [Interface do utilizador do AVG](#) padrão (síntese dos componentes)

8.8.3. 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:



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).

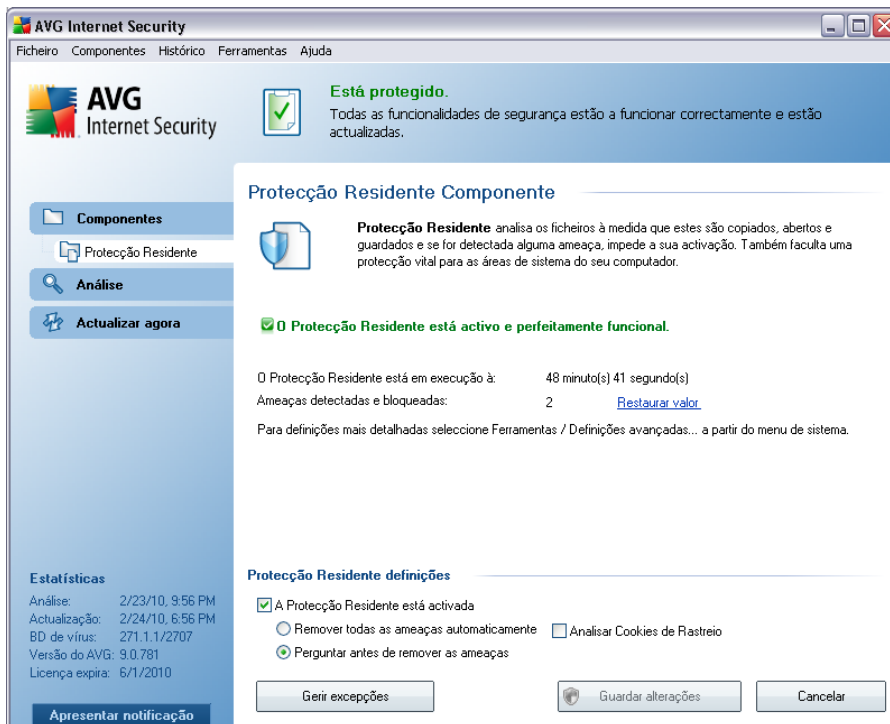
8.9. Protecção Residente

8.9.1. Protecção Residente Princípios

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.

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

8.9.2. Interface da Protecção Residente



Além da síntese dos dados estatísticos mais importantes e da informação sobre o estado actual do componente (*a Protecção Residente está activa e completamente funcional*), a interface do **Protecção Residente** também faculta algumas opções de configuração do componente elementares. As estatísticas são como segue:

- **A Protecção Residente está activa há** - faculta 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*)

Configuração básica do componente

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):

- o automaticamente (**Remover todas as ameaças automaticamente**)
- o 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 - Exclusões de Directórios](#) onde pode definir pastas que não devem ser verificadas 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)

8.9.3. Detecção da Protecção Residente

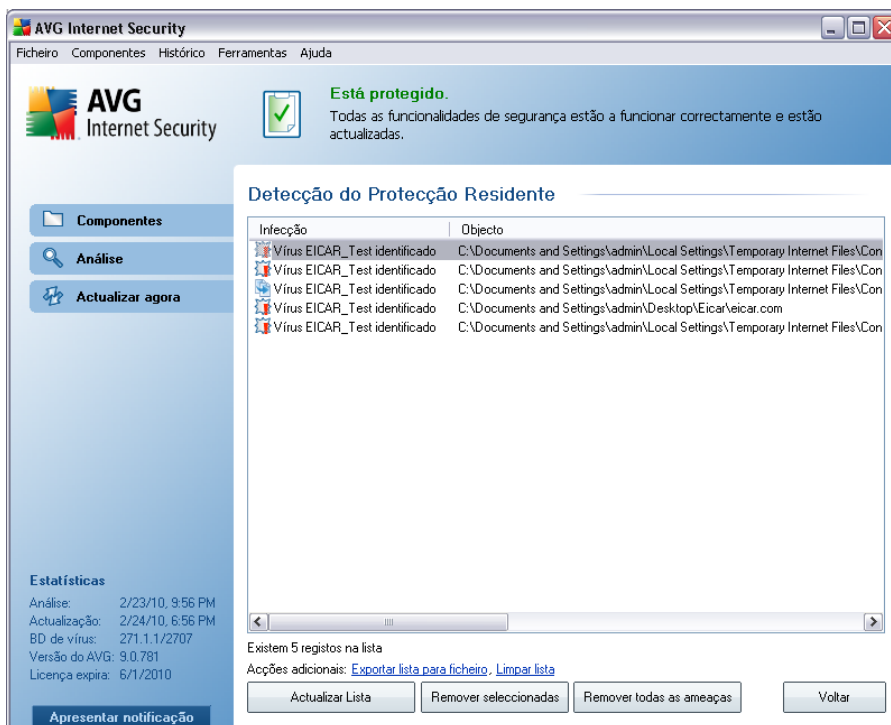
A **Protecção Residente** analisa ficheiros quando estes são copiados, abertos ou guardados. Quando um vírus ou qualquer tipo de ameaça for detectado, o utilizador será imediatamente notificado através da seguinte janela:



A janela proporciona informações sobre a ameaça detectada, e solicita-lhe uma decisão sobre a acção a tomar:

- **Restaurar** - se houver uma cura disponível, o AVG restaurará o ficheiro infectado automaticamente; esta opção é a acção recomendada
- **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!

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



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

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

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

entradas sobre objectos detectados (**Lista vazia**). O botão **Actualizar lista** procederá à actualização da lista de detecções da **Protecção Residente**. O botão **Retroceder** leva-o de volta à [**Interface do utilizador do AVG**](#) padrão (síntese de componentes).

8.10. Actualizações

8.10.1. 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!

8.10.2. Interface de Actualizações



A interface de **Actualizações** apresenta informações acerca da funcionalidade do componente e ao seu estado actual (*Actualizações está activo.* , e facultar os dados estatísticos relevantes:

- **Última actualização**- especifica quando e a que horas a base de dados foi actualizada
- **Versão da base de dados de vírus** - define o número da versão da mais recente base de dados de vírus; e este número aumenta com cada actualização da base de dados de vírus
- **Próxima actualização agendada** - especifica para quando e a que hora a próxima actualização da base de dados está agendada

Configuração básica do componente

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 **A uma hora específica** - defina o dia e a hora exactos

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)

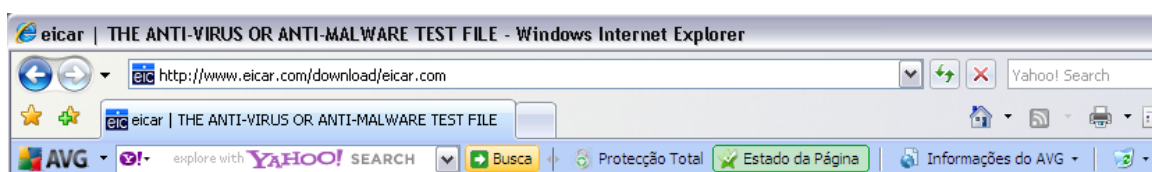
9. Barra de Ferramentas de Segurança do AVG

A **Barra de Ferramentas de Segurança do AVG** é uma nova ferramenta que funciona em conjunto com o componente **AVG Link Scanner** e verifica os resultados de pesquisa dos motores de busca suportados (*Yahoo!*, *Google*, *Bing*, *Altavista*, *Baidu*). A **Barra de Ferramentas de Segurança do AVG** pode ser usada para controlar as funções do **AVG Link Scanner** e para ajustar o seu comportamento.

Se optar pela instalação da barra de ferramentas durante a instalação do **AVG 9 Anti-Virus plus Firewall**, esta será adicionada ao seu browser automaticamente. Na eventualidade de utilizar um browser alternativo (ex. *Avant Browser*) pode ocorrer um comportamento inesperado.

9.1. Interface da Barra de Ferramentas de Segurança do AVG

A **Barra de Ferramentas de Segurança do AVG** foi concebida para funcionar com o **MS Internet Explorer** (versão 6.0 ou superior) e o **Mozilla Firefox** (versão 2.0 ou superior). Uma vez decidido pela instalação da **Barra de Ferramentas de Segurança do 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:



Nota: A Barra de Ferramentas de Segurança do AVG não se destina a plataformas de servidores!

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

- **Logótipo AVG** - faculta acesso a itens gerais da barra de ferramentas. Clique no botão de logótipo para ser redireccionado para o website da AVG (<http://www.avg.com/>). Clicar com o cursor junto ao ícone AVG abrirá as seguintes opções:
 - o **Informação da Barra de Ferramentas** - link para a página inicial da **Barra de Ferramentas de Segurança do AVG com informações detalhadas relativas à protecção da barra de ferramentas**
 - o **Iniciar o AVG 9 Anti-Virus plus Firewall** - abre a interface do utilizador do **AVG 9 Anti-Virus plus Firewall**

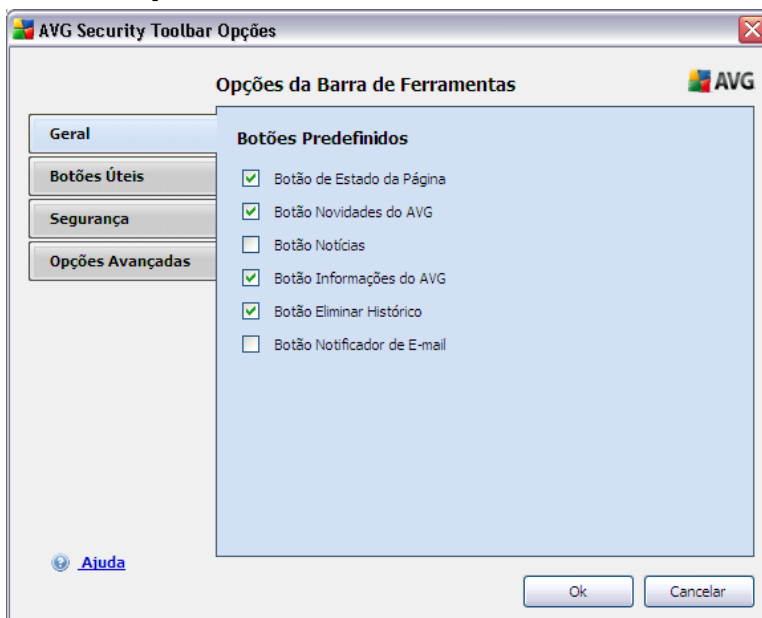
- o **Opções** - abre uma janela de configuração onde pode ajustar as definições da **Barra de Ferramentas de Segurança do AVG** conforme as suas necessidades - consulte o seguinte capítulo [Opções da Barra de Ferramentas de Segurança do AVG](#)
- o **Eliminar Histórico** - permite-lhe *Eliminar todo o histórico* da Barra de Ferramentas de Segurança do AVG, ou *Eliminar o histórico de pesquisa*, *Eliminar o histórico de navegação*, *Eliminar o histórico de transferências* e *Eliminar cookies*.
- o **Actualizar** - verifica a existência de novas actualizações para a sua **Barra de Ferramentas de Segurança do AVG**
- o **Ajuda** - faculta opções para abrir o ficheiro de ajuda, submeter feedback do produto ou visualizar os detalhes da versão actual da barra de ferramentas
- **Caixa de procura** - Introduza uma palavra ou oração na caixa de procura. Clique em **Procurar** para iniciar a procura com o motor de busca especificado (*pode especificar o motor de busca pretendido nas [Opções Avançadas da Barra de Ferramentas de Segurança do AVG](#), e pode optar pelo Yahoo!, Wikipédia, Baidu, WebHledani ou Yandex*), independentemente da página 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 [AVG Search-Shield](#).
- **Protecção Total** - este botão é apresentado opcionalmente como **Protecção Total / Protecção Limitada / Sem Protecção** consoante a configuração do **AVG 9 Anti-Virus plus Firewall**
- **Estado da Página** - directamente na barra de ferramentas, este botão apresenta a avaliação da página Web actualmente apresentada com base nos critérios do componente [AVG Search-Shield](#) *a página é segura / suspeita / positivamente perigosa / contém ameaças / não foi possível analisar*). Clique no botão para abrir um painel informativo com dados detalhados sobre a página específica.
- **Informações do AVG** - disponibiliza links para informações importantes de segurança localizadas no website da AVG (<http://www.avg.com/>).
 - o **Informação da Barra de Ferramentas** - link para a página inicial da **Barra de Ferramentas de Segurança do AVG com informações detalhadas relativas à protecção da barra de ferramentas**

- o **Acerca de ameaças** - abre a página da AVG com informações sobre vírus e ameaças actualmente na Internet
- 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 **Enciclopédia de Vírus** - abre a página da Enciclopédia de Vírus onde pode pesquisar vírus específicos por nome e obter informações detalhadas sobre os mesmos

9.2. Opções da Barra de Ferramentas de Segurança do 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:

9.2.1. Separador Geral

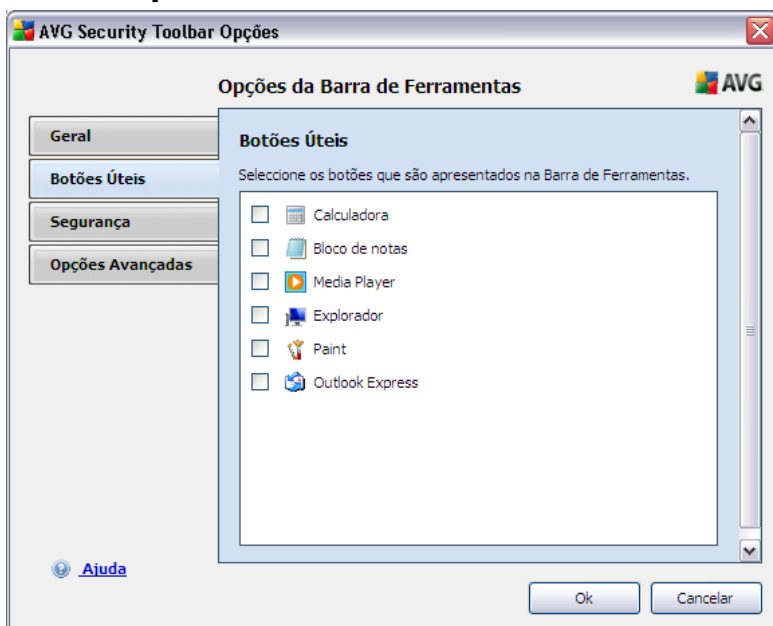


Neste separador, pode especificar os botões de controlo da barra de ferramentas que

devem ser apresentados ou ocultos no painel da **Barra de Ferramentas de Segurança do 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 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 Informações do AVG** - o botão disponibiliza informações sobre a barra de ferramentas do AVG, ameaças actuais e o nível de ameaças na Internet; abre a enciclopédia de vírus e fornece notícias sobre outros produtos AVG
- **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 do AVG.

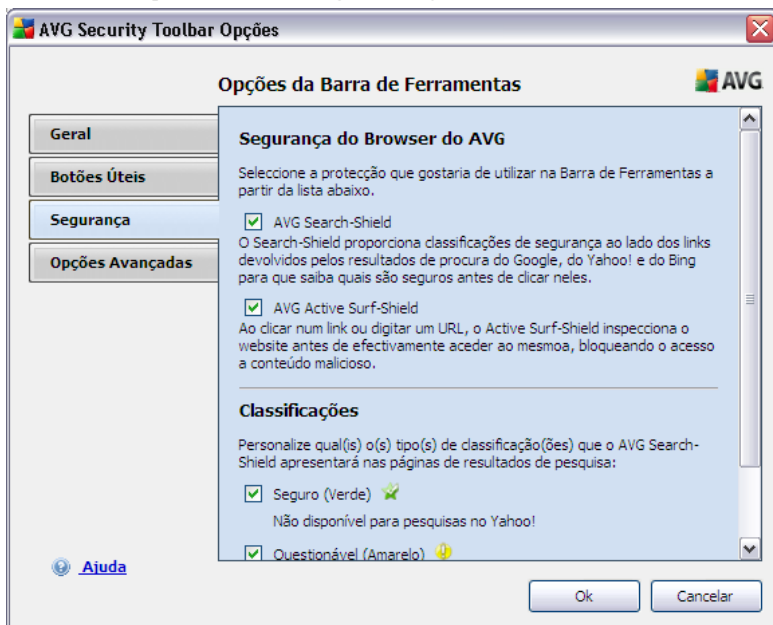
9.2.2. Separador Botões Úteis



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.

9.2.3. Separador Segurança



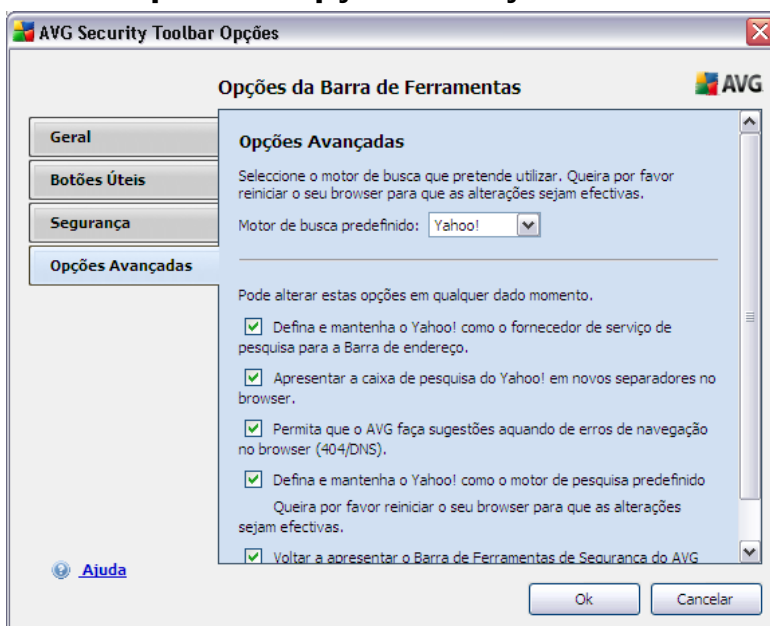
O separador **Segurança** está dividido em duas secções, **Segurança do Browser do AVG** e **Classificações**, onde pode marcar caixas específicas para atribuir à **Barra de Ferramentas de Segurança do AVG** funcionalidades que queira usar:

- **Segurança do Browser do AVG** - seleccione este item para activar ou desactivar o serviço [AVG Search-Shield](#) e/ou [AVG Active Surf-Shield](#)
- **Classificações** - seleccione os símbolos gráficos usados para a classificação de cada resultado pelo componente [AVG 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.***

9.2.4. Separador Opções Avançadas



No separador ***Opções Avançadas*** seleccione primeiro o motor de busca que pretende utilizar por predefinição. Pode optar entre *Yahoo!*, *Baidu*, *WebHledani* e *Yandex*. Uma vez alterado o motor de busca predefinido, queira reiniciar o seu browser para que a alteração produza efeito.

Além disso, pode activar ou desactivar outras definições específicas da ***Barra de Ferramentas de Segurança do AVG***:

- ***Defina e mantenha o Yahoo! como a utilização da Barra de endereços como motor de busca*** - (activado por predefinição) - se seleccionada, esta opção permite-lhe digitar palavras-chave de pesquisa directamente na barra de endereços no seu browser e será usado o serviço Yahoo! automaticamente para procurar os websites relevantes.

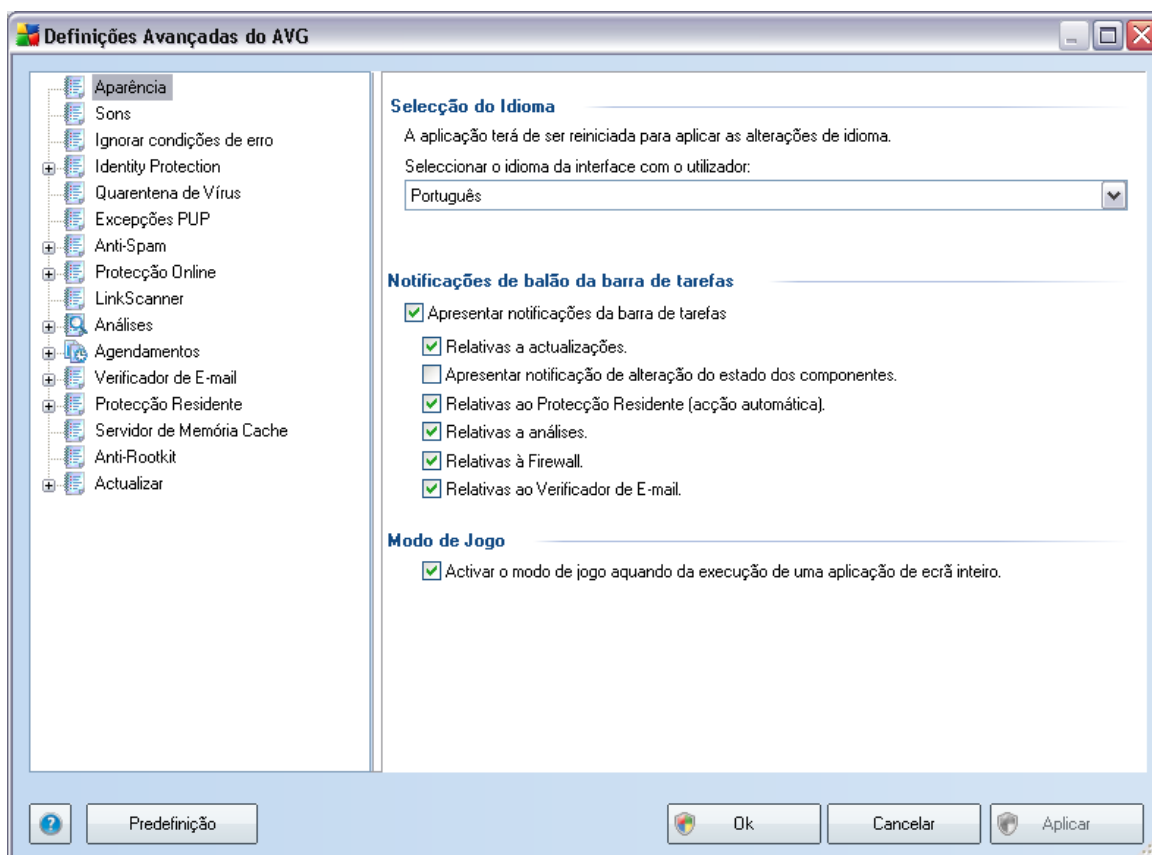
- **Permitir que o AVG faça sugestões aquando de erros de navegação (404/DNS)** - (activado por predefinição) - se for parar a uma página inexistente durante a navegação Web, ou a uma página que não pode ser apresentada (erro 404), será automaticamente redireccionado para uma página Web que lhe disponibiliza opções de selecção entre páginas alternativas com associação temática.
- **Defina e mantenha o Yahoo! na qualidade de motor de busca do seu browser** - (desactivado por predefinição) - o Yahoo! é o motor de busca predefinido para pesquisas na Internet da Barra de Ferramentas de Segurança do AVG, e, ao activar esta opção, poderá ser também o motor de busca predefinido do seu browser.
- **Voltar a apresentar a Barra de Ferramentas de Segurança do AVG se oculta (semanalmente)** - (activado por predefinição) - esta opção está activada por predefinição e, quando o **Barra de Ferramentas de Segurança do AVG** for inadvertidamente oculta, voltará a apresentá-la novamente no prazo de uma semana.

10. Definições Avançadas do AVG

A janela de configuração avançada do **AVG 9 Anti-Virus plus Firewall** 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.

10.1. Aparência

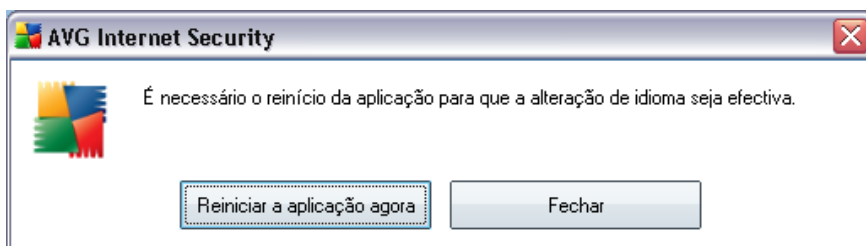
O primeiro item da árvore de navegação, **Aparência**, refere-se às definições gerais da [Interface do utilizador do AVG](#) e a algumas opções elementares do comportamento da aplicação:



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](#). A Lista de Opções só disponibiliza os idiomas que seleccionou previamente para serem instaladas durante o [processo de instalação](#) (consulte o capítulo [Instalação Personalizada - Seleção de Componentes](#)). No entanto, para concluir a alteração de idioma da aplicação terá de reiniciar a interface do utilizador; siga os passos seguintes:

- Selecciono 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 seleccionado/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.

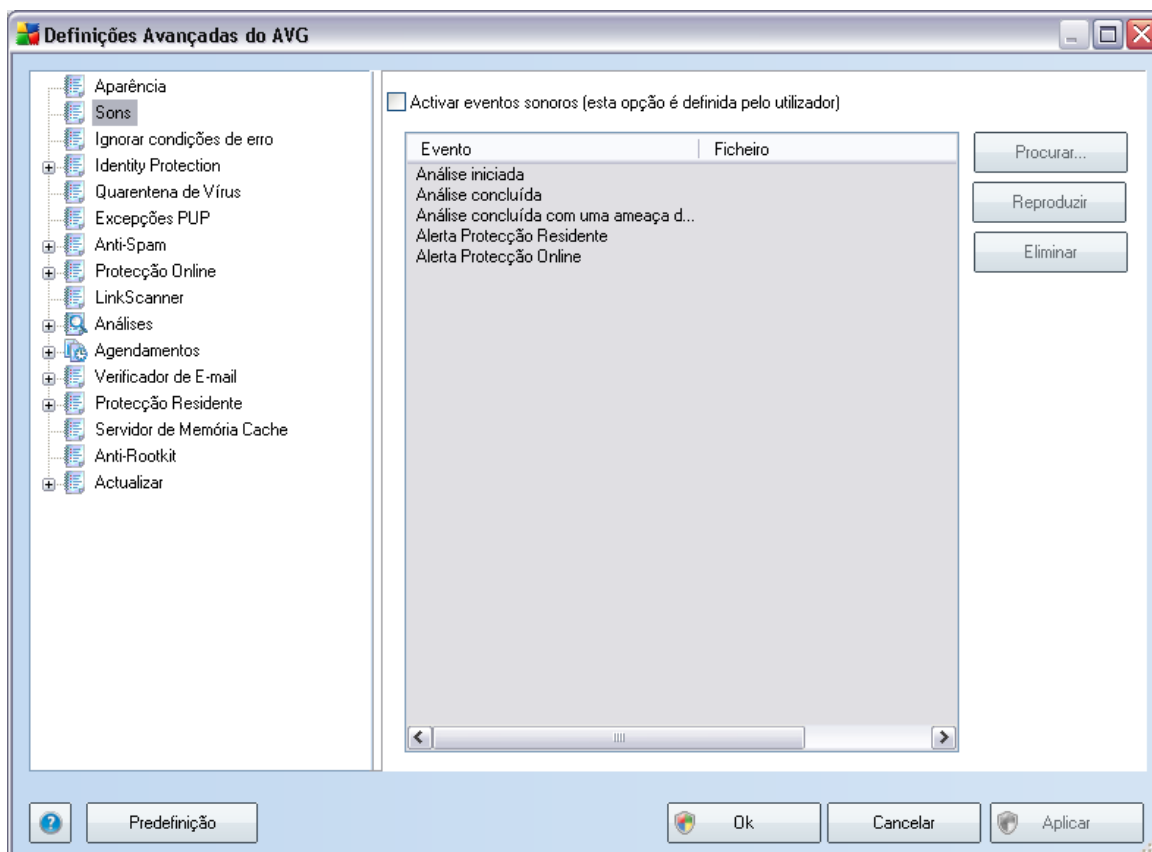
- o **Apresentar notificações da barra de notificação relativas a actualizações** - decida se as informações relativas ao início, progresso, e finalização da actualização do AVG deverão ser apresentadas;
- o **Apresentar notificações relativas a alterações de estado dos componentes** - decida se as informações 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** - decida se as informações relativas aos processos de armazenamento, cópia e abertura de ficheiros devem ser apresentadas ou ocultas (*esta configuração só é possível se a opção de Restauro automático da Protecção Residente estiver activada*);
- 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 de entrada e a enviar deverão ser apresentadas.

Modo de Jogo

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

10.2. Sons

Na janela **Sons** pode especificar se quer ser informado de acções específicas do AVG 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:

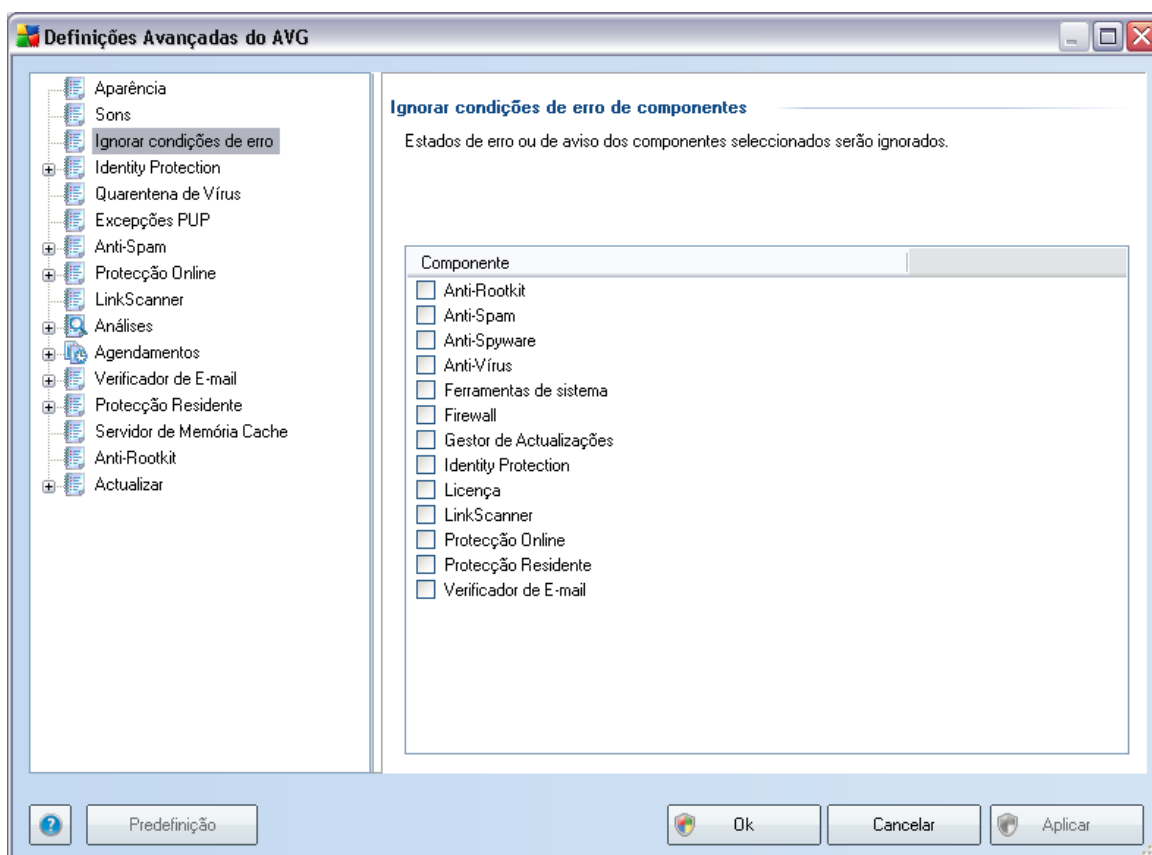


Depois, seleccione o evento respectivo a partir da lista procure (**Procurar**) no seu disco um som adequado que pretenda atribuir a este evento. Para ouvir o som seleccionado, realce o evento na lista e prima o botão **Reproduzir**. Use o botão **Eliminar** para remover o som atribuído a um evento específico.

