AVG 8.5 Anti-Vírus

Manual do Utilizador

Revisão do documento 85.7 (8.9.2009)

Índice

1. Introdução 6

2. Requisitos de Instalação do AVG 7

2.1 Sistemas Operativos Suportados 7
2.2 Requisitos Mínimos de Hardware 7

3. Opções de Instalação do AVG 8

4. Gestor de Transferências do AVG 9

4.1 Selecção do Idioma 9
4.2 Verificação de Conectividade 9
4.3 Definições de Proxy 11
4.4 Seleccione o Tipo de Licença 12
4.5 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 16
5.4 Seleccionar Tipo de Instalação 17
5.5 Activar a Licença do seu AVG 17
5.6 Instalação Personalizada - Pasta de Destino 19
5.7 Instalação Personalizada - Selecção de Componentes 20
5.8 Barra de Ferramentas de Segurança do AVG 21
5.9 Resumo da Configuração 22
5.10 Encerramento de Aplicação 22
5.11 A instalar o AVG 23
5.12 Instalação Concluída 24

6. Assistente da Primeira Execução AVG 25

6.1 Apresentando o Assistente da Primeira Execução do AVG 25
6.2 Agendar análises e actualizações regulares 26
6.3 Ajude-nos a identificar novas ameaças on-line 26
6.4 Configurar a Barra de Segurança do AVG 27
6.5 Actualizar a protecção do AVG 28
6.6 Configuração do AVG Concluída 28

7. Após a Instalação 30

7.1 Registo do Produto 30
7.2 Aceder à Interface do Utilizador 30
7.3 Análise de todo o computador 30
7.4 Teste Eicar 30
7.5 Configuração Predefinida do AVG 31

8. Interface de Utilizador AVG 32

8.1 Menu de Sistema 33
8.1.1 Ficheiro 33
8.1.2 Componentes 33
8.1.3 Histórico 33
8.1.4 Ferramentas 33
8.1.5 Ajuda 33
8.2 Informação de Estado de Segurança 36
8.3 Links Rápidos 37
8.4 Síntese de Componentes 37
8.5 Estatísticas 39
8.6 Ícone da barra de tarefas 39

9. Componentes do AVG 41

9.1 Anti-Vírus 41
9.1.1 Anti-Vírus Princípios 41
9.1.2 Interface do Anti-vírus 41
9.2 Anti-Spyware 43
9.2.1 Anti-Spyware Princípios 43
9.2.2 Interface do Anti-Spyware 43
9.3 Anti-Rootkit 45
9.3.1 Princípios do Anti-Rootkit 45
9.3.2 Interface do Anti-Rootkit 45
9.4 Licença 47
9.5 Link Scanner 48
9.5.1 Princípios do Link Scanner 48
9.5.2 Interface do Link Scanner 48
9.5.3 AVG Search-Shield 48
9.5.4 AVG Active Surf-Shield 48
9.6 Protecção Web 52
9.6.1 Principios da Protecção Web 52

9.6.2 Interface da Protecção Web 52
9.6.3 Detecção Protecção Web 52
9.7 Protecção Residente 56
9.7.1 Protecção Residente Princípios 56
9.7.2 Interface da Protecção Residente 56
9.7.3 Detecção da Protecção Residente 56
9.8 Actualizações 60
9.8.1 Princípios de Actualizações 60
9.8.2 Interface de Actualizações 60
9.9 Barra de Ferramentas de Segurança do AVG 62

10. Definições Avançadas do AVG 66

10.1 Aparência 66
10.2 Ignorar Condições de Erro 69
10.3 Quarentena de Vírus 70
10.4 Excepções PUP 71
10.5 Protecção Web 73
10.5.1 Protecção na Internet 73
10.5.2 Mensagens Instantâneas 73
10.6 Link Scanner 76
10.7 Análises 77
10.7.1 Analisar todo o computador 77
10.7.2 Análise em contexto 77
10.7.3 Analisar pastas ou ficheiros específicos 77
10.7.4 Análise de Dispositivo Amovível 77
10.8 Agendamentos 84
10.8.1 Análise agendada 84
10.8.2 Agendamento de actualização da base de dados de vírus 84
10.8.3 Agendamento de actualização do programa 84
10.8.4 Agendamento de Actualização do Anti-Spam 84
10.9 Verificador de E-mail 94
10.9.1 Certificação 94
10.9.2 Filtro de E-mail 94
10.9.3 Relatórios e Resultados 94
10.9.4 Servidores 94
10.10 Protecção Residente 103
10.10.1 Definições Avançadas 103
10.10.2 Excepções 103

10.11 Anti-Rootkit 106
10.12 Actualizar 107
10.12.1 Proxy 107
10.12.2 Acesso telefónico 107
10.12.3 URL 107
10.12.4 Gerir 107

11. Análise do AVG 114

11.1 Interface de Análise 114
11.2 Análises Predefinidas 115
11.2.1 Analisar todo o computador 115
11.2.2 Analisar pastas ou ficheiros específicos 115
11.3 A analisar no Explorador do Windows 121
11.4 Análise da Linha de Comandos 122
11.4.1 Parâmetros da Análise CMD 122
11.5 Agendamento de Análise 125
11.5.1 Definições de agendamento 125
11.5.2 Como Analisar 125
11.5.3 O que Analisar 125
11.6 Resumo dos Resultados da Análise 133
11.7 Detalhes dos Resultados da Análise 134
11.7.1 Separador Resumo dos Resultados 134
11.7.2 Separador Infecções 134
11.7.3 Separador Spyware 134
11.7.4 Separador Avisos 134
11.7.5 Separador Rootkits 134
11.7.6 Separador Informações 134
11.8 Quarentena de Vírus 142

12. Actualizações do AVG 144

12.1 Níveis de Actualização 144
12.2 Tipos de Actualização 144
12.3 Processo de Actualização 144

13. Histórico de Eventos 146

14. FAQ e Suporte Técnico 147

1. Introdução

Este manual do utilizador faculta documentação compreta para o **AVG 8.5 Anti-Vírus** .

Parabéns pela sua aquisição do AVG 8.5 Anti-Vírus!

AVG 8.5 Anti-Vírus 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 8.5 Anti-Vírus** foi completamente re-desenhado, de raiz, para proporcionar a renomeada e acreditada protecção de segurança do AVG de uma forma nova, mais fácil de utilizar e mais eficiente.

O seu novo**AVG 8.5 Anti-Vírus** produto possui uma interface vanguardista combinada com uma análise mais agressiva e mais rápida. Foram automatizadas mais funcionalidades de segurança para a sua conveniência, e foram incluidas novas einteligentes opções de utilizador para que possa adequar as nossas funcionalides 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

AVG 8.5 Anti-Vírus destina-se a proteger postos 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)

(e service packs possivelmente superiores para sistemas operativos específicos).

2.2. Requisitos Mínimos de Hardware

Requisitos mínimos de hardware para o **AVG 8.5 Anti-Vírus**são os seguintes:

- Intel Pentium CPU 1,2 GHz
- 250 MB de espaço livre no disco rígido (para propósitos de instalação)
- 256 MB de memória RAM

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 (www.avg.com).

Antes de iniciar a instalação do AVG, recomenda-se vivamente que visite o website da AVG para verificar a existência de um novo ficheiro de instalação. Desta forma, tem a certeza de que instala a versão mais recente do AVG 8.5 Anti-Vírusdisponível.

Recomendamos que experimente a nossa nova ferramenta Gestor de Transferências do AVG que o ajudará a seleccionar o ficheiro de instalação adequado!

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

Gestor de Transferências do AVG é uma ferramenta simples que o ajuda a seleccionar o ficheiro de instalação adequado para o seu 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, **Gestor de Transferências do AVG** prosseguirá para a transferência e iniciará o processo de instalação correspondente.

De seguida é disponibilizada uma breve descrição de cada passo individualmente que deverá seguir no**Gestor de Transferências do AVG**:

4.1. Selecção do Idioma

No primeiro passo do **Gestor de Transferências do AVG** 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.

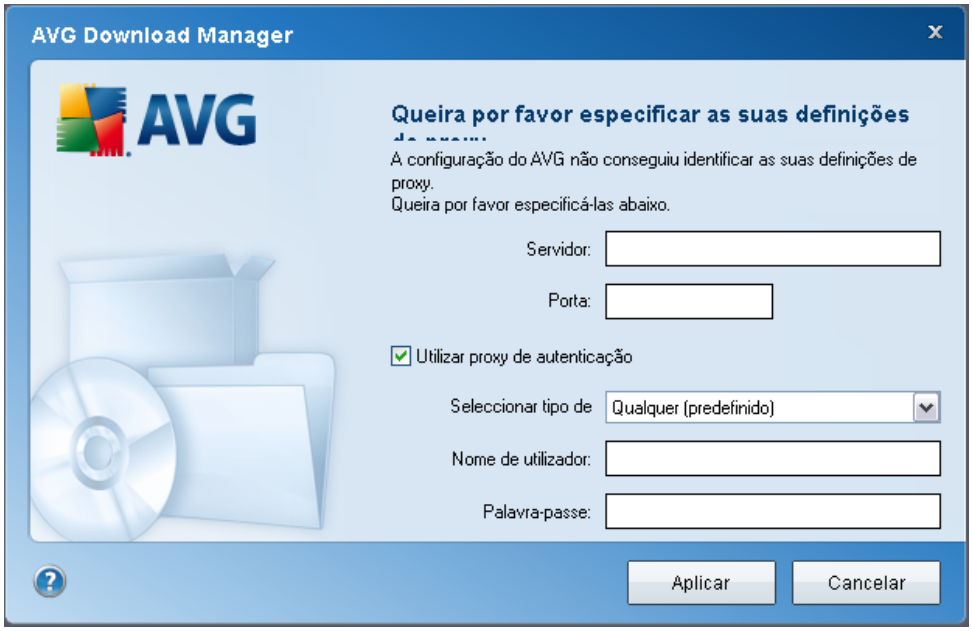
4.2. Verificação de Conectividade

No passo seguinte, **Gestor de Transferências do AVG** tentar-se-á efectuar uma ligação à Internet para que as actualizações possam ser localizadas. Não lhe será permitido continuar o processo de transferência até o **Gestor de Transferências do**

AVG conseguir completar o teste de conectividade.

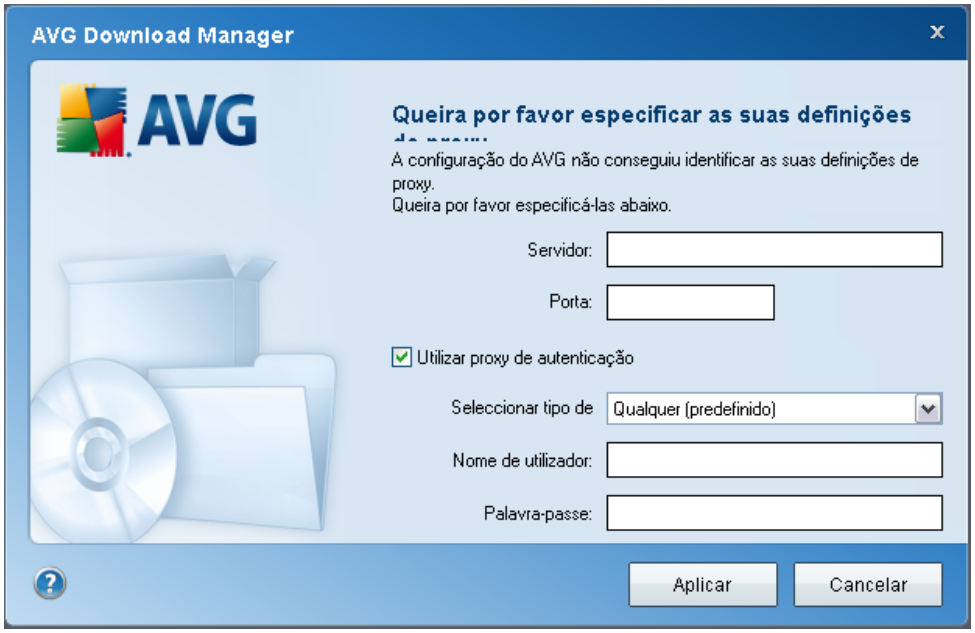
- Se o teste não apresentar qualquer conectividade, certifique-se de que está efectivamente conectado à Internet. Depois clique no botão ***Tentar de novo***.

- 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. Seleccione o Tipo de Licença

Neste passo é-lhe pedido que escolha o tipo de licença do produto que pretende transferir. A descrição facultada permite-lhe escolher o tipo de produto mais adequado:

- ***Versão Completa*** - ex.***Anti-Vírus AVG***, ***AVG Anti-Virus plus Firewall***, ou ***AVG Internet Security***
- ***Versão Experimental*** - proporciona-lhe uma oportunidade de utilizar todas as funcionalidades da versão completa do produto AVG durante o período limitado de 30 dias
- ***Versão Gratuita*** - proporciona protecção para utilizadores domésticos gratuitamente, no entanto as funções da aplicação são limitadas! Além disso, a versão gratuita inclui apenas algumas das funcionalidades disponíveis no produto pago.

4.5. 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.

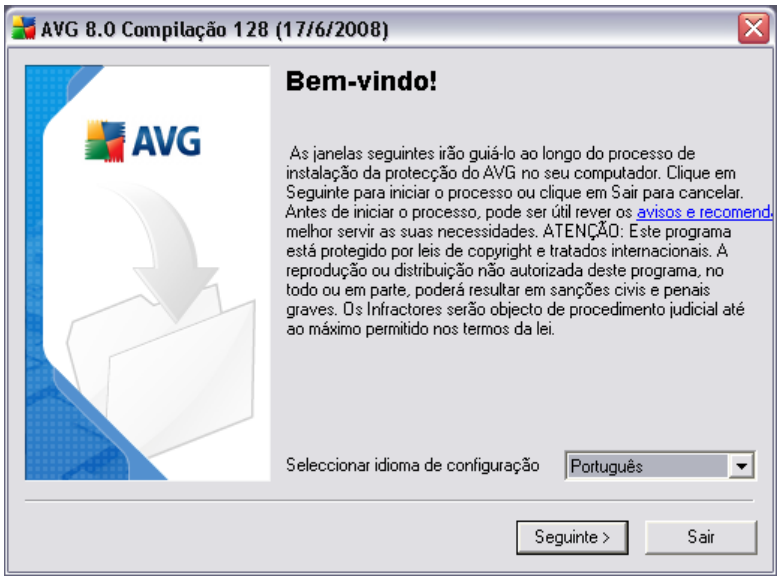
5. Processo de Instalação do AVG

Para instalar oAVG no seu computador, precisa de obter o mais recente ficheiro de instalação. Pode utilizar o ficheiro de instalação a partir do CD facultado na caixa da sua edição, mas este ficheiro pode estar desactualizado.

Como tal, recomendamos que obtenha o ficheiro de instalação mais recente ficheiro on-line. Pode descarregar o ficheiro a partir do website da AVG (em www.avg.com) / secção de ***Downloads.*** Ou, pode utilizar a nossa nova ferramenta **Gestor de Transferências do 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:

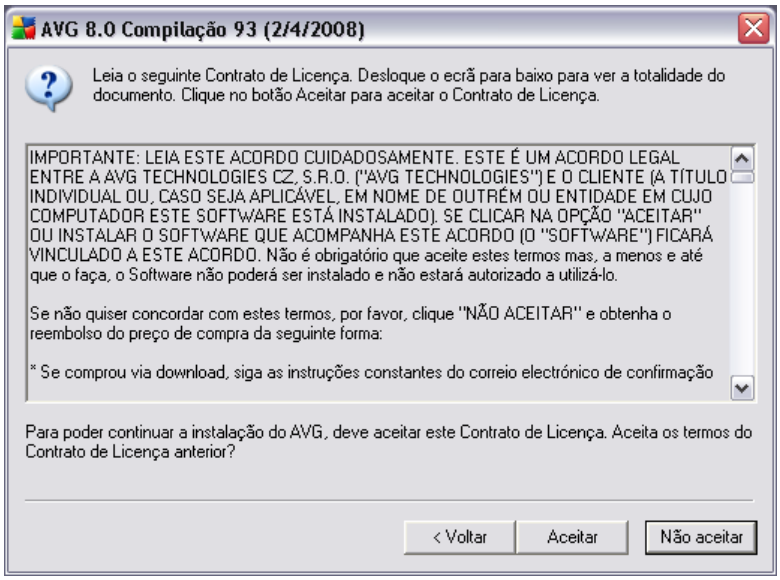
5.1. Execução da Instalação



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.

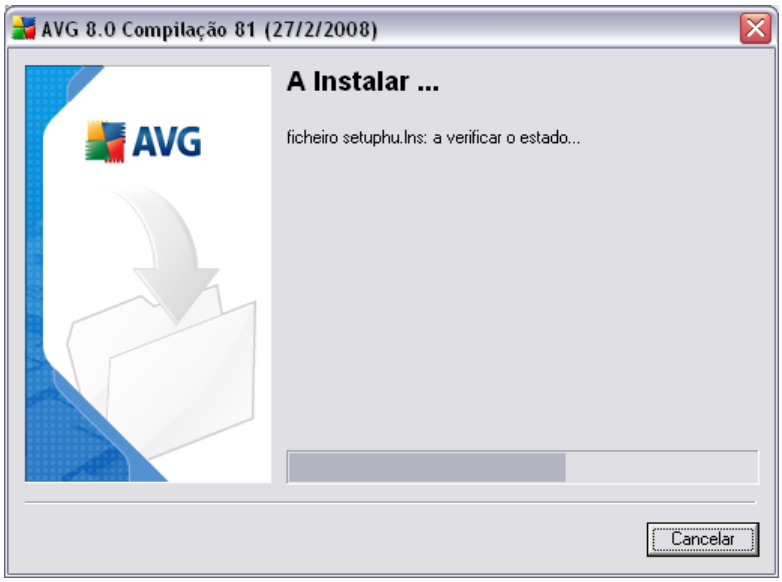
Atenção:*Aqui pode escolher o idioma exclusivamente para o processo de instalação. Não está a seleccionar o idioma para a aplicação AVG - isso pode ser especificado mais tarde durante o processo de instalação!*

5.2. Contrato de Licença



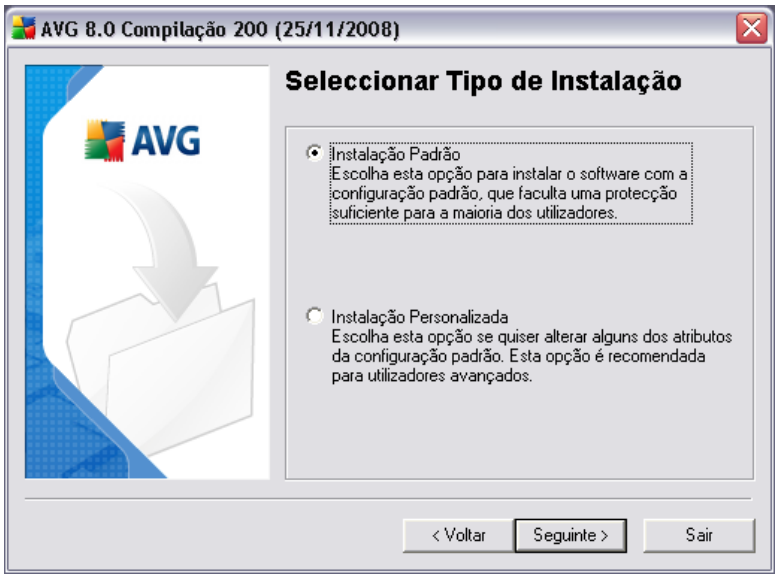
A janela ***Acordo de Licenciamento*** faculta o texto integral do acordo de Licenciamento do AVG. por favor leia atentamente e confirme que leu, compreendeu e aceita o acordo clicando o botão***Aceitar***. Se não concordar com o acordo de licença clique no botão ***Não aceito*** , e o processo de instalação 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.