Nota: Só são suportados sons *.wav!

10.3. Ignorar Condições de Erro

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



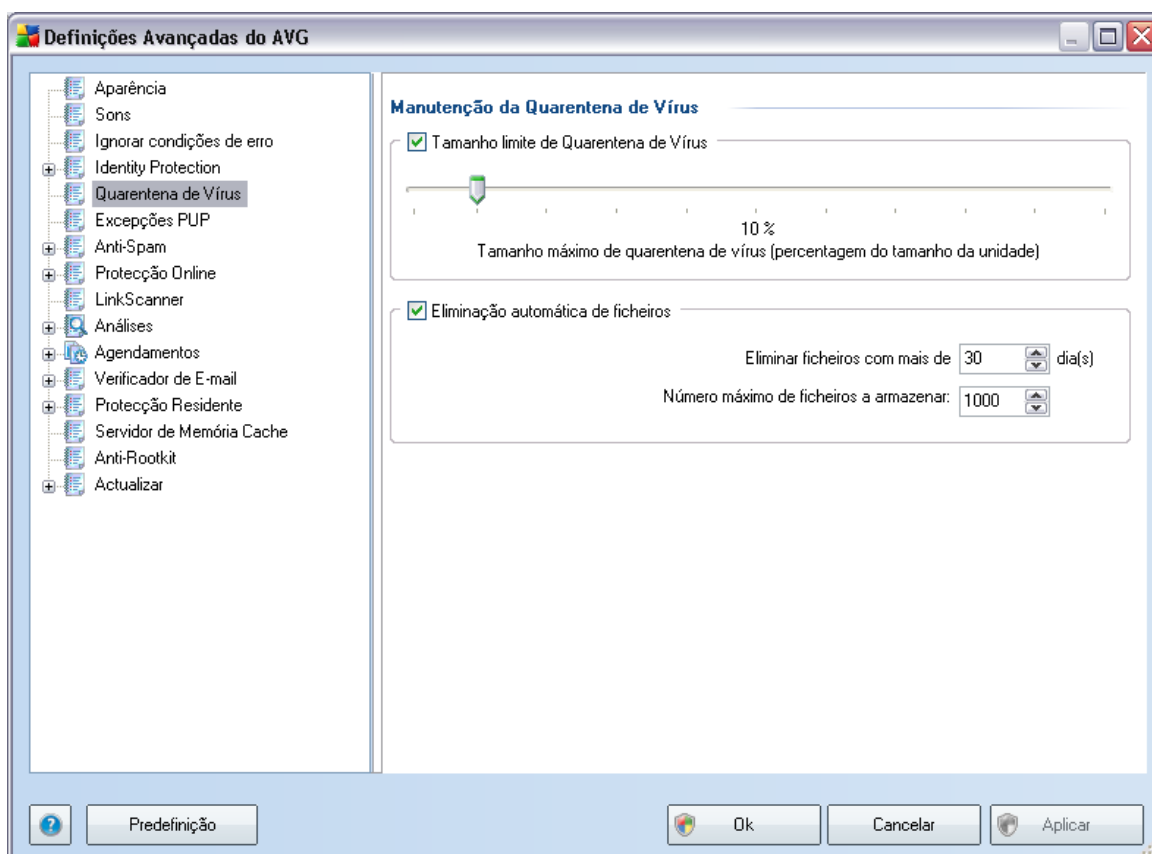
Por predefinição, nenhum dos componentes na lista está seleccionado. O que significa que se algum componente obtiver um estado de erro, será informado imediatamente dessa situação através:

- **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](#).

10.4. Quarentena de Vírus



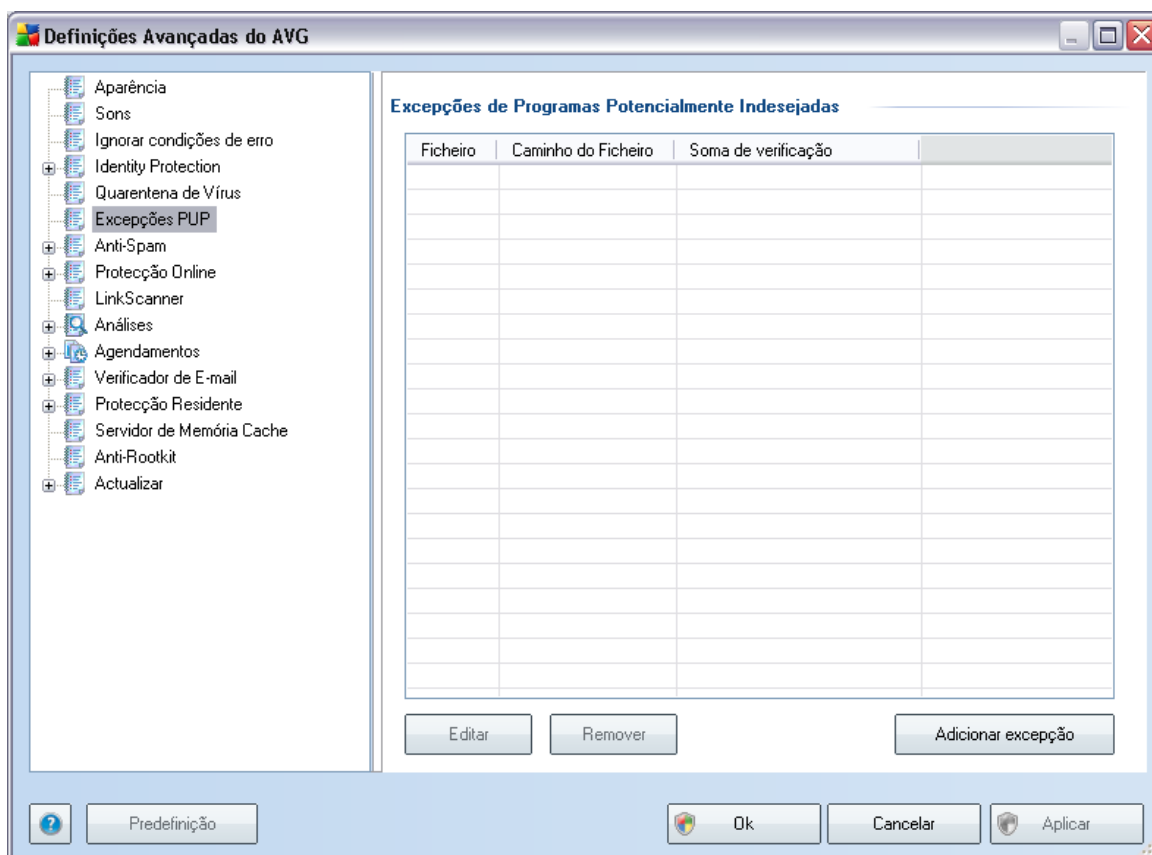


A janela **Manutenção da Quarentena de Vírus** permite-lhe definir vários parâmetros em relação à administração dos objectos armazenados na **Quarentena de Vírus**:

- **Tamanho Limite da Quarentena de Vírus** - utilize o cursor para definir o tamanho máximo da **Quarentena de Vírus**. O tamanho é especificado proporcionalmente ao tamanho do seu disco local.
- **Eliminação automática de ficheiro** - nesta secção defina o tempo máximo que os objectos deverão ficar armazenados na **Quarentena de Vírus** (**Eliminar ficheiros mais antigos do que ...dias**), e o número máximo de ficheiros a serem armazenados na **Quarentena de Vírus** (**Número máximo de ficheiros a serem armazenados**)

10.5. Excepções PUP

O **AVG 9 Anti-Virus plus Firewall** 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:

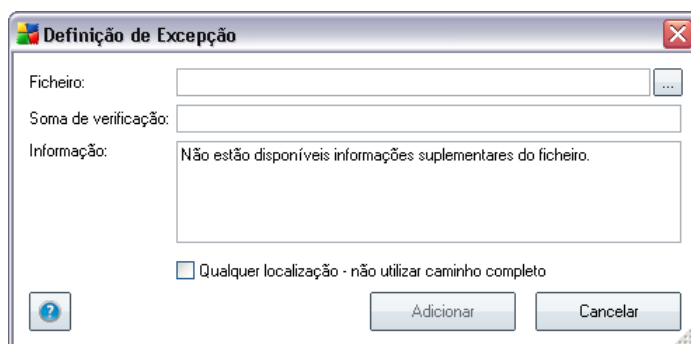


A janela das **Exceções de Programas Potencialmente Indesejados** apresenta uma lista de excepções actualmente válidas e já definidas de programas potencialmente indesejados. Pode editar a lista, eliminar itens existentes, ou adicionar novas excepções. As seguintes informações podem ser encontradas na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

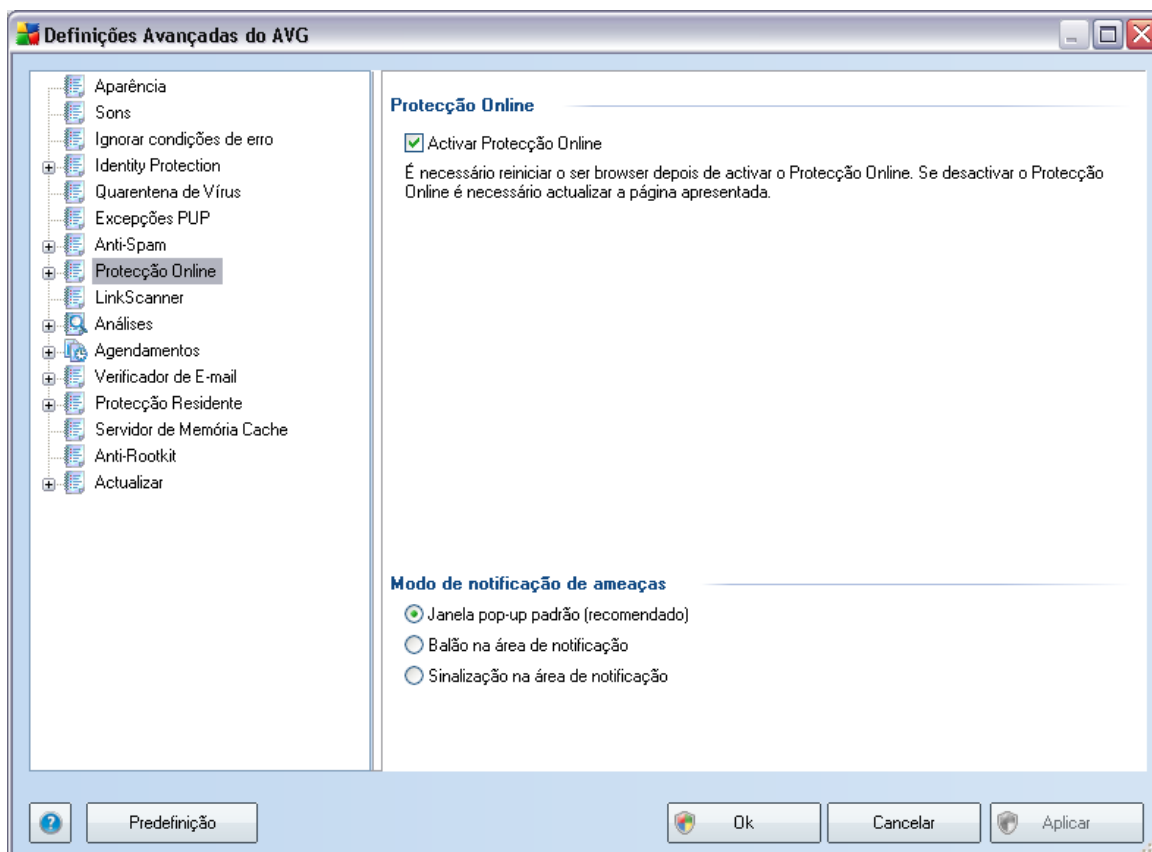
Botões de controlo

- **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 de verificação desmarcada.

10.6. Protecção Online



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

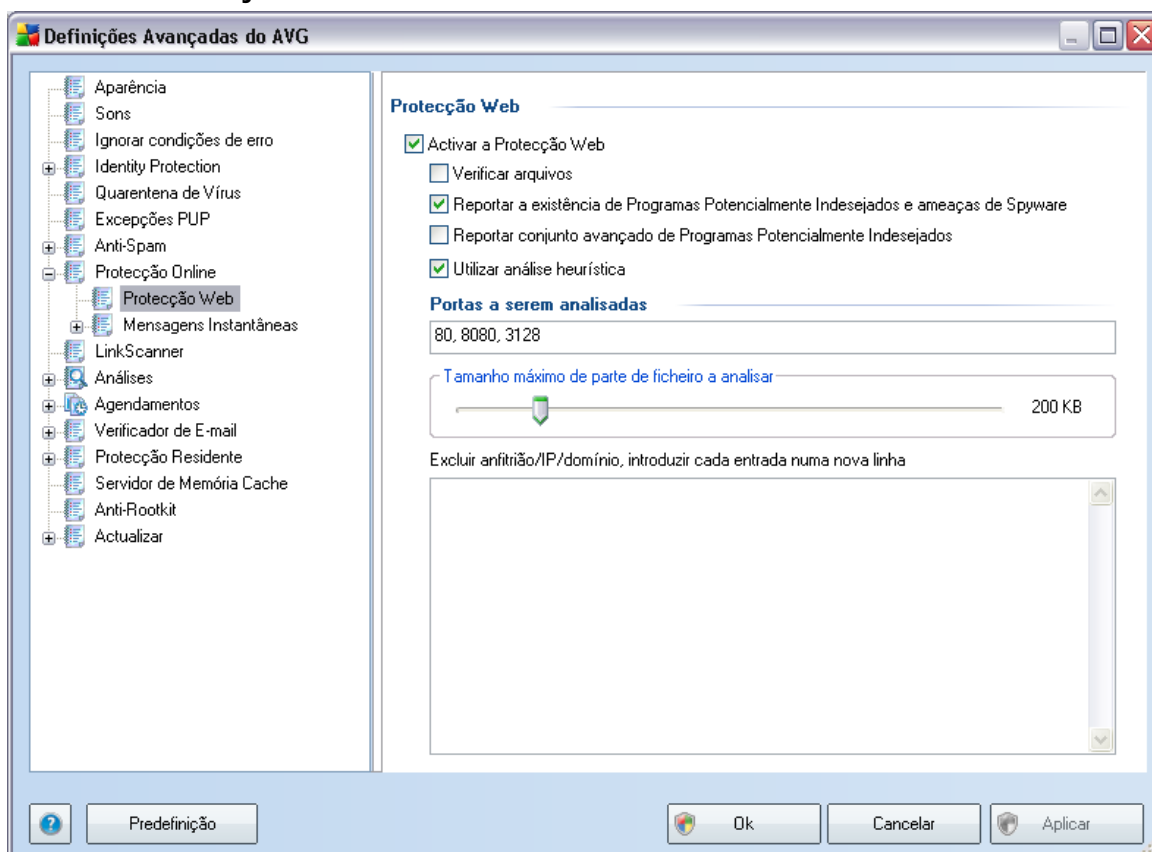
- [**Protecção na Internet**](#)
- [**Mensagens Instantâneas**](#)

Modo de notificação de ameaça

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.

10.6.1. Protecção na Internet



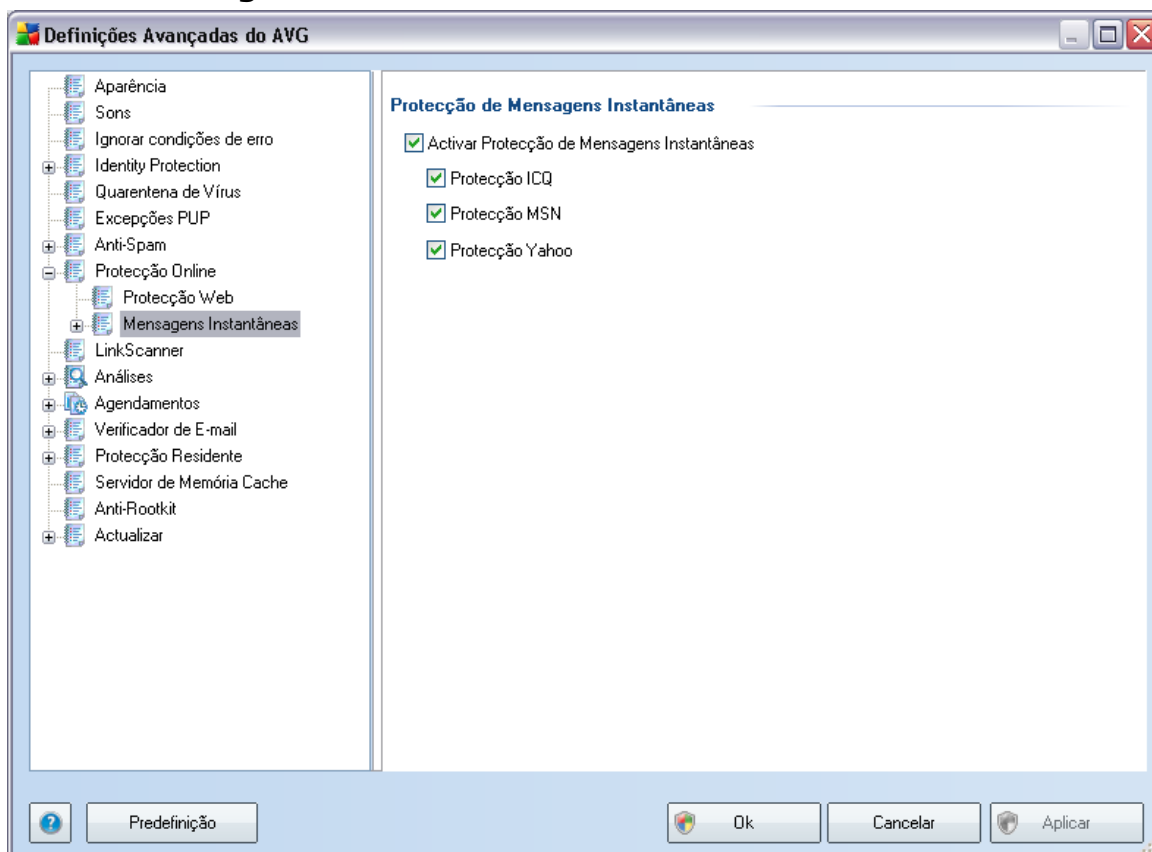
Na janela **Protecção na Internet** pode editar a configuração do componente em relação à análise do conteúdo de websites. A interface de edição permite-lhe configurar as seguintes opções elementares:

- **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** - 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** - se a opção anterior estiver activada, também pode marcar esta caixa 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** - 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 **Portas a serem verificadas** - este campo lista os números padrão das portas de comunicação http. Se a configuração do seu computador for diferente, pode alterar os números das portas conforme necessário.
- 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.

10.6.2. Mensagens Instantâneas

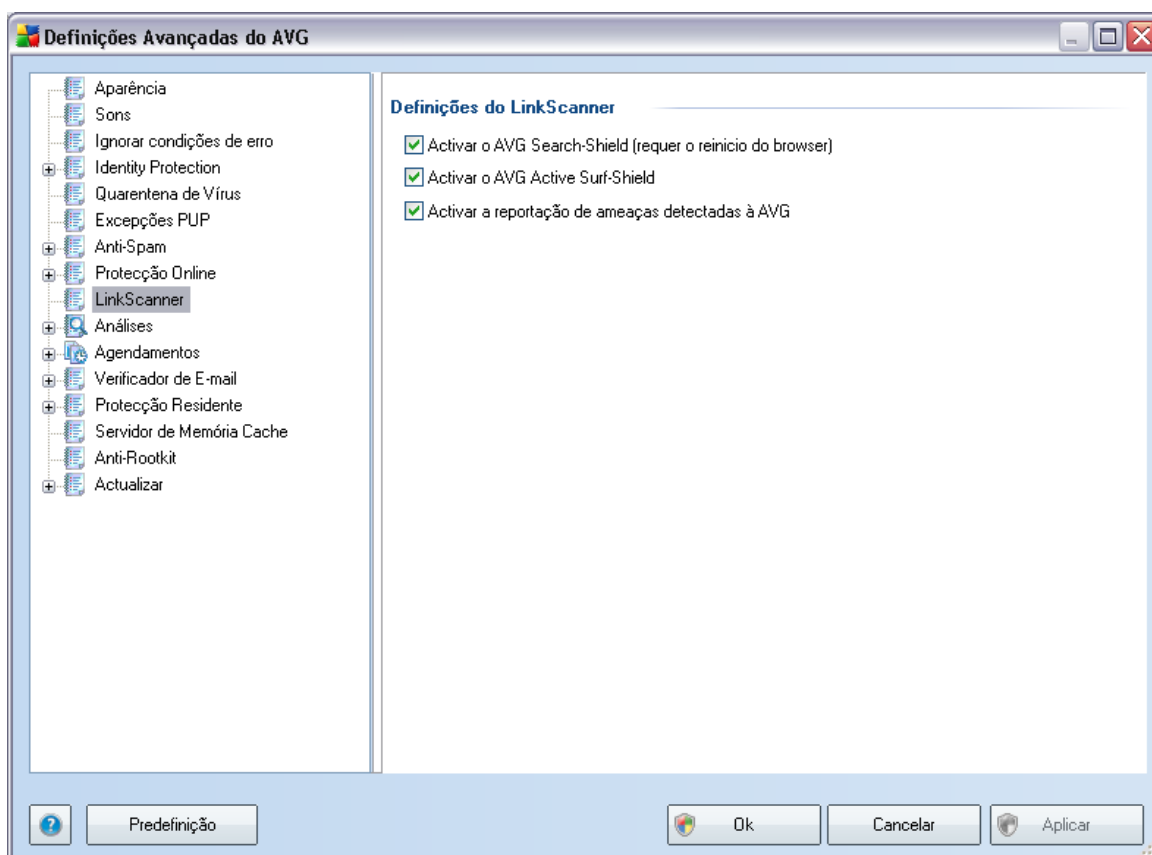


Na janela **Protecção de Mensagens Instantâneas** pode editar as definições dos componentes da **Protecção Online** relativos à análise de mensagens instantâneas. São actualmente suportados os três programas de mensagens instantâneas seguintes: **ICQ**, **MSN** e **Yahoo** - marque o item respectivo 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).

10.7. Link Scanner

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



- **Activar o AVG Search-Shield-** (*activado por predefinição*): ícones de notificação de aviso em procuras efectuadas no Google, Yahoo, Bing, Yandex, Altavista ou Baidu, tendo verificado antecipadamente o conteúdo dos websites facultados pelo motor de busca.
- **Activar o AVG Active 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*).
- **Activar a reportação de ameaças detectadas à AVG** - (*activado por*

predefinição): seleccione este item para permitir a reportação de exploits e websites maliciosos encontrados pelos utilizadores seja através do **AVG Active Surf-Shield** ou do **AVG Search-Shield** para juntar à base de dados de recolha de informação relativa a actividade maliciosa na Web.

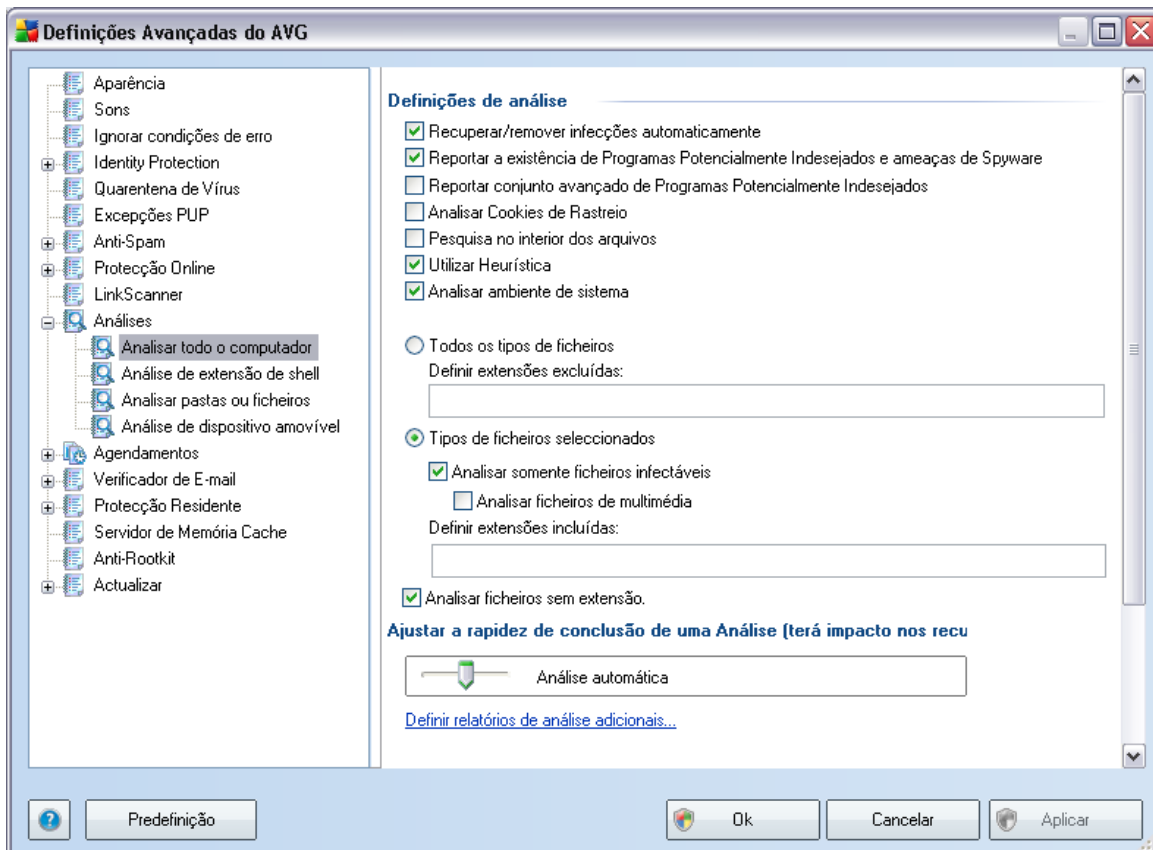
10.8. Análises

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

- **Analisar 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

10.8.1. Analisar todo o computador

A opção **Analisar todo o computador** permite-lhe editar os parâmetros de uma das análises predefinidas pelo fornecedor do software, **Analisar 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** - se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Se o ficheiro infectado não puder ser restaurado automaticamente, o objecto infectado será movido para a **Quarentena de Vírus**.

- **Reportar Programas Potencialmente Indesejados e ameaças de Spyware** - (activado por predefinição): marque para activar o componente [Anti-Spyware](#) e analisar a existência de spyware assim como de vírus. [O Spyware](#) representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.
- **Reportar conjunto avançado de Programas Potencialmente Indesejados** - se a opção anterior estiver activada, também pode marcar esta caixa para detectar pacotes expandidos de [spyware](#): programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.
- **Analisar a Existência de Cookies de Rastreio** este parâmetro do componente [Anti-Spyware](#) define que as cookies deverão ser detectadas; (*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*)
- **Analisar no interior de arquivos** - 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** - análise heurística (*a 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**- a análise verificará também as áreas de sistema do seu computador.

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.

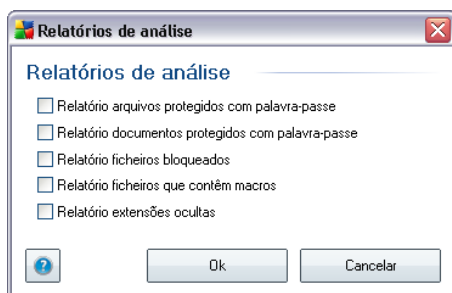
- Opcionalmente, pode decidir se pretende **Analisar ficheiros sem extensão** - esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

Prioridade do processo de análise

Na secção **Prioridade do processo de 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 médio de utilização automática de recursos. Se quiser que a análise seja executada mais rapidamente, esta demorará menos tempo mas a utilização de recursos do sistema aumentará significativamente durante a sua execução, e diminuirá o desempenho de outras actividades no seu PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir a utilização dos recursos do sistema prolongando a duração da análise.

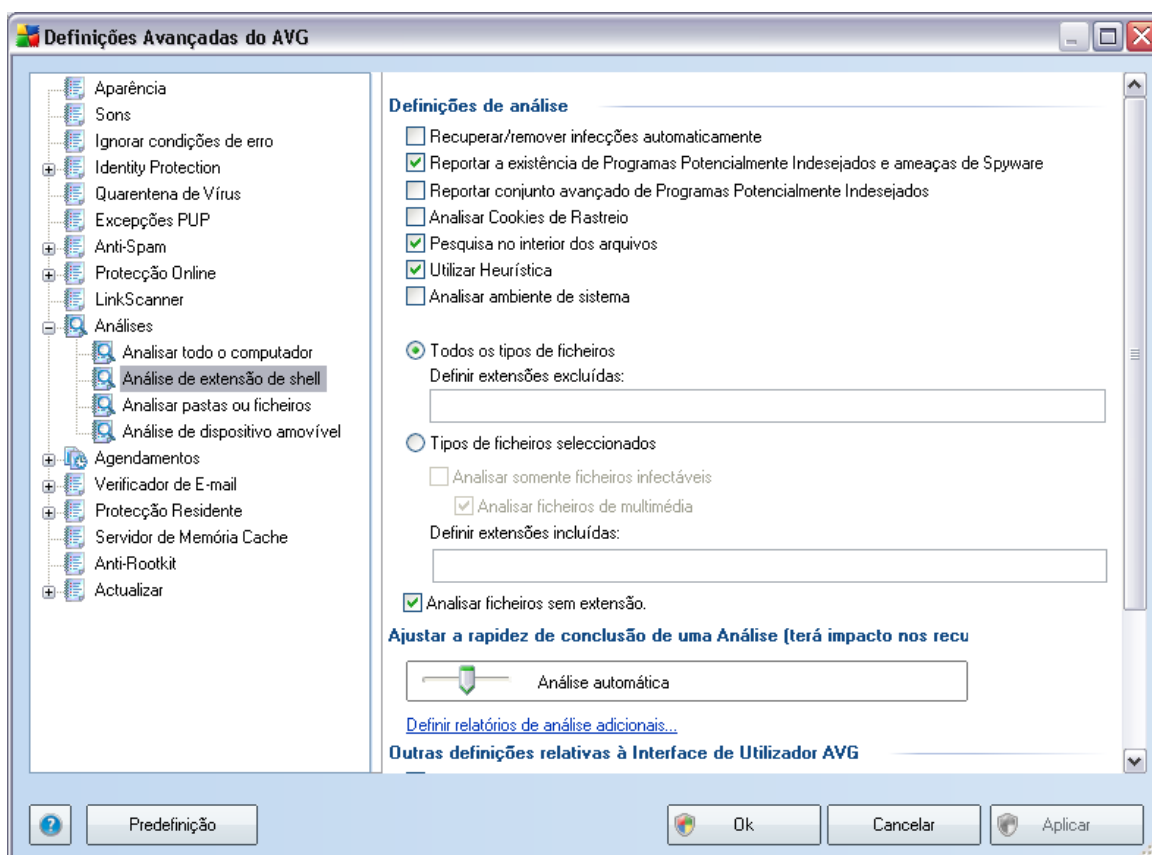
Definir relatórios de análise adicionais...

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



10.8.2. Análise em contexto

À semelhança do item anterior a análise [Analisar 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](#):

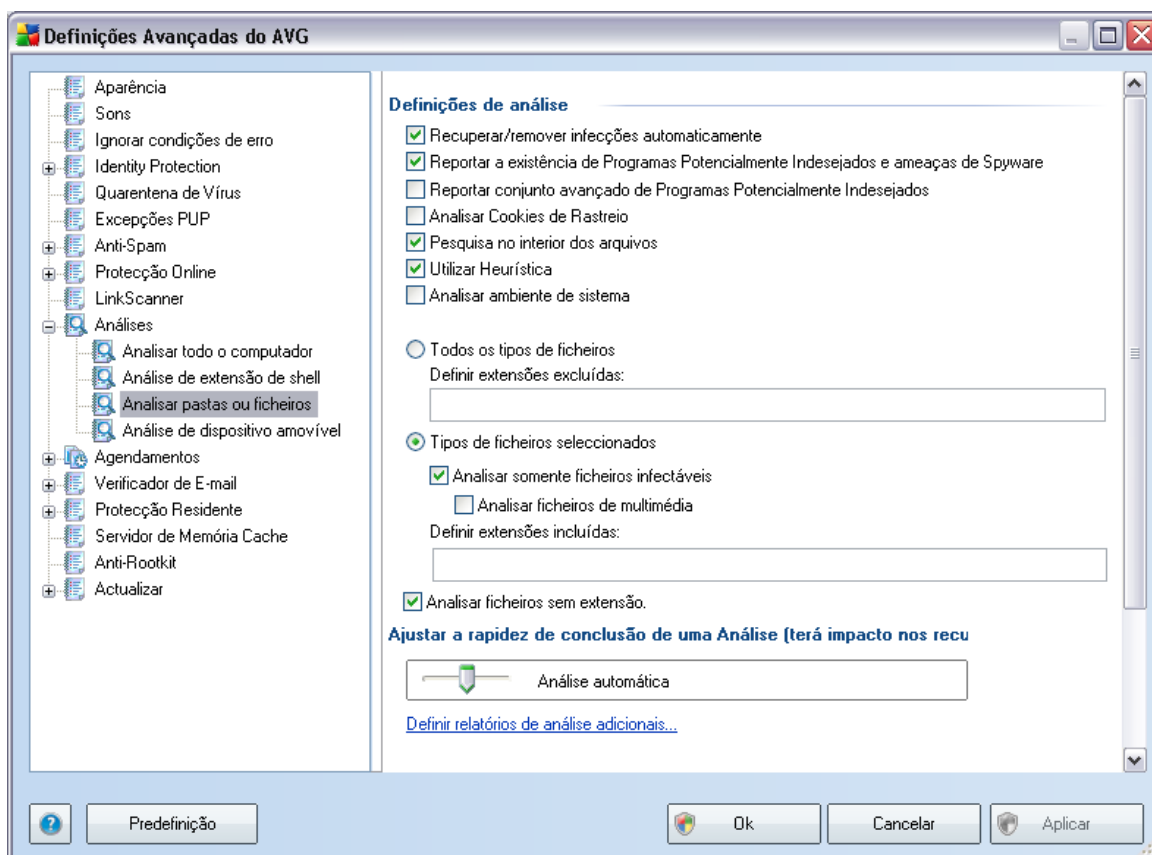


A lista de parâmetros é idêntica aos disponíveis para a análise [Analisar todo o computador](#). No entanto, as definições padrão diferem: com a análise **Analisar Todo o Computador** a maioria dos parâmetros são seleccionados enquanto que para a **Análise de extensão da Shell** (([Análise no Explorador do Windows](#))) só os parâmetros relevantes estão activados.

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

10.8.3. Analisar pastas ou ficheiros específicos

A interface de edição para a análise **Analisar pastas ou ficheiros específicos** é idêntica à janela de edição da análise **Analisar 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**:

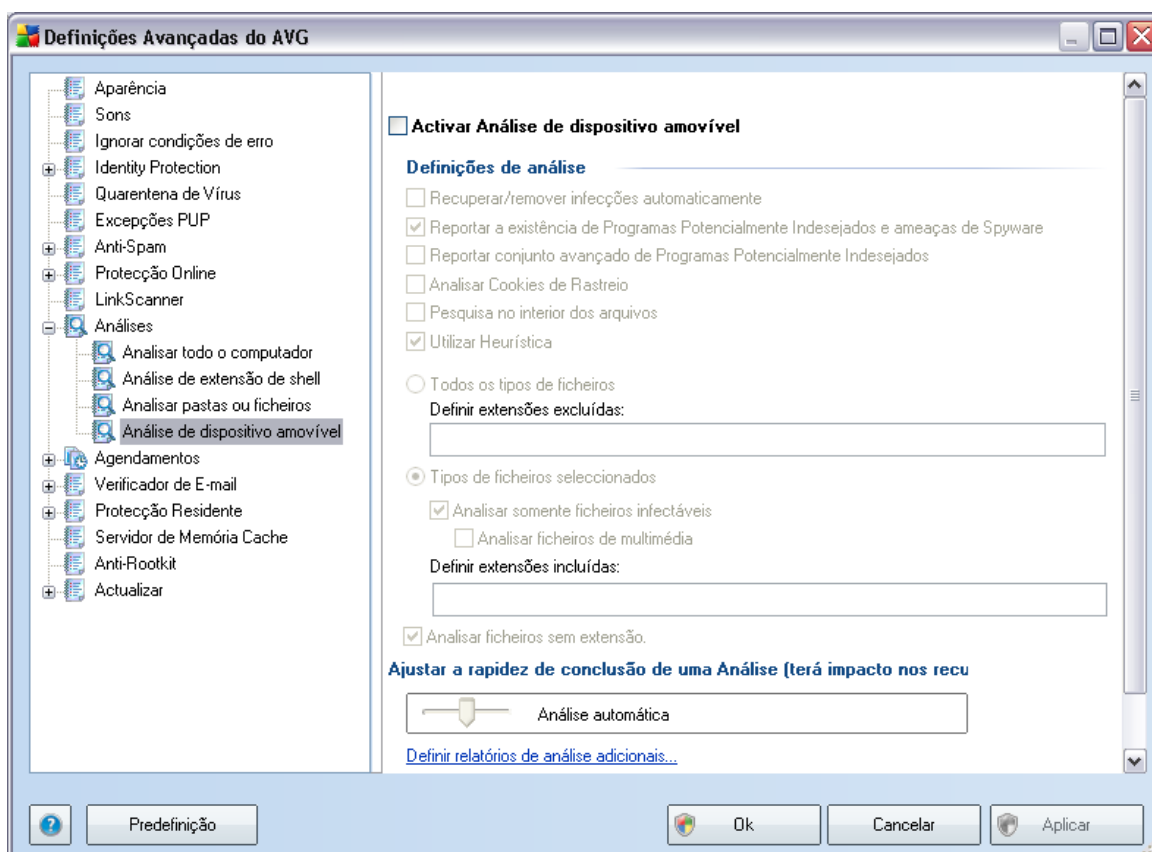


Todos os parâmetros definidos nesta janela de configuração aplicam-se apenas às áreas seleccionadas para análise com a **Análise de ficheiros e pastas específicos**!

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

10.8.4. Análise de Dispositivo Amovível

Esta 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 / Analisar Todo o Computador](#).

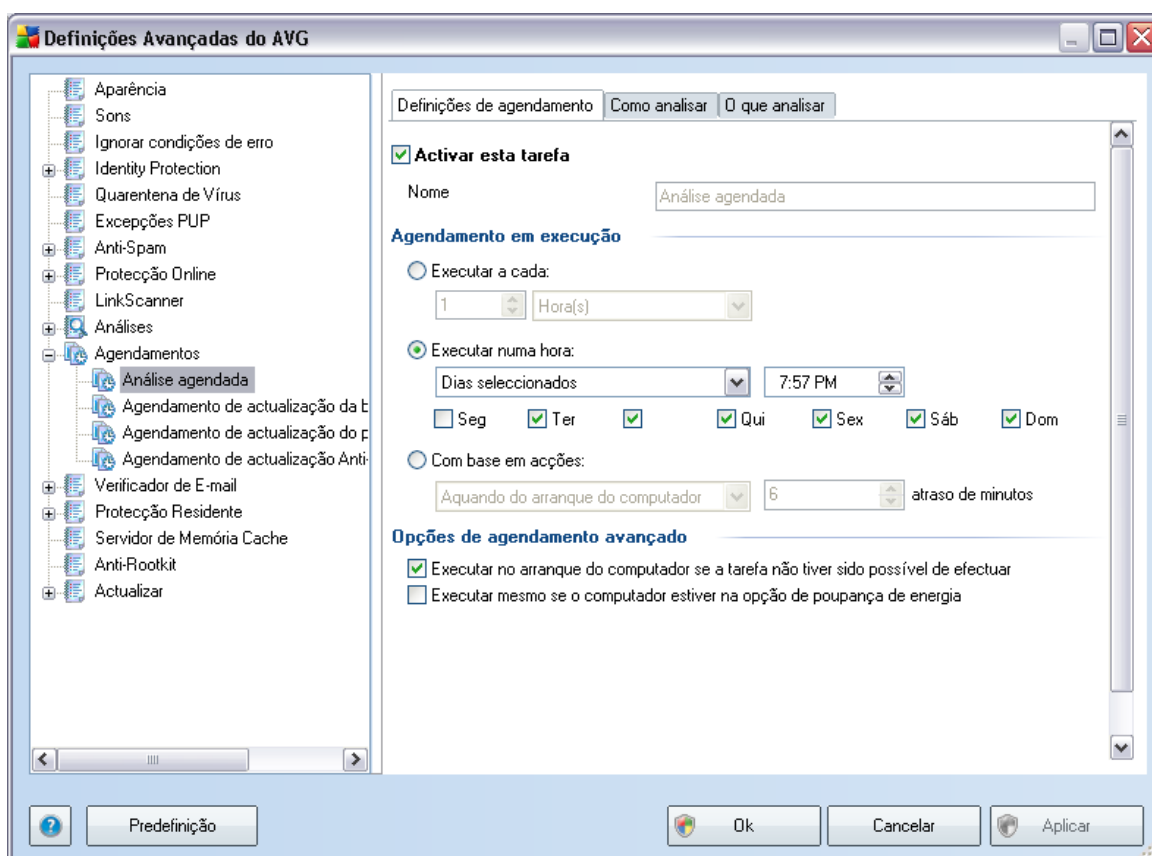
10.9. Agendamentos

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

- [Agendamento de análise a todo o computador](#)
- [Agendamento de actualização da base de dados de vírus](#)
- [Agendamento de actualização do programa](#)

10.9.1. Análise agendada

Os parâmetros da análise agendada podem ser editados (*ou configurado um novo agendamento*) nos três separadores:



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, 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:

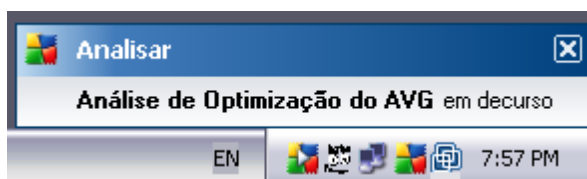
Agendamento em execução

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

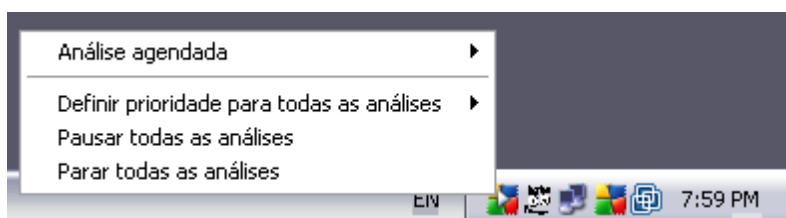
Opções de agendamento avançado

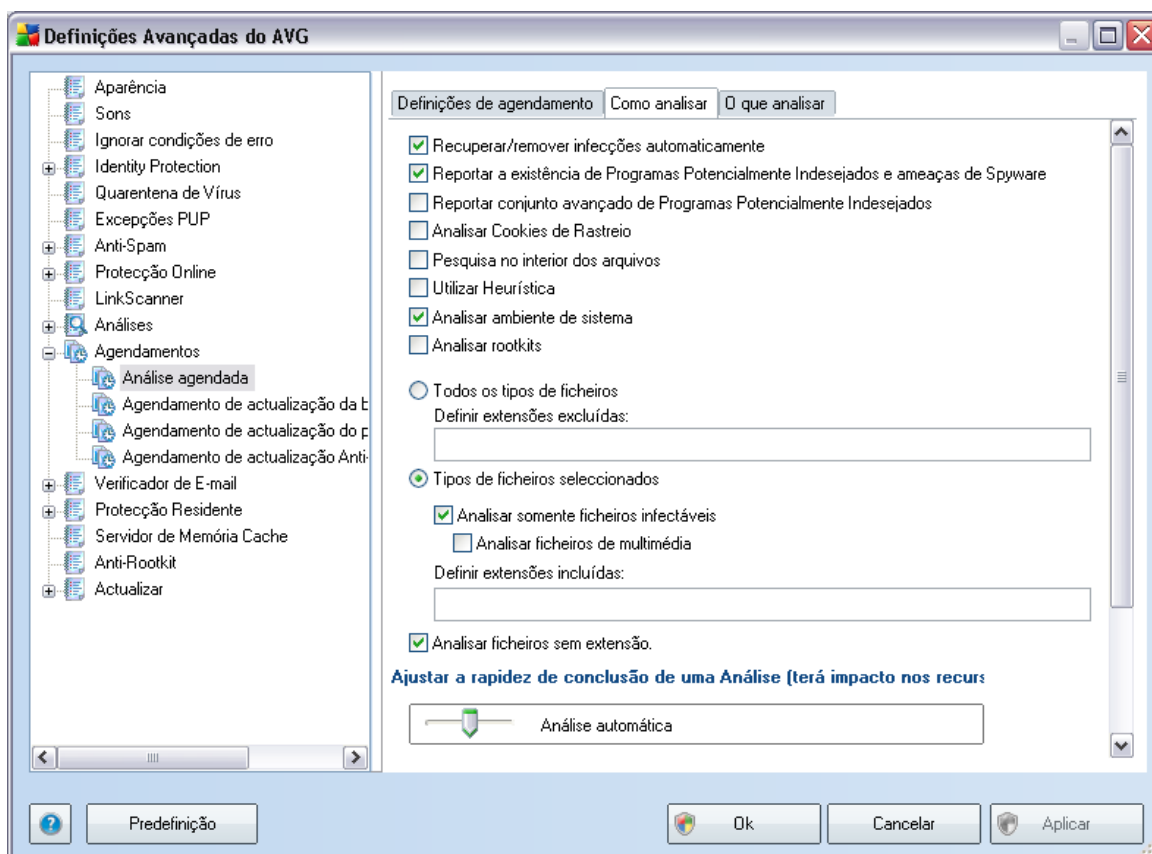
Esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

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 da barra de notificação](#) (de cor cheia com uma seta branca - 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 para abrir um menu de contexto onde pode decidir pausar ou até mesmo parar a análise em execução:





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** - se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Se o ficheiro infectado não puder ser restaurado automaticamente, o objecto infectado será movido para a [Quarentena de Vírus](#).
- **Reportar Programas Potencialmente Indesejados e ameaças de Spyware** - (activado por predefinição): marque para activar o componente [Anti-Spyware](#) e analisar a existência de spyware assim como de vírus. [O Spyware](#) representa uma categoria de malware questionável: apesar de

normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade activada uma vez que aumenta a segurança do seu computador.

- **Reportar conjunto avançado de Programas Potencialmente Indesejados** - se a opção anterior estiver activada, também pode marcar esta caixa para detectar pacotes expandidos de [spyware](#): programas que são perfeitamente fidedignos e inofensivos quando adquiridos directamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desactivada por predefinição.
- **Analisar a existência de Cookies de Rastreio** - (activado por predefinição): este parâmetro do componente [Anti-Spyware](#) define que as cookies deverão ser detectadas durante a análise; (cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação específica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras electrónicos dos mesmos)
- **Analisar no interior de arquivos** - (activado por predefinição): este parâmetro define que a análise deverá verificar todos os ficheiros mesmo se estes estiverem comprimidos em arquivos, ex. ZIP, RAR,...
- **Utilizar Heurística** - (activado por predefinição): análise heurística (a 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;
- **Analisar a existência de rootkits** - 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

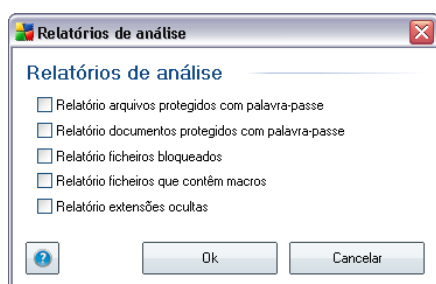
apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo - se deixar esta caixa desmarcada, reduzirá 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.

Prioridade do processo de análise

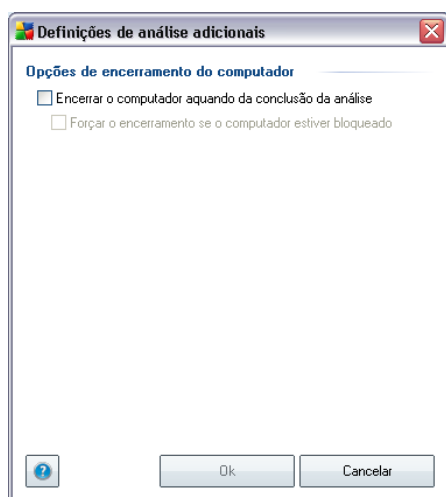
Na secção **Prioridade do processo de análise** pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. O valor desta opção está por predefinição definido para o nível médio de utilização automática de recursos. Se quiser que a análise seja executada 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.

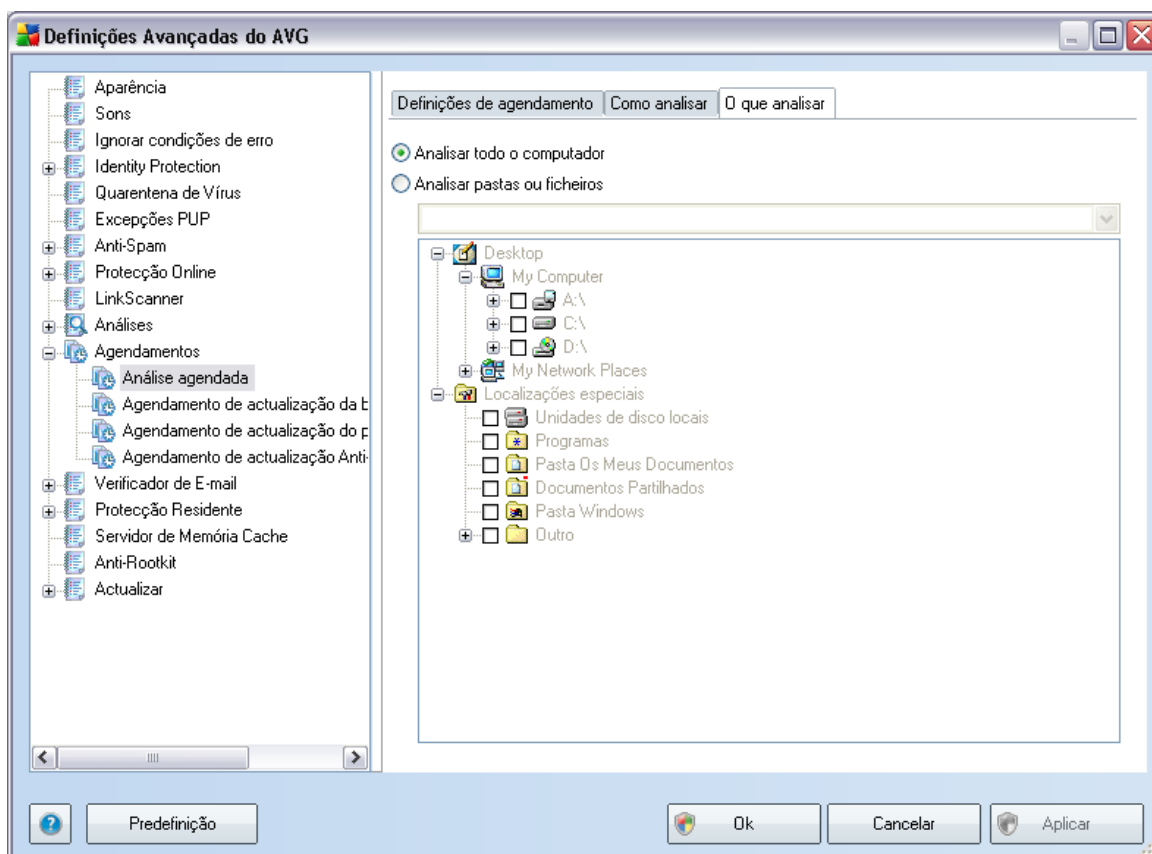
Clique no link **Configurar relatórios de análise adicionais ...** para abrir uma janela independente apelidada **Relatórios de análise** onde pode seleccionar vários itens para definir quais as detecções que deverão ser reportadas:



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**),

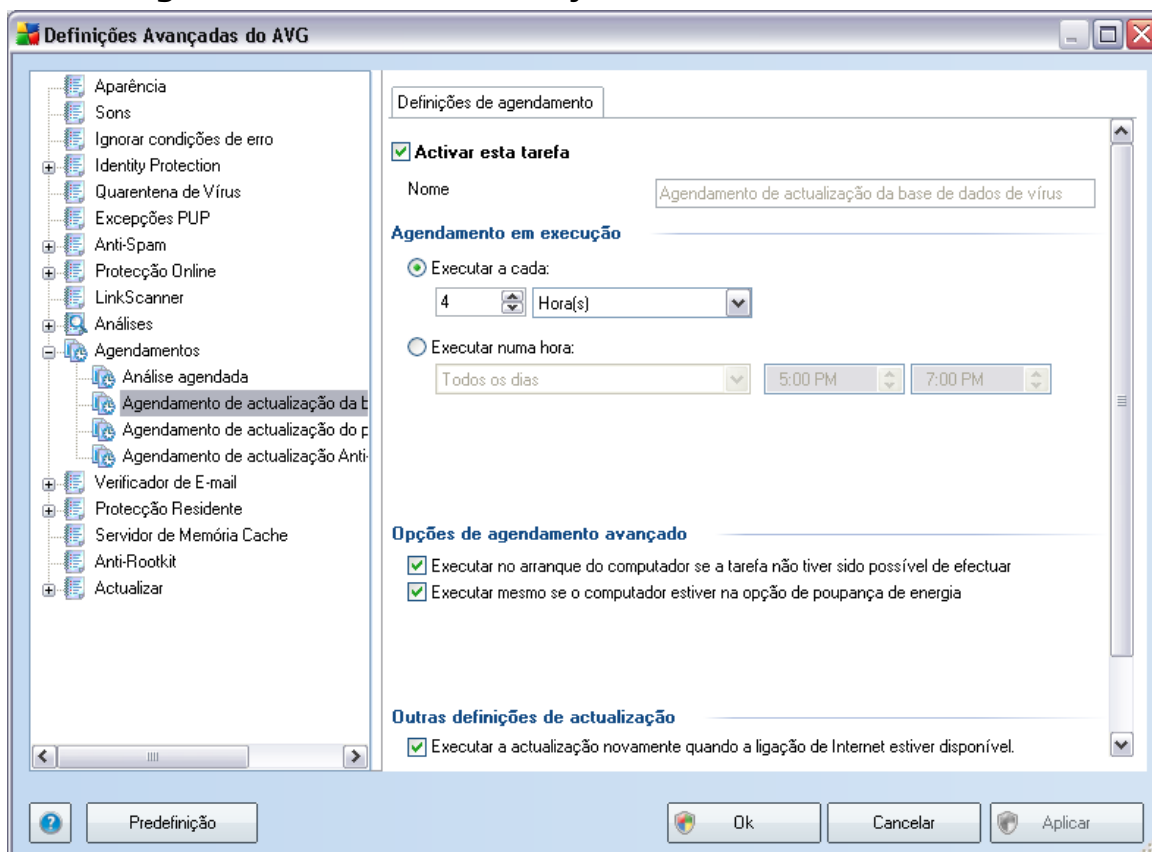
será activada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar encerramento se o computador estiver bloqueado***).





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.

10.9.2. Agendamento de actualização da base de dados de vírus



No separador **Definições de agendamento** pode seleccionar/desseleccionar o item **Activar esta tarefa** para desactivar temporariamente o agendamento de actualização da base de dados de vírus, e voltar a activá-lo conforme necessário. O agendamento de actualização da base de dados de vírus básico está previsto no componente **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...***).

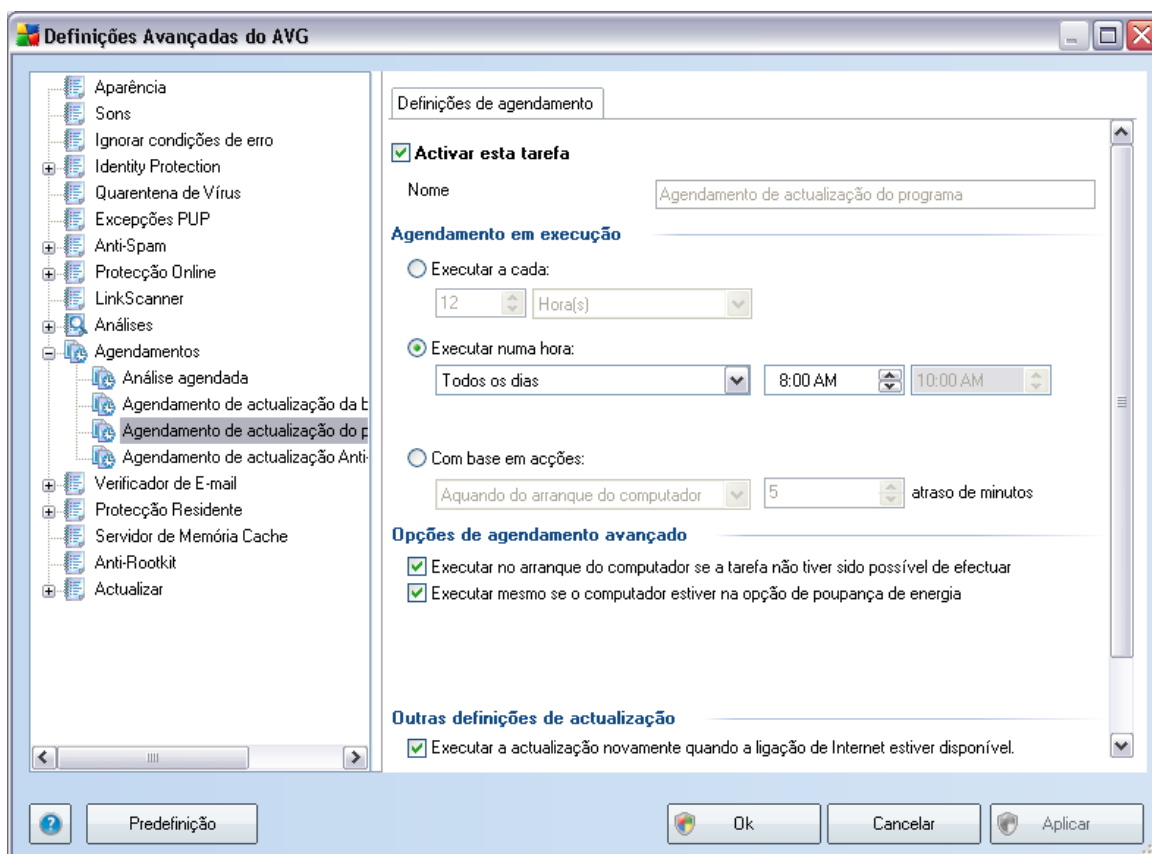
Opções de agendamento avançado

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](#).



No separador **Definições de agendamento** pode seleccionar/desseleccionar primeiro o item **Activar esta tarefa** para desactivar temporariamente o agendamento de actualização do Anti-Spam, e voltar a activá-lo conforme necessário. 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.

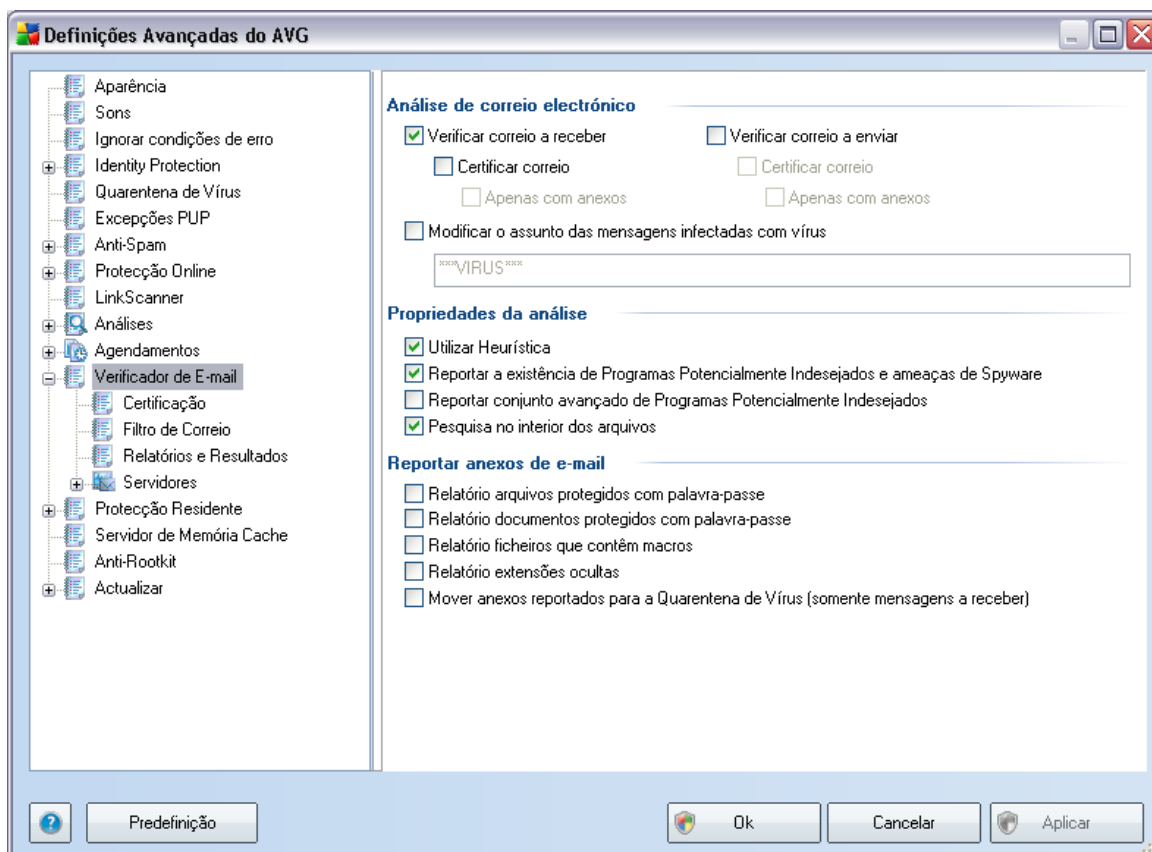
Outras definições de actualização

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.

10.10. Verificador de E-mail



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

- **Análise do E-mail**- nesta secção, pode configurar estas definições básicas para as mensagens de e-mail a receber e/ou a enviar:
 - o Se as mensagens e-mail devem ser analisadas pela existência de vírus.
 - o Se o texto de certificação deve ser adicionado no final de cada mensagem para especificar que esta não contém vírus. O texto pode ser editado na janela [Certificação](#).
 - o Se o texto de certificação deve ser adicionado somente às mensagens que contém anexos.