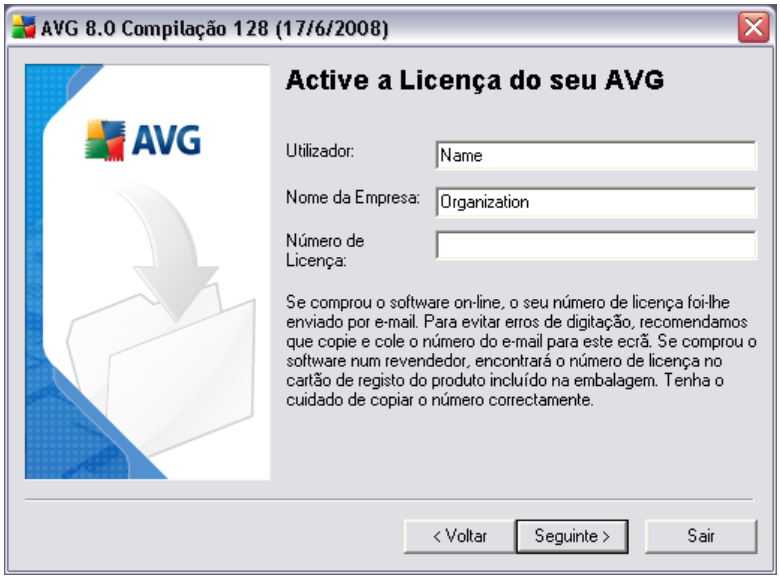
A instalação personalizadasó deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o AVG com definições que não as padrão. Ex. para ajustar a requisitoss de sistema especificos.

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/Venda***. O número de venda pode ser encontrado na embalagem do CD na caixa do seu AVG. O número de licença estará na mensagem de e-mail de

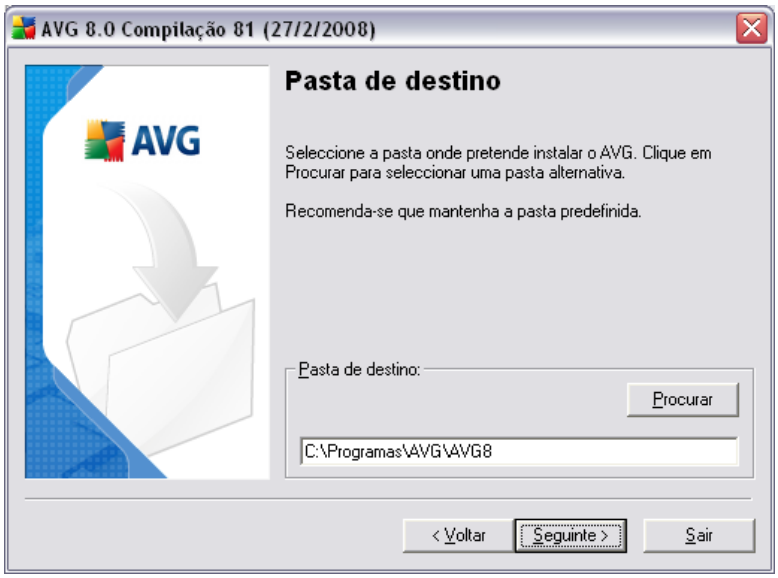
confirmação que recebeu após comprar o seu AVG on-line. Tem de digitar o número exactamente conforme apresentado. Se o formulário digital do número de licença estiver disponível (na mensagem de e-mail), é recomendável que utilize o método copiar e colar para o inserir.



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

Se tiver seleccionado instalação padrão no passo anterior, será reencaminhado directamente para a janela ***Sumário da Instalação*** . Se tiver seleccionado o 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 deverá ser instalado. O AVG será instalado por predefinição na pasta de ficheiros de programas localizada na unidade C:. Se quiser alterar esta localização, utilize o botão ***Procurar*** para visualizar a estrutura da unidade, e seleccione a respectiva pasta. Prima o botão ***Seguinte*** para confirmar.

5.7. Instalação Personalizada - Selecção de Componentes

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

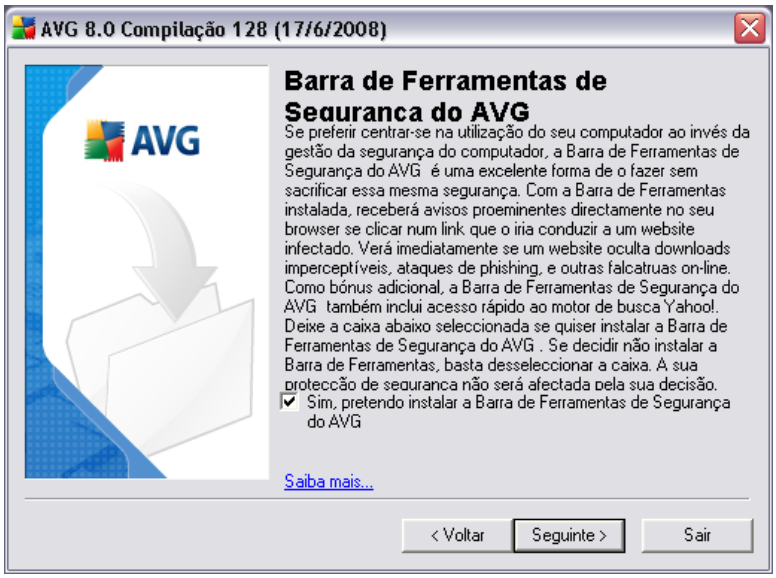
No entanto, só pode seleccionar entre os componentes que estão incluídos na edição do AVG que adquiriu. Só esses componentes serão facultados para instalação na janela de Selecção de Componentes!

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

Clique no item ***Verificador de Correio Electrónico*** 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 Correio Electrónico Pessoal*** para activar automaticamente a protecção das suas comunicações de correio electrónico independentemente do programa de correio electrónico que utilizar .

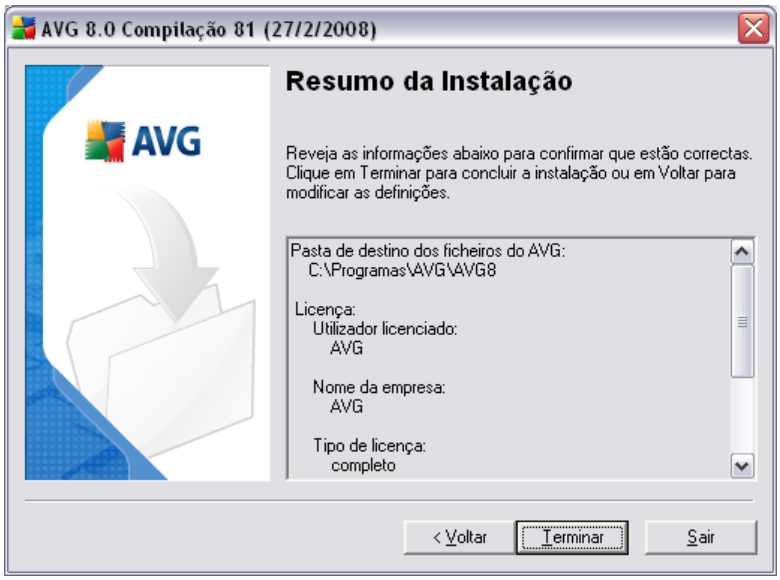
Continue clicando no botão ***Seguinte***.

5.8. Barra de Ferramentas de Segurança do AVG



Na janela ***Barra de Ferramentas de Segurança do AVG*** , decida se pretende instalar a ***Barra de Ferramentas de Segurança do AVG*** - se não alterar as definições predefinidas este componente será instalada automaticamente no seu browser da Internet; em conjunção com as tecnologias do AVG 8.0 e do AVG XPL para lhe facultar protecção online completa enquanto navega na Internet.

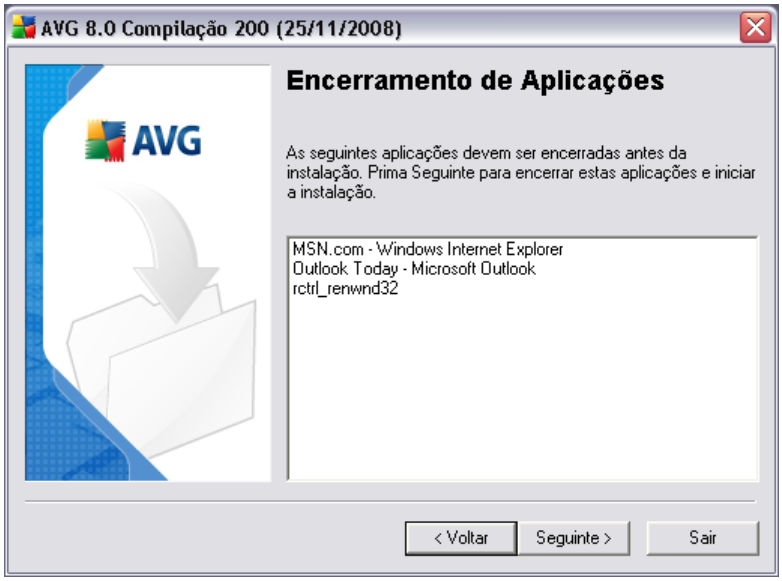
5.9. Resumo da Configuração



A janela ***Sumário de Instalação*** faculta uma síntese de todos os parâmetros do processo de instalação. Por favor certifique-se de que todas as informações estão correctas. Se assim for, clique no botão ***Concluir***para continuar. Caso contrário, pode utilizar o botão ***Retroceder*** para retornar à janela respectiva e corrigir a informação.

5.10. Encerramento de Aplicação

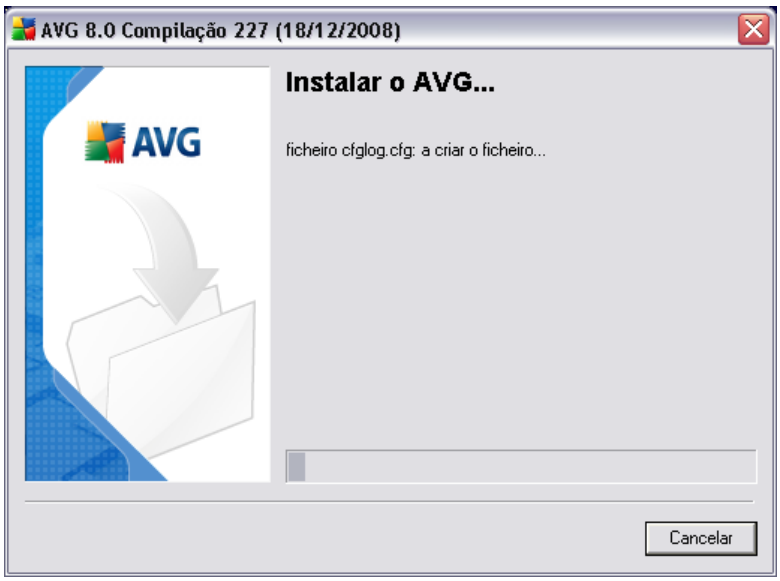
Antes do início do processo de instalação, pode ser-lhe solicitado o encerramento de algumas das aplicações actualmente em execução que podem entrar em conflito com o processo de instalação do AVG. Se for o caso, ser-lhe-á apresentada a seguinte janela de ***Encerramento de Aplicação***. Esta janela tem uma finalidade meramente informativa e não requer qualquer intervenção - se concordar em fechar automaticamente os programas listados, clique em ***Seguinte*** para continuar:



Nota: *Queira por favor certificar-se de que guardou todos os dados antes de confirmar que pretende fechar as aplicações em execução.*

5.11. A instalar o AVG

A janela ***A instalar o AVG*** apresenta o progresso do processo de instalação, e não necessita de qualquer intervenção.



Por favor aguarde até que a instalação esteja completa, depois será reencaminhado para a janela ***Instalação Concluída***.

5.12. Instalação Concluída

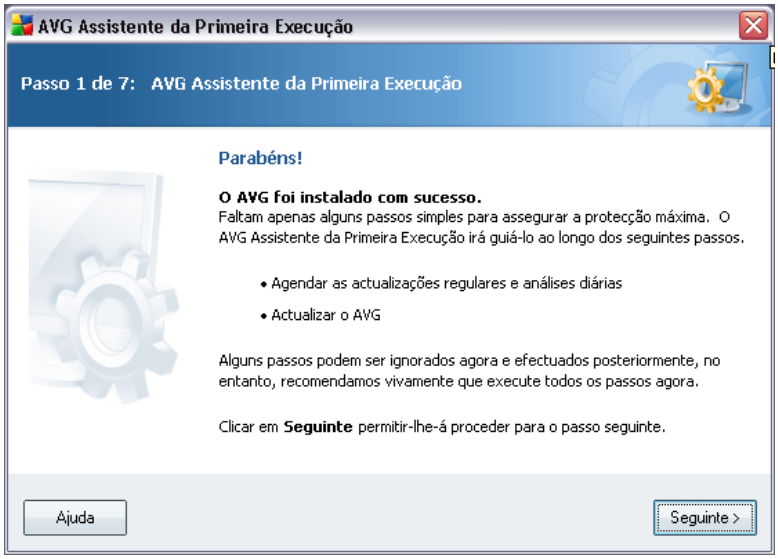
A ***Instalação está concluída!*** Esta janela é o último passo do processo de instalação do AVG. O AVG está agora instalado no seu computador e totalmente funcional. O programa está em execução em segundo plano em modo completamente automático.

Depois da instalação, será iniciado automaticamente o ***Assistente de Configuração Básica do AVG*** que o irá guiar ao longo de alguns breves passos pela configuração elementar do **AVG 8.5 Anti-Vírus**. Apesar do facto de a configuração do AVG ser acessível a qualquer momento durante e execução do AVG, recomendamos vivamente que use esta opção e proceda à configuração básica com a ajuda do assistente.

6. Assistente da Primeira Execução AVG

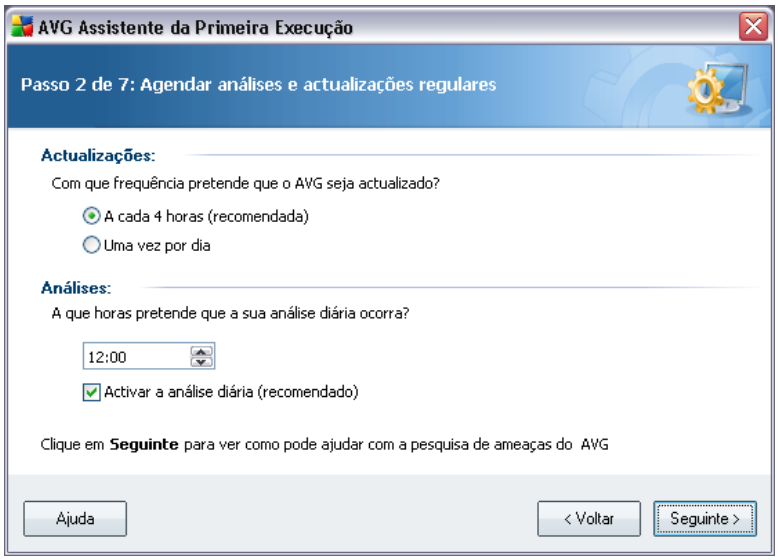
Ao instalar o AVG no computador pela primeira vez, o ***Assistente de Configuração Básica do AVG*** surge para ajudá-lo com das definições **AVG 8.5 Anti-Vírus**iniciais. Embora seja possível definir todos os parâmetros sugeridos posteriormente, recomenda-se que siga o assistente para assegurar a protecção do computador de forma simples e imediata. Siga os passos descritos em cada uma das janelas do assistente:

6.1. Apresentando o Assistente da Primeira Execução do AVG



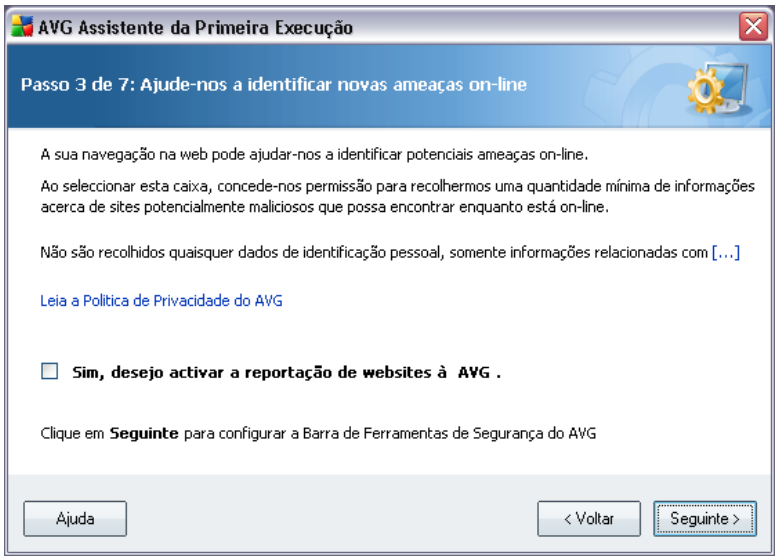
A janela de boas-vindas do ***Assistente da Primeira Execução do AVG*** apresenta um breve resumo do estado do AVG no computador e sugere os passos a executar para obter protecção completa. Clique no botão ***Seguinte*** para continuar.

6.2. Agendar análises e actualizações regulares



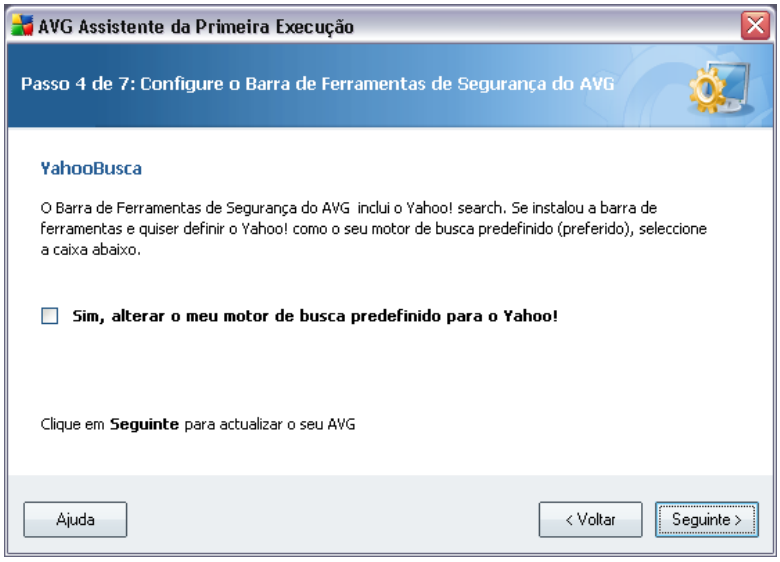
Na janela ***Agendamento de análises e actualizações regulares*** defina o intervalo para verificação de acessibilidade de novos ficheiros de actualização, e defina a hora em que a análise agendada deve ser iniciada. É recomendável que mantenha os valores predefinidos. Clique no botão ***Seguinte***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

6.3. Ajude-nos a identificar novas ameaças on-line



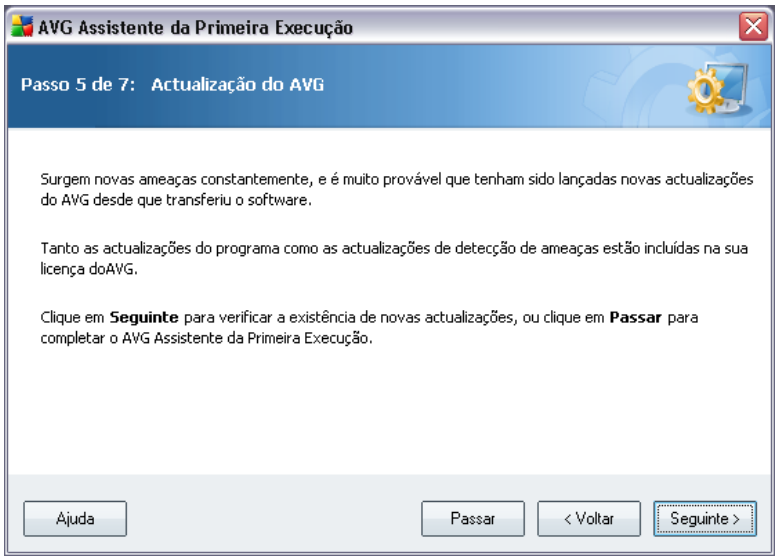
Na janela ***Ajude-nos a identificar novas ameaças*** decida se quer activar a opção de reportação de exploits e websites maliciosos encontrados pelos utilizadores através das funcionalidades ***Surf-Shield / AVG Search-Shield*** do componente ***LinkScanner*** para juntar à base de dados de recolha de informações relativas a actividade maliciosa na Web. É recomendável que mantenha o valor predefinido e tenha a reportação activada. Clique no botão ***Seguinte*** para continuar.