Para **Modificar o assunto das mensagens infectadas com vírus**, marque a

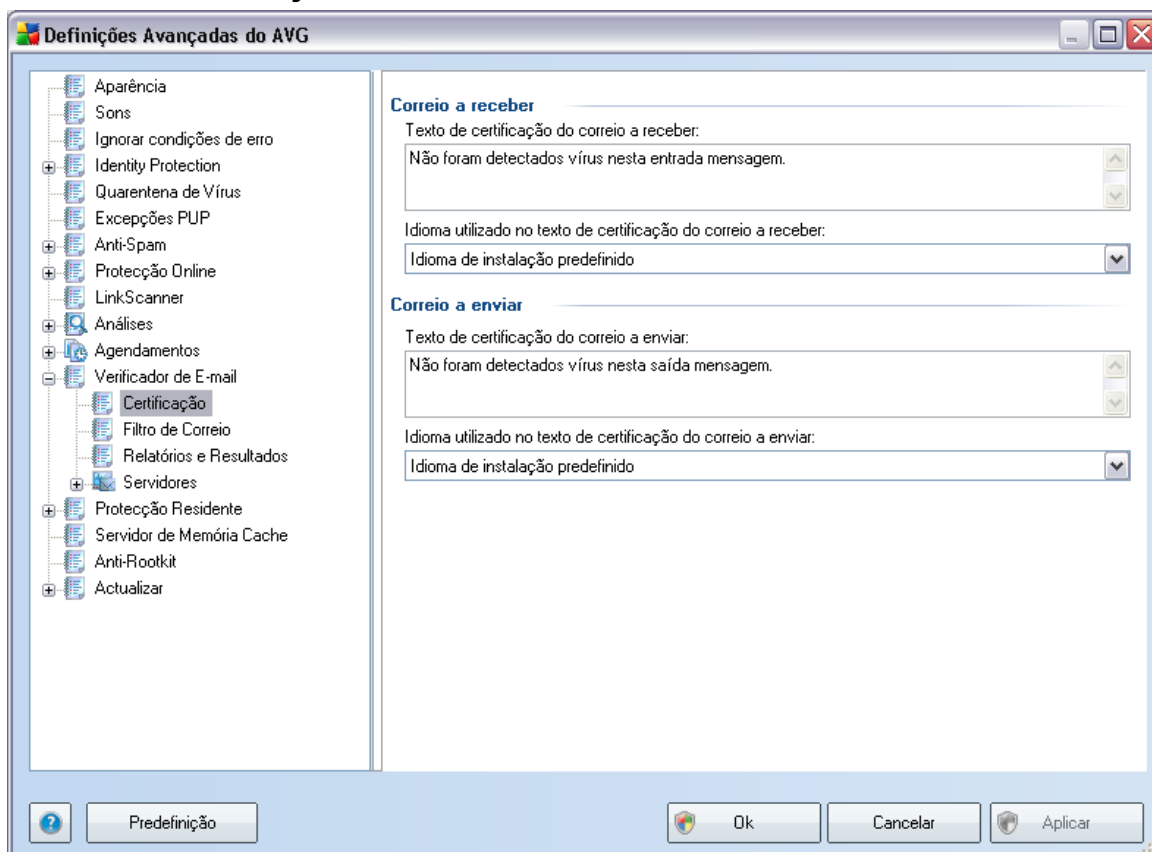
caixa e o digite o valor pretendido no campo de texto. Será então adicionado ao campo de assunto do e-mail infectado para uma identificação e filtragem facilitada. O valor predefinido é ***VÍRUS***, que recomendamos que mantenha.

- **Propriedades da análise** - nesta secção, pode especificar como as mensagens de correio electrónico serão analisadas:
 - o **Utilizar a heurística** - marque a caixa para utilizar o [método de detecção da análise heurística](#) durante a análise 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](#).
 - 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** - se a opção anterior estiver activada, também pode marcar esta caixa 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 no interior de arquivos** - seleccione para analisar os conteúdos de arquivos anexados a mensagens de e-mail.
- **Relatórios de 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](#).
- o **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.

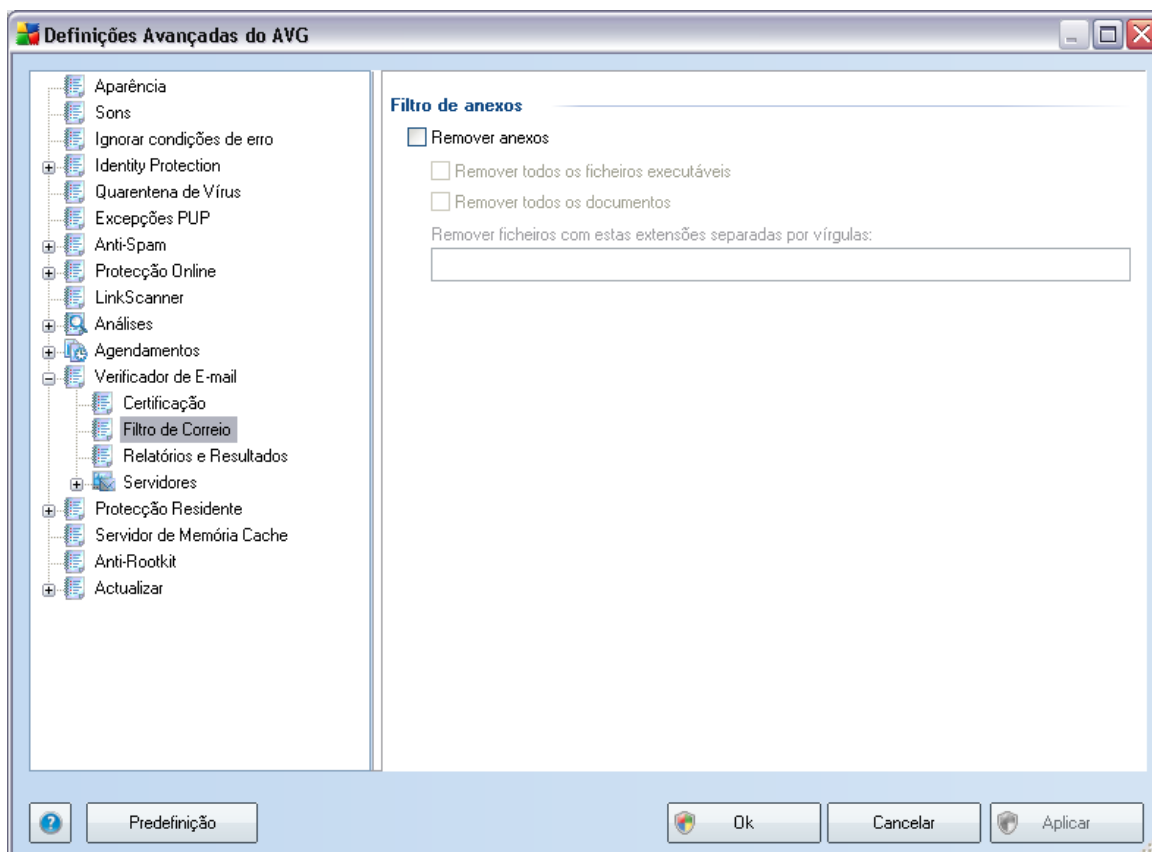
- o **Reportar documentos protegidos por palavra-passe** - documentos que estão protegidos por palavra-passe e que não podem ser analisados pela existência de vírus; seleccione a caixa para os reportar como potencialmente perigosos.
- o **Reportar ficheiros que contenham macros**- uma macro é uma sequência 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.
- o **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.
- o **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](#).

10.10.1. Certificação



Na janela **Certificação** pode especificar exactamente qual o texto que a nota de certificação deverá conter, e em que idioma. Este deve ser especificado separadamente para **o e-mail a receber** *ee-mail a enviar*.

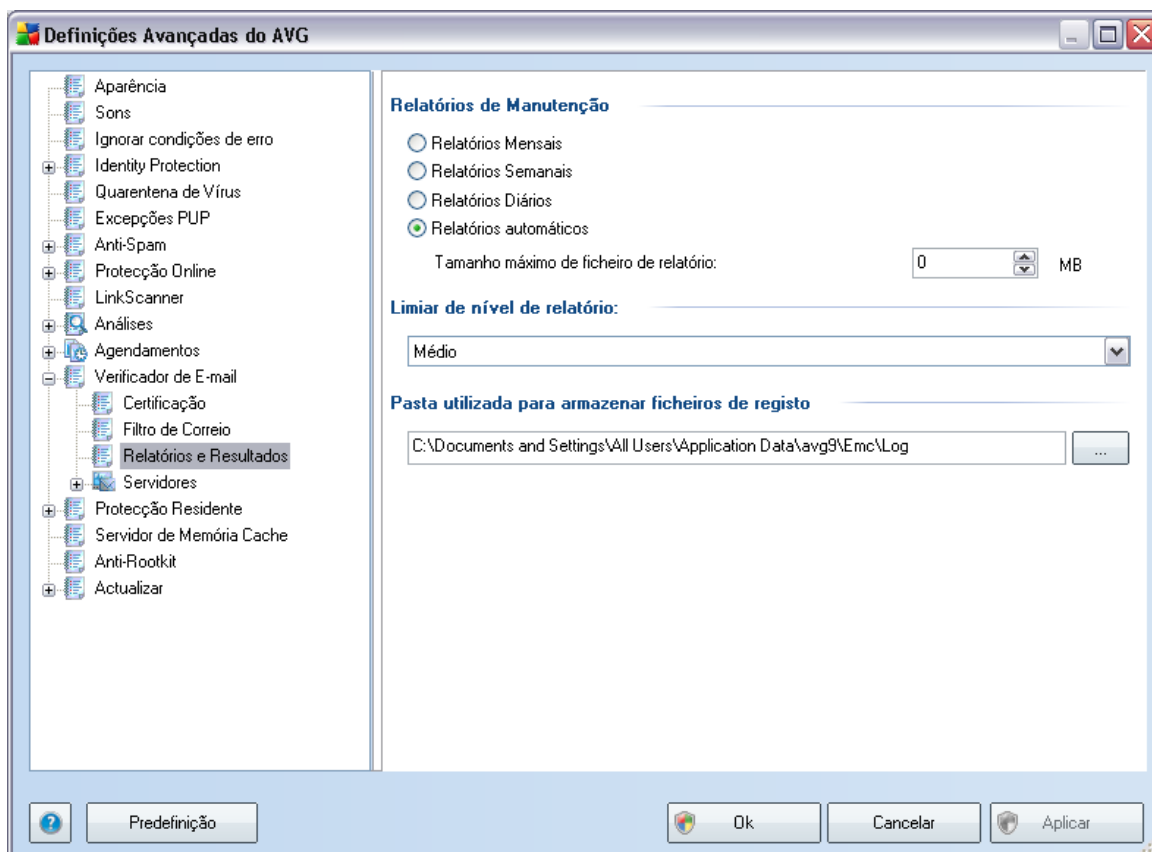
10.10.2. Filtro de Correio



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, selecione 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

10.10.3. Relatórios e Resultados

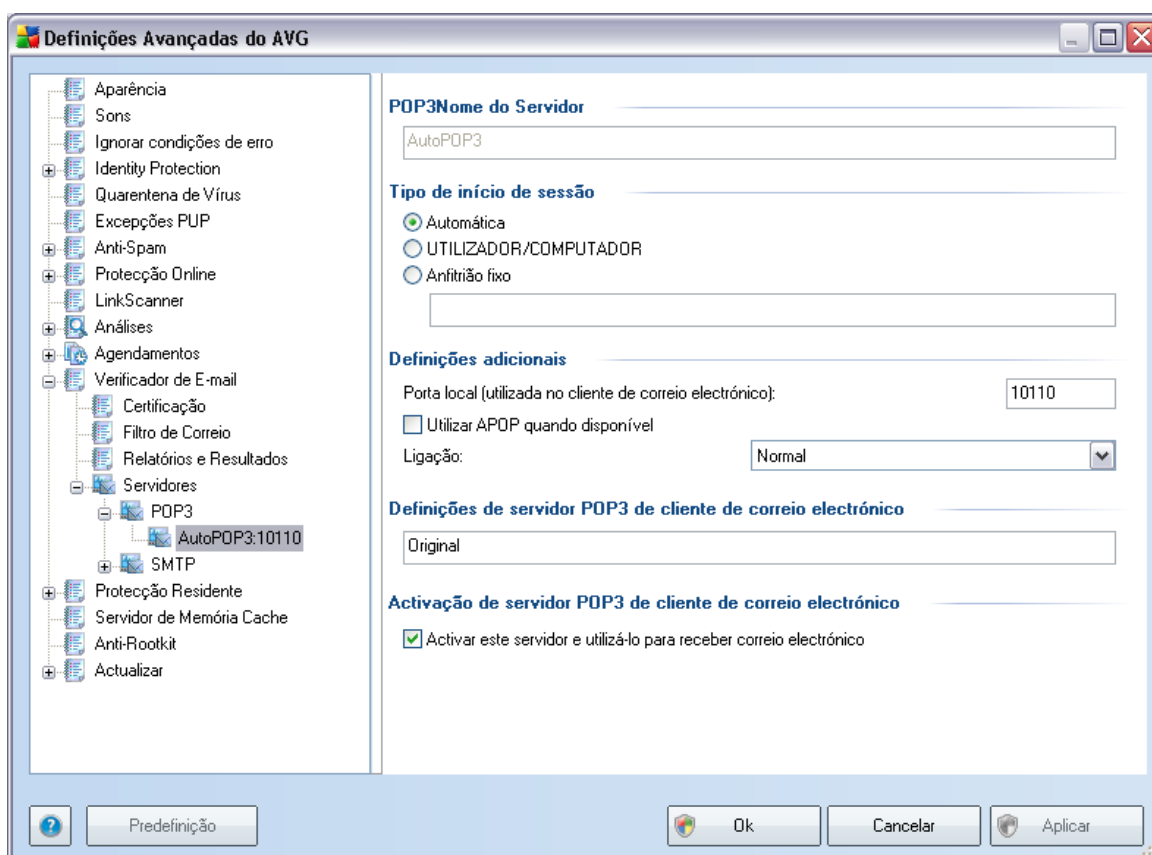


A janela aberta através do item de navegação **Relatórios e Resultados** permite-lhe especificar parâmetros para a manutenção dos resultados de análise de e-mail. A janela de diálogo está dividida em várias secções:

- **Relatórios de Manutenção** - defina se pretende registar as informações de análise de e-mail diariamente, semanalmente, mensalmente,...; e especifique também o tamanho máximo do ficheiro de registo (*em MB*)
- **Limiar de nível de Registo** - o nível médio é configurado por predefinição - pode seleccionar um nível inferior (*registar informações de ligação elementares* ou nível superior (*registar todo o tráfego*)
- **Pasta utilizada para armazenar ficheiros de registo** - defina onde o ficheiro de registo deve estar localizado

10.10.4. 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 de Servidor POP3** - digite o nome do servidor ou mantenha o nome predefinido AutoPOP3
- **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 **UTILIZADOR/COMPUTADOR**- O método mais simples e mais utilizado para determinar o servidor de correio de destino é o método proxy. Para utilizar este método, indique o nome e o endereço (ou também a porta) como parte do nome de utilizador de início de sessão para o servidor de e-mail indicado, separando-os com uma barra /. Por exemplo, para a conta user1 do servidor pop.acme.com e porta 8200, o nome de início de sessão será user1/pop.acme.com:8200.
- 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.

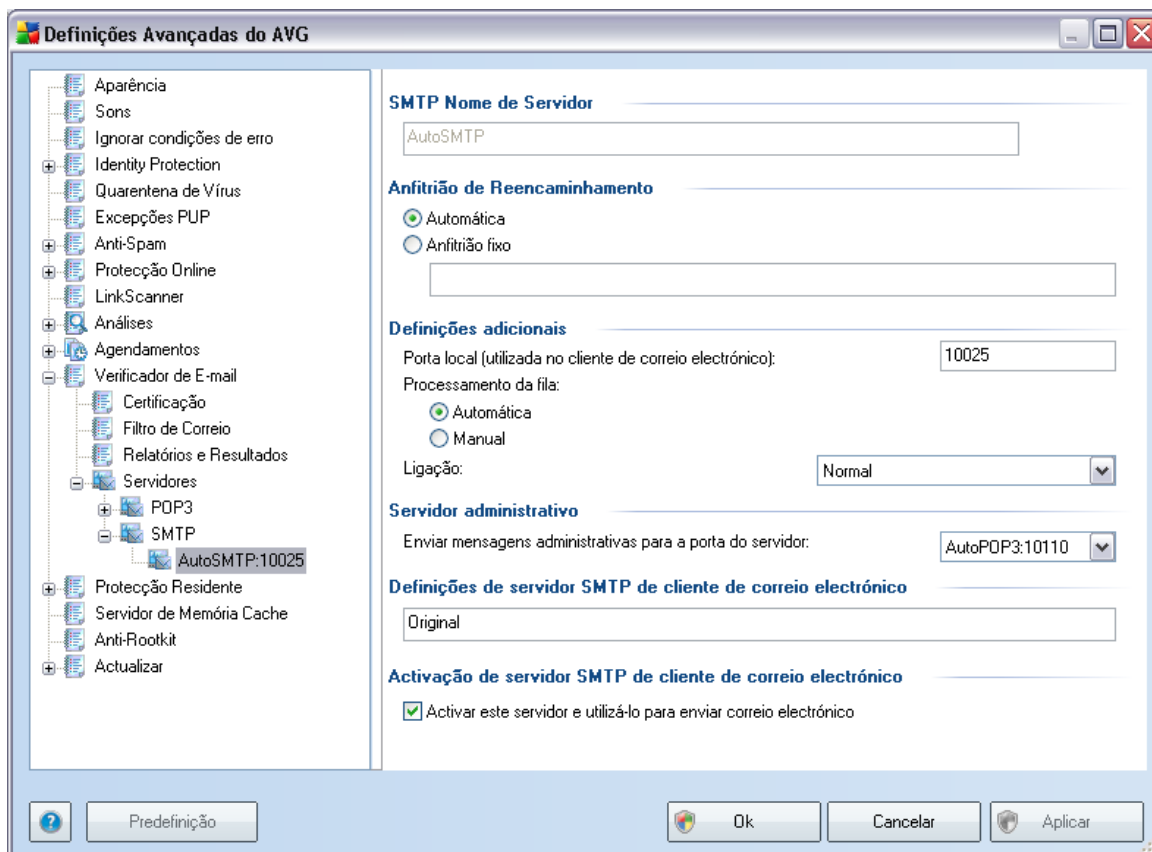
- **Definições adicionais** - especifica parâmetros mais detalhados:

- 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 **Utilizar APOP quando disponível** - esta opção providencia um início de sessão no servidor de correio electrónico mais seguro. Desta forma, terá a certeza de que o [Verificador de E-mail](#) utiliza um método alternativo de reencaminhamento da palavra-passe da conta de utilizador para início de sessão, enviando a palavra-passe ao servidor, não em formato aberto, mas encriptada, utilizando uma sequência de variáveis recebida do servidor. Naturalmente, esta funcionalidade só estará disponível se o servidor de e-mail de destino a suportar.
- 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.

- **Definições do servidor POP3 do cliente de e-mail** - fornece breves informações sobre as definições de configuração necessárias para configurar correctamente o seu cliente de e-mail (para que o [Verificador de E-mail](#) verifique todo o e-mail a receber). Trata-se de um resumo baseado nos parâmetros correspondentes especificados nesta caixa de diálogo e noutras

caixas de diálogo relacionadas.

- **Activação do servidor POP3 do cliente de correio electrónico** - marque/desmarque este item para activar ou desactivar o servidor POP3 especificado



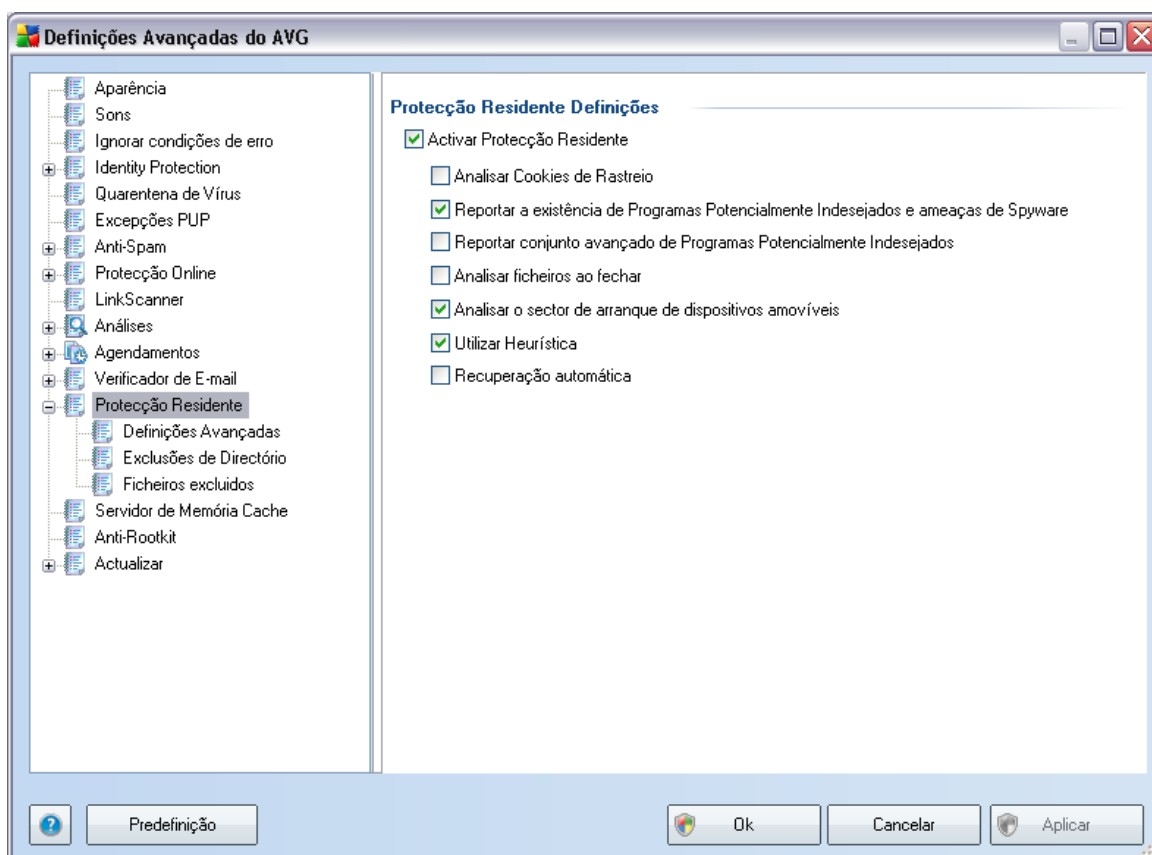
Nesta janela (acessível via **Servidores / SMTP**) pode configurar um novo servidor do **Verificador de E-mail** utilizando o protocolo SMTP para e-mail a enviar:

- **Nome de Servidor SMTP** - digite o nome do servidor ou mantenha o nome predefinido AutoSMTP
- **Relay Host**-define o método para determinar o servidor de e-mail utilizado para o 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) bem como um endereço IP (por exemplo, 123.45.67.89) para um nome. Se o servidor de e-mail utilizar uma porta não padrão, pode escrever esta porta atrás do nome do servidor, utilizando dois pontos 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 **Processamento da fila** - determina o comportamento do [Verificador de E-mail](#) aquando do processamento de pedidos para o envio de e-mails:
 - Automático - O e-mail a enviar é imediatamente entregue (enviado) para o servidor de e-mail de destino
 - Manual - a mensagem é inserida na fila de mensagens a enviar e enviada mais tarde
 - 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.
- **Servidor administrativo**-apresenta o número da porta do servidor que será utilizado para a devolução de relatórios de administração. Estas mensagens são geradas, por exemplo, quando o servidor de e-mail alvo rejeita a mensagem a enviar ou quando este servidor de e-mail não está disponível.
- **Definições do servidor SMTP do cliente de e-mail**- fornece informações sobre como configurar a aplicação de cliente de e-mail para que as mensagens de e-mail a enviar sejam verificadas utilizando o servidor actualmente modificado para verificar o e-mail a enviar. Trata-se de um resumo baseado nos parâmetros correspondentes especificados nesta caixa de diálogo e noutras caixas de diálogo relacionadas.
- **Activação do servidor SMTP do cliente de e-mail** - marque/desmarque esta caixa para activar/desactivar o servidor SMTP especificado acima

10.11. Protecção Residente

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



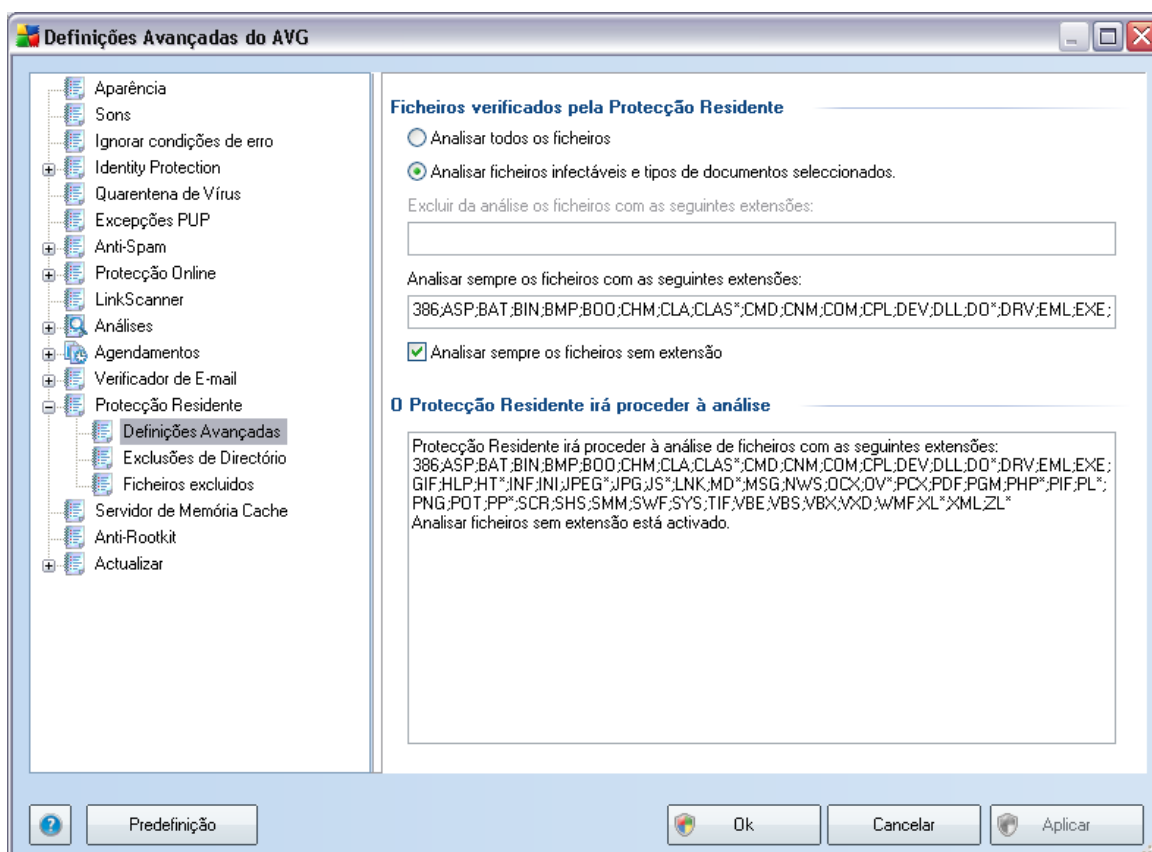
Na janela **Definições da Protecção Residente** pode activar ou desactivar a protecção **Protecção Residente** completamente ao seleccionar/desmarcar o item **Activar Protecção Residente** (esta opção está activada por predefinição). Adicionalmente, pode seleccionar quais as funcionalidades da **Protecção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

- **Analisar a Existência de Cookies de Rastreo**- 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** - se a opção anterior estiver activada, também pode marcar esta caixa 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** - 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*)
- **Recuperação Automática** - quaisquer infecções detectadas serão recuperadas automaticamente se houver uma cura disponível

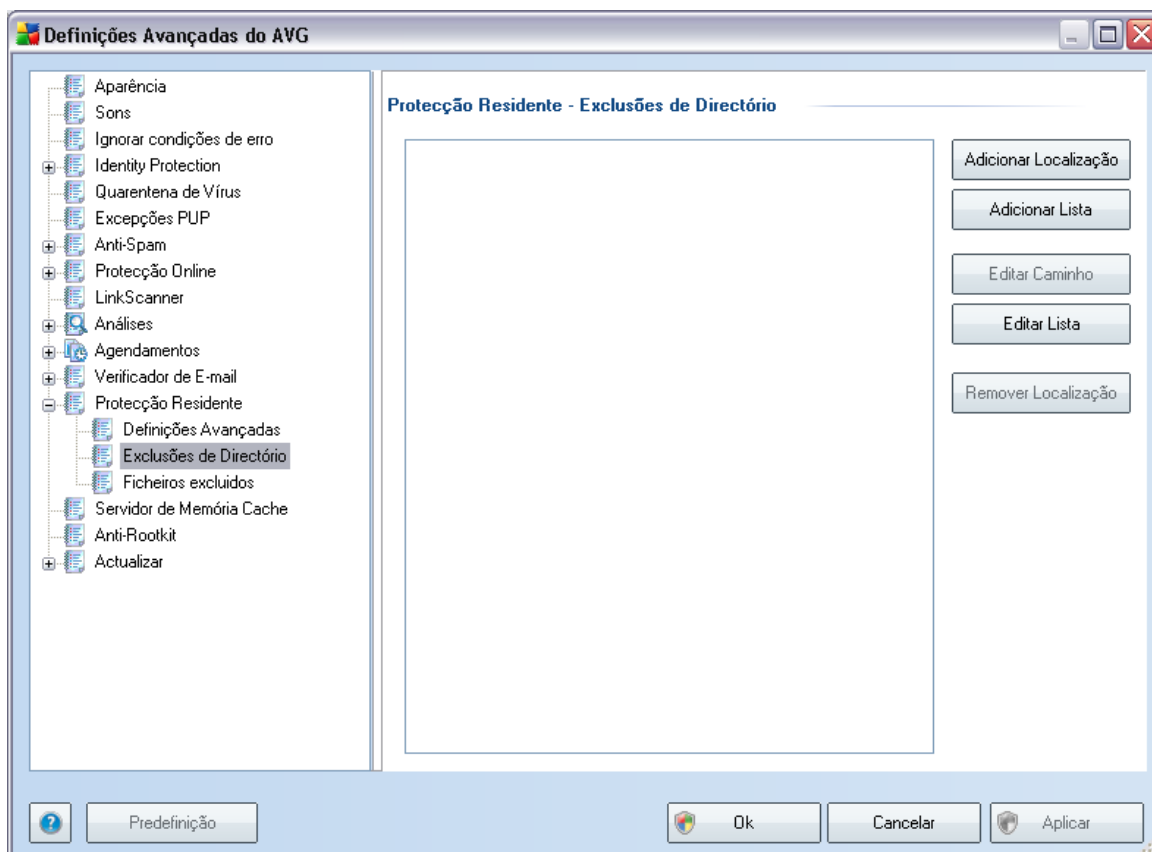
10.11.1. Definições Avançadas

Na janela **Ficheiros verificados pela Protecção Residente** é possível configurar os ficheiros a analisarem *termos de 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.