6.4. Configurar a Barra de Segurança do AVG



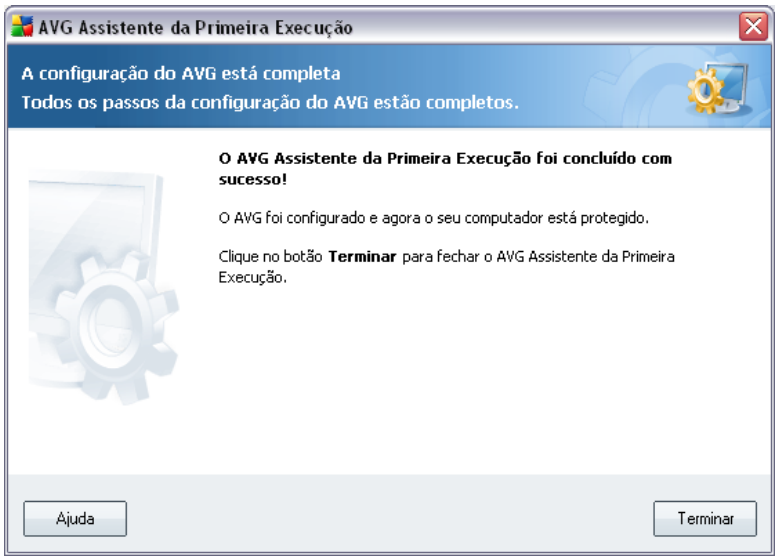
Na janela ***Configurar a Barra de Ferramentas de Segurança do AVG*** pode seleccionar a caixa de verificação para definir que pretende que o Yahoo! seja o seu motor de busca predefinido.

6.5. Actualizar a protecção do AVG



A janela ***Actualizar protecção do AVG*** verifica e transfere automaticamente as Actualizações do AVG mais recentes. Clique no botão***Seguinte*** para transferir os ficheiros de actualização mais recentes e executar a actualização.

6.6. Configuração do AVG Concluída



Agora o seu **AVG 8.5 Anti-Vírus** já está configurado, clique no botão ***Concluir*** para começar a trabalhar com o AVG.

7. Após a Instalação

7.1. Registo do Produto

Estando terminada a **AVG 8.5 Anti-Vírus**instalação, por favor registe o seu produto on-line no website da AVG , ***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.

7.2. 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 8.0/Interface do Utilizador***

7.3. Análise de todo o computador

Existe um risco potencial de que um vírus informático tenha sido transmitido ao seu computador antes da **AVG 8.5 Anti-Vírus** instalação. 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***.

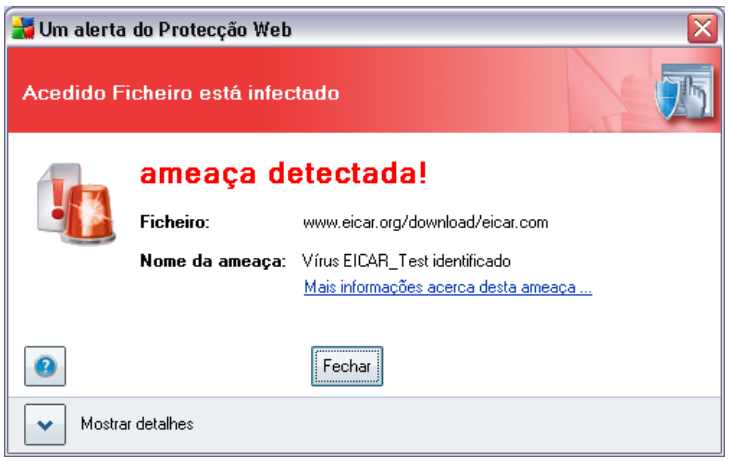
7.4. Teste Eicar

Para confirmar que o **AVG 8.5 Anti-Vírus**foi instalado correctamente pode efectuar o teste EICAR.

O teste Eicar é um método padrão e absolutamente seguro concebido para testar o funcionamento de sistemas antivírus. Pode ser transmitido com segurança, uma vez que não é um vírus verdadeiro e não contém fragmentos de código de vírus. A maioria dos produtos reage como se tratasse de um vírus (*embora o refiram normalmente com um nome óbvio, tal como "EICAR-AV-Test"*). Pode transferir o vírus

EICAR a partir do website da Eicar em www.eicar.com, onde poderá encontrar igualmente todas as informações necessárias sobre o teste.

Tente transferir o ficheiro ***eicar.com***e guardá-lo no disco local. Imediatamente após a confirmação da transferência do ficheiro de teste, a ***Protecção Web*** reagirá com um aviso. Este aviso da ***Protecção Web***demonstra que o AVG está correctamente instalado no seu computador.



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

7.5. Configuração Predefinida do AVG

A configuração predefinida *,ou seja, a forma como a aplicação está configurada imediatamente após a instalação* do **AVG 8.5 Anti-Vírus** 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 doscomponentes 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.

8. Interface de Utilizador AVG

AVG 8.5 Anti-Vírus abra a janela principal:

A janela principal está dividida em várias secções:

- ***Menu de Sistema*** *(linha superior do sistema na janela)* é a navegação standard que lhe permite aceder a todos os componentes, serviços, e funcionalidades do AVG -detalhes >>
- ***Informação de Estado de Segurança*** *(secção superior da janela)* faculta-lhe informação relativa ao estado actual do seu programa AVG - detalhes >>
- ***Links rápidos*** *(secção esquerda da janela)* permite-lhe aceder rapidamente às tarefas mais importantes e utilizadas mais frequentemente do AVG - detalhes >>
- ***Síntese de Componentes*** *(secção central da janela)* faculta uma síntese de

todos os componentes instalados do AVG - detalhes >>

- ***Estatísticas*** *(secção inferior esquerda da janela)*fornece-lhe todos os dados estatísticos relativos ao funcionamento do programa - detalhes >>
- ***Ícone da Barra de Notificação do Sistema*** *(canto inferior direito do monitor, na barra de notificação do sistema)* indica o estado actual do AVG - detalhes >>

8.1. Menu de Sistema

O***menu de sistema*** é a navegação padrão utilizada em todas as aplicações do Wndows. Está localizada horizontalmente no topo da **AVG 8.5 Anti-Vírus**janela principal. Utilize o menu de sistema para aceder a compoentes, funcionalidades e serviços específicos do AVG.

O menu de sistema está dividido em cinco secções pricnipais:

8.1.1. Ficheiro

- ***Sair*** - fecha a interface do utilizador do**AVG 8.5 Anti-Vírus** . No entanto, a aplicação AVG continuará a ser executada em segundo plano e o seu computador continuará protegido!

8.1.2. 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***
- ***Verificador de E-mail*** - abre a página predefinida do componente ***Verificador de E-mail***
- ***Licença*** - abre a página predefinida do componente ***Licença***

- ***LinkScanner*** - abre a página predefinida do componente ***LinkScanner***
- ***Protecção Web*** - abre a página predefinida do componente ***Protecção Web***
- ***Protecção Residente*** - abre a página predefinida do componente ***Protecção Residente***
- ***Actualizações*** - abre a página predefinida do componente ***Actualizações***

8.1.3. Histórico

- ***Resultados da análise***- muda para a interface de teste do AVG, mais especificamente para a janela ***Síntese de Resultados de Análise***
- ***Detecção da Protecção Residente*** - abre uma janela com a síntese das ameaças detectadas pela ***Protecção Residente***
- ***Detecção do Verificador de E-mail*** - abre a janela com a síntese dos anexos das mensagens de e-mail detectadas pelo componente ***Verificador de E-mail***
- ***Detecção da Protecção Web***- abre uma janela com a síntese das ameaças detectadas pela ***Protecção Web***
- ***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 8.5 Anti-Vírus** .
- ***Firewall*** - abre a interface das definições da Firewall no separador ***Registos*** com uma síntese detalhada de todas as acções da Firewall

8.1.4. 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 ainterface 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 8.5 Anti-Vírus**

- ***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 **AVG 8.5 Anti-Vírus** configuração. Regra geral, é recomendável que mantenha as definições da aplicação conforme definidas pelo vendedor do software.

8.1.5. Ajuda

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

- ***Obter Ajuda On-line*** - abre o website do AVGna página do centro de apoio ao cliente

- ***O seu AVG Web*** - abre a página inicial do AVG (emwww.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 ao website de registo em 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.

- ***Acerca do AVG*** - abre a janela de ***Informação*** 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***.

8.2. 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 8.5 Anti-Vírus**. 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 qualque momento a partir do*[*ícone da barra de notificação*](#)*.*

8.3. 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*** >>
- ***Análise*** - 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 capitulo ***Testes 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 - *veja a imagem 2*.

8.4. 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

Na secção **AVG 8.5 Anti-Vírus** ***Síntese de Componentes*** encontra informações acerca dos 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 >>
- ***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*** faculta o texto integral do Acordo de Licença AVG - detalhes >>
- ***LinkScanner*** analisa os resultados de busca apresentados no seu browser da Internet - detalhes >>
- ***Protecção Web*** analisa todos os dados transferidos por uma browser da Internet - 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***. Seleccione esta opção para exprimir que está consciente do estado de erro do componente mas que por alguma razão pretende manter o AVG neste estado, e não pretende ser avisado pela cor cinzenta do ícone da barra de notificação.

8.5. 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 8.0.xx, em que 8.0 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

8.6. Ícone da barra de tarefas

Ícone da Barra de Notificação (*na barra de tarefas do Windows*) indica o estado actual do seu **AVG 8.5 Anti-Vírus**. É vísivel constantemente na sua barra de notificação, independentemente de a janela principal do AVG estar aberta ou fechada.

Se tiver 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***.

Uma coloração cinzenta do ícone com um ponto de exclamação  indica um problema (componente inactivo, estado de erro, etc.). Clique duas vezes no ***ìcone da Barra de Notificação*** para abrir a janela principal e editar um componente.

O ícone da barra de notificação informa ainda sobre as actividades do AVG e possíveis alterações de estado no programa *ex. início automático de uma análise ou actualização agendadas, , alteração de estado de um componente, ocorrência de estado de erro, ...* por meio de um pop-up aberto 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 ***Íconde 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
- ***Sair*** - clique para fechar o AVG*(Só pode fechar a interface do utilizador, o AVG continua a ser executado em segundo plano e o seu computador continua perfeitamente protegido!)*

9. Componentes do AVG

9.1. Anti-Vírus

9.1.1. 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 colocadas 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 siginifica que o verificador anti-vírus consegue detectar um novo vírus, desconhecido, se o vírus tiver algumas das características habituais dos vírus existentes.

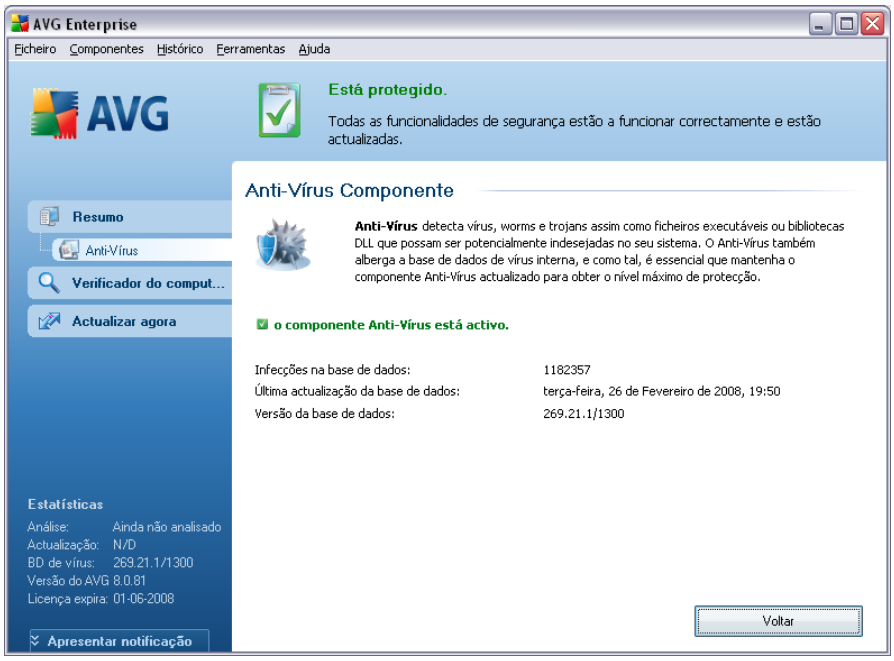
A característica mais importante da protecção anti-vírus é que nenhum vírus conhecido pode ser executado no computador!

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 spayware, 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.

9.1.2. 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.*

9.2. Anti-Spyware

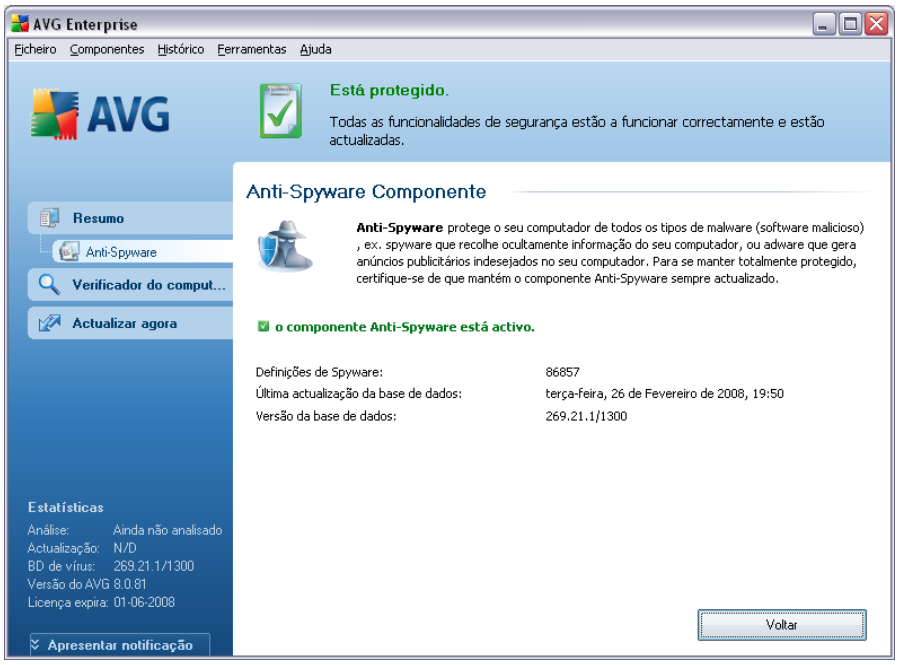
9.2.1. Anti-Spyware Princípios

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 **AVG 8.5 Anti-Vírus** actualizações com as bases de dados mais recentes e as actualizações do programa. 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.

9.2.2. 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.*

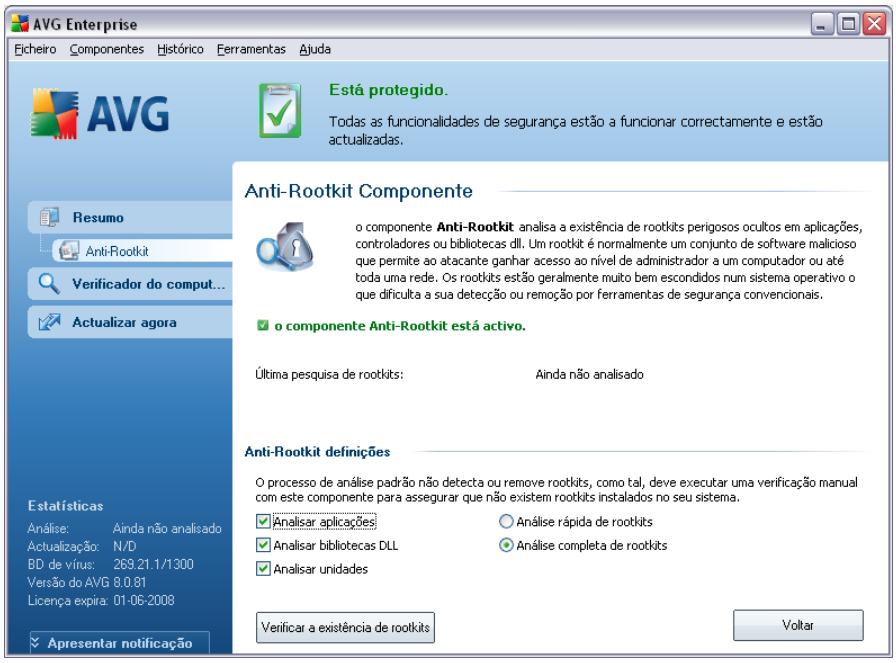
9.3. Anti-Rootkit

9.3.1. Princípios do Anti-Rootkit

O componente Anti-Rootkit é uma ferramenta especializada na detecção e remoção efectiva de perigosos rootkits, ou seja, programas e tecnologias que podem camuflar a presença de software malicioso no seu computador.

Um rootkit é um programa concebido para assumir um 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.

9.3.2. Interface do Anti-Rootkit



A interface do utilizador do ***Anti-Rootkit*** faculta uma breve descrição da funcionalidade do componente, informa acerca do estado actual do componente (*O componente Anti-Rootkit está activo.* e faculta igualmente informações relativas à última análise efectuada com o ***Anti-Rootkit*** .

Na parte inferior da janela pode encontrar a secção ***Definições do Anti-Rootkit*** onde pode configurar algumas funções elementares da análise de presença de rootkits. Primeiro, seleccione as caixas 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:

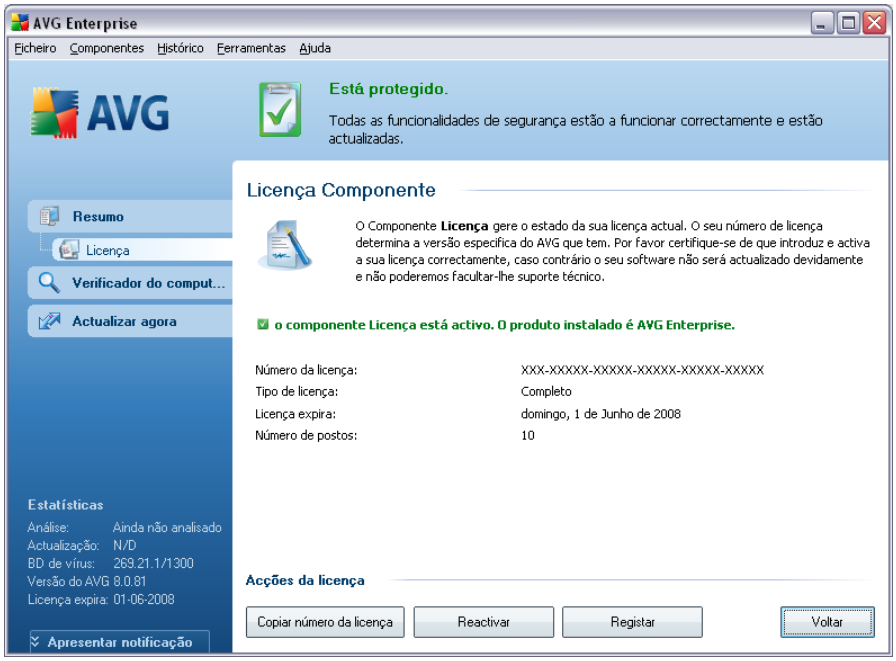
- ***Análise rápida de rootkits*** - analisa somente a pasta sistema *regra geral localizada em c:\Windows*)
- ***Análise completa de rootkits*** - analisa todos os discos acessíveis com a

excepção de A: e B:

Botões de controlo disponível:

- ***Verificar a existência de rootkits*** - uma vez que a análise de rootkits não é uma parte implícita da ***Análise completa de rootkits***, pode executar a análise de rootkits directamente a partir da interface do ***Anti-Rootkit*** utilizando para o efeito este botão
- ***Guardar alterações*** -prima este botão para guardar todas as alterações efectuadas nesta interface e para regressar à ***Interface do utilizador do AVG***(síntese de componentes)
- ***Cancelar*** -prima este botão para regressar à ***Interface do utilizador do AVG*** (síntese de componentes) sem ter guardado quaisquer alterações efectuadas

9.4. 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. Para o seu conforto, a janela ***Licença*** faculta o botão ***Copiar número da licença*** : clique no botão para copiar o número de licença para a área de transferência, e depois pode simplesmente colá-lo onde quiser (***CTRL+V***).