10.11.2. Exclusões de Directórios



A janela **Protecção Residente - Exclusões de Directórios** oferece a possibilidade de definir as pastas que devem ser excluídas da análise do **Protecção Residente**.

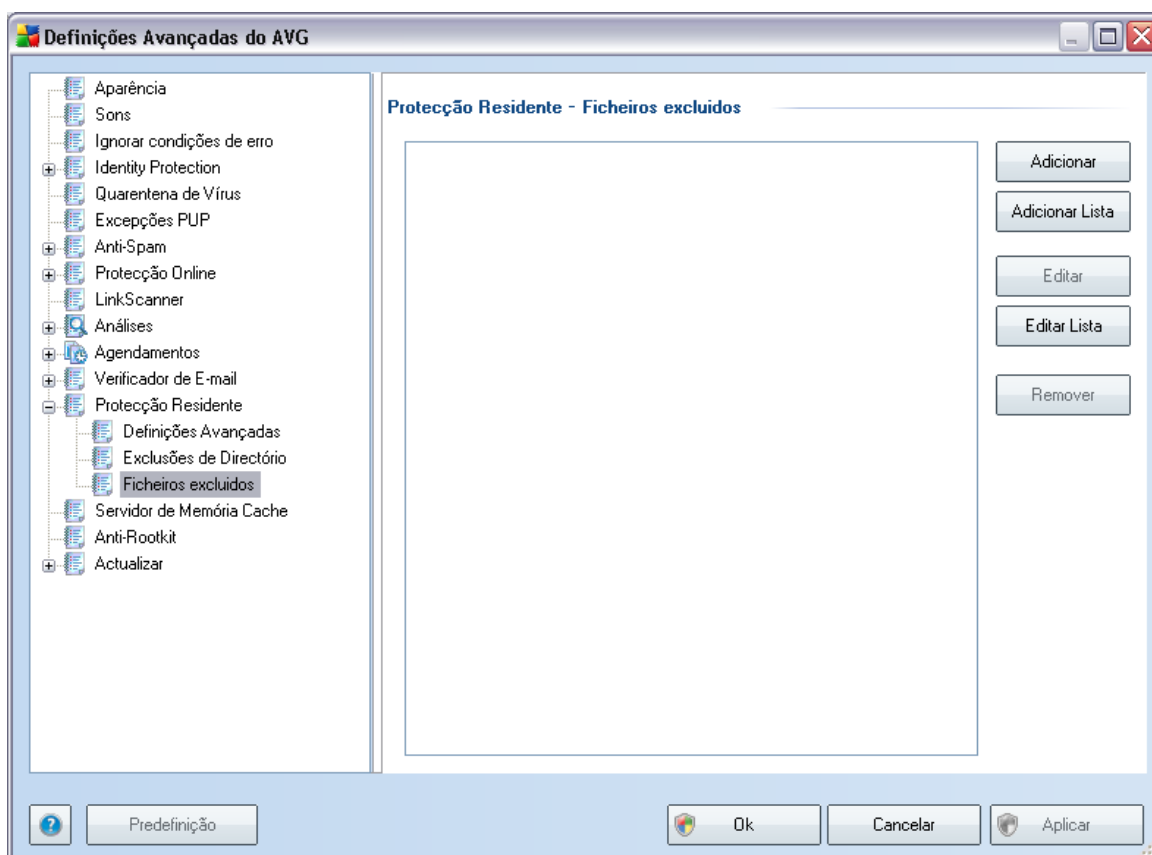
Se não for estritamente necessário, recomenda-se vivamente que não exclua directórios!

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 lista**-Adicionar lista – permite introduzir toda a lista de directórios a excluir da análise do **Protecção Residente**

- **Editar localização**- permite editar o caminho especificado para uma pasta seleccionada
- **Editar lista** - permite editar a lista de pastas
- **Remover localização**- permite eliminar o caminho para uma pasta seleccionada na lista

10.11.3. Ficheiros Excluídos



A janela **Protecção Residente - Ficheiros excluídos** é semelhante à janela **Protecção Residente - Exclusões de Directórios** mas em vez de pastas, agora pode definir ficheiros específicos que devem ser excluídos da análise da **Protecção Residente**.

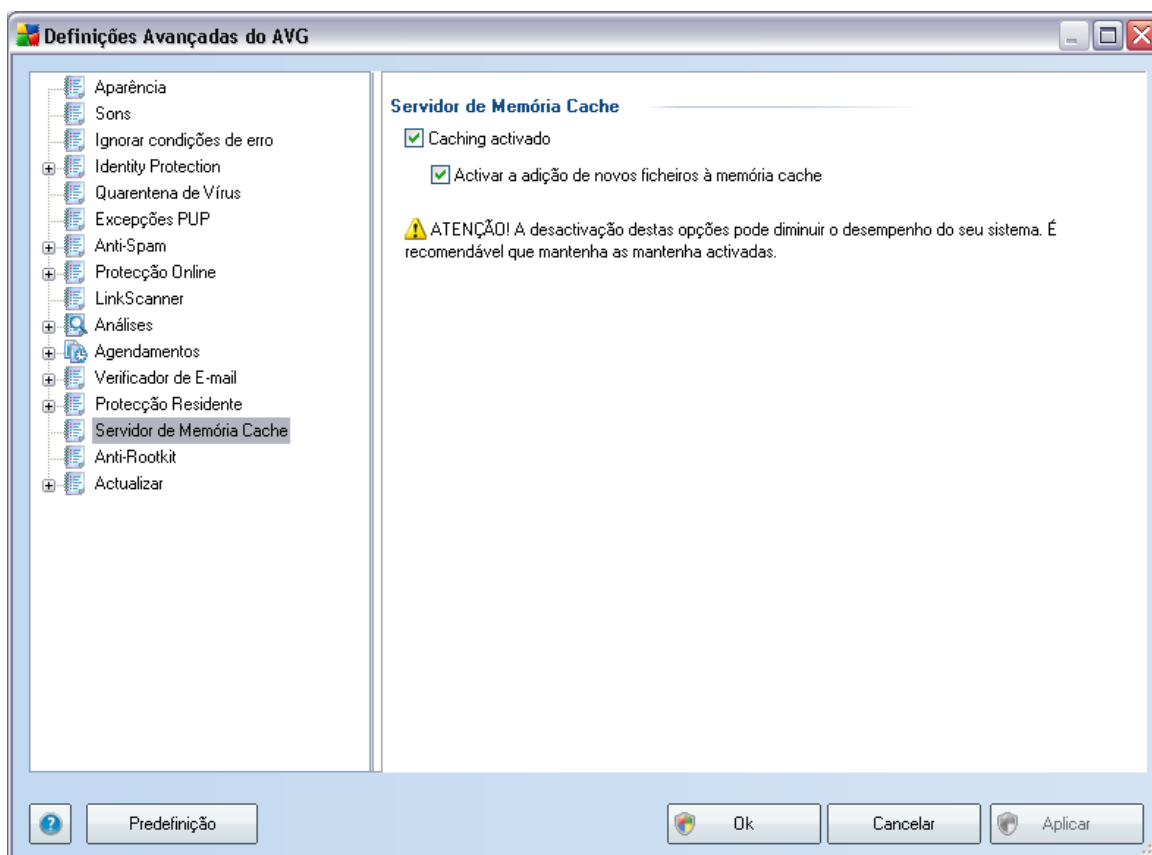
Se não for estritamente necessário, recomenda-se vivamente que não exclua quaisquer ficheiros!

A janela inclui os seguintes botões de controlo:

- **Adicionar**- especifique ficheiros a excluir da análise, seleccionando-os individualmente a partir da árvore de navegação do disco local
- **Adicionar lista** – permite-lhe introduzir toda a lista de ficheiros a excluir da análise da [Protecção Residente](#)
- **Editar**- permite-lhe editar o caminho especificado para um ficheiro seleccionado
- **Editar lista** – permite-lhe editar a lista de ficheiros
- **Remover**- permite-lhe eliminar o caminho para um ficheiro seleccionado na lista

10.12. 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.

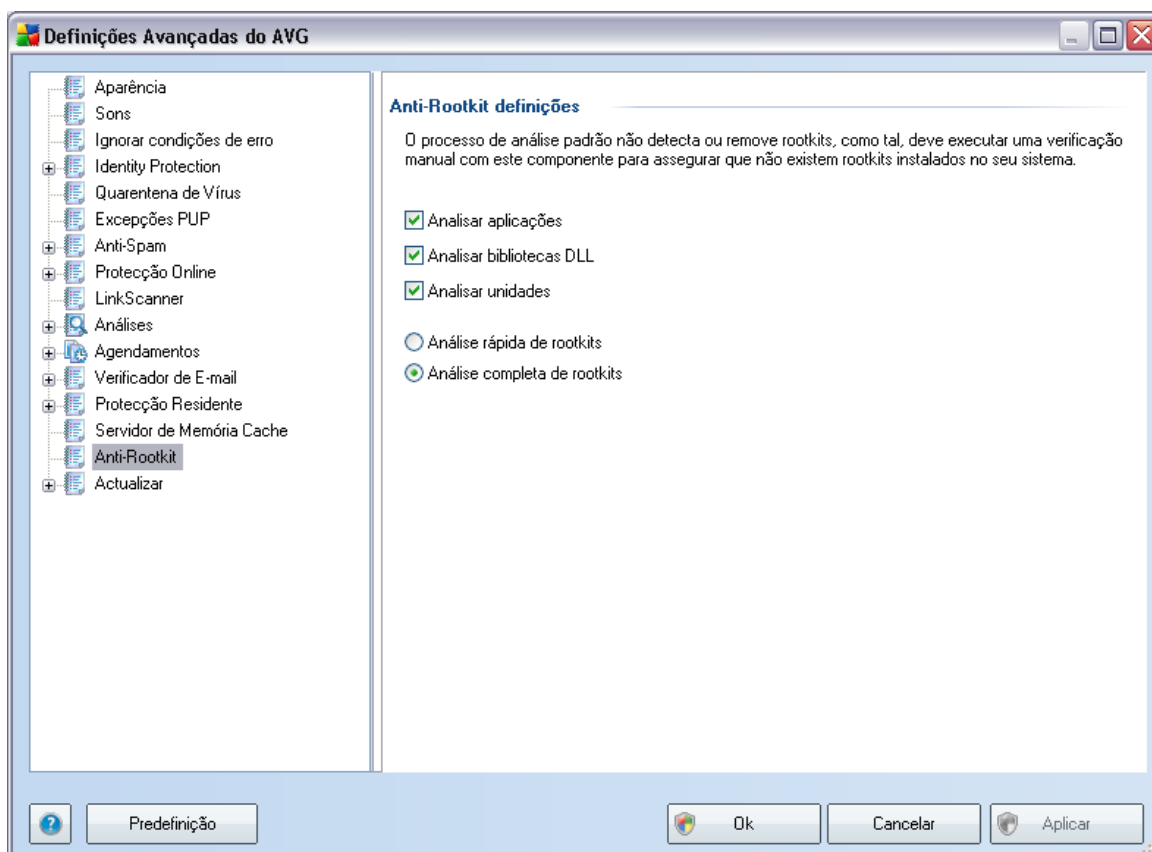


A janela de definições disponibiliza duas opções:

- **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.

10.13. 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**.

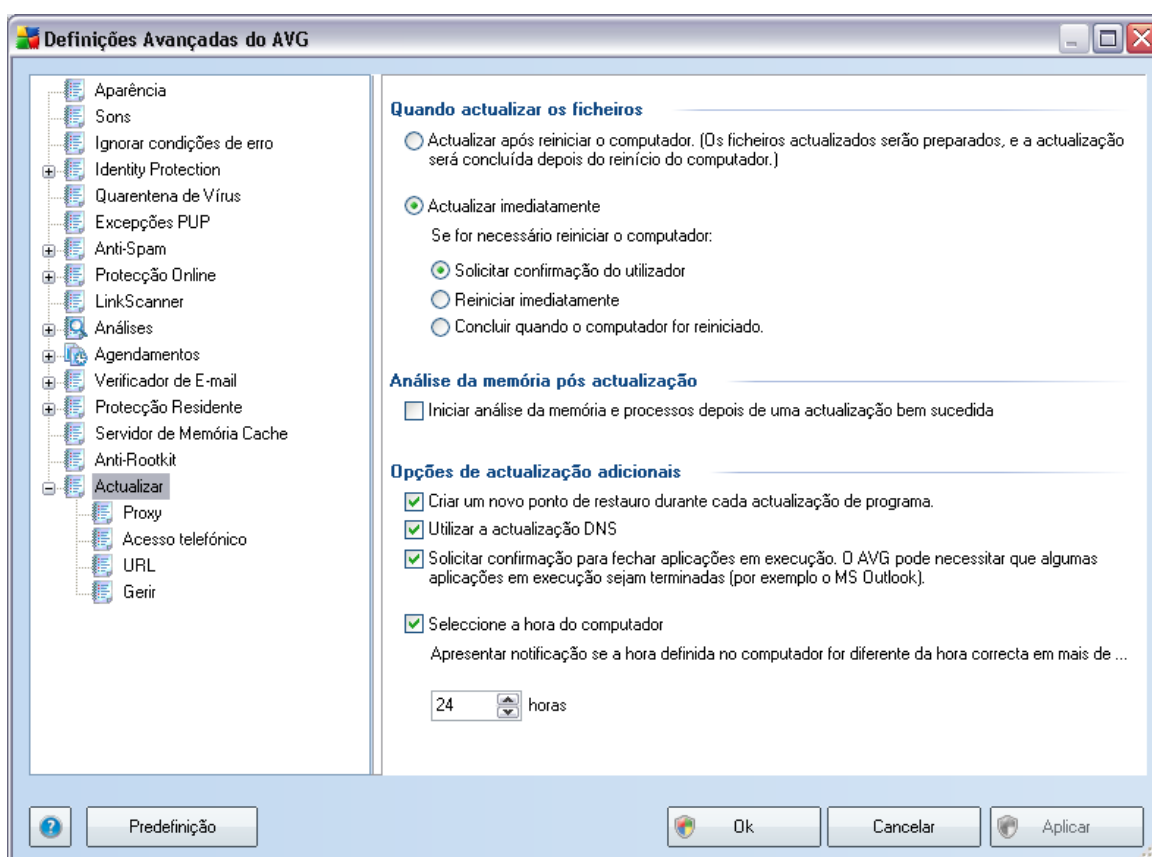
Primeiro, seleccione as caixas de verificação respectivas para especificar objectos que devem ser analisados:

- **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*)

10.14. 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 seleccionar entre duas opções alternativas: [a actualização](#) pode ser agendada para o próximo arranque do computador ou pode executar a [actualização](#) imediatamente. A opção de actualização imediata está seleccionada por predefinição uma vez que desta forma o AVG pode assegurar o nível de protecção máximo. Agendar uma actualização para o próximo arranque do PC só é recomendável se tiver a certeza que o computador é reiniciado regularmente, no mínimo diariamente.

Se decidir manter a configuração predefinida e executar o processo de actualização imediatamente, pode especificar as circunstâncias em que um possível reinício deverá ser efectuado:

- **Requerer confirmação ao utilizador** - ser-lhe-á pedido que aprove 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 finalização do [processo de actualização](#) será adiado até ao próximo arranque do computador - novamente, por favor tenha em consideração que esta opção só é recomendável se tiver a certeza que o computador é reiniciado regularmente, no mínimo diariamente

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.

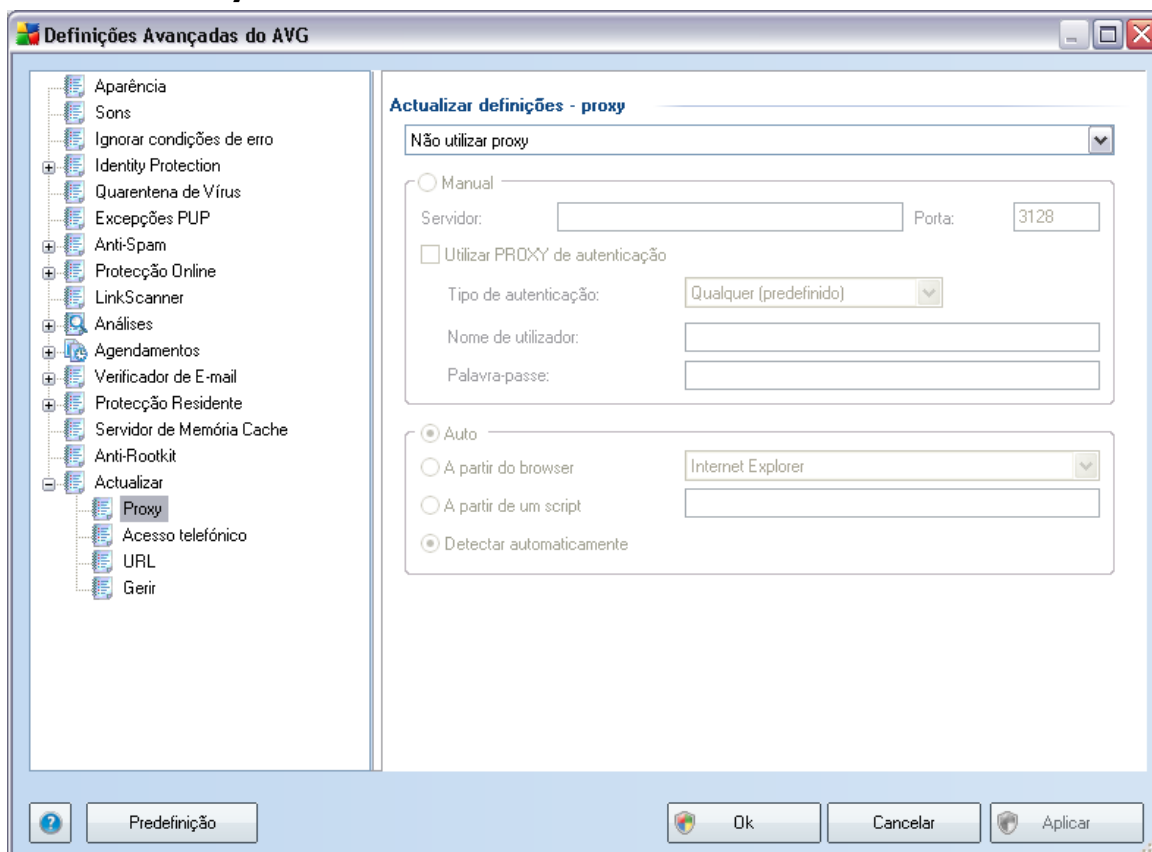
Opções de actualização adicionais

- **Criar um novo ponto de restauro do sistema após 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** - seleccione esta caixa para confirmar se

pretende utilizar o método de detecção de ficheiros de actualização que elimina a quantidade de dados transferidos entre o servidor de actualização e o cliente do AVG;

- **Requerer confirmação para fechar aplicações em execução** (activado por predefinição) estará a certificar-se de que não serão fechadas quaisquer aplicações actualmente em utilização sem a sua permissão - se necessário para que o processo de actualização seja concluído;
- **Verificar a hora do computador** - seleccione esta opção para especificar que pretende que seja apresentada uma notificação na eventualidade de a hora do computador ser diferente da hora correcta além do número de horas especificado.

10.14.1. 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.

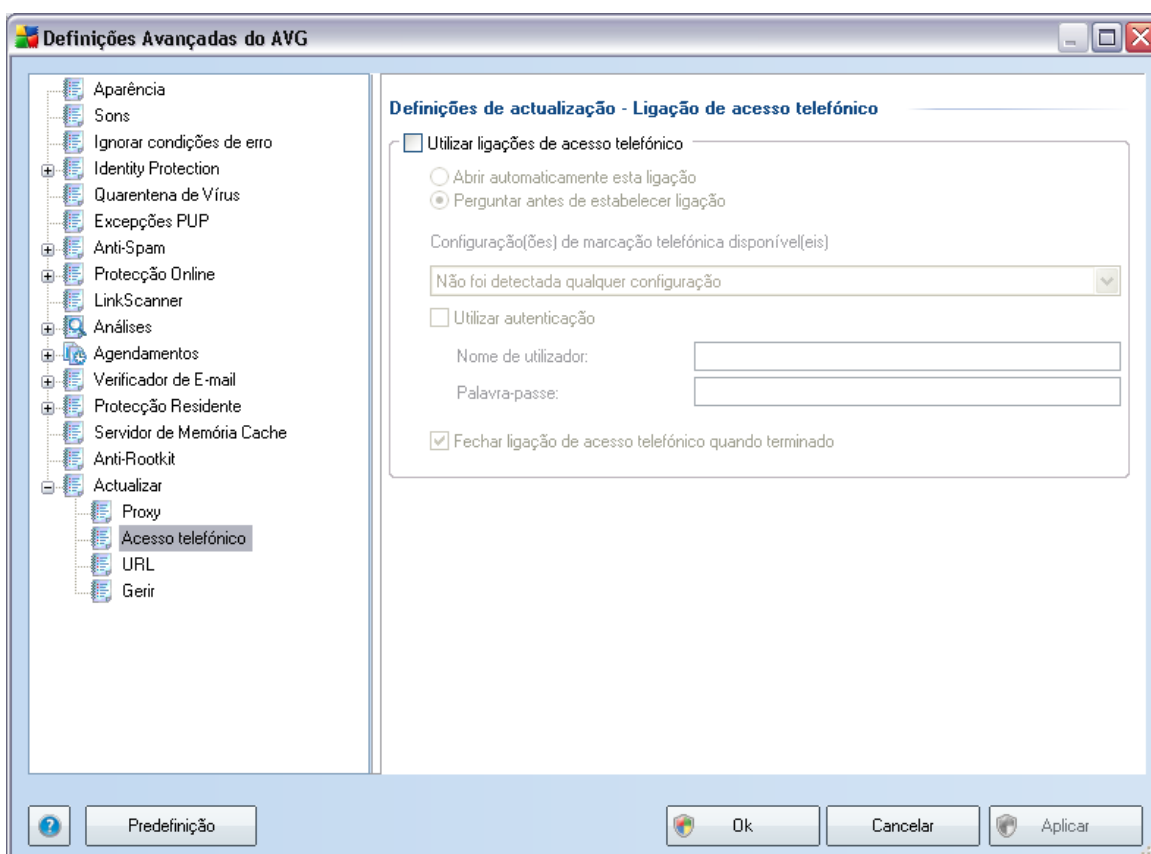
Configuração automática

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
- **Autodetecção** - a configuração será detectada automática e directamente a partir do servidor proxy

10.14.2. Acesso telefónico

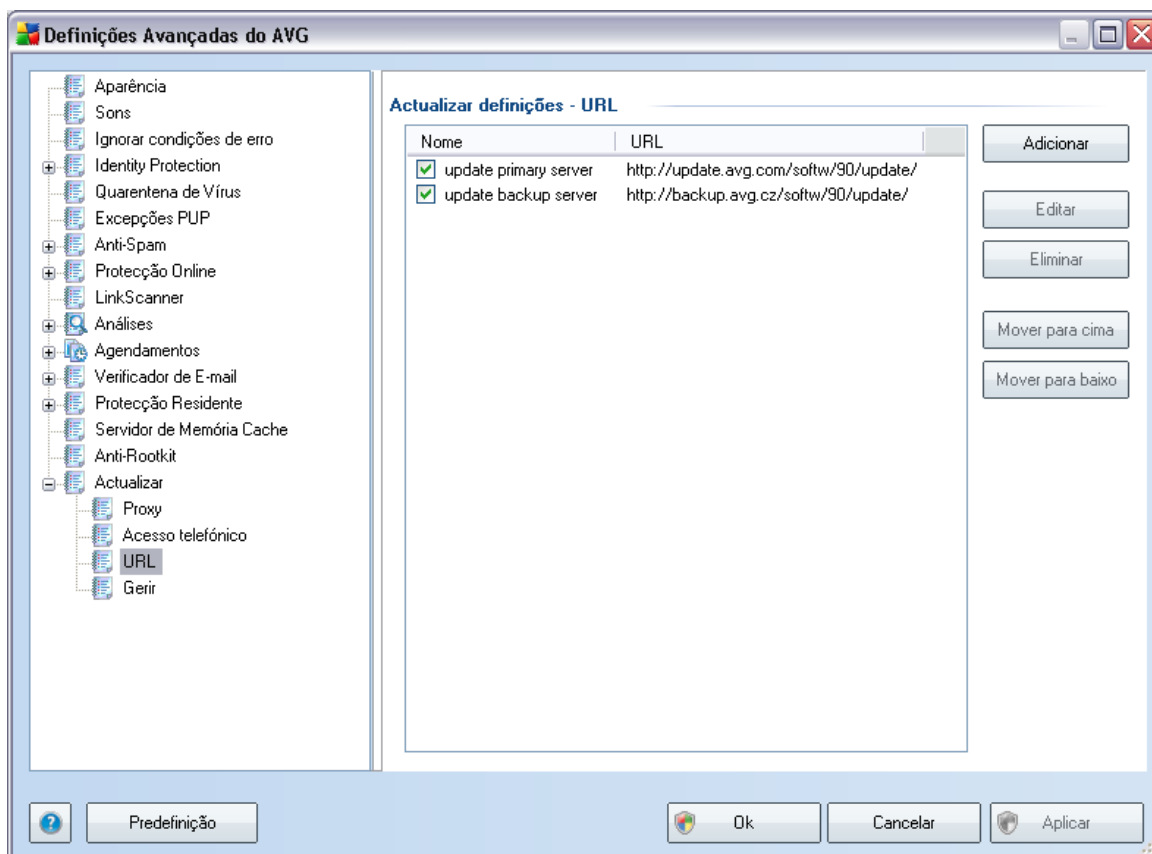


Todos os parâmetros definidos na janela **Definições de Actualização - Ligação de acesso telefónico** referem-se à ligação à Internet de Acesso telefónico. Os campos do separador estão inactivos até que seja marcada a opção **Utilizar ligações de Acesso Telefónico** que activa os campos.

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

Fechar ligação de acesso telefónico quando terminado).

10.14.3. URL



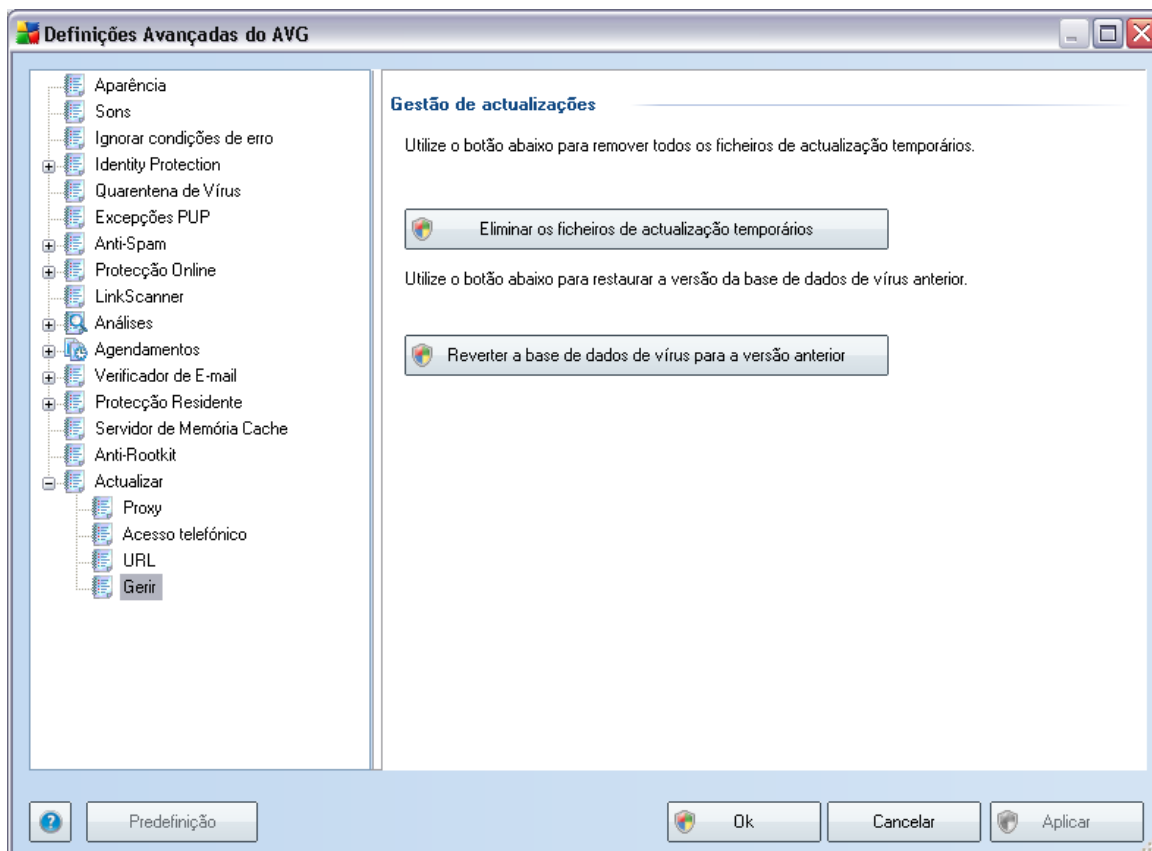
A janela **URL** apresenta uma lista de endereços da Internet a partir dos quais pode transferir os ficheiros de actualização. A lista e os respectivos itens podem ser modificados, utilizando os botões de controlos seguintes:

- **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

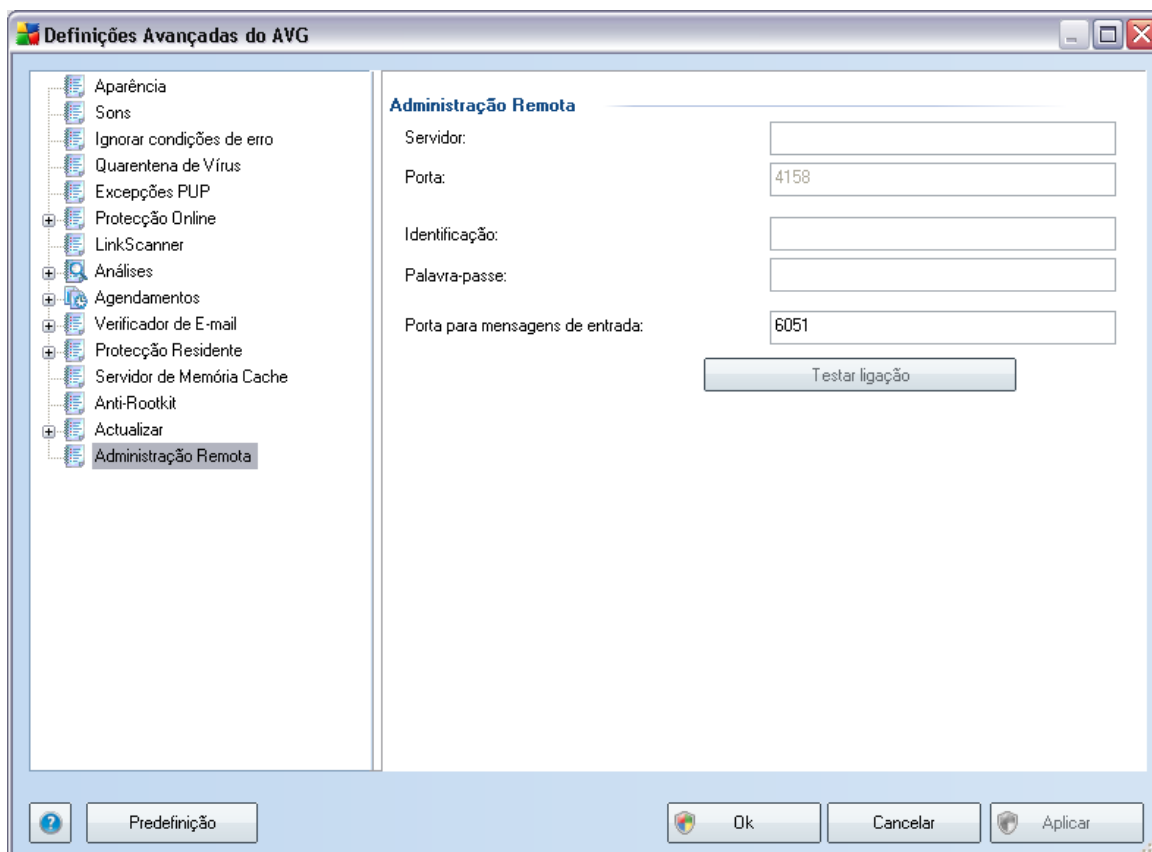
10.14.4. Gerir

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*)

10.15. Administração Remota



As definições da **Administração Remota** referem-se à ligação entre o posto cliente AVG e o sistema de administração remota. Se pretende ligar o posto respectivo à administração remota, por favor especifique os seguintes parâmetros:

- **Servidor** - nome do servidor (ou endereço IP do servidor) onde o AVG Admin Server está instalado
- **Porta** - faculte o número da porta através da qual o cliente AVG comunica com o AVG Admin Server (*o número de porta 4158 é considerado padrão - se utilizar este número de porta não tem de especificá-lo explicitamente*)
- **Início de Sessão** - se a comunicação entre o cliente AVG e o AVG Admin Server estiver definida como segura, faculte o seu nome de utilizador ...
- **Palavra-passe** - e a sua palavra-passe



- **Porta para mensagens a receber** - número da porta onde o cliente AVG aceita mensagens do AVG Admin Server

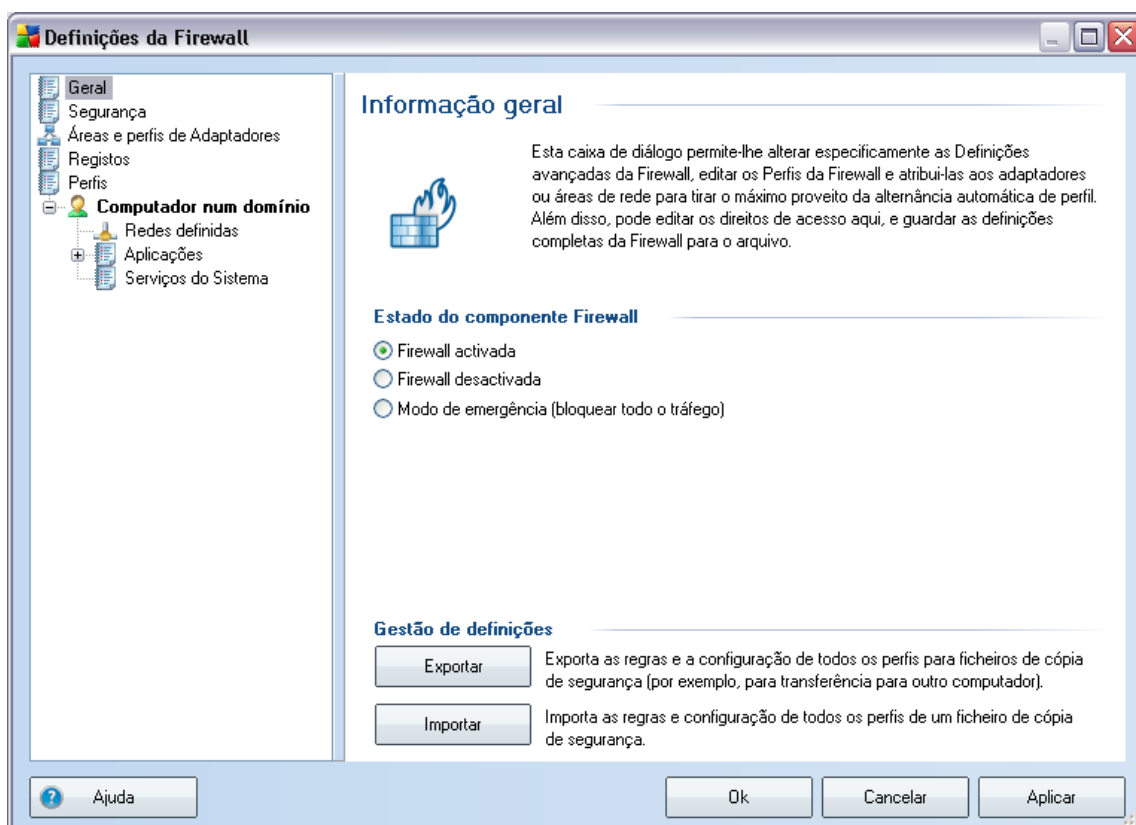
O botão **Testar ligação** ajuda-o a verificar se todos os dados especificados acima são válidos e podem ser usados para ligar com sucesso ao DataCenter.

Atenção: Para uma descrição detalhada acerca de administração remota por favor consulte a documentação do AVG Network Edition.

11. Definições da Firewall

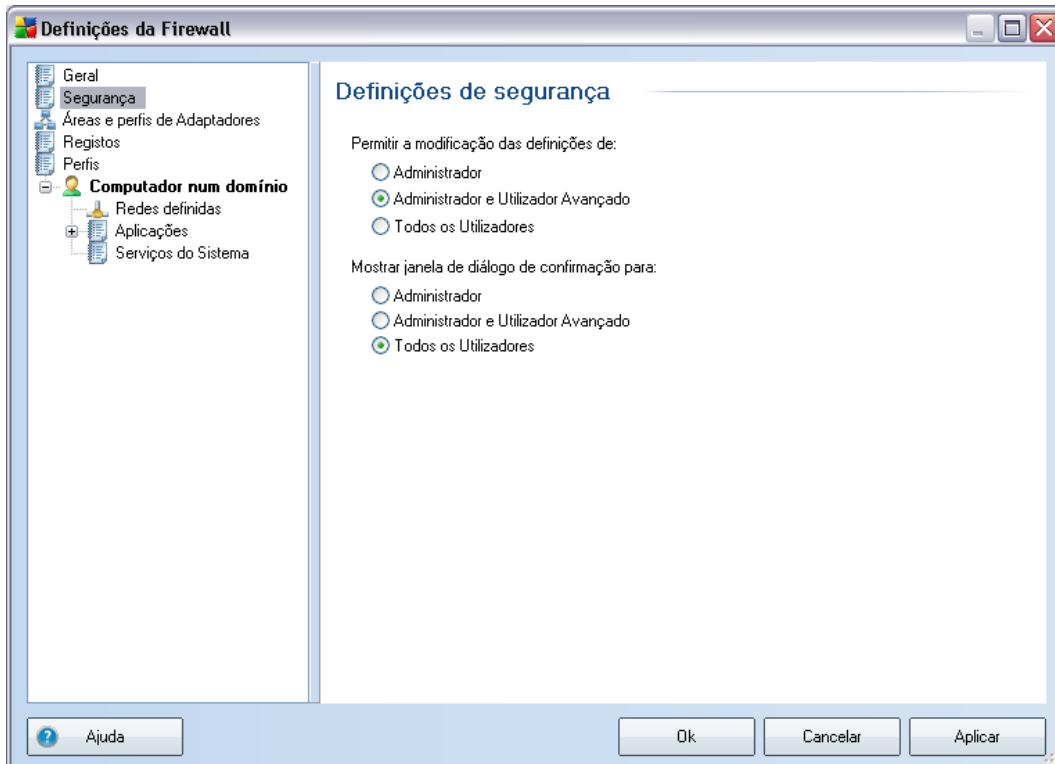
A configuração da **Firewall** abre numa nova janela onde pode configurar através de várias janelas parâmetros muito avançados do componente. **No entanto, a edição de configuração avançada é destinada apenas a utilizadores especialistas e experientes.**

11.1. Geral



Na janela **Informação geral** 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.

11.2. Segurança



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

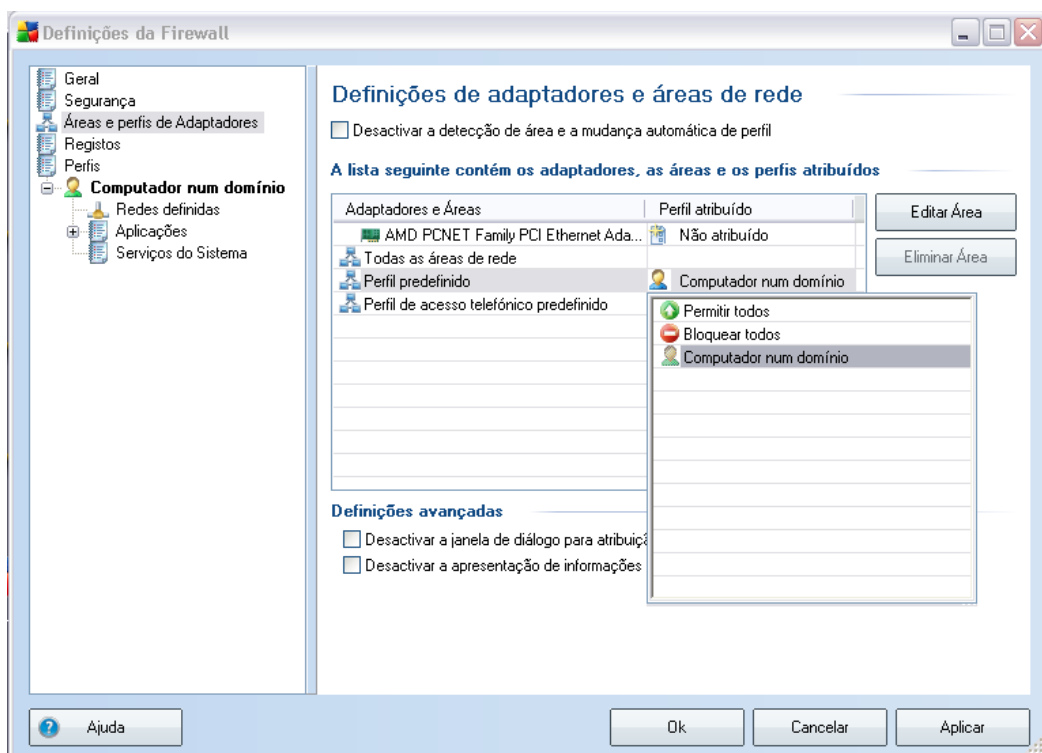
- **Permitir modificação de definições para** . especifique a quem é permitido alterar a configuração da **Firewall**
- **Apresentar janela de confirmação para**- especifique a quem a janela de confirmação (*janela a solicitar uma decisão numa situação que não está prevista por uma regra da **Firewall***)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

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

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

- o **Administrador e Utilizador Avançado** - o administrador pode incluir qualquer utilizador num determinado grupo (*Utilizador Avançado*) e definir autorizações para os membros desse grupo.
- o **Todos os Utilizadores** - outros utilizadores não associados a nenhum grupo específico

11.3. Áreas e perfis de Adaptadores



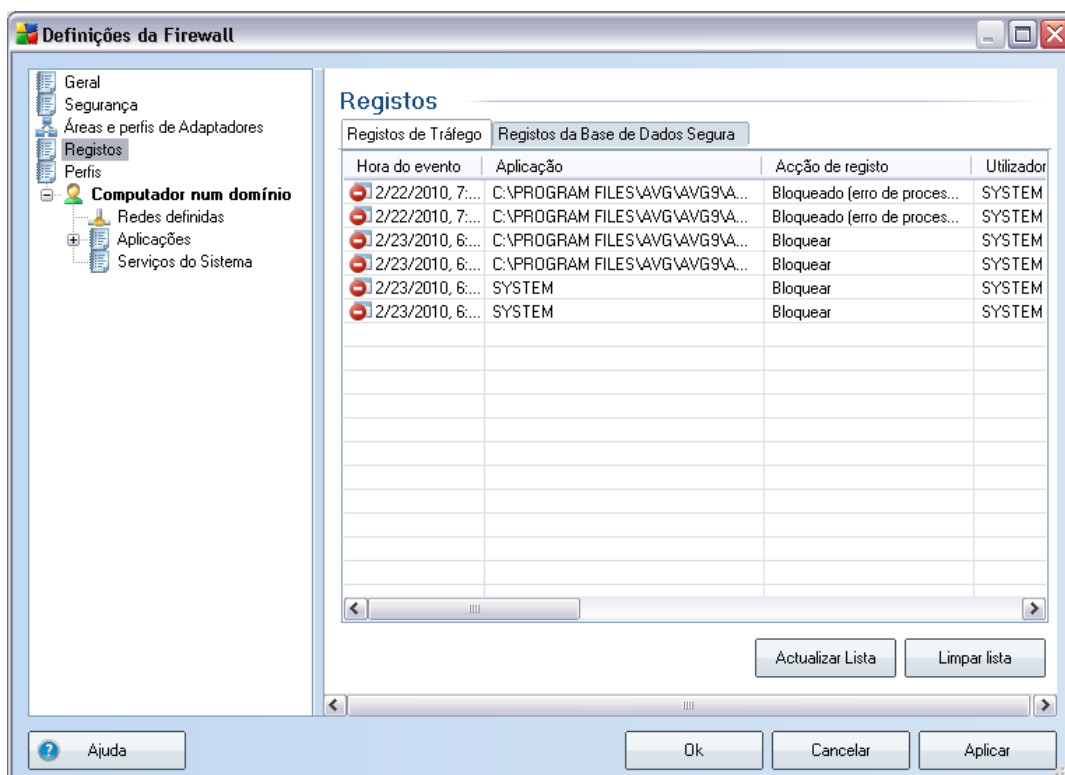
Na janela **Definições de adaptadores e áreas de rede** pode editar definições relativas a atribuição de perfis definidos a adaptadores específicos e redes referentes e respectivas:

- **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 baseado nas suas selecções de [utilização do computador](#) e [concepção de utilização da Internet do computador](#) durante o **Processo de Instalação**. 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** - seleccionar a opção respectiva desactivará a funcionalidade de apresentação de uma mensagem de informação.

11.4. 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 dois separadores:

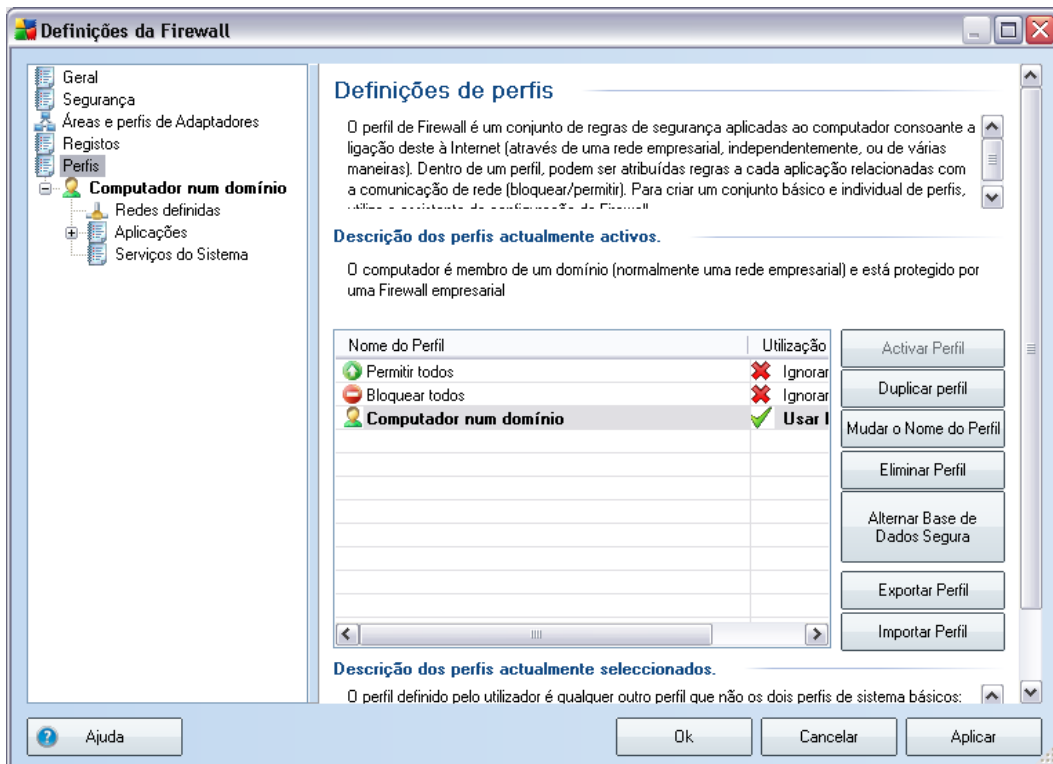
- **Registos de Tráfego** - providencia informações sobre a actividade de todas as aplicações que tentaram ligar à rede.
- **Registos da Base de Dados Segura** - A *Base de Dados Segura* é uma base de dados interna do AVG que recolhe informações sobre aplicações certificadas e seguras que podem ter sempre 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.

Botões de controlo

- **Ajuda** - abre a janela do ficheiro de ajuda relacionado.
- **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.

11.5. 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** - pode seleccionar para o perfil seleccionado 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
- **Ajuda** - abre a janela do ficheiro de ajuda relacionado

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*):

11.5.1. Informação do perfil



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

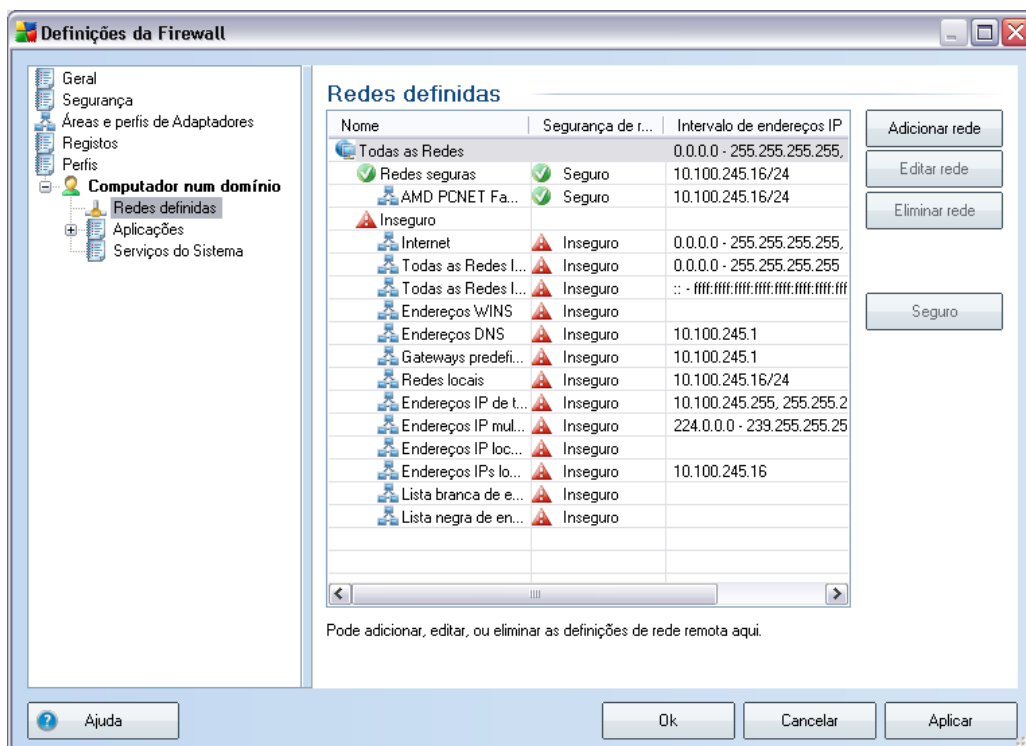
- **Usar a Base de Dados Segura para este perfil** - (activado por predefinição) marque esta opção para activar a *Base de Dados Segura* (ou seja, a base de dados interna do AVG que recolhe informações sobre aplicações certificadas e seguras que comunicam on-line. Se ainda não houver nenhuma regra especificada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

Definições de modo de jogo

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

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

11.5.2. Redes definidas



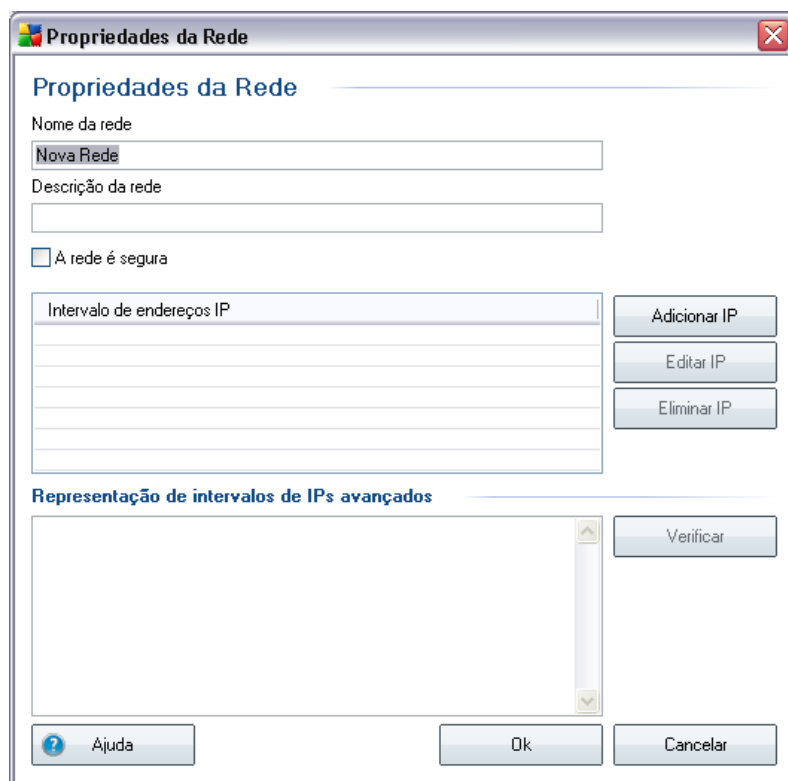
A janela **Redes definidas** faculta uma lista de todas as redes às quais o seu computador está conectado. É fornecida a seguinte informação sobre cada rede

detectada:

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

Botões de controlo

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



Nesta janela, pode especificar o **Nome da rede**, facultar a **Descrição da rede** e possivelmente atribuir a rede como segura. A nova rede pode ser definida manualmente numa janela independente aberta via o botão **Adicionar IP** (alternativamente **Editar IP**/**Eliminar IP**, nesta janela pode especificar a rede ao facultar o Intervalo ou máscara de IP.

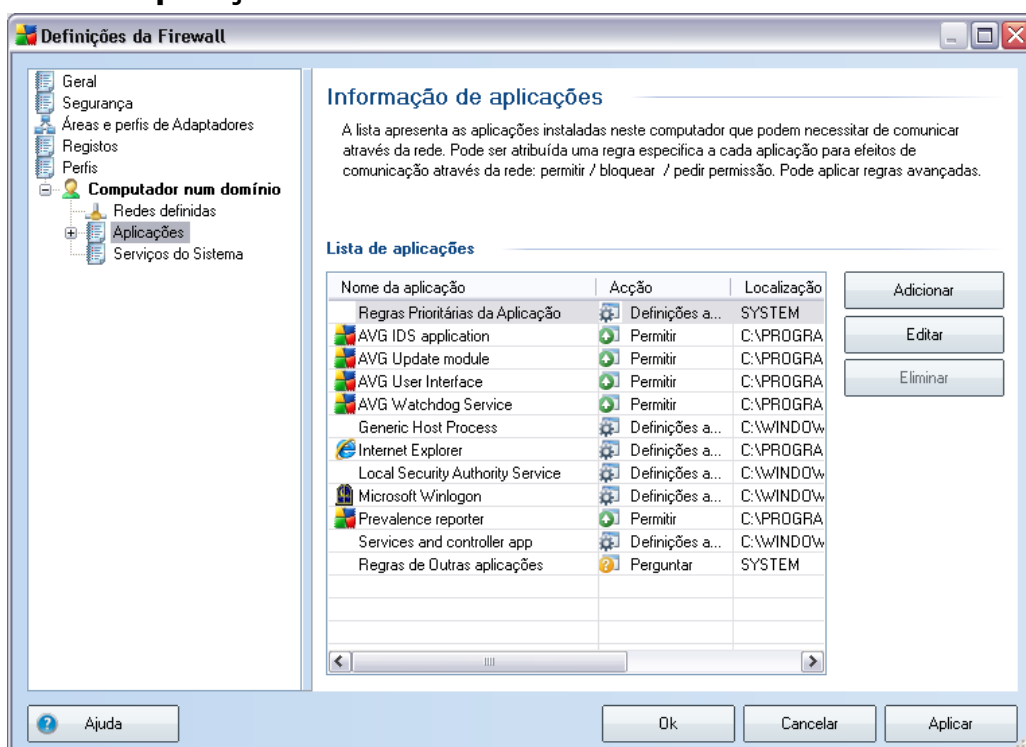
Para um número de redes mais amplo que devem ser definidas como parte da rede recentemente criada, pode usar a opção da **Representação avançada de Intervalo de IPs**: introduza a lista de todas as redes no campo de texto respectivo (*qualquer formato standard é suportado*) e clique no botão **Verificar** para se certificar de que o formato pode ser reconhecido. Depois clique em **OK** para confirmar e guardar os dados.

- **Editar rede**- abre a janela **Propriedades de rede** (veja acima) onde pode editar parâmetros de uma rede já definida (a janela é idêntica à janela para adicionar uma nova rede, consulte a descrição no parágrafo anterior)
- **Eliminar rede** - remove o visto de uma rede seleccionada da lista de redes
- **Marcar como segura** - por predefinição, todas as redes são consideradas não

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

- **Ajuda** - abre a janela do ficheiro de ajuda relacionado

11.5.3. Aplicações



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

-  Permitir comunicação para todas as redes
-  Permitir comunicação somente para redes definidas como Seguras
-  Bloquear comunicação
-  Apresentar janela de solicitação (o utilizador poderá decidir no momento se pretende permitir ou bloquear a comunicação)

-  Definições avançadas definidas

As aplicações na lista foram detectadas no seu computador (e atribuídas acções respectivas) durante a procura do [Assistente de Configuração da Firewall](#), ou, caso seja uma aplicação desconhecida ou nova, posteriormente.

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

Obviamente, também pode definir regras para a nova aplicação imediatamente - nesta janela, clique em **Adicionar** e preencha os detalhes da aplicação.

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

- **Regras Prioritárias da Aplicação** (no topo da lista) são preferenciais e são sempre aplicadas antes das regras de qualquer aplicação individual.
- **Outras Regras da Aplicação** (no fundo da lista) são usadas como "último recurso", quando nenhuma regra da aplicação seja aplicável, ex. para uma aplicação desconhecida e indefinida.

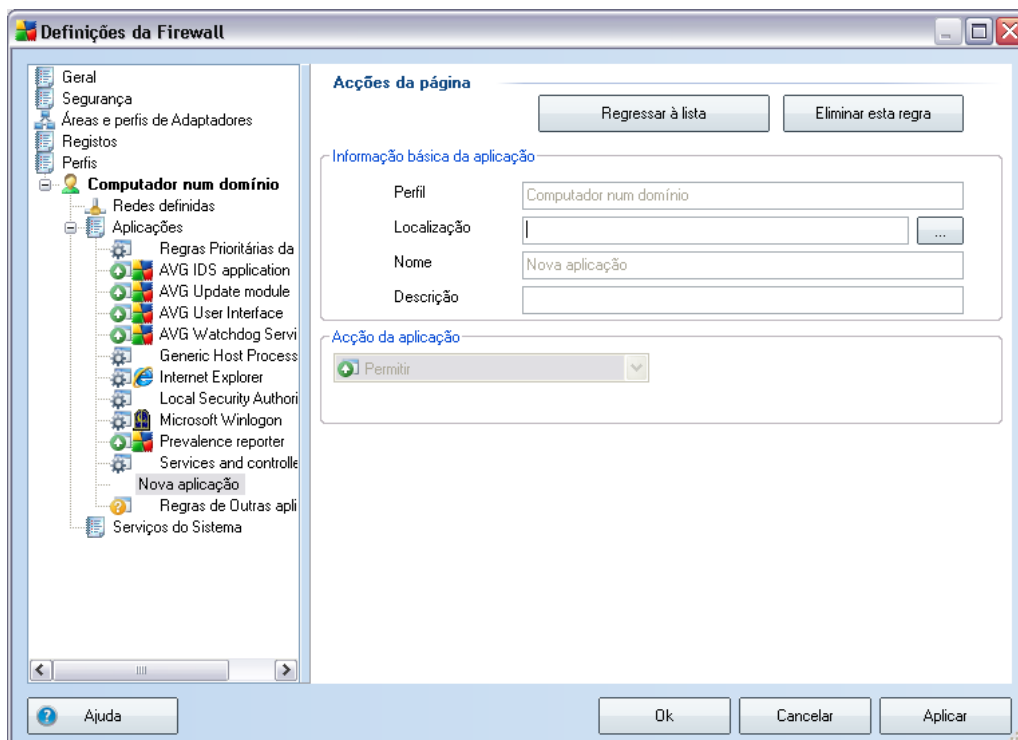
Estes itens têm opções de configuração diferentes das aplicações comuns, e são destinadas exclusivamente a utilizadores experientes. Recomendamos vivamente que não modifique estas definições

Botões de controlo

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

- **Adicionar** - abre uma janela de [Acções da Página](#) em branco para definição de novas regras de aplicações
- **Editar** - abre a mesma janela de [Acções da Página](#) com dados disponibilizados para edição de um conjunto de regras de aplicações existente
- **Eliminar** - remove a aplicação seleccionada da lista

- **Ajuda** - abre a janela do ficheiro de ajuda relacionado



Nesta janela pode configurar detalhadamente definições para a respectiva aplicação.

Acções da página

- O botão **Regressar à lista** apresenta a síntese de todas as regras de aplicação definidas.
- O botão **Eliminar esta regra** eliminará a regra de aplicação actualmente apresentada. Tenha em atenção que esta acção não pode ser desfeita!

Informação básica da aplicação

Nesta secção, preencha o **Nome** da aplicação, e opcionalmente uma **Descrição** (um breve comentário para sua informação). No campo **Caminho**, introduza a localização

completa para a aplicação (*o ficheiro executável*) no disco; alternativamente, pode localizar a aplicação convenientemente na estrutura em árvore depois de clicar no botão "...".

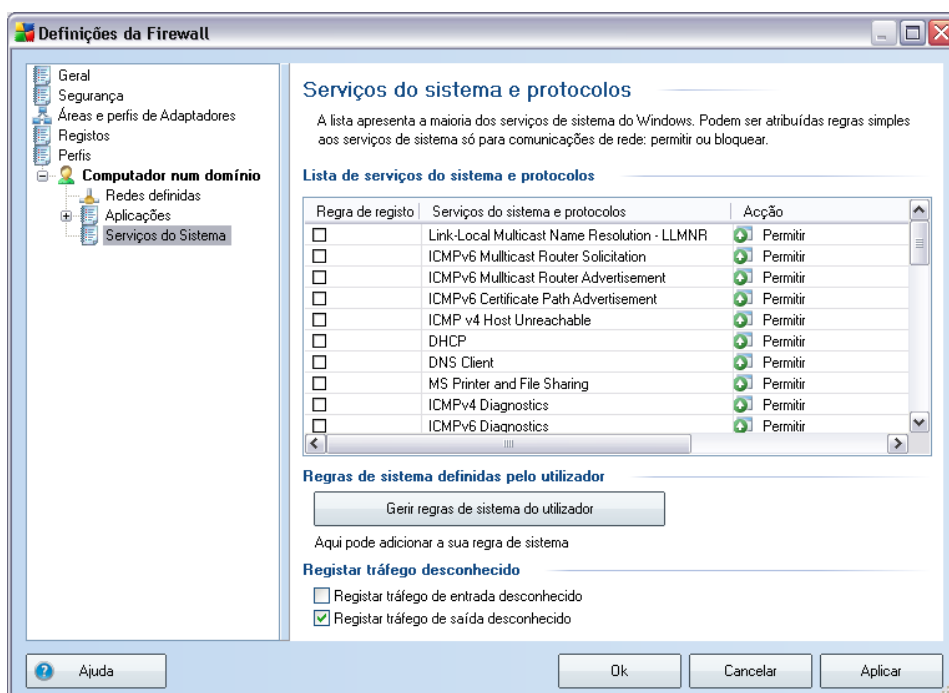
Acção da aplicação

No menu de opções, pode seleccionar a regra da Firewall para a aplicação, ou seja, o que a Firewall deve fazer quando a aplicação tenta comunicar através da rede:

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

11.5.4. Serviços do Sistema

Qualquer edição na janela *Serviços de sistema e protocolos*, é recomendável APENAS para utilizadores experientes!