- ***Tipo de licença*** - especifique a edição do produto definido pelo seu número de licença.

- ***A licença expira*** - esta data determina o período de validade da sua licença. Se quiser continuar a utilizar o AVG após esta data terá de renovar a sua licença. A renovação da licença pode ser efectuada on-line no website do AVG.

- ***Número de postos de trabalho*** - quantos postos de trabalho nas quais pode instalar o seu AVG.

Botões de controlo

- ***Copiar número da licença*** - clique no botão para inserir o número de licença actual para a área de transferência (*exactamente como CTRL+C*), e pode colá-lo quando for necessário

- ***Reactivar*** - abre a janela ***Activar AVG***com os dados que introduziu na janela ***Personalizar AVG***doprocesso 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***- conecta ao website do registo em 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.

- ***Retroceder*** - prima este botão para retroceder para a Interface do utilizador do AVGpadrão (síntese dos componentes)

9.5. Link Scanner

9.5.1. Princípios do Link Scanner

O LinkScanner é composto por duas funcionalidades: o ***AVG Active Surf-Shiled*** e o ***AVG Active Search-Shield***.

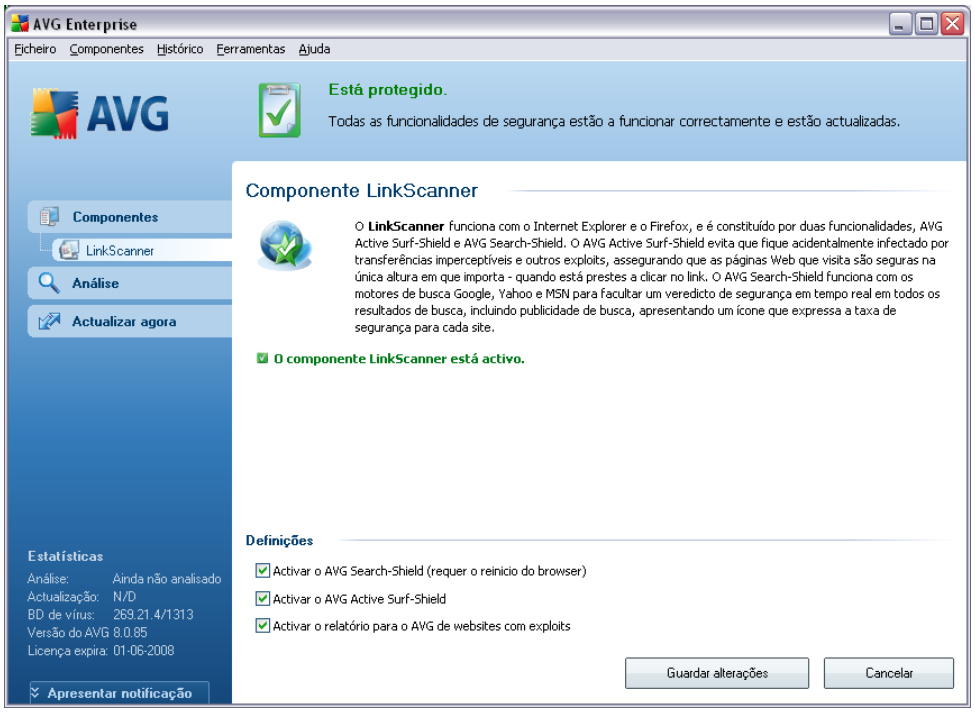
O AVG Active Surf-Shield evita que fique acidentalmente infectado por transferências imperceptíveis e outros exploits, assegurando que as páginas Web que visita são seguras na única altura em que importa - quando está prestes a clicar no link.

O AVG Search Shield funciona com os motores de busca Google, Yahoo! e MSN para facultar um veredicto de segurança em tempo real em todos os resultados de busca, incluindo publicidade de busca, apresentando um ícone que expressa a taxa de segurança para cada site.

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

9.5.2. Interface do Link Scanner

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



- ***Activar AVG Search-Shield***- (*activado por predefinição*): ícones de notificação de aviso em procuras efectuadas no Google, Yahoo ou MSN 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*).

- ***Reportação de websites com exploits*** - seleccione este item para permitir a reportação 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.

9.5.3. 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, MSN, etc. serão avaliados pela existência de links perigosos ou suspeitos. Ao verificar estes links e marcando os perigosos, a ***Barra de Ferramentas de Segurança do AVG*** 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 naBarra de Ferramentas de Segurança do AVG* !).

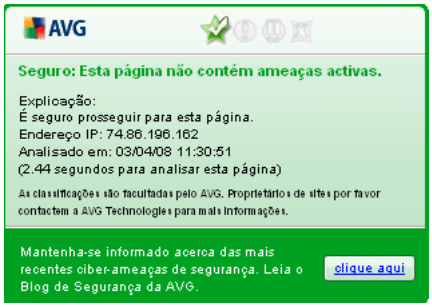
 A página de destino não contém ameaças mas é algo suspeita (*questionável em termos de origem ou motivo, como tal, não é recomendável para compras on-line, etc.*).

 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:



9.5.4. 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, a ***Barra de Ferramentas de Segurança do AVG*** não permitirá que o seu browser a apresente.

Se encontrar um website malicioso, a ***Barra de Ferramentas de Segurança do AVG*** incorporado no seu browser, avisá-lo-á com um ecrã semelhante a:

Se ainda quiser visitar a página infectada, estará disponível um link para a página neste ecrã, ***mas prosseguir para estas páginas não é recomendável!***

9.6. Protecção Web

9.6.1. Principios da Protecção Web

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

A Protecção Web 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 Web AVG não se destina a plataformas de servidores!*

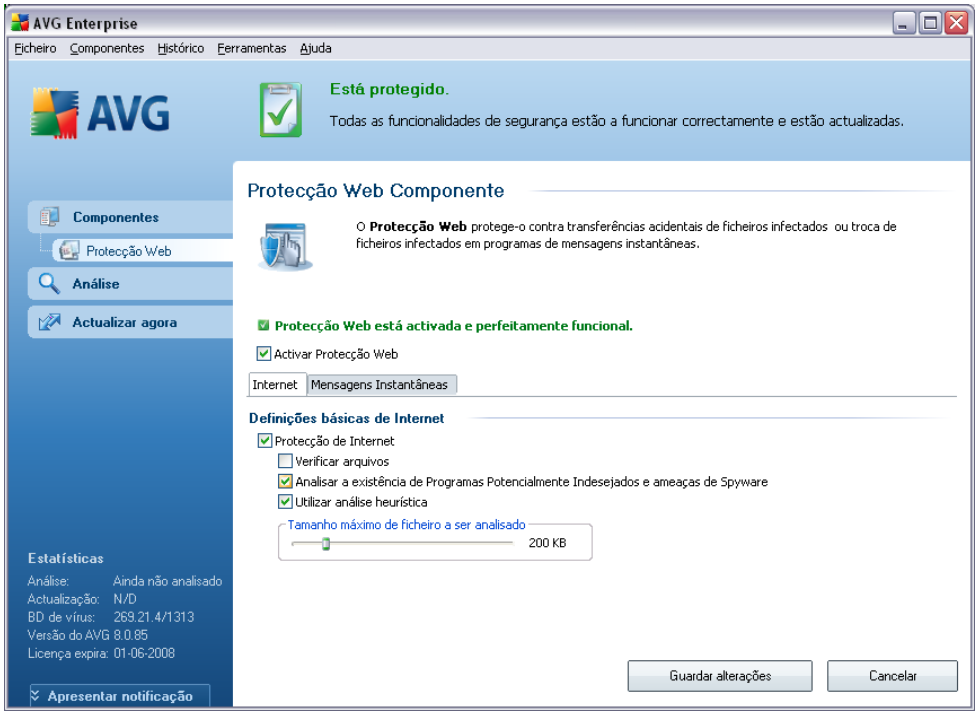
9.6.2. Interface da Protecção Web

A interface do componente ***Protecção Residente***descreve o comportamento deste tipo de protecção. Pode encontrar mais à frente informações relativas ao estado actual do componente (*A Protecção Residente está activo 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 o ***Protecção Residente*** ao marcar o item ***Activar Protecção Residente***. Esta opção está activada por predefinição, e o componente ***Protecção Residente*** 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 o ***Protecção Residente***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:

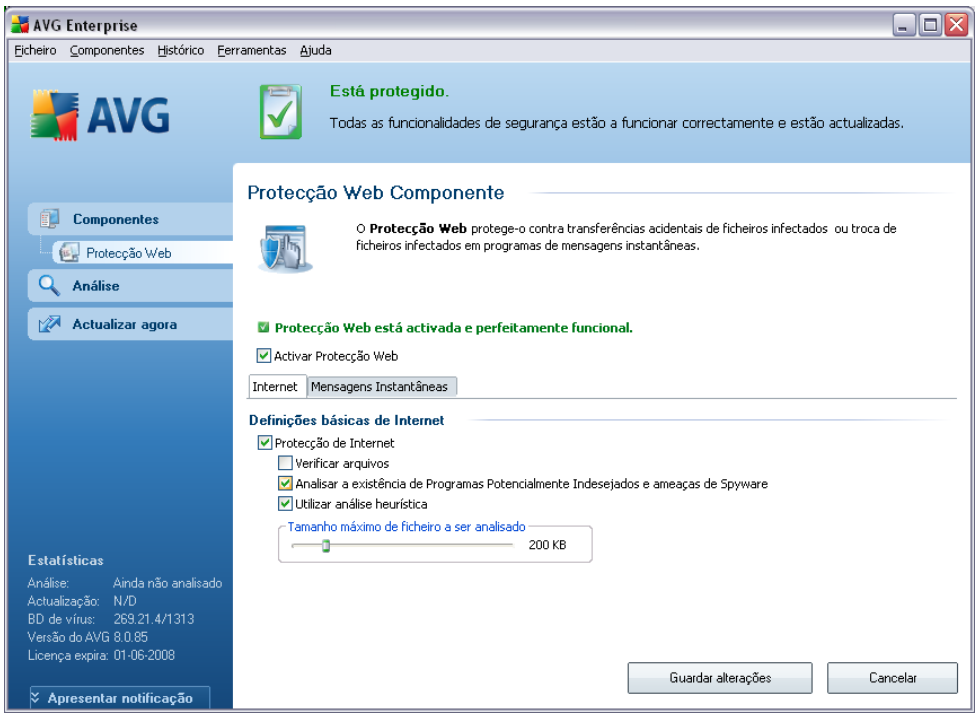


o ***Protecção na Internet*** - esta opção confirma que a***Protecção Web*** deve analisar o conteúdo das páginas www. Uma vez que esta opção está activada (*por predefinição*), pode ainda activar/desactivar estes itens:

- ***Verificar arquivos*** - analisar o conteúdo de arquivos possivelmente incluidos na página www a ser apresentada
- ***Analisar Programas Potencialmente Indesejados*** - analisar programas potencialmente indesejados (*programas executáveis que podem funcionar como spyware ou adware*) incluídos na página www a ser apresentada
- ***Utilizar a análise heurística*** - analisar o conteúdo da página a ser apresentada utilizando o método de análise heurística*(emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual - consulte o capítulo*Princípios de Anti-Vírus)
- ***Tamanho máximo de ficheiro a ser analisado*** - se os ficheiros incluidos 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 Web***. Mesmo que o ficheiro transferido seja superior ao tamanho especificado, e como tal não será analisado com o ***Protecção Web***, ainda está protegido: na eventualidade do ficheiro estar infectado, o ***Protecção Residente*** detecta-lo-á 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 Web verifique se a comunicação online está livre de vírus. Considerando que esta opção está activada, pode ainda especificar qual a aplicação de mensagens instantâneas que pretende controlar - actualmente **AVG 8.5 Anti-Vírus** 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, 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 Web***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*)

9.6.3. Detecção Protecção Web

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

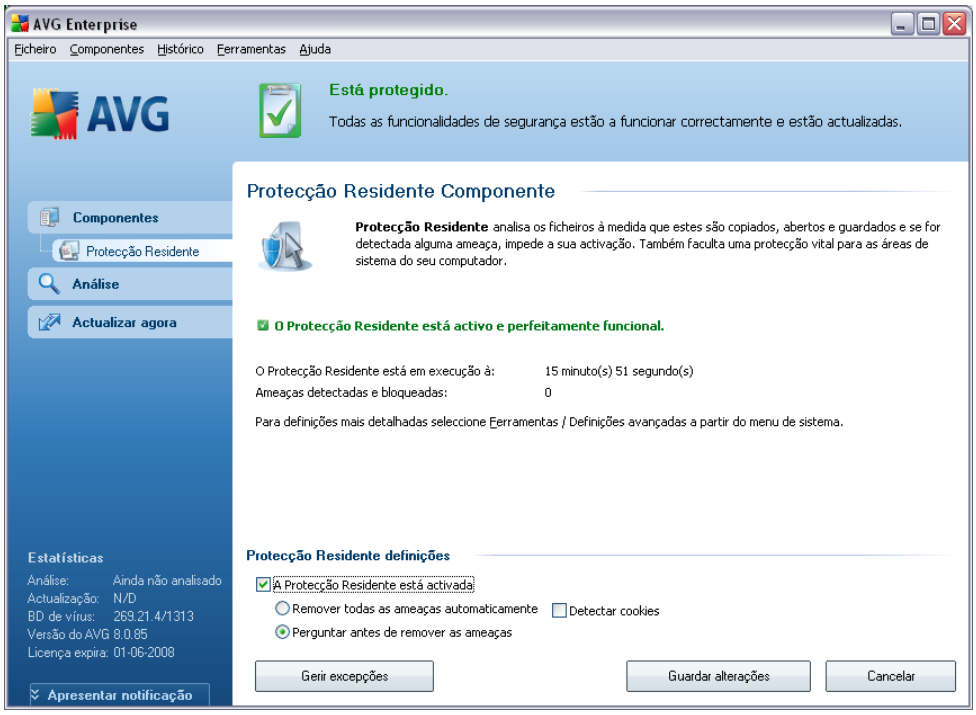
A página Web suspeita não será aberta, e a detecção da ameaça será registada na lista de ***Detecções da Protecção Web*** (*acessível via o menu de sistema Histórico / Detecções do Protecção Web*).

9.7. Protecção Residente

9.7.1. Protecção Residente Princípios

A ***Protecção Residente***analisa ficheiros quando estes são copiados, abertos ou guardados. Quando a ***Protecção Residente*** detecta um vírus num ficheiro acedido, interrompe a operação em curso, não permitindo a activação do vírus. a ***Protecção Residente***carregada para a memória do computador durante o arranque do sistema, também oferece uma protecção vital para as áreas de sistema do computador.

9.7.2. 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 for necessário, este valor pode ser restaurado; ex. para propósitos de estatística - 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 Ficheiro/Definições avançadas do menu de sistema*).

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

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

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

Em ambas as situações, pode ainda seleccionar se pretende ***Remover cookies automaticamente.*** 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

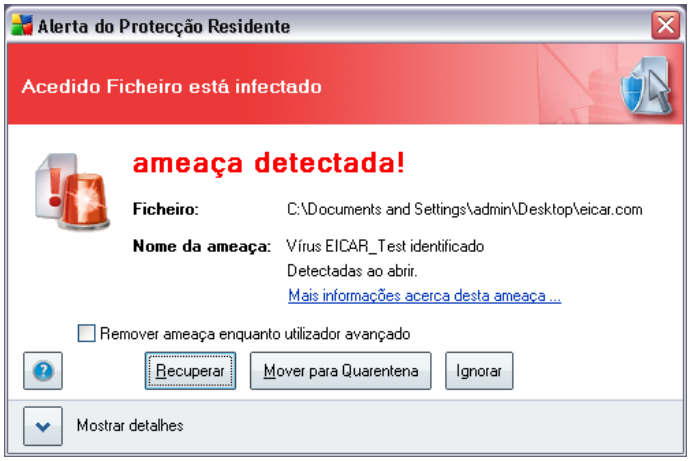
Os botões de controlo disponíveis na interface do ***Protecção Residente***são os

seguintes:

- ***Gerir excepções*** - abre a janela ***Protecção Residente - Exclusões de Directórios*** onde pode definir pastas que não devem ser verificadas pela análise do ***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)

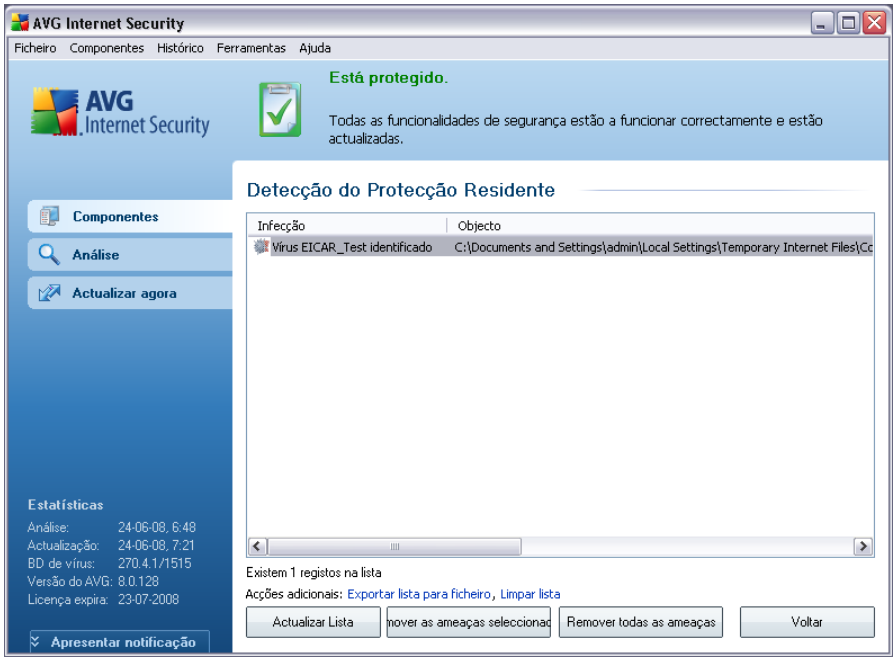
9.7.3. Detecção da Protecção Residente

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



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***
- ***Ignorar*** - recomendamos vivamente que NÃO utilize esta opção a menos que tenha uma razão verdadeiramente válida para isso!



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
- ***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).

9.8. Actualizações

9.8.1. Princípios de Actualizações

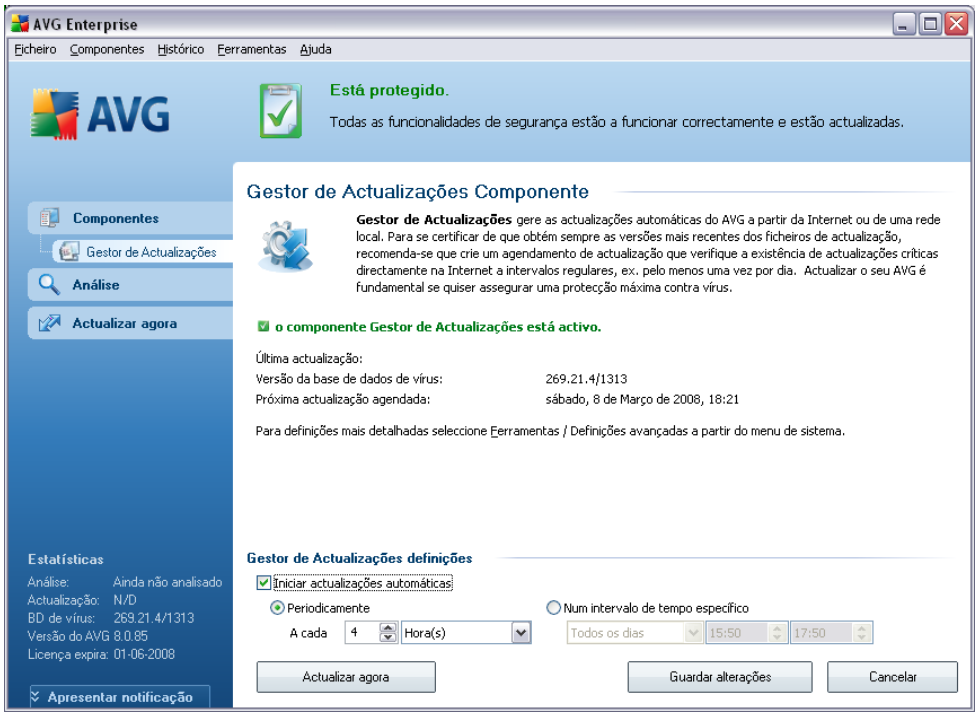
Nenhum software de segurança pode garantir uma protecção efectiva de vários tipos de ameaças a menos que seja actualizado regularmente! Os criadores de vírus estão constantemente à espreita de novas falhas que possam explorar tanto em software como nos sistemas operativos. Novos vírus, novo malware,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

9.8.2. Interface de Actualizações



A interface de ***Actualizações*** apresenta informações acercada funcionalidade do componente e ao seu estado actual (*Actualizações está activo.* , e faculta 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

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 mentenha neste estado! A transferência regular dos

mais recentes ficheiros de actuaização é essencial para o funcionamento apropriado de qualquer software de segurança!