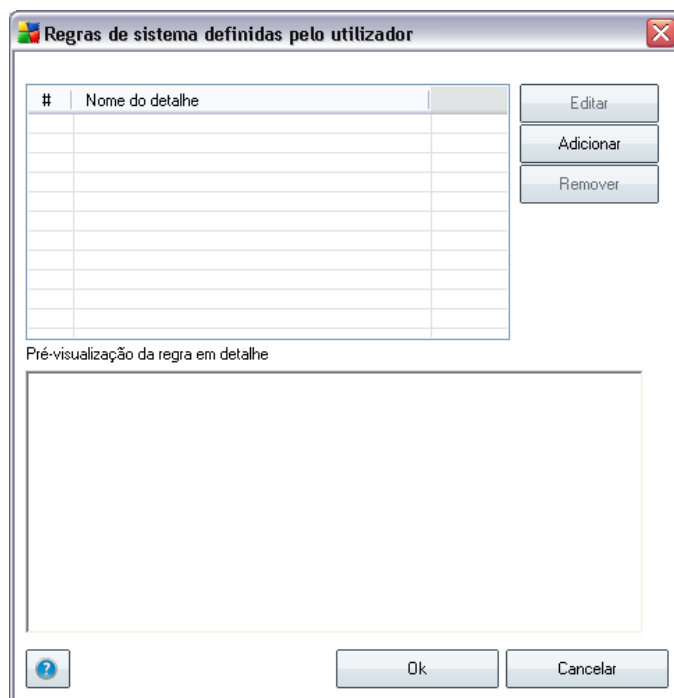
A janela ***Serviços de sistema e protocolos*** lista os serviços de sistema e protocolos padrão do Windows que possam precisar de comunicar através da rede. A tabela é composta por duas colunas:

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

- **Redes** - esta coluna detalha em que rede específica a regra de sistema é aplicável.

A lista (*incluindo acções atribuídos*) pode ser editada por meio dos seguintes botões:

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



Aviso: Tenha em atenção que as definições de detalhes de regras são avançadas, destinadas principalmente a administradores de redes que precisam de ter controlo absoluto sobre a configuração da Firewall. Se não estiver familiarizado com tipo de

protocolos de comunicação, números de portas de rede, definições de endereços IP, etc., é favor não modificar estas definições! Se precisar realmente de alterar a configuração, consulte por favor os ficheiros de ajuda da janela respectiva para informações específicas.

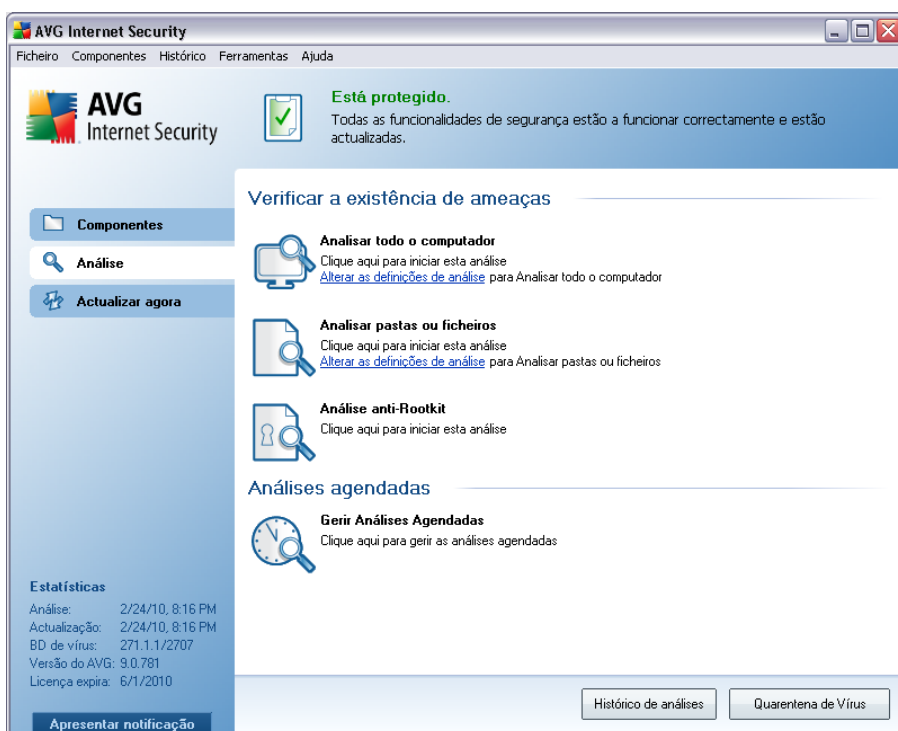
Registar tráfego desconhecido

- **Registar tráfego de entrada desconhecido** – seleccione a caixa para registar nos Registos cada tentativa de ligação desconhecida do exterior para o seu computador.
- **Registar tráfego de saída desconhecido** – seleccione a caixa para registar nos Registos cada tentativa de ligação desconhecida do seu computador para uma localização externa.

12. Análise do AVG

A análise é uma parte crucial do funcionamento do **AVG 9 Anti-Virus plus Firewall**. Pode executar testes a pedido ou [agendá-los para serem executados periodicamente](#) em alturas convenientes.

12.1. Interface de Análise



A interface de análise do AVG é acessível via **Análise do Computador** [link rápido](#). 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 [Analisar 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

12.2. Análises Predefinidas

Uma das principais funcionalidades do **AVG 9 Anti-Virus plus Firewall** 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.

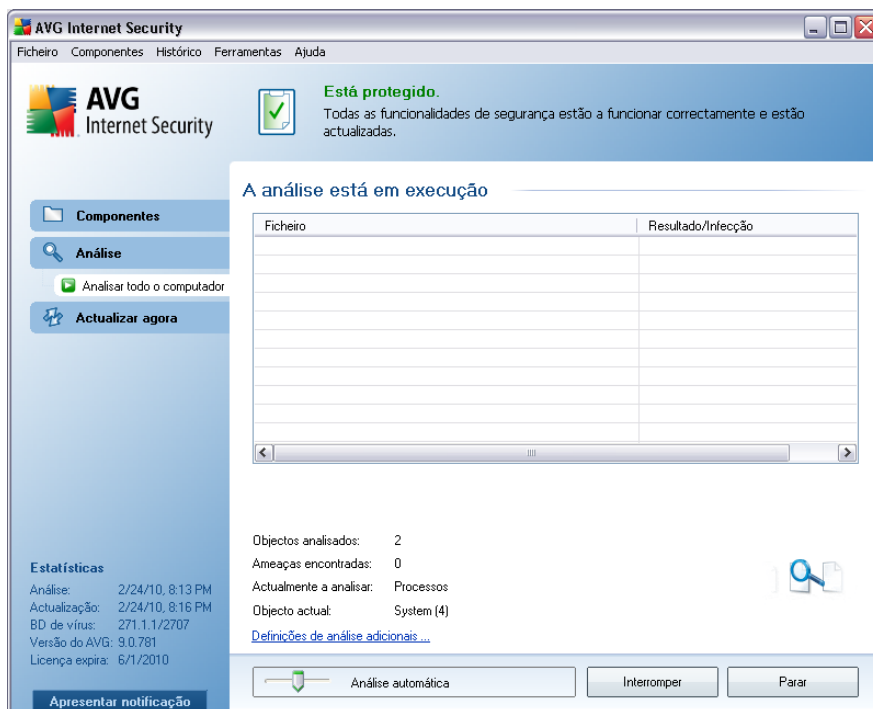
No **AVG 9 Anti-Virus plus Firewall** encontrará dois tipos de análises predefinidas pelo fornecedor do software:

12.2.1. Analisar todo o computador

Analisar 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.

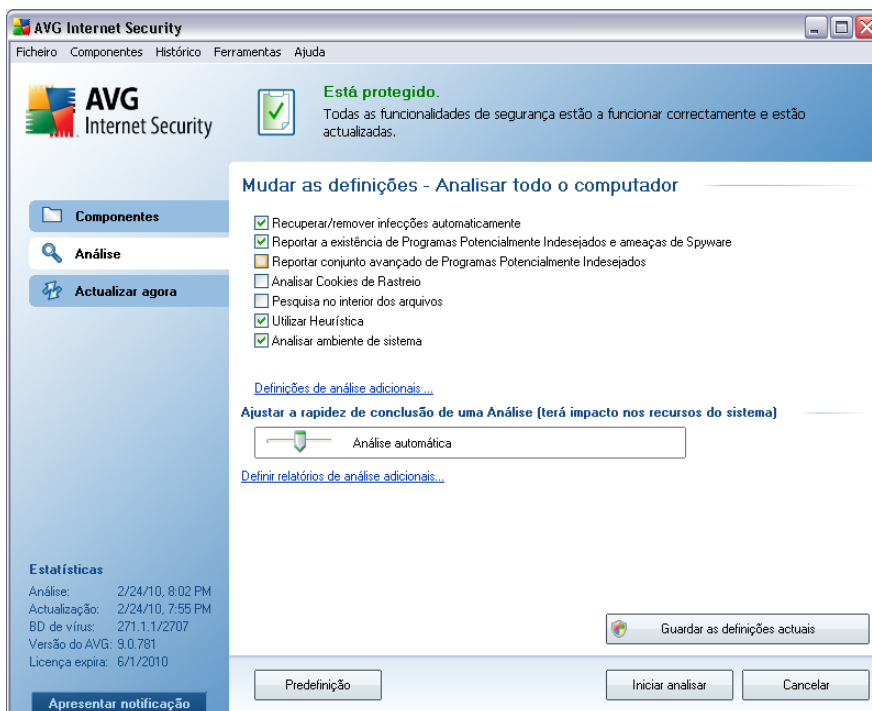
Início de análise

A **Análise de todo o computador** pode ser iniciada directamente a partir da [interface de análise](#) clicando no ícone 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 (**Suspender**) ou cancelada (**Cancelar**) se necessário.

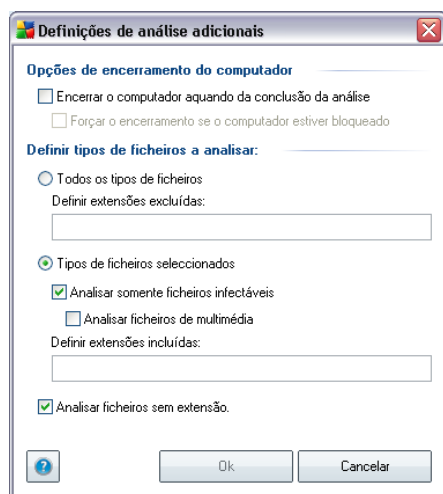


Edição da configuração de análise

Tem a opção de editar as definições padrão predefinidas da análise **Analisar todo o computador**. Clique no link **Alterar definições de análise** para ir para a janela **Alterar definições de análise para a Análise de todo o computador**. **É recomendável que mantenha das definições padrão a menos que tenha uma razão válida para as alterar!**



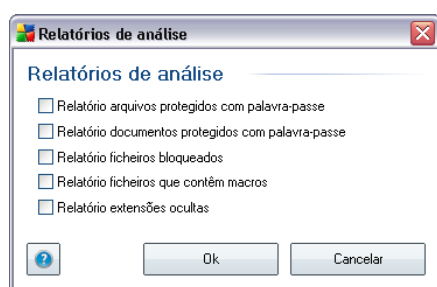
- **Parâmetros de análise** - na lista de parâmetros de análise pode activar/desactivar parâmetros específicos consoante necessário. A maioria dos parâmetros estão activados por predefinição e serão utilizados automaticamente durante a análise.
- **Definições de verificação adicionais** - a ligação abre 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. Por predefinição, a prioridade está definida para um nível médio (*Análise automática*) que optimiza a velocidade do processo de análise e a utilização dos recursos do sistema. Alternativamente, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (ex. *quando o computador não está a ser utilizado*).
- **Definir relatórios de análise adicionais** - a ligação abre uma nova janela de **Relatórios de Análise** onde pode seleccionar que tipos de possíveis detecções deverão ser reportadas:



Aviso: Estas definições de análise são idênticas aos parâmetros de uma análise nova - conforme descrito no capítulo [Análise do AVG / Agendamento de análises / Como Analisar](#). Na eventualidade de decidir alterar a configuração padrão da análise **Analisar todo o computador** pode guardar as suas novas definições como a definição padrão a ser utilizada para todas as análises de todo o computador.

12.2.2. Analisar pastas ou ficheiros específicos

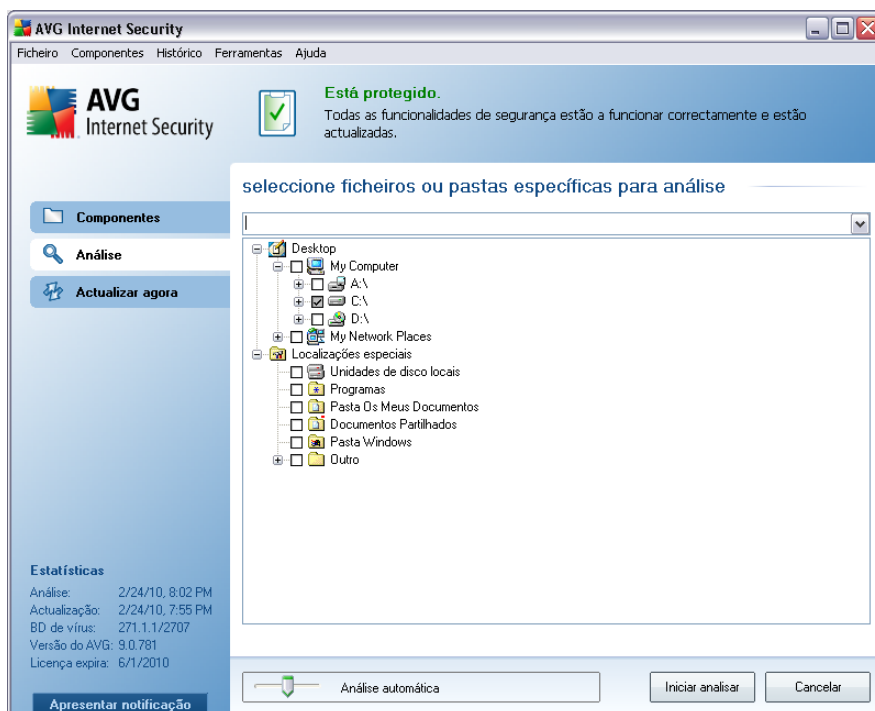
Analisar pastas ou ficheiros específicos - analisa apenas as áreas do seu computador que tiver seleccionado para o efeito (*pastas seleccionadas, discos rígidos, unidades de disquetes, CDs, etc.*). O progresso da análise na eventualidade da detecção de vírus e o seu tratamento é o mesmo que o da análise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

Início de análise

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

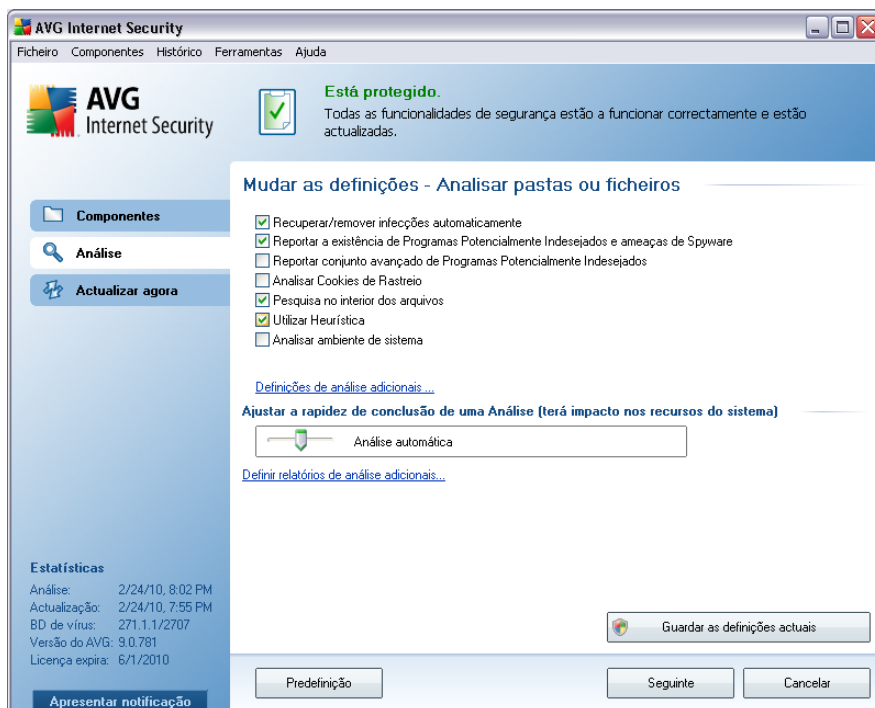
Também existe a possibilidade de analisar uma pasta específica excluindo todas as sub-pastas desta da análise; para isso deverá escrever um sinal de menos "-" à frente do caminho gerado automaticamente (veja a captura de ecrã). Para excluir toda a pasta da análise utilize o "!" parâmetro.

Finalmente, para iniciar a análise, clique no botão **Iniciar análise**; o processo de análise em si é idêntico ao da análise [análise de todo o computador](#).

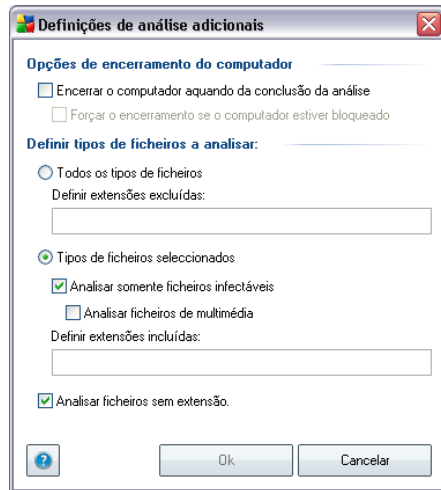


Edição da configuração de análise

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!**



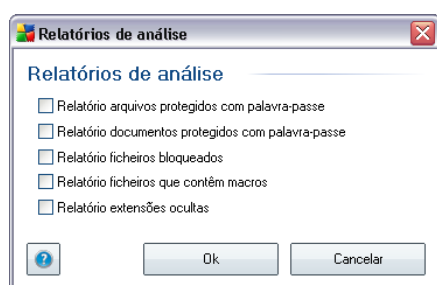
- **Parâmetros de análise** - na lista de parâmetros de análise pode activar/desactivar parâmetros específicos consoante necessário (*para descrições detalhadas destas definições por favor consulte o capítulo [Definições Avançadas do AVG / Análises / Analisar Pastas ou Ficheiros](#)*).
- **Definições de verificação adicionais** - a ligação abre uma nova janela de Definições de análise 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.

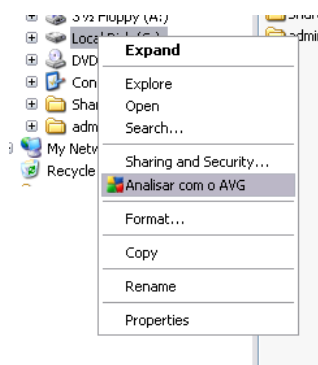
- **Prioridade do processo de análise** - pode usar o cursor para alterar a prioridade do processo de análise. Por predefinição, a prioridade está definida para um nível médio (*Análise automática*) que optimiza a velocidade do processo de análise e a utilização dos recursos do sistema. Alternativamente, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (ex. *quando o computador não está a ser utilizado*).
- **Definir relatórios de análise adicionais** - o link abre uma nova janela de **Relatórios de Análise** onde pode seleccionar que tipos de possíveis detecções deverão ser reportadas:



Aviso: Estas definições de análise são idênticas aos parâmetros de uma análise nova - conforme descrito no capítulo [Análise do AVG / Agendamento de análises / Como Analisar](#). Na eventualidade de decidir alterar a configuração padrão da análise **Analisar pastas ou ficheiros específicos** pode guardar as suas novas definições como a definição padrão a ser utilizada para todas as análises de ficheiros e pastas específicos. Além disso, esta configuração será utilizada como modelo para todos os novos agendamentos de análise ([todas as análises personalizadas são baseadas na configuração actual da análise Analisar ficheiros e pastas específicos](#)).

12.3. A analisar no Explorador do Windows

Para além das análises predefinidas executadas para todo o computador ou as suas áreas seleccionadas, o **AVG 9 Anti-Virus plus Firewall** 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 selecione o ficheiro (ou pasta) que pretende verificar
- Clique com o botão direito do rato sobre o objecto para abrir o menu de contexto
- Selecione a opção **Analisar com o AVG** para proceder à análise do ficheiro com o AVG

12.4. Análise da Linha de Comandos

No **AVG 9 Anti-Virus plus Firewall** existe ainda a opção de executar a análise a partir da linha de comandos. Pode utilizar esta opção em servidores por exemplo, ou ao criar um batch script a ser executado automaticamente após o arranque do computador. Pode iniciar a análise a partir da linha de comandos com várias parâmetros, como na interface gráfica do utilizador do AVG.

Para iniciar a análise do AVG a partir da linha de comandos, execute o seguinte comando na pasta em que o AVG está instalado:

- **avgscanx** para SO de 32 bits
- **avgscana** para SO de 64 bits

Sintaxe do comando

A sintaxe do comando é a seguinte:

- **avgscanx /parâmetro ...** ex. **avgscanx /comp** para analisar todo o computador

- **avgscanx /parâmetro /parâmetro** .. com vários parâmetros, estes deverão estar alinhados numa linha e separados por espaço e o símbolo "barra"
- se um parâmetro requerer que seja facultado um valor específico (ex. o parâmetro **/scan** que requer informação acerca das áreas seleccionadas do seu computador a serem analisadas, e o utilizador tiver de facultar a localização exacta da secção seleccionada), os valores são divididos por ponto e vírgula, por exemplo: **avgscanx /scan=C:\;D:**

Parâmetros de digitalização

Para visualizar uma síntese integral dos parâmetros disponíveis, digite o comando respectivo com o parâmetro **/?** ou **/HELP** (ex. **avgscanx /?**). O único parâmetro obrigatório é **/SCAN** para especificar que áreas do computador devem ser analisadas. Para uma explicação mais detalhada das opções consulte a [síntese de parâmetros da linha de comandos](#).

Para executar a análise prima **Enter**. Pode parar o processo durante a análise via as combinações **Ctrl+C** ou **Ctrl+Pause**.

Análise CMD iniciada a partir da interface gráfica

Ao iniciar o computador no Modo de Segurança do Windows, também existe a possibilidade de iniciar a análise da linha de comandos a partir da interface gráfica do utilizador. A análise em si será iniciada a partir da linha de comandos, a janela **Compositor de Linhas de Comando** só permite especificar a maioria dos parâmetros de análise no conforto da interface gráfica.

Uma vez que esta janela só é acessível no Modo de Segurança do Windows, para uma descrição detalhada desta janela queira por favor consultar o ficheiro de ajuda que pode ser aberto directamente a partir da janela.

12.4.1. Parâmetros da Análise CMD

A listagem seguinte oferece-lhe uma lista de todos os parâmetros disponíveis para a análise da linha de comandos:

- **/SCAN** [Analisar pastas ou ficheiros específicos](#) /SCAN=path;path
(e.g. /SCAN=C:\;D:\)
- **/COMP** [Analisar 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

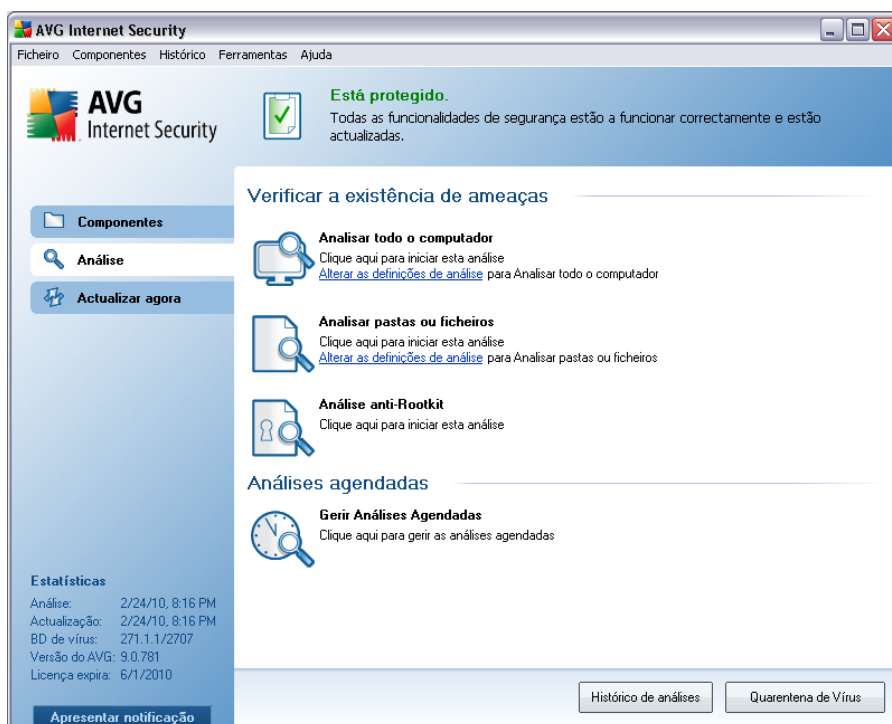
- **/PRIORITY** Defina a prioridade de análise /Baixa, Auto, Elevada/
(consulte a secção [Definições avançadas / Análises](#))
- **/SHUTDOWN** Encerrar o computador aquando da conclusão da análise
- **/FORCESHUTDOWN** Forçar o encerramento do computador após o término da análise
- **/ADS** Analisar Fluxos de Dados Alternados (somente NTFS)

12.5. Agendamento de Análise

Com o **AVG 9 Anti-Virus plus Firewall** 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.

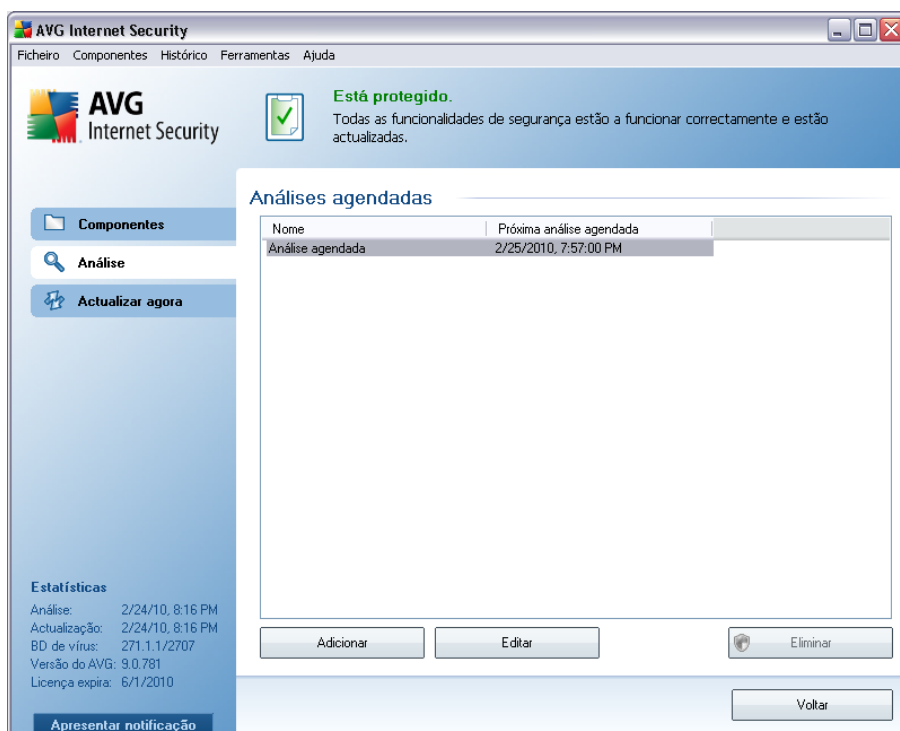
Deve executar a análise [Analisar todo o computador](#) regularmente, pelo menos uma vez por semana. No entanto, se possível, execute a análise de todo computador diariamente - conforme configurado na configuração de agendamento de análise predefinida. Se o computador estiver "sempre ligado" então pode agendar análises fora das horas de expediente. Se o computador for desligado ocasionalmente, então agende as análises para ocorrerem [aquando do arranque do computador quando a tarefa não tiver sido executada atempadamente](#).