Pode ainda definir quando a actualização deve ser executada:

- **Periodicamente** - define o intervalo de tempo
- **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 imediatamanualmente
- ***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)

9.9. 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 ***Mozilla Firefox*** (*versão 1.5 ou superior*).

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

Uma vez instalada, a ***Barra de Ferramentas de Segurança do AVG*** ficará

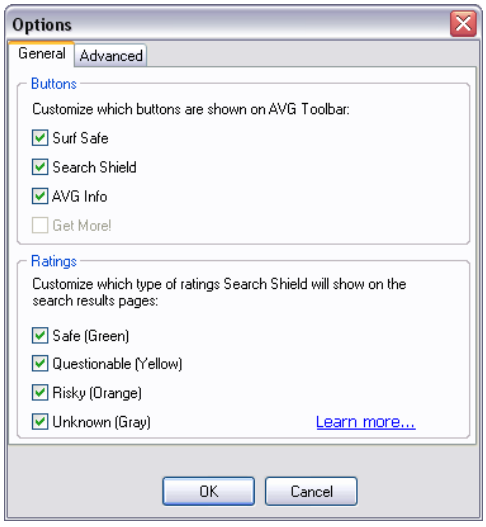
localizada por predefinição sob a barra de endereço do ser browser:

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

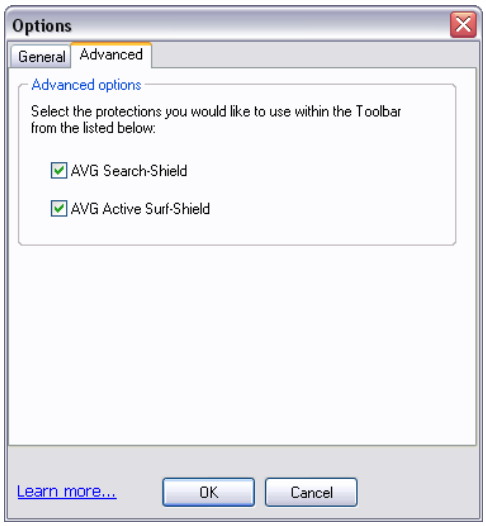
- ***Botão de logótipo AVG*** - faculta acesso a itens gerais da barra de ferramentas. Clique no botão de logótipo para ser redireccionado para o website da AVG (www.avg.com). Clicar com o cursor junto ao ícone AVG abrirá as seguintes opções:
    - ***Informação da Barra de Ferramentas*** - link para a página inicial da ***Barra de Ferramentas de Segurança do AVG*** com informações detalhadas relativas à protecção da barra de ferramentas
    - ***Iniciar o AVG 8.0*** - abre a interface do utilizador do AVG 8
    - ***Opções*** - abre uma janela de configuração onde pode ajustar as definições da ***Barra de Ferramentas de Segurança do AVG*** conforme as suas necessidades, a janela está dividida em dois separadores:
        - ***Geral*** - neste separador pode encontrar duas secções apelidadas ***Botões*** e ***Classificações***.

          A secção ***Botões*** permite-lhe configurar quais os botões que estarão visíveis ou ocultos na ***Barra de Ferramentas de Segurança do AVG*** . Por predefinição todos os botões estão visíveis.

          A secção ***Classificações*** permite-lhe determinar que tipo de classificações pretende que sejam apresentadas para os seus resultados de pesquisa. Por predefinição todas as classificações estão visíveis, mas pode ocultar algumas (*ao pesquisar com o caixa de pesquisa do Yahoo!, só serão apresentados os resultados seguros).*



☼ ***Avançado*** - neste separador pode editar as funcionalidades de segurança da ***Barra de Ferramentas de Segurança do AVG*** . Por predefinição, tanto a funcionalidade ***AVG Search-Shield*** como a funcionalidade ***AVG Active Surf-Shield*** estão activadas.



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, contactar o ***suporte técnico da AVG*** , ou visualizar os detalhes da versão actual da

barra de ferramentas

- ***Yahoo Caixa de pesquisa*** - uma forma fácil e segura de pesquisar na Web usando a pesquisa do Yahoo!. Digite uma palavra ou frase na caixa de pesquisa e clique em ***Procurar*** para iniciar a pesquisa directamente no servidor Yahoo!, independentemente da página que está actualmente apresentada. A caixa de pesquisa também lista o seu histórico de pesquisa. As pesquisas efectuadas via a caixa de pesquisa são analisadas pela protecção ***AVG Search-Shield***.

- ***O botão AVG Active Surf-Shield*** - botão activar/desactivar que controla o estado da protecção ***AVG Active Surf-Shield***.

- ***O botão AVG Search-Shield*** - botão activar/desactivar que controla o estado da protecção ***AVG Search-Shield***.

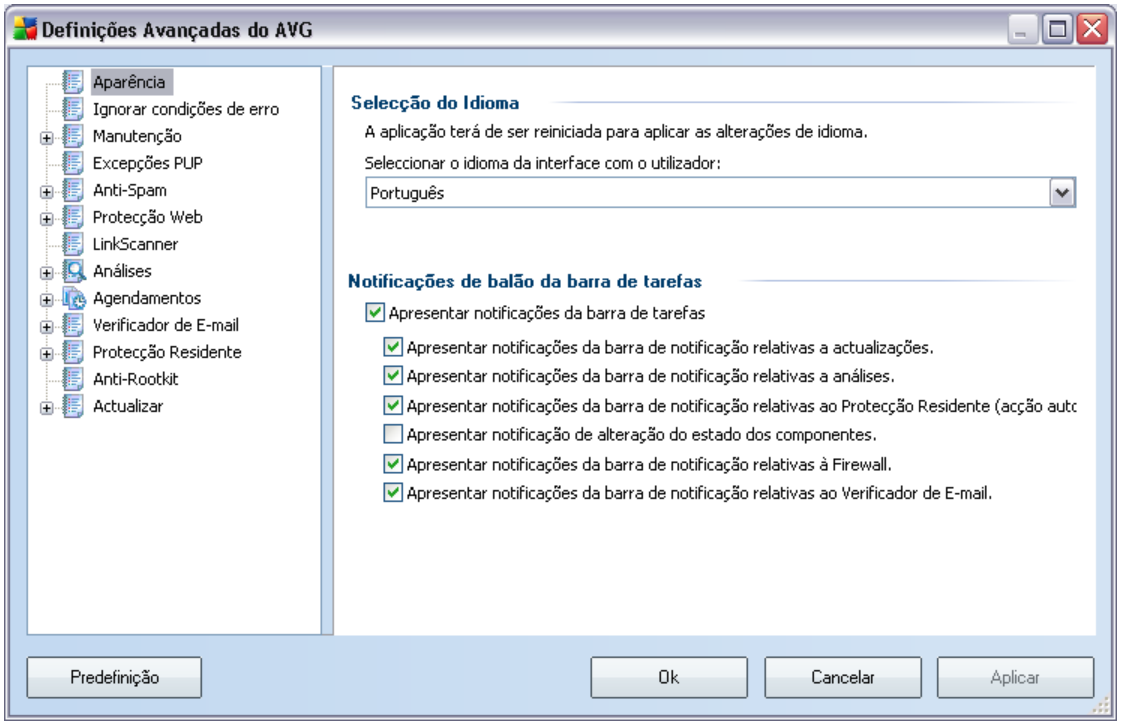
- ***Botão de informação AVG*** - providencia links para importantes informações de segurança localizadas no website da AVG (www.avg.com)

10. Definições Avançadas do AVG

A janela de configurações avançadas do**AVG 8.5 Anti-Vírus** abre uma nova janela com o nome ***Definições Avançadas do AVG***. A janela está dividida em duas secções: a parte esquerda disponibiliza uma navegação esquematizada em árvore às opções de configuração do programa. Seleccione o componente ao qual pretende alterar a configuração (*ou a parte especifica deste*) para abrir a janela de edição na janela na secção do lado direito.

10.1. Aparência

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



Selecção do Idioma

Na secção ***Selecção 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 - Selecção de Componentes). No entanto, para concluir a alteração de idioma da aplicação terá de reiniciar a interface do utilizador; siga os passos seguintes:

- Seleccione o idioma da aplicação pretendido e confirme a selecção clicando no botão ***Aplicar*** (canto inferior direito)
- Clique no botão ***OK*** para fechar a janela de edição ***Definições Avançadas do AVG***
- Feche a Interface do Utilizador do AVG via a opção do item menu de sistema ***Ficheiro/Sair***
- Volte a abrir a Interface do utilizador do AVG procedendo a uma das seguintes opções: duplo clique sobre o ícone do AVG na barra de notificação, duplo clique sobre o ícone do AVG no seu ambiente de trabalho, ou através do menu ***Iniciar/Todos os Programas/AVG 8.0/Interface do utilizador do AVG*** (consulte o capitulo***Aceder à Interface do Utilizador***). A interface do utilizador será então apresentada no idioma seleccionado.

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.
    - ***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;

- ***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;

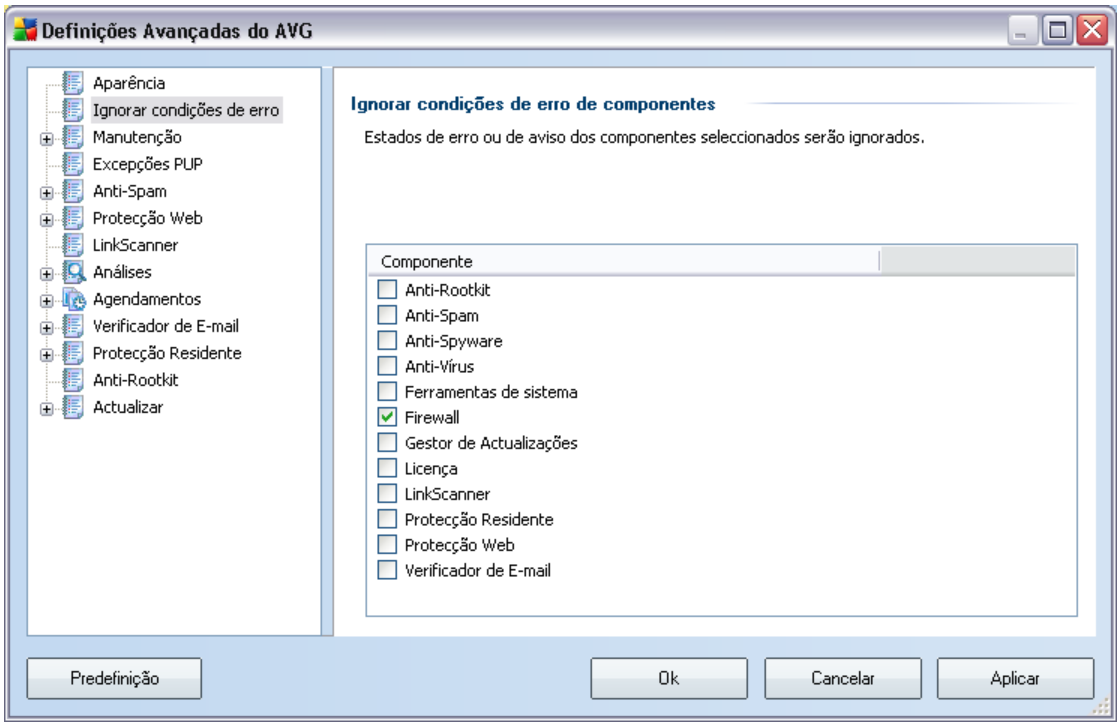
- ***Apresentar notificações da barra de notificação relativas à Protecção Residente*** - decide se as informações relativas a processos de guardar, copiar, e abrir ficheiros deverão ser apresentados ou suprimidos;

- ***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.

- ***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.

10.2. 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:

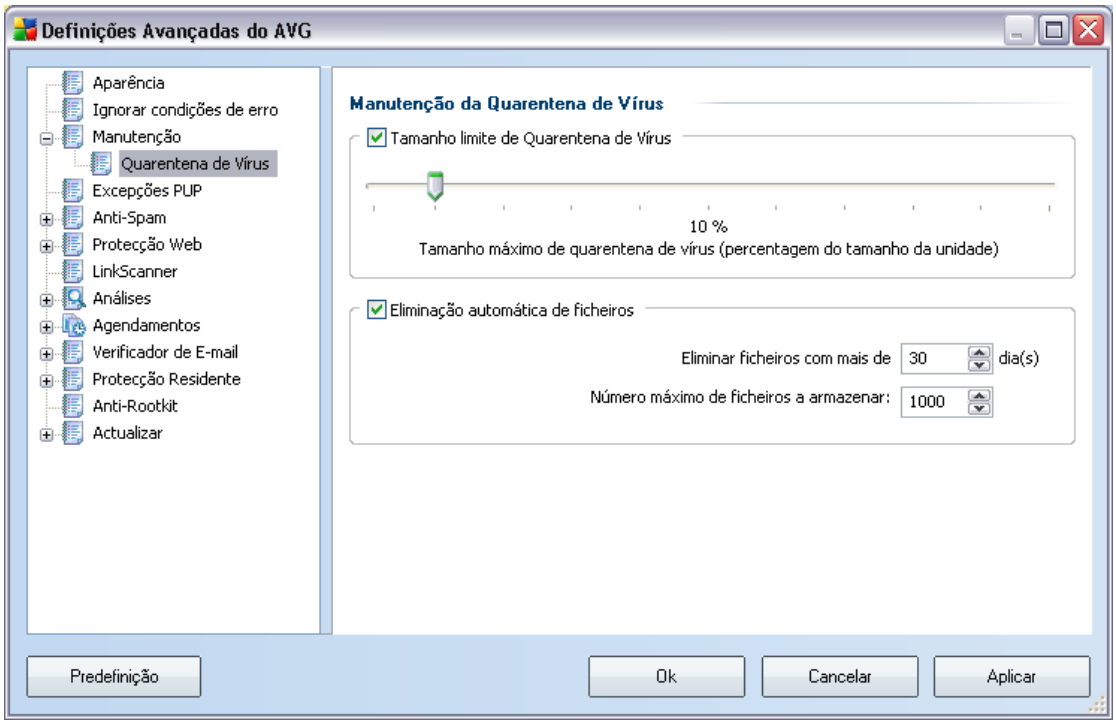
- ***ícone da barra de notificação*** - enquanto todas os componentes do AVG estiverem a funcionar devidamente o ícone é apresentado com quatro cores; no entanto, se ocorrer um erro, os ícones serão apresentados com um ponto de exclamação amarelo,
- uma descrição textual do problema existente na secção ***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.

10.3. Quarentena de Vírus



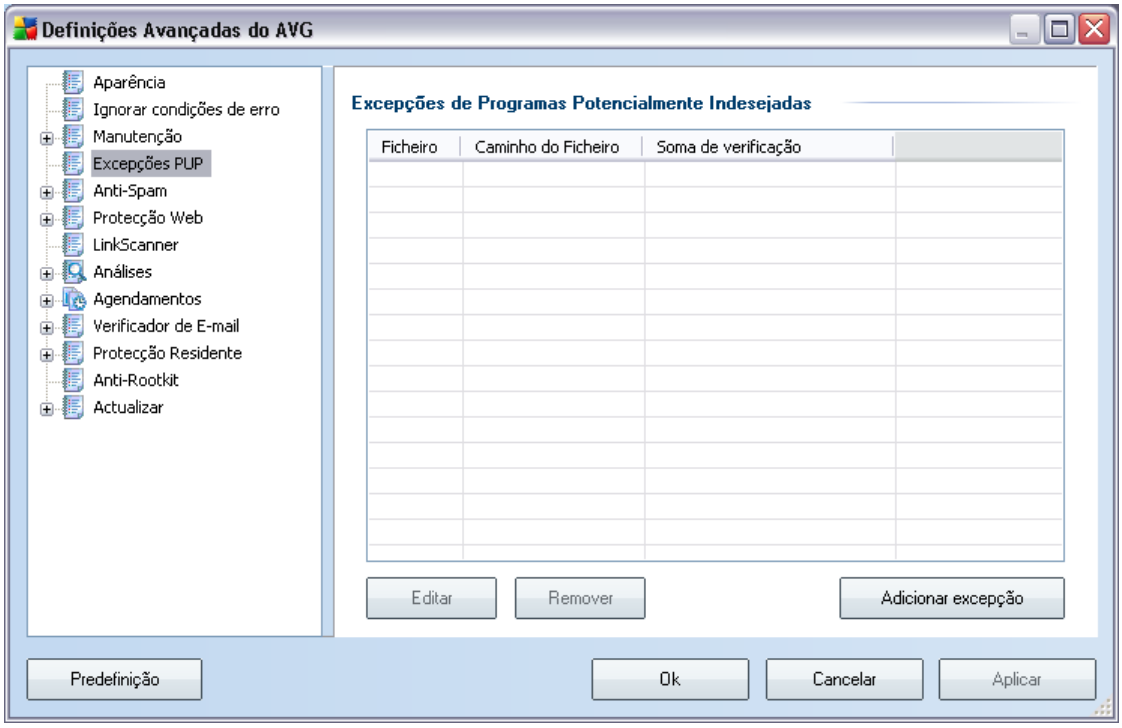
A janela ***Manutenção da Quarentena de Vírus*** permite-lhe definir vários parâmetros em relação à administração dos objectos armazenados na***Quarentena de Vírus***:

- ***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***)

10.4. Excepções PUP

O AVG 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:



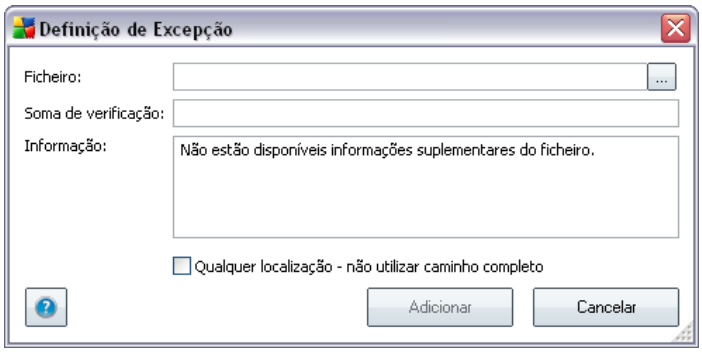
A janela das ***Excepções de Programas Potencialmente Indesejados*** apresenta uma lista de excepções actualmente válidas e já definidas de programas potencialmente indesejados. Pode editar, eliminar, ou adicionar uma nova excepção.