Para criar novos agendamentos de análise, consulte a [interface de análise do AVG](#) e veja na secção inferior apelidada **Agendamento de Análises**:



Análises agendadas

Clique no ícone gráfico na secção **Análises agendadas** para abrir uma nova janela de **Análises agendadas** onde pode encontrar uma listagem de todas as análises actualmente agendadas:

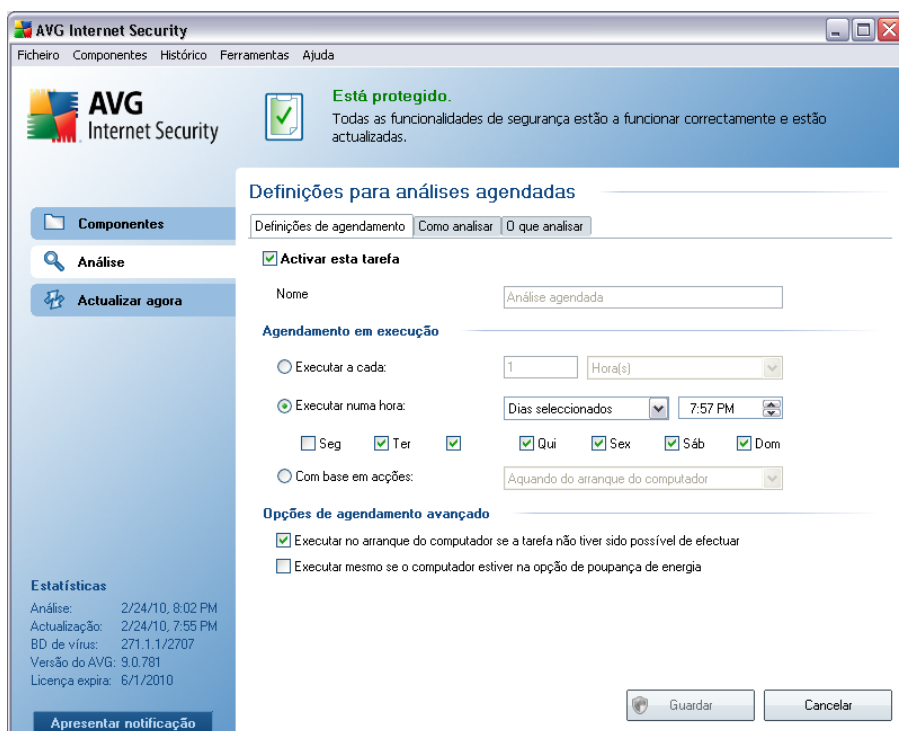


Pode editar / adicionar análises por meio dos seguintes botões de controlo:

- **Adicionar agendamento de análise** - o botão abre a janela **Definições para agendamento de análises**, separador [Definições de agendamento](#). Nesta janela pode especificar os parâmetros do teste definido.
- **Editar agendamento de análise** - este botão só pode ser utilizado se já tiver seleccionado um teste existente a partir da lista de testes agendados. Nesse caso o botão aparece como activo e pode clicar nele para alternar para a janela **Definições para análise agendada**, separador [Definições de agendamento](#). Os parâmetros do teste seleccionado já estão especificados e podem ser editados.
- **Eliminar agendamento de análise** - este botão só pode ser utilizado se já tiver seleccionado um teste existente a partir da lista de testes agendados. Este teste pode então ser eliminado da lista clicando no botão de controlo. No entanto, só pode remover os teste que tiver criado; o **Agendamento de análise a todo o computador** predefinido nas configurações padrão nunca pode ser eliminado.
- **Retroceder** - regressar à [interface de análise do AVG](#)

12.5.1. Definições de agendamento

Se quiser agendar um novo teste e a sua execução regular, aceda à janela **Definições para teste agendado** ((clique no botão **Adicionar agendamento de análise** na janela **Análises agendadas**). 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:

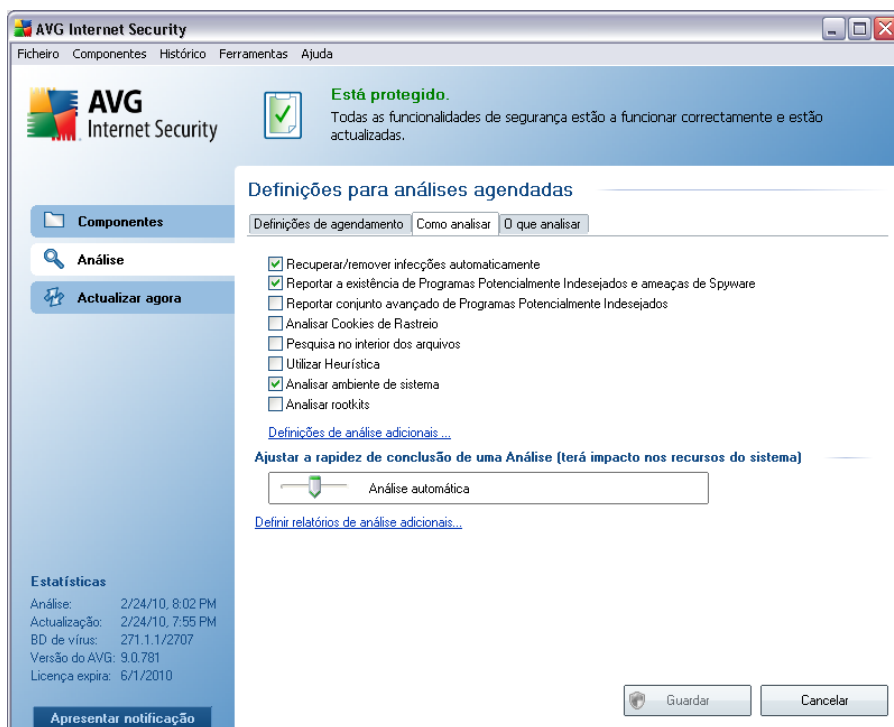
- **Agendamento em execução** - especifique os intervalos de tempo para a execução do novo agendamento de análise. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (**Executar a cada ...** ou definindo uma data e hora precisas (**Executar a uma hora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

12.5.2. Como Analisar



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

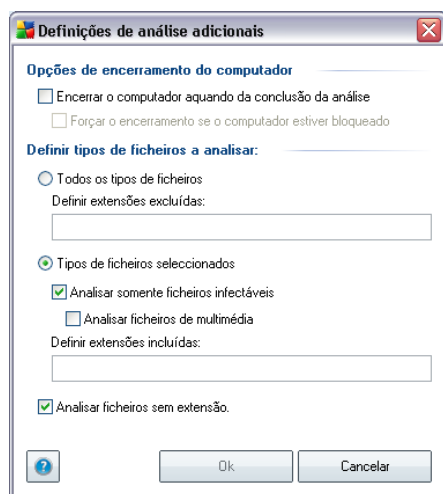
- **Recuperar automaticamente/remover infecção** - (activado por predefinição): se um vírus for detectado durante a análise pode ser restaurado automaticamente se houver uma cura disponível. Na eventualidade de o ficheiro infectado não poder ser recuperado automaticamente, ou se decidir desactivar esta 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**
- se a opção anterior estiver activada, também pode marcar esta caixa 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** - (activado 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): análise heurística (a 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;

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

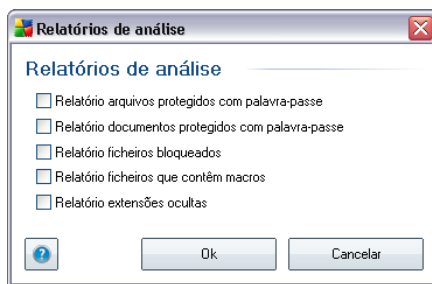
- **Definições de verificação adicionais** - a ligação abre uma nova janela de **Definições de verificação adicionais** onde pode especificar os seguintes parâmetros:



- 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.

- **Prioridade do processo de análise** - pode usar o cursor para alterar a prioridade do processo de análise. Por predefinição, a prioridade está definida para um nível médio (*Análise automática*) que optimiza a velocidade do processo de análise e a utilização dos recursos do sistema. Alternativamente, 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

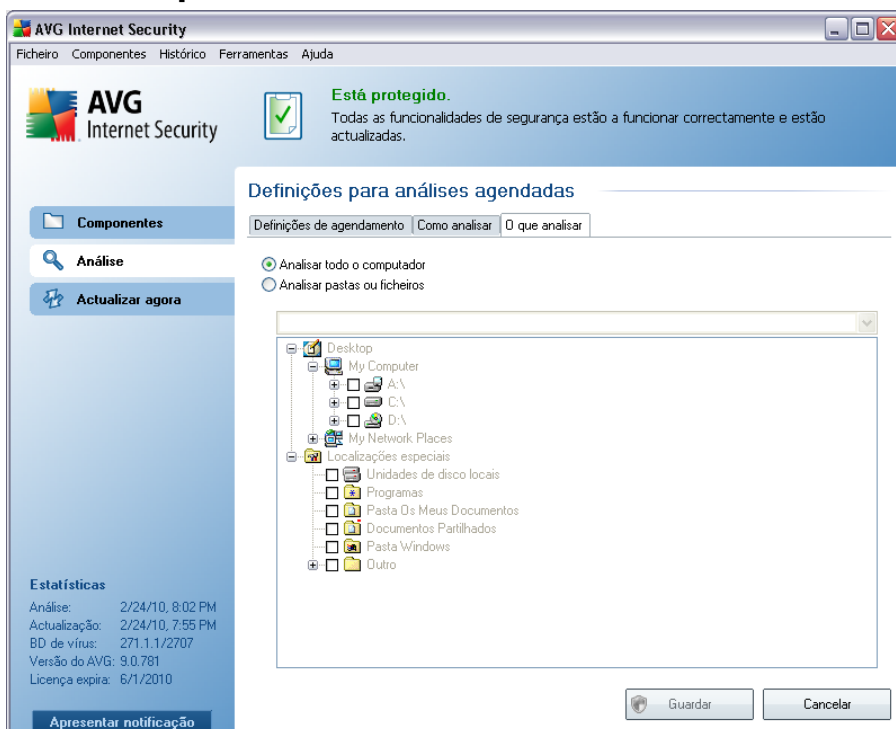
Existem dois botões de controlo disponíveis nos três separadores da janela **Definições para análises agendadas** ([Definições de agendamento](#), [Como analisar](#) e [O que analisar](#)) e estes têm as mesmas funcionalidades independentemente do separador activo:

- **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](#).

12.5.3. O que Analisar



No separador **O que analisar** pode definir se pretende agendar uma [análise a todo o computador](#) ou [analisar ficheiros e pastas específicos](#).

Na eventualidade de seleccionar a análise de ficheiros ou pastas específicos, a estrutura em árvore apresentada na parte inferior desta janela é activada e pode especificar as pastas a serem analisadas (*expanda os itens ao clicar no 'mais' até encontrar a pasta que pretende analisar*). Pode seleccionar várias pastas ao seleccionar as caixas respectivas. As pastas seleccionadas irão aparecer no campo de texto no topo da janela, e a lista de opções guardará o histórico das suas análises seleccionadas para utilização futura. Em alternativa, pode introduzir a localização completa da pasta pretendida manualmente (*se introduzir várias localizações, é*

necessário separá-los com ponto e vírgula sem quaisquer espaços adicionais).

Na estrutura em árvore pode igualmente visualizar uma secção com a identificação **Localizações especiais**. De seguida, dispõe de uma lista de localizações que serão analisadas se a respectiva caixa estiver marcada:

- **Unidades de disco locais** - todas as unidades de disco do seu computador
- **Ficheiros de programas** - C:\Ficheiros de Programas\
- **Pasta Os meus Documentos** - C:\Documentos e Definições\Utilizador\Os meus Documentos
- **Documentos Partilhados** - C:\ Documentos e Definições\Todos os Utilizadores\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* - Windows/System32
 - o *Pasta de Ficheiros Temporários* - Documentos e Definições/Utilizador/Definições Locais/Temp
 - o *Ficheiros da Internet Temporários* - Documentos e Definições/Utilizador/Definições Locais/Ficheiros da Internet Temporários

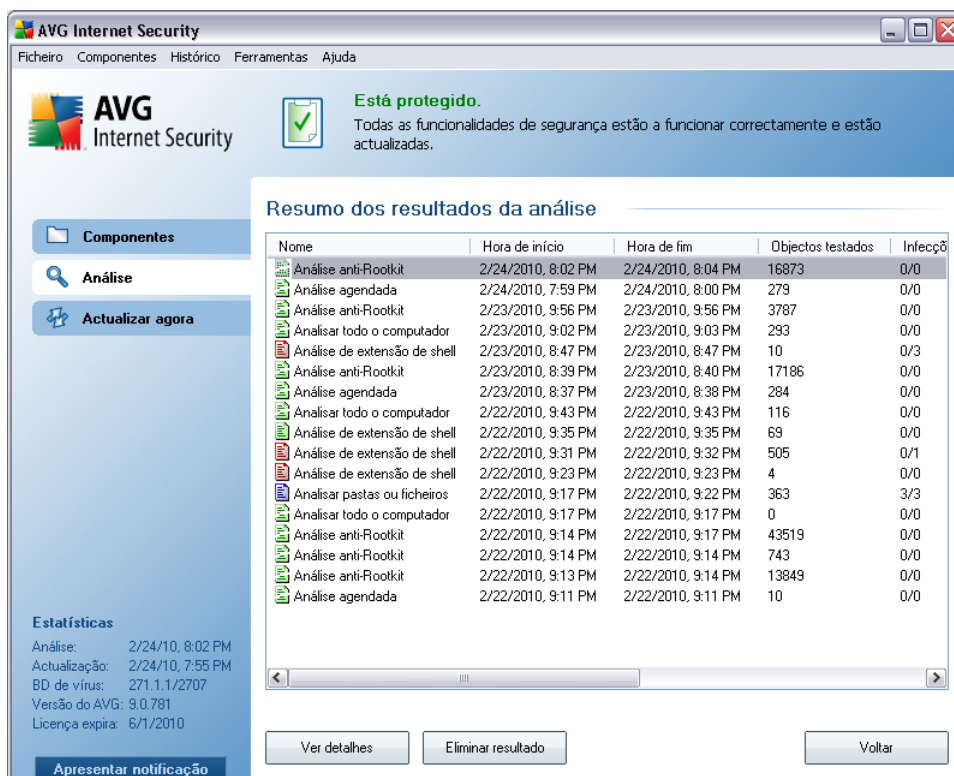
Botões de controlo da janela de Definições para análises agendadas

Existem dois botões de controlo disponíveis nos três separadores da janela **Definições para análises agendadas** (**Definições de agendamento**, **Como analisar** e **O que analisar**) e estes têm as mesmas funcionalidades independentemente do separador activo:

- **Guardar** - guarda todas as alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a [interface padrão de análise do AVG](#). Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos

- **Cancelar** - cancela quaisquer alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a [interface padrão de análise do AVG](#).

12.6. Resumo dos Resultados da Análise



A janela **Síntese dos resultados da análise** é acessível a partir da [interface de análise do AVG](#) via o botão **Histórico de análises**. A janela faculta uma lista de todas as análises executadas anteriormente e informações relativas aos seus resultados:

- **Nome** - designação da análise; pode ser o nome de uma das [análises predefinidas](#) ou um nome que tenha atribuído à sua [própria análise agendada](#). Cada nome inclui um ícone indicando o resultado da análise.

 - ícone verde informa que não foram detectadas quaisquer infecções durante a análise

 - ícone azul anuncia que foi detectada uma infecção durante a análise mas que o objecto infectado foi removido automaticamente

 - ícone vermelho avisa que foi detectada uma infecção durante a análise e que não pôde ser removida!

Cada ícone pode ser sólido ou cortado ao meio - o ícone sólido representa uma análise que foi concluída devidamente; o ícone cortado ao meio significa que a análise foi cancelada ou interrompida.

Atenção: Para informações detalhadas de cada análise por favor consulte a janela [Resultados da Análise](#) acessível via o 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
- **Infecções** - número de [infecções de vírus](#) detectadas / removidas
- **Spyware** - número de [spyware](#) detectado / removido
- **Avisos** - número de [objectos suspeitos](#)
- **Rootkits** - número de [rootkits](#)
- **Informação de registo de análise** - informações relativas ao decurso da análise e resultados (normalmente sobre a sua finalização ou interrupção)

Botões de controlo

Os botões de controlo para a janela **Resumo dos resultados da análises** 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 seleccionada da síntese de resultados de análise
- **Retroceder** - alterna para a janela padrão da [interface de análise do AVG](#)

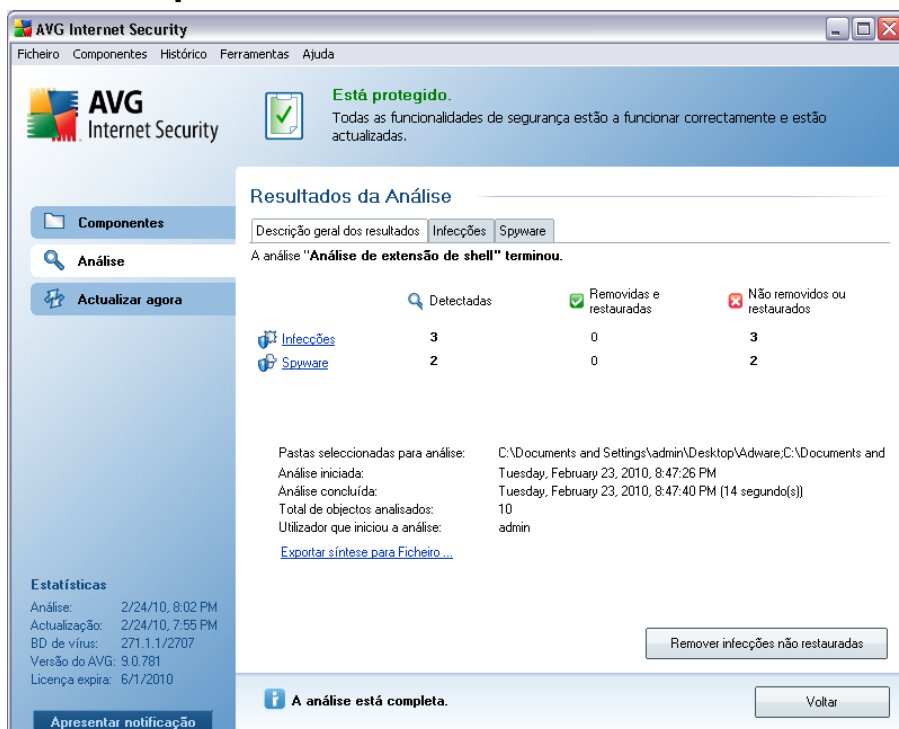
12.7. Detalhes dos Resultados da Análise

Se, na janela [Síntese dos Resultados da Análise](#), estiver seleccionado um item específico, pode então clicar no botão **Ver detalhes** para alternar para a janela **Resultados de Análise** que providencia dados detalhados relativos ao decurso e resultado da análise seleccionada.

A janela de diálogo está dividida em vários separadores:

- [Síntese de Resultados](#) - este separador é apresentado constantemente e faculta dados estatísticos que descrevem o progresso da análise
- [Infecções](#) - este separador só é apresentado se tiver sido detectada alguma [infecção de vírus](#) durante a análise
- [Spyware](#) - este separador só é apresentado se tiver sido detectado algum [spyware](#) durante a análise
- [Avisos](#) - este separador é apresentado, por exemplo, se tiverem sido detectados cookies durante a análise
- [Informação](#) - este separador só é apresentado se tiverem sido detectadas ameaças potenciais mas que não podem ser classificadas em qualquer das categorias acima descritas; nesse caso o separador faculta mensagem de aviso aquando da detecção. Além disso, encontrará aqui informações sobre objectos que não foi possível analisar (ex. arquivos protegidos por palavra-passe).

12.7.1. Separador Resumo dos Resultados



No separador **Resultados da Análise** pode encontrar estatísticas detalhadas com informação relativa a:

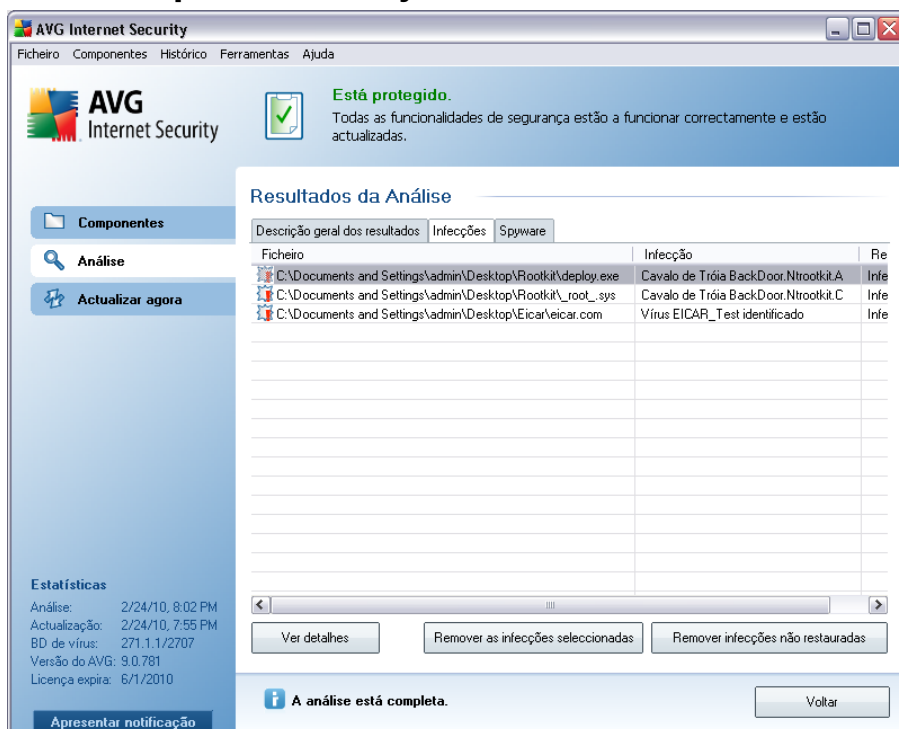
- [infecções de vírus/spyware detectadas](#)
- [infecções de vírus/spyware removidas](#)
- o número de [infecções de vírus](#) / [spyware](#) que não podem ser removidas ou recuperadas

Adicionalmente, encontrará informações relativas à data e hora exacta do 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](#).

12.7.2. 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:

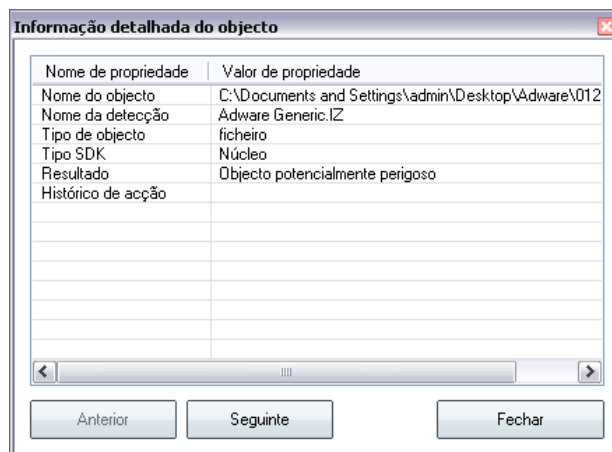
- **Ficheiro** - localização original completa do objecto infectado
- **Infecções** - nome do [vírus detectado](#) (*para detalhes específicos relativos a vírus por favor consulte a [Enciclopédia de vírus](#) on-line*)
- **Resultado** - define o estado actual do objecto infectado que foi detectado durante 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 resultado de análise**:



Nesta janela pode encontrar informações relativas à localização do objecto

infeccioso detectado (**Nome de propriedade**). Ao utilizar os botões **Anterior/ Seguinte** pode visualizar informações relativas a detecções específicas. utilizar o botão **Fechar** para fechar esta janela.

- **Remover as infecções seleccionadas** - utilize o botão para mover as detecções seleccionadas para a [Quarentena de Vírus](#)
- **Remover todas as infecções não recuperadas** - este botão elimina todas as detecções que não possam ser recuperadas ou movidas para a [Quarentena de Vírus](#)
- **Fechar resultados** conclui a síntese de informações detalhadas e retorna à janela [Resumo dos resultados da análise](#)

12.7.3. Separador Spyware

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

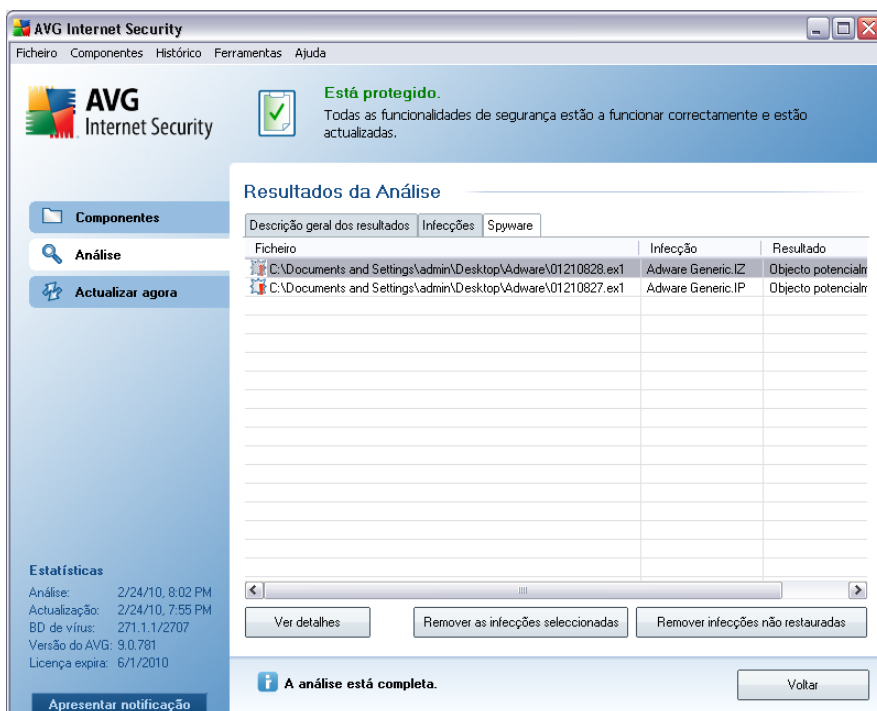
- **Ficheiro** - localização original completa do objecto infectado
- **Infecções** - nome do [spyware detectado](#) (para detalhes relativos a vírus específicos por favor consulte a [Enciclopédia de vírus](#) on-line)
- **Resultado** - define o estado actual do objecto infectado que foi detectado durante a análise:
 - 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



- **Fechar resultados** conclui a síntese de informações detalhadas e retorna à janela [Resumo dos resultados da análise](#)

12.7.4. Separador Avisos

O separador **Avisos** apresenta informações acerca de objectos "suspeitos" (*normalmente ficheiros*) detectados durante as análises. Ao serem detectados pela [Protecção Residente](#), o acesso a estes ficheiros é bloqueado. Exemplo típicos deste tipo de detecções são: ficheiros ocultos, cookies, chaves de registo suspeitas, documentos ou arquivos protegidos por palavra-passe, etc. Esses ficheiros não representam qualquer ameaça directa para o seu computador ou a segurança do mesmo. As informações sobre estes ficheiros são úteis na eventualidade de ser detectado um adware ou um spyware no seu computador. Se 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.

12.7.5. Separador Rootkits

O separador **Rootkits** apresenta informações acerca de rootkits detectados durante a análise se o utilizador tiver iniciado a **Análise Anti-Rootkit**, ou se tiver adicionado manualmente a opção da análise anti-rootkit à [**Análise de todo o computador**](#) (esta opção está desactivada por predefinição).

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 pressupõe a assunção do 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 standard dos sistemas operativos. Acontece que estes são também frequentemente trojans, como tal enganam os utilizadores para que estes pensem que os mesmos podem ser executados com segurança nos seus sistemas. As técnicas utilizadas para este efeito podem incluir ocultar processos em execução de programas de monitorização, ou esconder ficheiros ou dados de sistema do sistema operativo.

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

12.7.6. Separador Informações

O separador **Informação** contém dados acerca dessas "detecções" que não podem ser categorizadas como infecções, spyware, etc. Não podem ser positivamente etiquetadas como perigosas mas contudo carecem da sua atenção. A análise do AVG 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*).

12.8. Quarentena de Vírus



A Quarentena de Vírus é um ambiente seguro para a gestão de objectos suspeitos/ infectados detectados durante os testes AVG. Se um objecto infectado for detectado durante a análise e o AVG não puder recuperá-lo automaticamente, deverá decidir o que fazer com o objecto suspeito. A solução recomendada consiste em mover o objecto para a **Quarentena de Vírus** para tratamento futuro. O propósito principal da **Quarentena de Vírus** é manter qualquer ficheiro eliminado durante um determinado período de tempo, para que possa certificar-se de que já não necessita do ficheiro na localização original. Se, porventura, descobrir que a ausência do ficheiro causa problemas, pode enviar o ficheiro em questão para análise ou restaurá-lo para a localização original.

A interface da **Quarentena de vírus** abre numa janela separada e oferece uma

síntese da informação dos objectos infectados colocados em quarentena:

- **Gravidade** - 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** - na eventualidade de decidir mover o objecto infeccioso detectado da **Quarentena de Vírus** para uma determinada pasta, utilize este botão. O objecto suspeito detectado será guardado com o seu nome original. Se o nome original não for conhecido, será usado o nome padrão.
- **Detalhes** - este botão só é aplicável a ameaças detectadas pela **Protecção de Identidade**. Ao clicar, apresenta uma síntese sinóptica das informações da ameaça (*que ficheiros/processos foram afectados, características do processo, etc.*). Tenha em atenção que para todos os restantes itens que não tenham sido detectados pela PID, este botão será apresentado a cinzento e inactivo!
- **Eliminar** - remove o ficheiro infectado da **Quarentena de Vírus** completa e irreversivelmente



- **Quarentena vazia** -remover todos **Quarentena de Vírus** conteúdo completamente. Ao remover os ficheiros da Quarentena de Vírus, esses ficheiros são irremediavelmente removidos do disco (não movidos para a Reciclagem).

13. Actualizações do AVG

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

Durante o [processo de instalação do AVG](#) foi-lhe solicitado que especificasse a frequência com que pretendia actualizar o AVG. As opções disponíveis são **A cada 4 horas**, ou **Todos os dias** (consulte a janela [Agendar análises e actualizações regulares](#)). 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. Fazer uma verificação a cada 4 horas garantirá que o seu **AVG 9 Anti-Virus plus Firewall** também é mantido actualizado durante o dia.

13.1. 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.

13.2. 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.

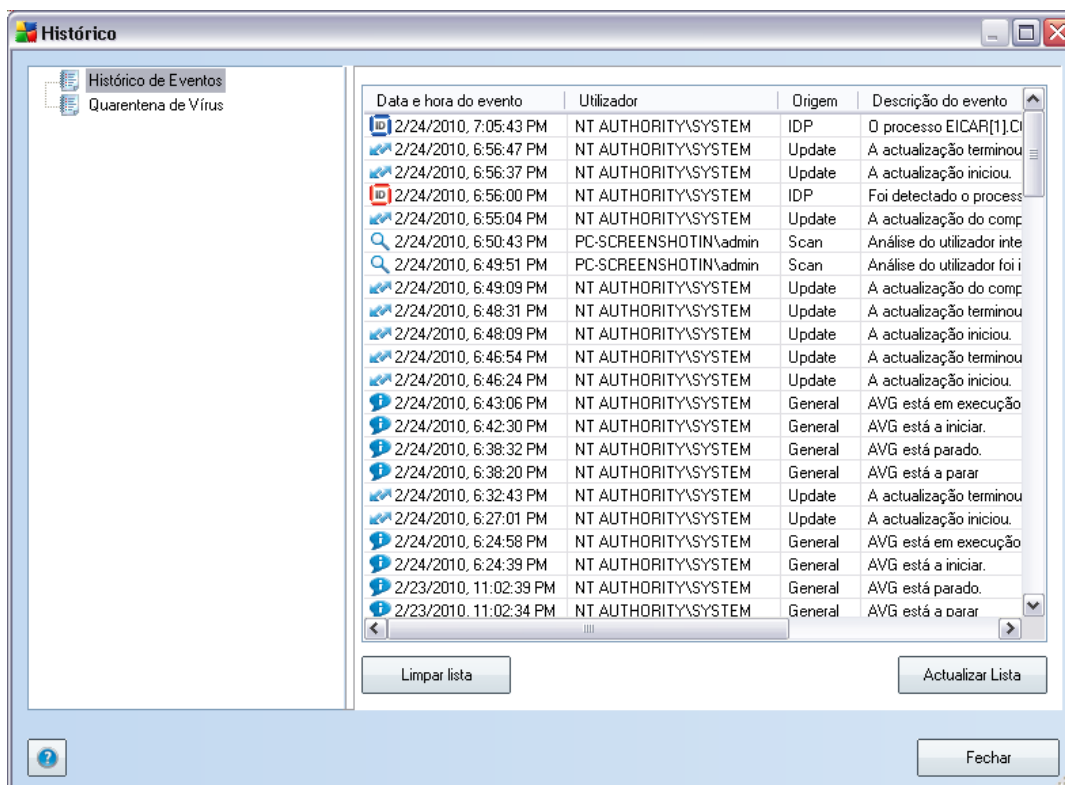
13.3. Processo de Actualização

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 exposto 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!

14. Histórico de Eventos



A janela **Histórico de Eventos** 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 9 Anti-Virus plus Firewall**. O **Histórico de Eventos** 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 (pelo [Protecção Residente](#) ou [análise](#)) incluindo a localização da ocorrência
- Outros eventos importantes

Botões de controlo



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



15. 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/Perguntas-Frequentes) 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**.