Botões de controlo

- ***Editar***- abre uma janela de edição (*idêntica à janela para definição de novas excepções, veja abaixo*) de uma excepção já definida, onde pode alterar os parâmetros de excepção

- ***Remover*** - elimina o item seleccionado da lista de excepções

- ***Adicionar excepção***- abre uma janela de edição onde pode definir os parâmetros da nova excepção a ser criada:



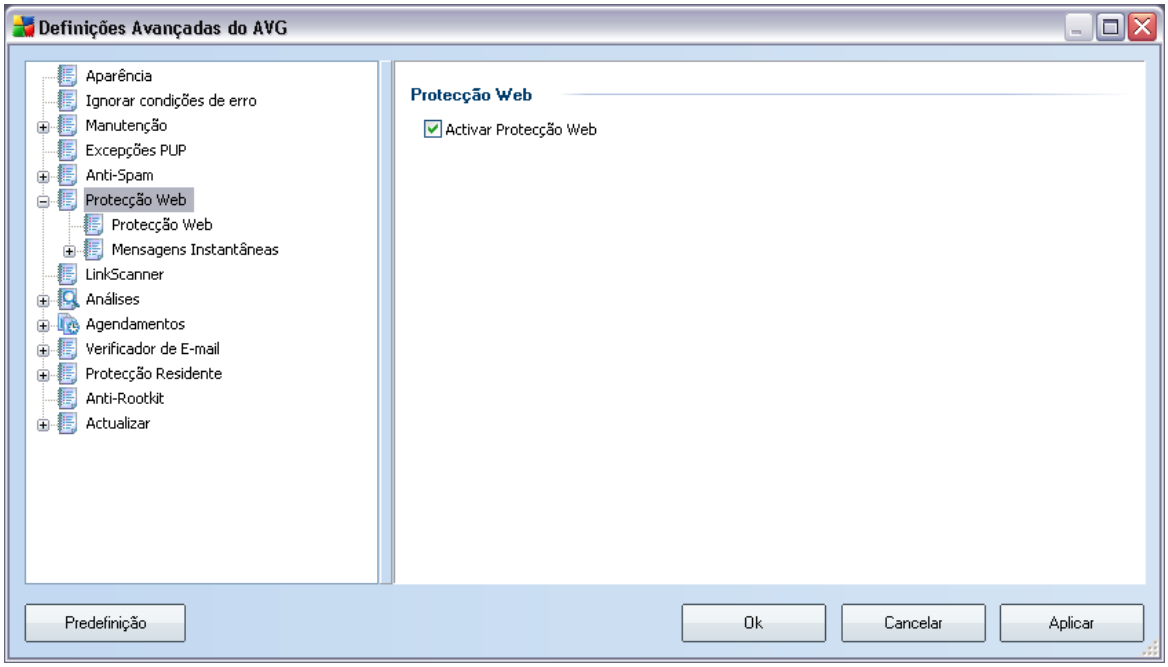
  - ***Ficheiro***- digite o caminho completo do ficheiro que pretende marcar como excepção

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

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

  - ***Qualquer localização - não utilize a localização completa*** - se pretender definir este ficheiro como uma excepção para a localização específica, deixe esta caixa de verificação desmarcada.

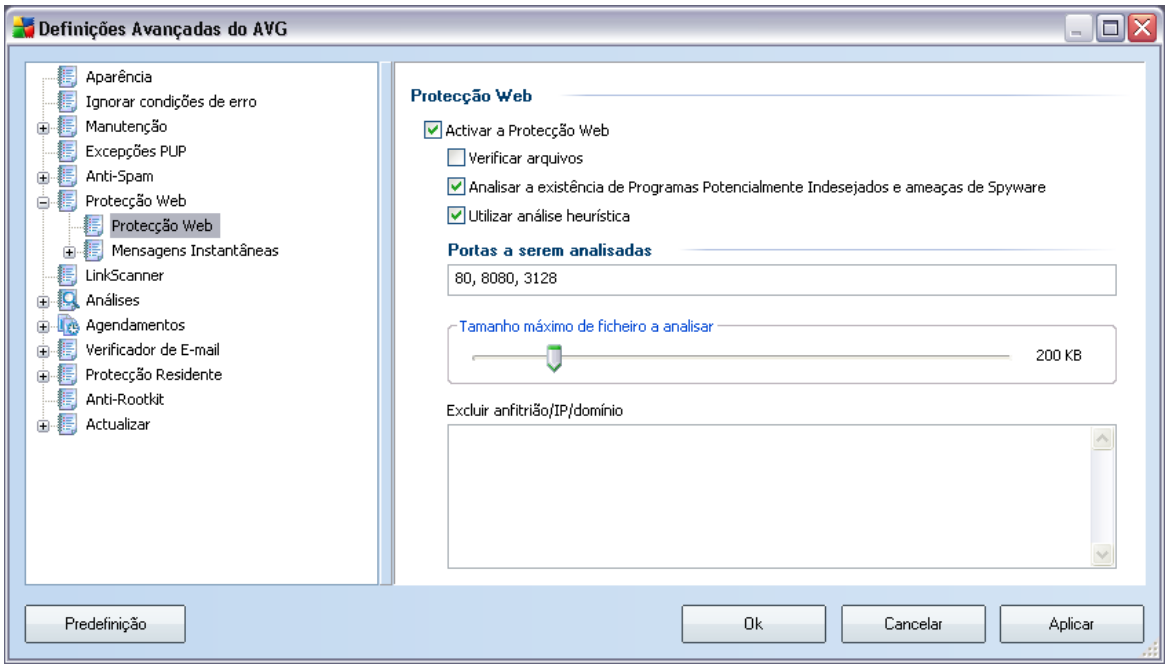
10.5. Protecção Web



A janela ***Protecção Web*** permite-lhe activar/desactivar na integra o componente ***Protecção Web*** (*activado por predefinição*). Para mais definições avançadas deste componente por favor continue para as janelas subsequentes conforme listado na árvore de navegação.

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 sinalização de ícone na barra de notificação.

10.5.1. 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:

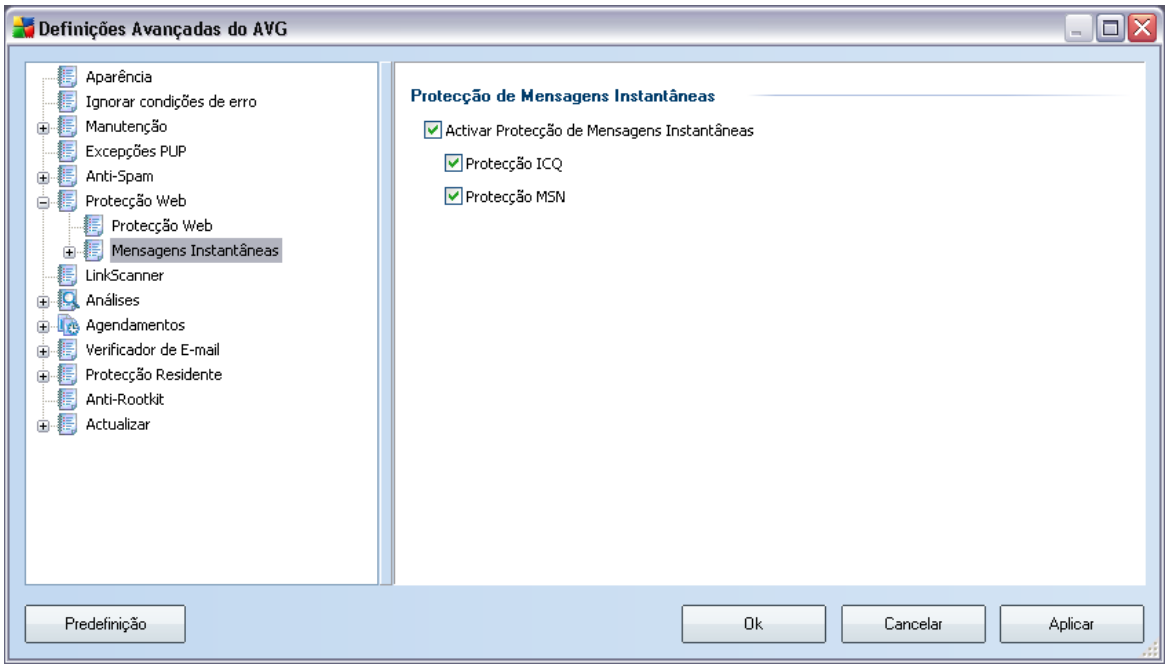
- ***Protecção na Internet*** - esta opção confirma que a***Protecção Web*** deve analisar o conteúdo das páginas www. Uma vez que esta opção está activada (*por predefinição*), pode ainda activar/desactivar estes itens:
    - ***Verificar arquivos*** - analisar o conteúdo de arquivos possivelmente incluídos na página www a ser apresentada .
    - ***Analisar Programas Potencialmente Indesejados e ameaças de Spyware*** - analisar programas potencialmente indesejados (*programas executáveis que podem funcionar como spyware ou adware*) incluidos na página www a ser apresentada, e infecções de spyware.
    - ***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*).

- ***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.

- ***Tamanho máximo de ficheiro a ser analisado*** - se os ficheiros incluidos 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 estaja para ser analisado com a***Protecção Web***. Mesmo que o ficheiro transferido seja superior ao tamanho especifcado, e como tal não será analisado pela Protecção Web, ainda está protegido: na eventualidade do ficheiro estar infectado, a ***Protecção Residente*** detectalo-á imediatamente.

- ***Excluir anfitrião/IP/domínio*** - pode digitar no campo de texto o nome exacto de um servidor(*anfitrião, endereço de IP, endereço de IP com máscara, ou URL*)ou um domínio que deverá ser analisado pelo ***Protecção Web***. Como tal, exclua somente anfitriões que tenha a certeza absoluta que nunca providenciarão conteúdo perigoso.

10.5.2. Mensagens Instantâneas

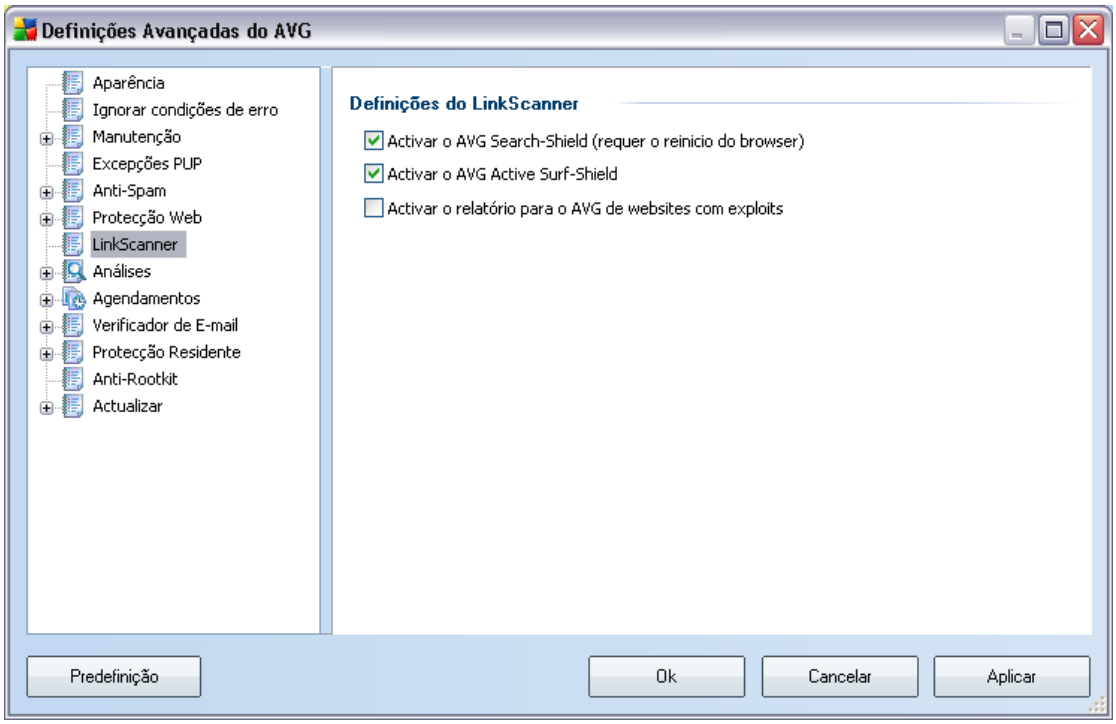


-

Na janela ***Protecção de Mensagens Instantâneas*** pode editar as definições dos componentes da ***Protecção Web*** relativos à análise de mensagens instantâneas. São actualmente suportados os três programas de mensagens instantâneas seguintes: ***ICQ***, ***MSN***, e ***Yahoo*** - seleccione o item respectivo para cada um deles se pretender que a Protecção Web 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***) e especificar a ***Lista Branca*** (*lista de utilizadores que poderão comunicar consigo*) e ***Lista Negra*** (*utilizadores que deverão ser bloqueados*).

10.6. Link Scanner



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

- ***Activar o Safe Search***- (*activado por defeito*): ícones de notificação de aviso em procuras efectuadas no Google, Yahoo, MSN ou Baidu tendo verificado antecipadamente o conteúdo dos websites apresentados pelo motor de busca.

- ***Activar a Navegação Segura***- (*activado por predefinição*): protecção activa (*em tempo real*): contra exploits de websites à medida que estes são acedidos. Ligações a websites maliciosos conhecidos e ao seu conteúdo são bloqueados à medida que são acedidos pelo utilizador via um Web browser (*ou qualquer outra aplicação que utilize HTTP*).

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

10.7. 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

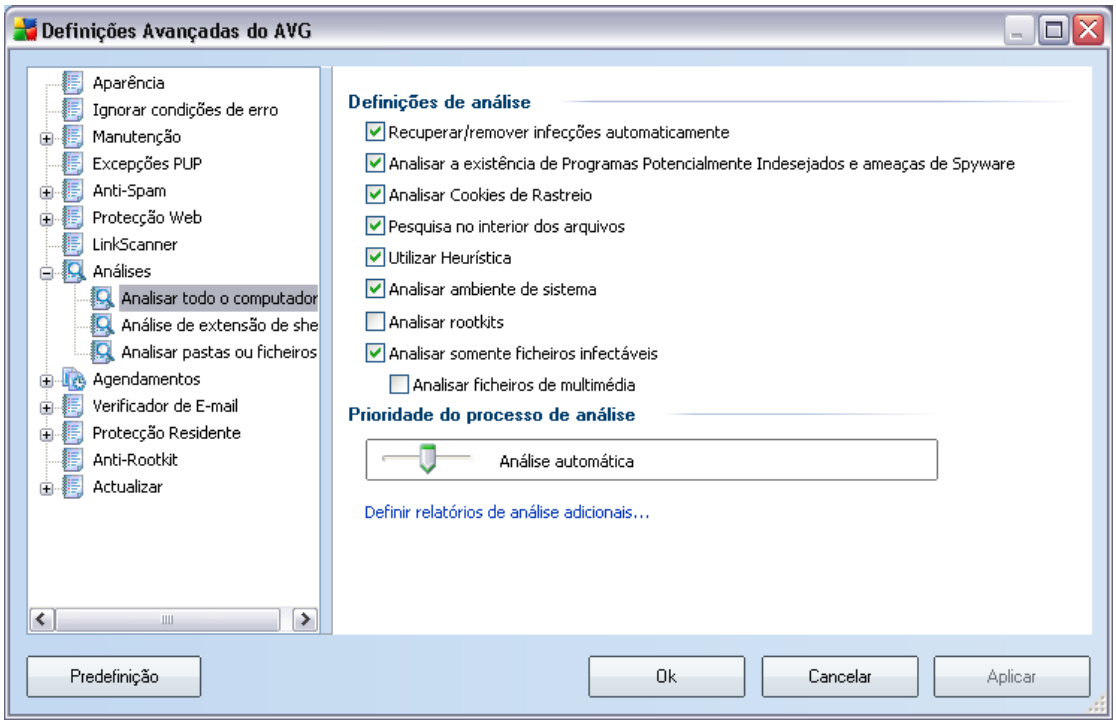
- ***Analise em Contexto*** - análise específica de um objecto seleccionado directamente no ambiente do Explorador do Windows

- ***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

10.7.1. 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. 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. O método recomendado é a remoção do ficheiro infectado para a Quarentena de Vírus.

- ***Analisar Programas Potencialmente Indesejados*** : este parâmetro controla a funcionalidade Anti-Vírusque permite adetecção de programas

potencialmente perigosos (*ficheiros executáveis que podem ser executados como spyware ou adware* e que podem ser bloqueados, ou removidos;

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

- ***Analisar no interior de arquivos*** - 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;

- ***Analisar a existência de rootkits*** - seleccione este item se pretender incluir a detecção de rootkits na análise de todo o computador. A detecção de rootkits também está disponível independentemente no componente ***Anti-Rootkit***;

- ***Analisar somente ficheiros infectáveis*** - com esta opção activada, os ficheiros que não podem ser infectados não serão analisados. Estes podem ser por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis.

    - ***Analisar ficheiros de multimédia*** -– seleccione a caixa para analisar ficheiros de multimédia (Vídeo, Áudio, etc.). Se deixar esta caixa desseleccionada reduzirá o tempo de análise ainda mais uma vez que os ficheiros são regra geral bastante grandes e é pouco provável que estejam infectados com vírus.

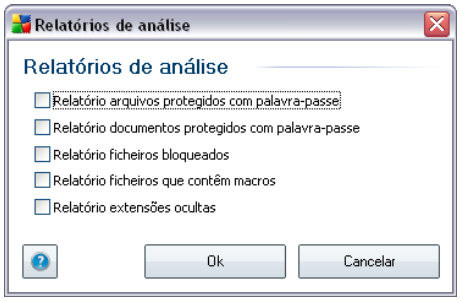
Prioridade do processo de análise

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 significantivamente

durante a sua execução, e diminuirá o desempenho de outras actividades no seu PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir a utilização dos recursos do sistema prolongando a duração da análise.

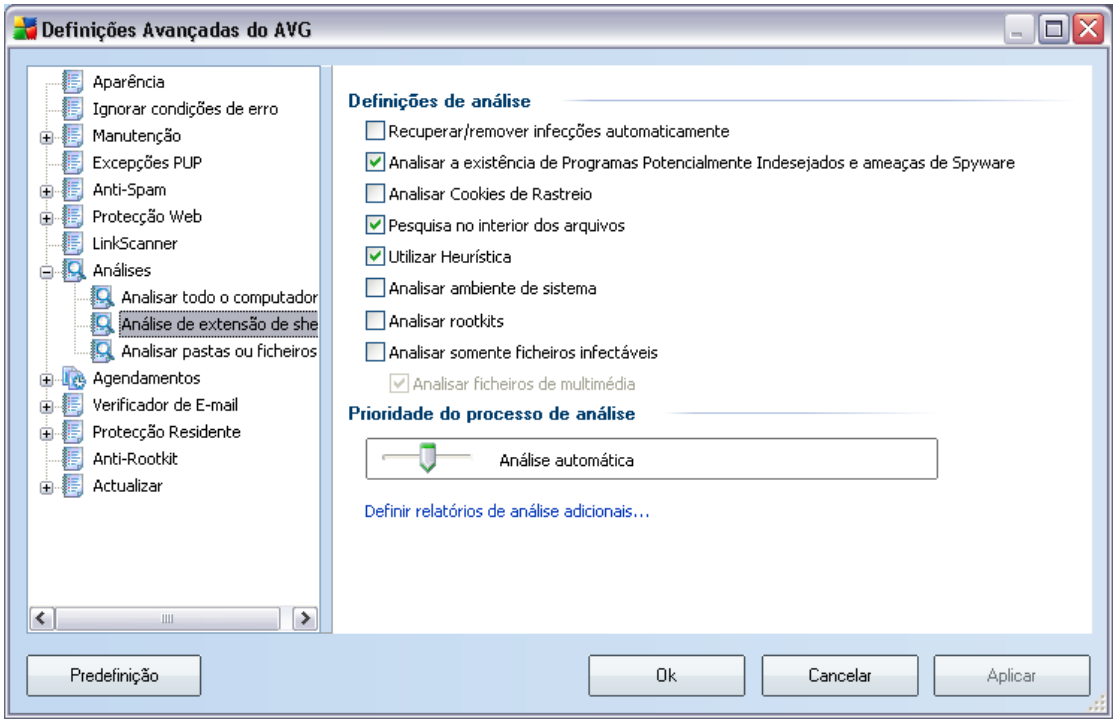
Definir relatórios de análise adicionais...

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



10.7.2. Análise em contexto

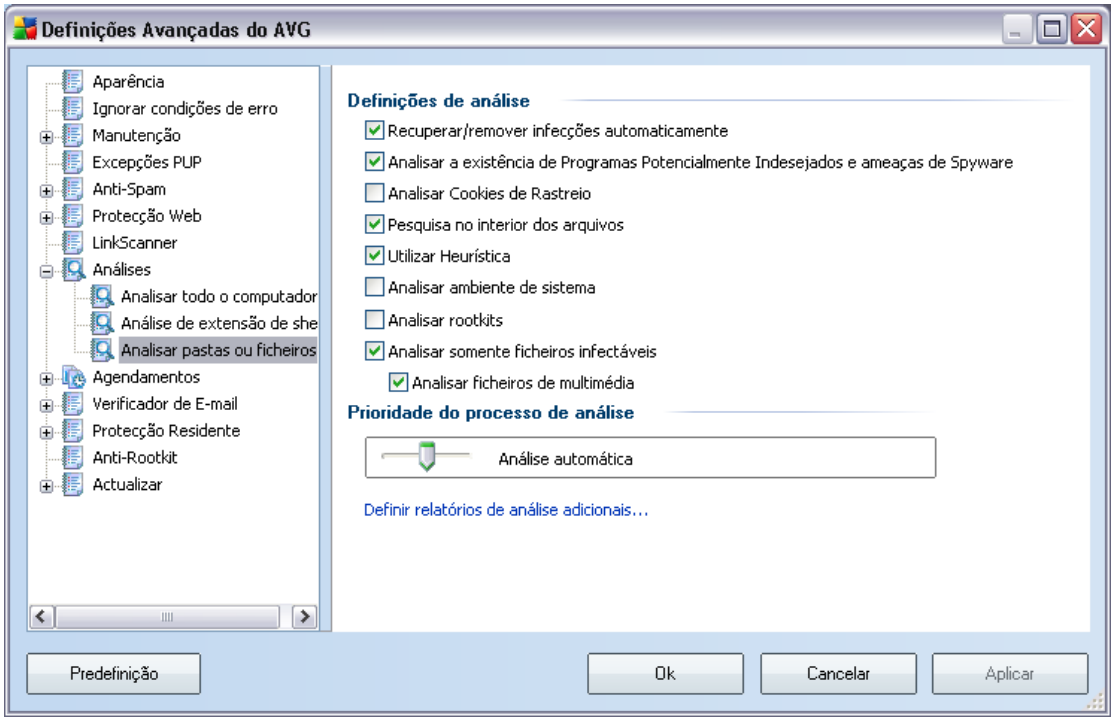
À semelhança do item anterior a análise ***Analisar todo o computador*** , este item apelidado ***Análise em Contexto***também oferece várias opções para edição da análise predefinida pelo fornecedor do software. Desta vez a configuração está relacionada com a análise de objectos específicos executada 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 em Contexto*** (***A analisar no Explorador do Windows*** só os parâmetros relevantes estão activados.

10.7.3. 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***:

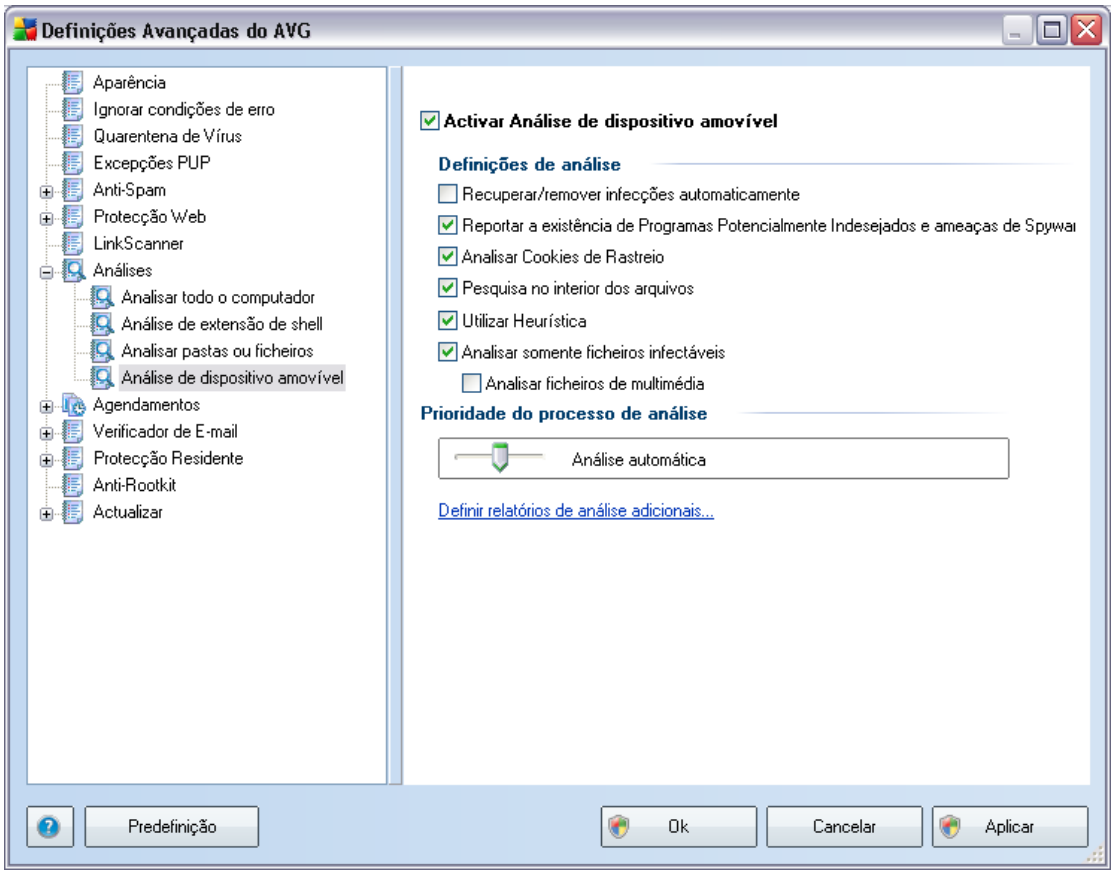


Todos os parâmetros definidos nesta janela de configuração aplicam-se apenas às áreas seleccionadas para análise com a ***Análise de ficheiros e pastas específicos***! Se seleccionar a opção ***Analisar pela existência de rootkits*** nesta janela de configuração, só será efectuado um teste rápido, ex. somente análise de rootkits das áreas seleccionadas.

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

10.7.4. 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*** *:*

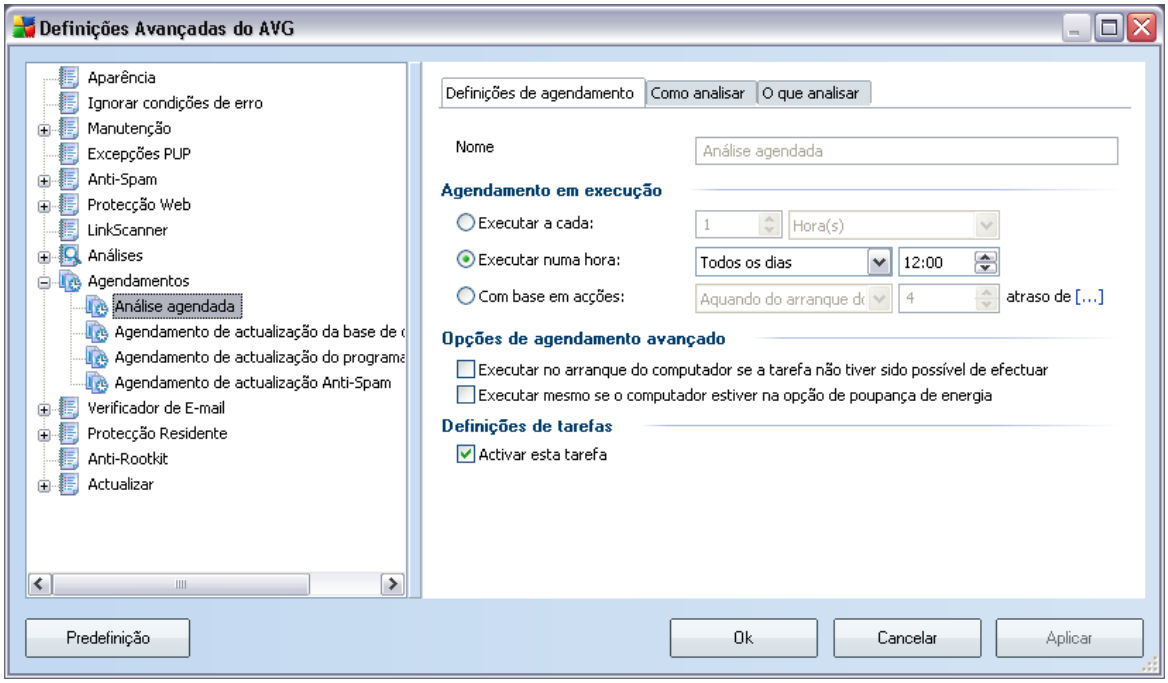
10.8. Agendamentos

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
- Agendamento de Actualização do Anti-Spam

10.8.1. Análise agendada

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



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

De seguida atribua um nome à análise que está em vias de criar e agendar. Digite o nome no campo de texto ao lado do item ***Nome***. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir.

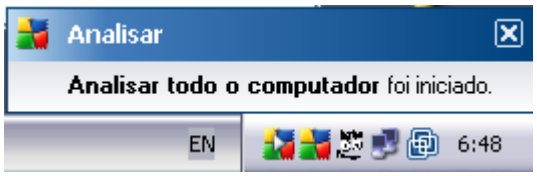
Exemplo:*Não é adequado nomear uma análise com o nome "Nova análise" ou "A minha análise" uma vez que estes nomes não referem o que a análise efectivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc. Também não é necessário especificar no nome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

Nesta janela pode ainda definir os seguintes parâmetros de análise:

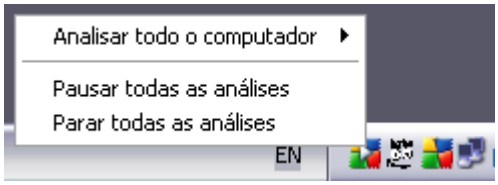
- ***Agendamento em execução*** - especifique os intervalos de tempo para a execução do novo agendamento de análise. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (***Executar a cada ...***ou definindo uma data e hora precisas (***Executar a uma hora específica ...***), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Acção baseada no arranque do computador***).

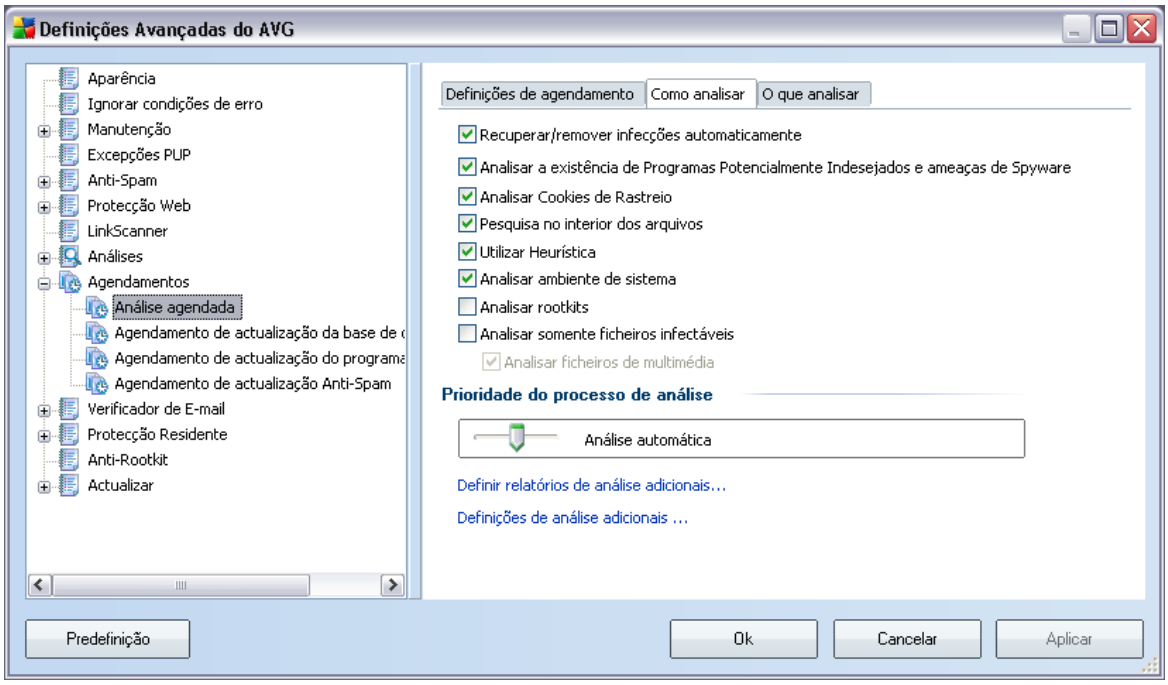
- ***Opções de agendamento avançado*** - esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

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 automaticamente/remover infecção*** - (*activado por predefinição*): se um vírus for detectado durante a análise pode ser recuperado automaticamente se houver uma cura disponível. Na eventualidade de o ficheiro infectado não poder ser recuperado automaticamente, ou se decidir desactivar esta opção, será notificado aquando da detecção de um vírus e terá de decidir o que fazer com a infecção detectada. A acção recomendada é a remoção do ficheiro infectado para a Quarentena de Vírus.

- ***Analisar Programas Potencialmente Indesejados*** - (*activado por predefinição*): este parâmetro controla a funcionalidade Anti-Vírus que permite a detecção de programas potencialmente perigosos (*ficheiros executáveis que podem ser executados como spyware ou adware* e que podem ser bloqueados, ou removidos;

- ***Analisar a existência de cookies*** - (*activado por predefinição*). este parâmetro do componente Anti-Spyware define que as cookies deverão ser detectadas durante a análise (cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação especifica dos utilizadores, tal como preferências em 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;

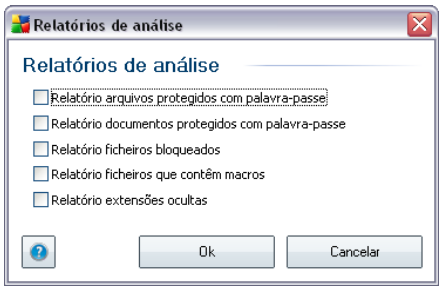
- ***Analisar a existência de rootkits*** - seleccione este item se pretender incluir a detecção de rootkits na análise de todo o computador. A detecção apenas de rootkits está disponível no componente ***Anti-Rootkit***;

- ***Analisar somente ficheiros infectáveis*** - (*desactivado por predefinição*): com esta opção activada, a análise não será aplicada a ficheiros que não podem ser infectados. Estes podem ser por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis.

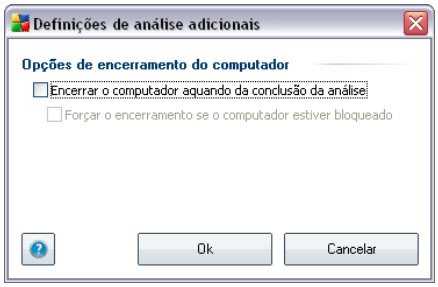
Na secção ***Prioridade do processo de análise*** pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. O valor desta opção está por predefinição definido para o nível médio de utilização automática de recursos. Se quiser que a análise seja executada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

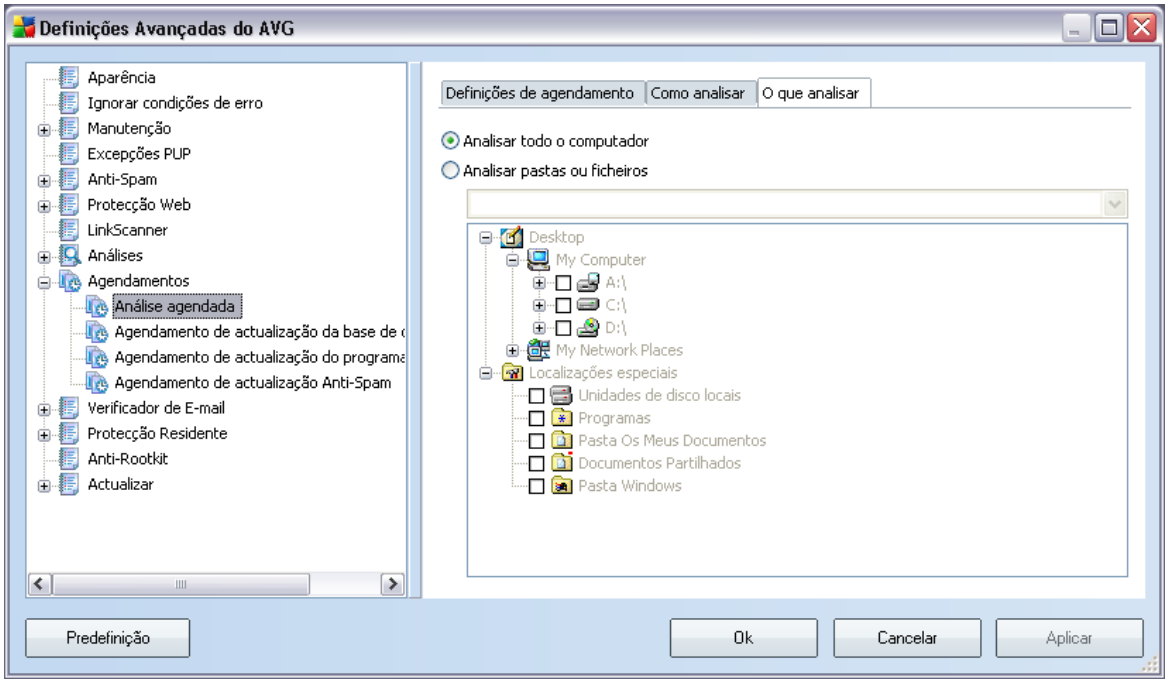
Clique no link ***Configurar relatórios de análise adicionais ...*** para abrir uma janela

independente apelidada ***Relatórios de análise*** onde pode seleccionar vários itens para definir quais as detecções que deverão ser reportadas:



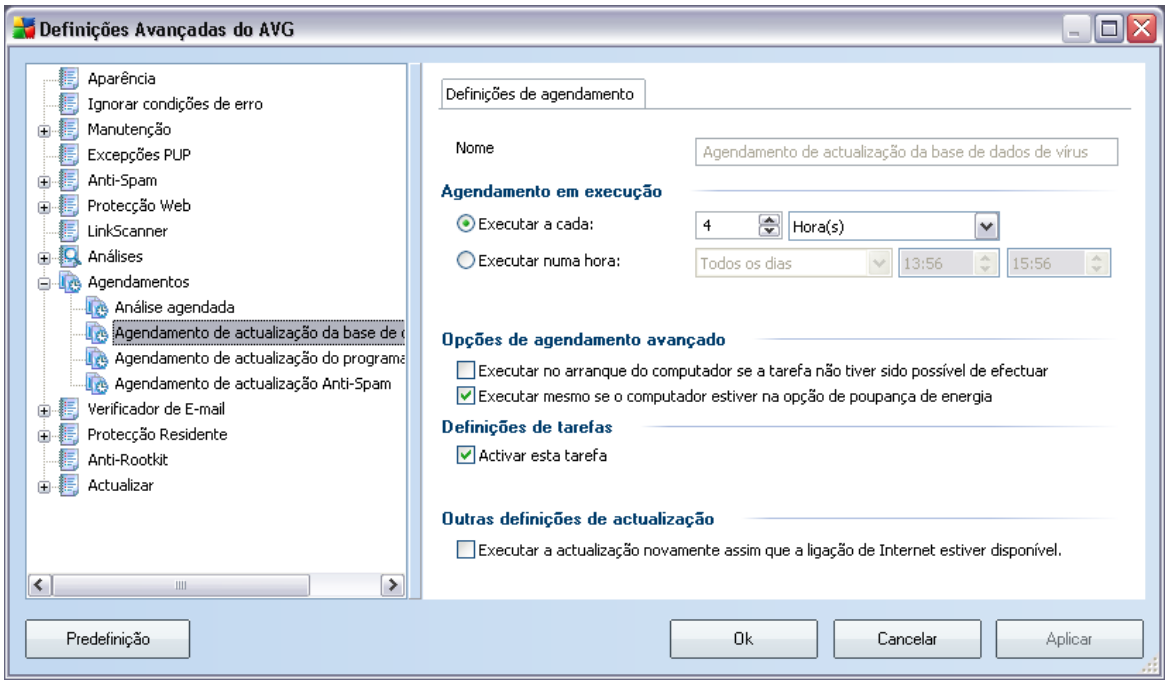
Clique nas ***Definições de análise adicionais...*** para abrir uma nova janela de ***Opções de encerramento do computador*** onde pode decidir se o computador deve ser encerrado automaticamente aquando do término do processo de análise. Tendo confirmado esta opção (***Encerrar o computador aquando do 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.

10.8.2. 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 esta previsto no componente ***Actualizações*** . Nesta janela pode configurar alguns parâmetros detalhados do agendamento de actualização da base de dados de vírus:

Atribua um nome ao agendamento de actualização da base de dados de vírus que vai criar. Digite o nome no campo de texto ao lado do item ***Nome***. Tente utilizar nomes curtos, descritivos e apropriados de agendamentos de actualização para que futuramente seja mais fácil distinguir os agendamentos de outros que venha a definir.

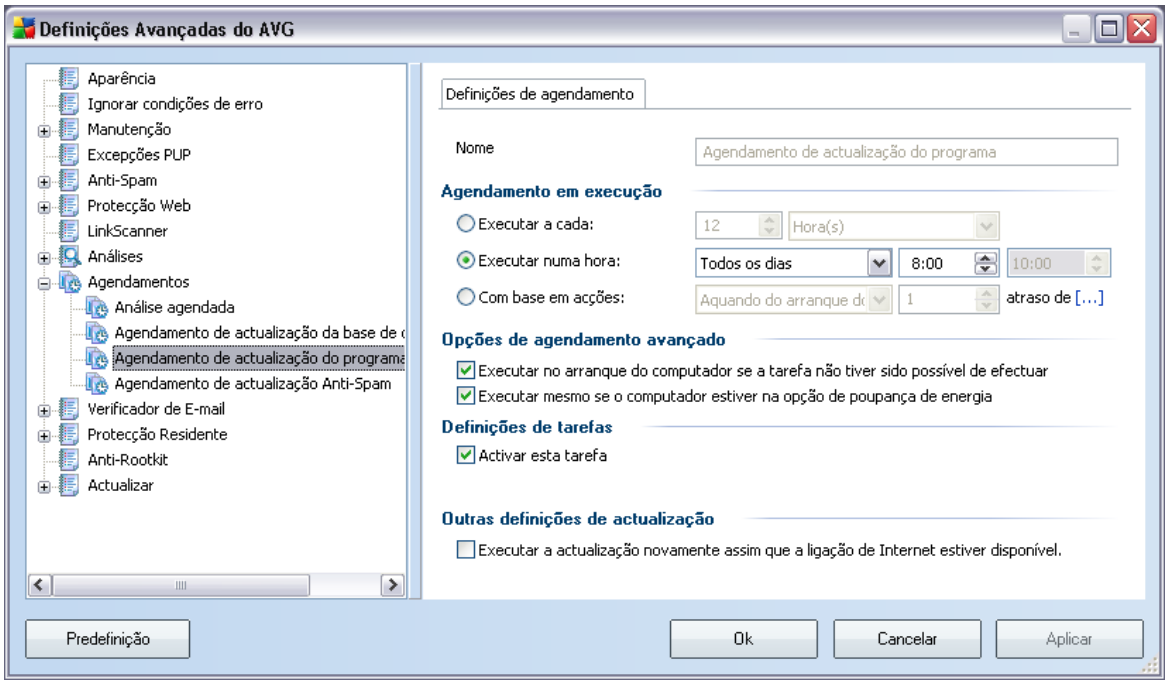
- ***Agendamento em execução*** - especifique os tempos de intervalo para a execução do novos agendamentos de actualização da base de dados de vírus. A temporização pode ser definida pela execução repetida da actualização após um determinado período de tempo (***Executar a cada ...***ou definindo uma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

- ***Opções de agendamento avançado*** - esta secção permite-lhe definir em que condições a actualização da base de dados de vírusdeverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

- ***Outras definições de actualização*** - seleccione esta opção para se certificar de que se a ligação à Internet ficar corrompida e o processo de actualização falhar, o mesmo será executado imediatamente assim que a ligação à Internet for restaurada.

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

10.8.3. Agendamento de actualização do programa



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.

De seguida, atribua um nome ao agendamento de actualização do programa que vai criar. Digite o nome no campo de texto ao lado do item ***Nome***. Tente utilizar nomes curtos, descritivos e apropriados de agendamentos de actualização para que

futuramente seja mais fácil distinguir os agendamentos de outros que venha a definir.

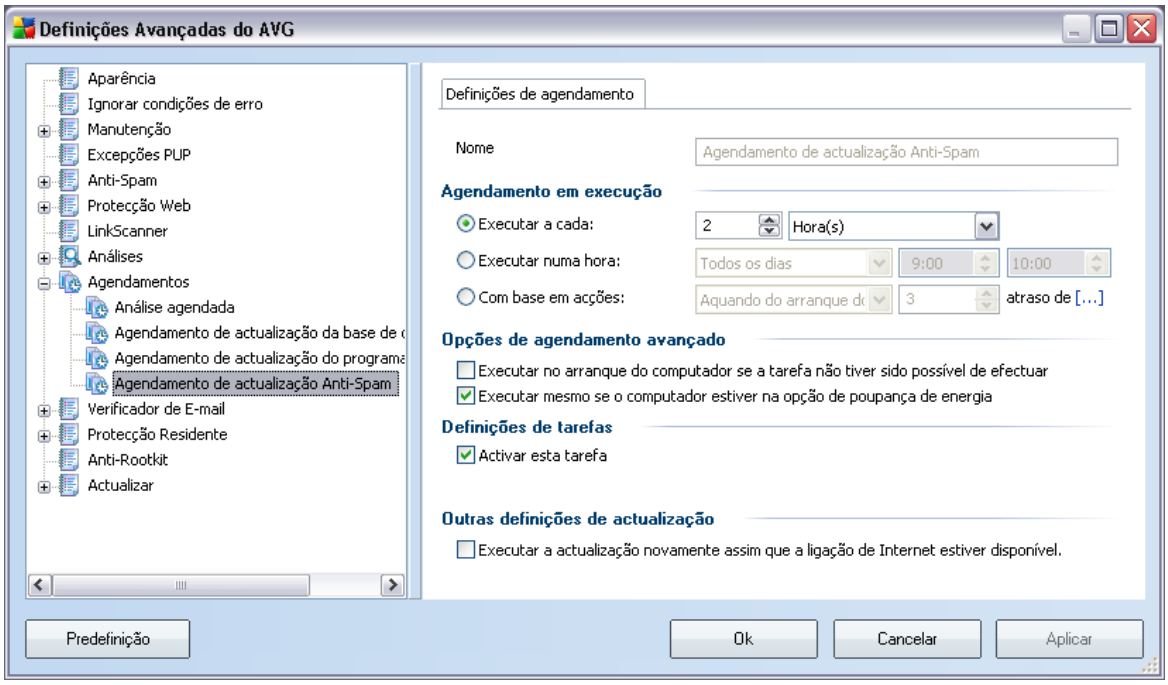
- ***Agendamento em execução*** - especifique os intervalos de tempo para a execução do novo agendamento de do programa. A temporização pode ser definida pela execução repetida da actualização após um determinado período de tempo (***Executar a cada ...***ou definindo uma data e hora precisas (***Executar a uma hora específica ...***), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Acção baseada no arranque do computador***).

- ***Opções de agendamento avançadas*** - 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*** - seleccione esta opção para se certificar de que se a ligação à Internet ficar corrompida e o processo de actualização do falhar, o mesmo será executado imediatamente assim que a ligação à Internet for restaurada.

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

10.8.4. Agendamento de Actualização do Anti-Spam



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

O agendamento de actualizações básicas do componente ***Anti-Spam*** está previsto no componente ***Actualizações*** . Nesta janela pode configurar alguns parâmetros detalhados do agendamento de actualização:

De seguida, atribua um nome agendamento de actualização do ***Anti-Spam*** que vai criar. Digite o nome no campo de texto ao lado do item ***Nome***. Tente utilizar nomes curtos, descritivos e apropriados de agendamentos de actualização para que futuramente seja mais fácil distinguir os agendamentos de outros que venha a definir.

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

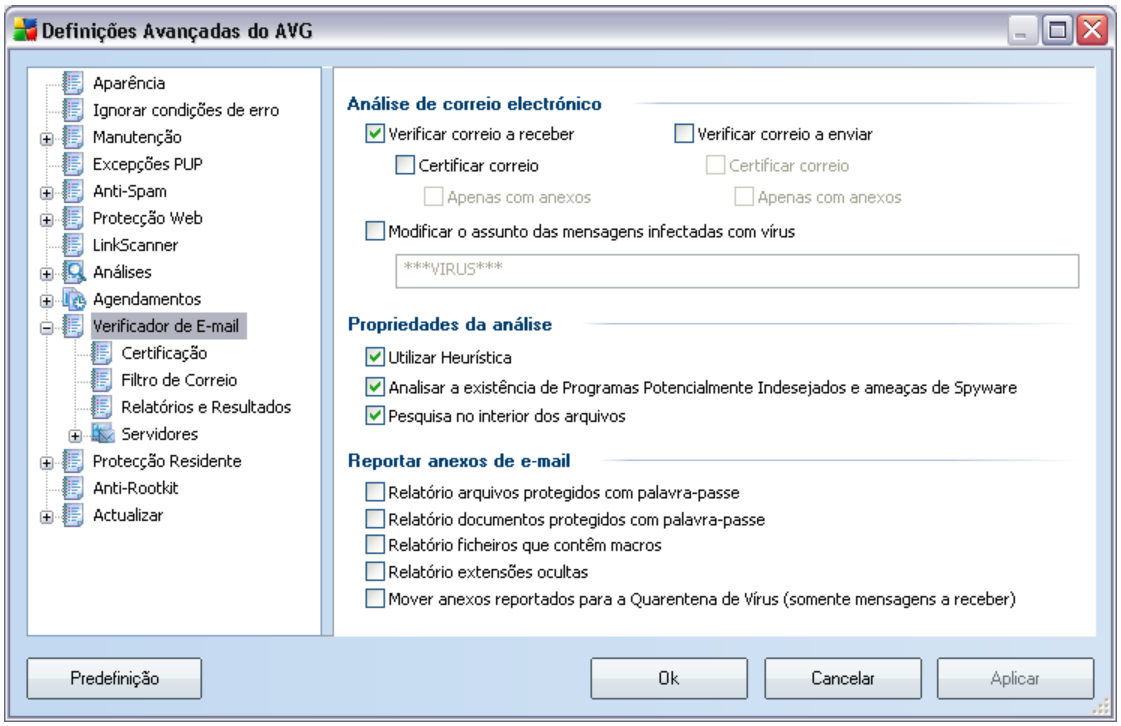
- ***Opções de agendamento avançado*** - esta secção permite-lhe definir em que condições a actualização do ***Anti-Spam*** deverá/não deverá ser executada se o computador estiver em modo de bateria fraca.

- ***Definições de tarefas*** - nesta secção pode desmarcar o item ***Activar esta tarefa*** para desactivar o agendamento de actualização do ***Anti-Spam*** temporariamente, e voltar a activá-lo conforme necessário.

- ***Outras definições de actualização*** - seleccione esta opção para se certificar de que se a ligação à Internet ficar corrompida e o processo de actualização do***Anti-Spamfalhar, o mesmo será executado imediatamente assim que a ligação à Internet for*** restaurada.

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

10.9. Verificador de E-mail



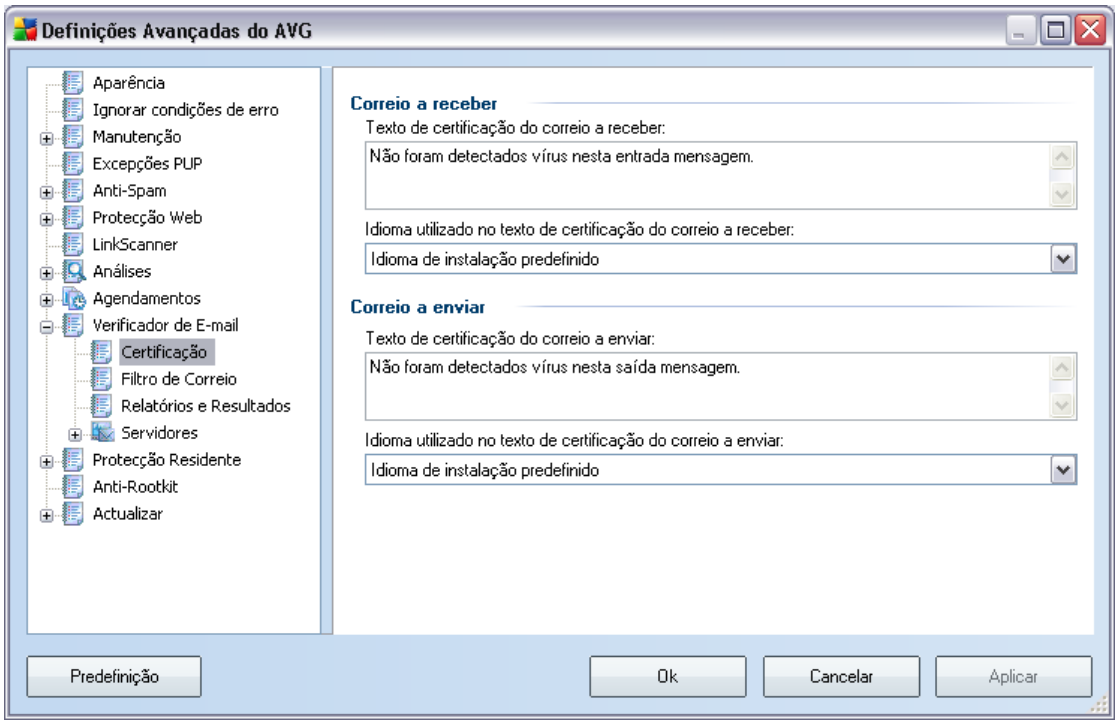
A janela ***Verificador de E-mail*** está dividida em três secções:

- ***Análise de e-mail***- nesta secção seleccione se pretende analisar as mensagens de e-mail a receber/a enviar e se todas as mensagens devem ser certificadas, ou somente as mensagens com anexos (*a certificação livre de vírus não é suportada no formato HTML/RTF*). Adicionalmente, pode seleccionar se pretende que o AVG modifique o assunto das mensagens que contêm potenciais vírus. Seleccione a caixa de verificação ***Modificar o assunto das mensagens infectadas com vírus*** e altere o respectivo texto (*o valor predefinido é ***VIRUS****).

- ***Propriedades de análise*** - especifique se o método análise heurística deve ser utilizado durante a análise (***Utilizar heurística***), se pretende verificar a presença de programs potencialmente indesejados (***Analisar Programas Potencialmente Indesejados***), e se os arquivos deverão ser igualmente analisados (***Analisar no interior de arquivos***).

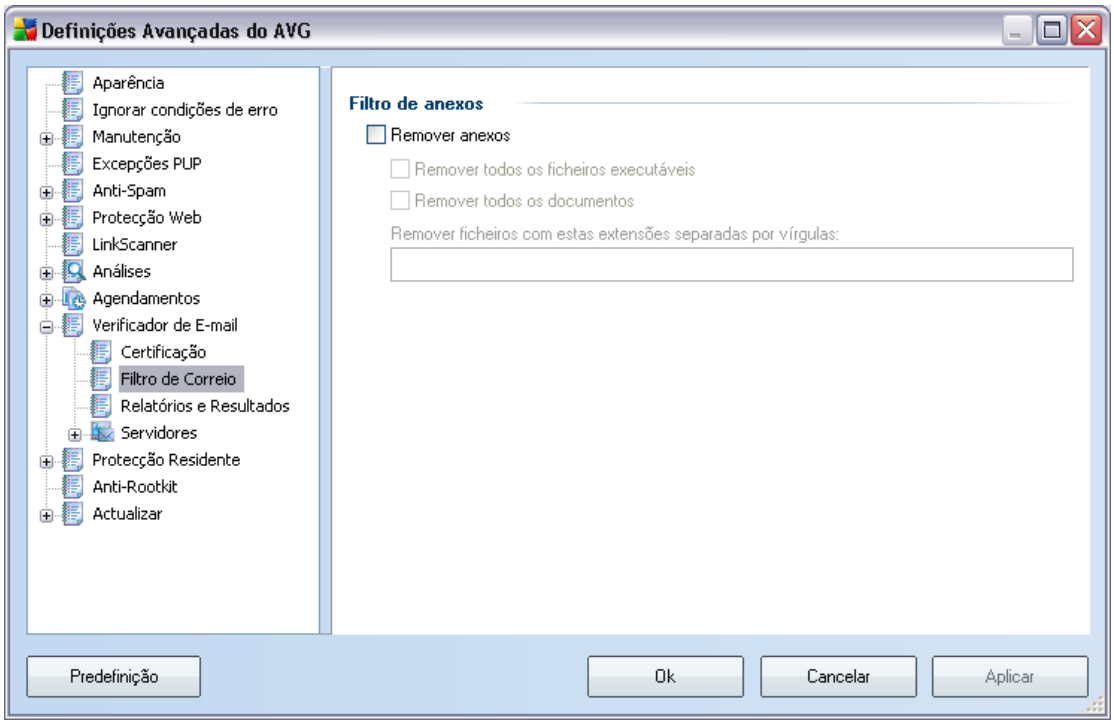
- ***Relatórios de anexos de e-mail*** - especifique se pretende ser notificado via e-mail acerca de arquivos protegidos com palavra-passe,documentos protegidos com palavra-passe, ficheiros que contenham macros e/ou ficheiros com extensões ocultas detectadas como anexos das mensagens de e-mail analisadas.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

10.9.1. 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*** e***e-mail a enviar***.

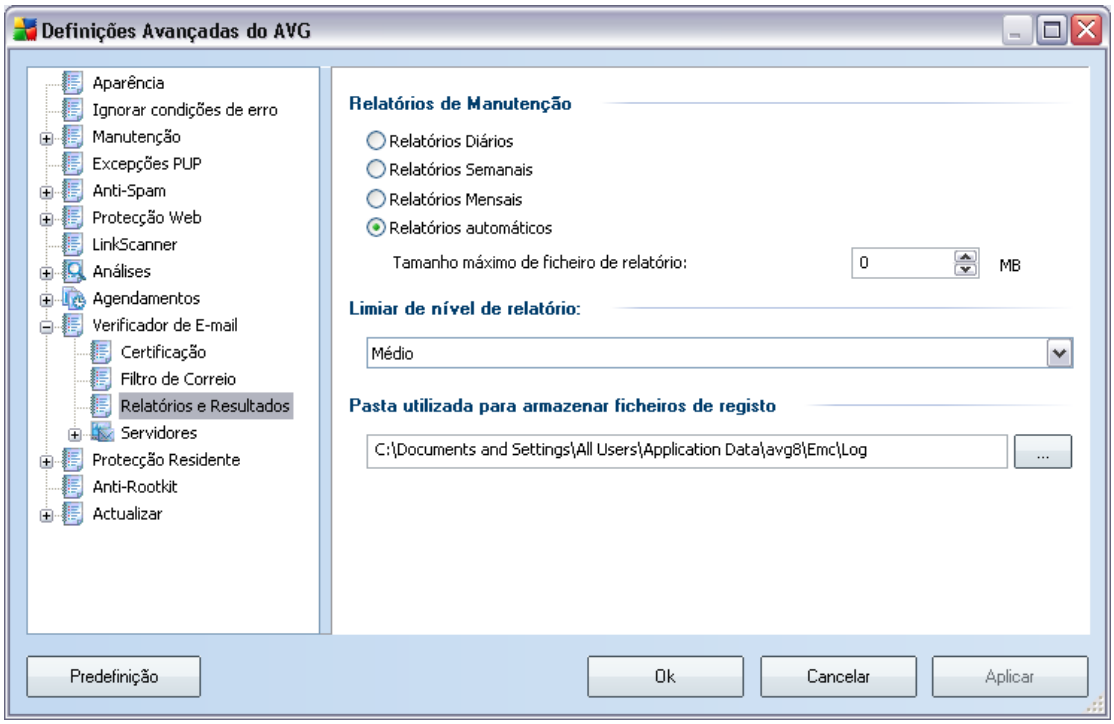
10.9.2. Filtro de E-mail



A janela ***Filtro de anexos*** permite-lhe configurar parâmetros parta 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 especificos de anexos que podem ser removidos, seleccione a opção respectiva:

- ***Remover todos os ficheiros executáveis*** - todos os ficheiros *.exe serão eliminados
- ***Remover todos os documentos*** - todos os ficheiros *.doc serão eliminados
- ***Remover ficheiros com estas extensões*** - removerá todos os ficheiros com as extensões definidas

10.9.3. Relatórios e Resultados

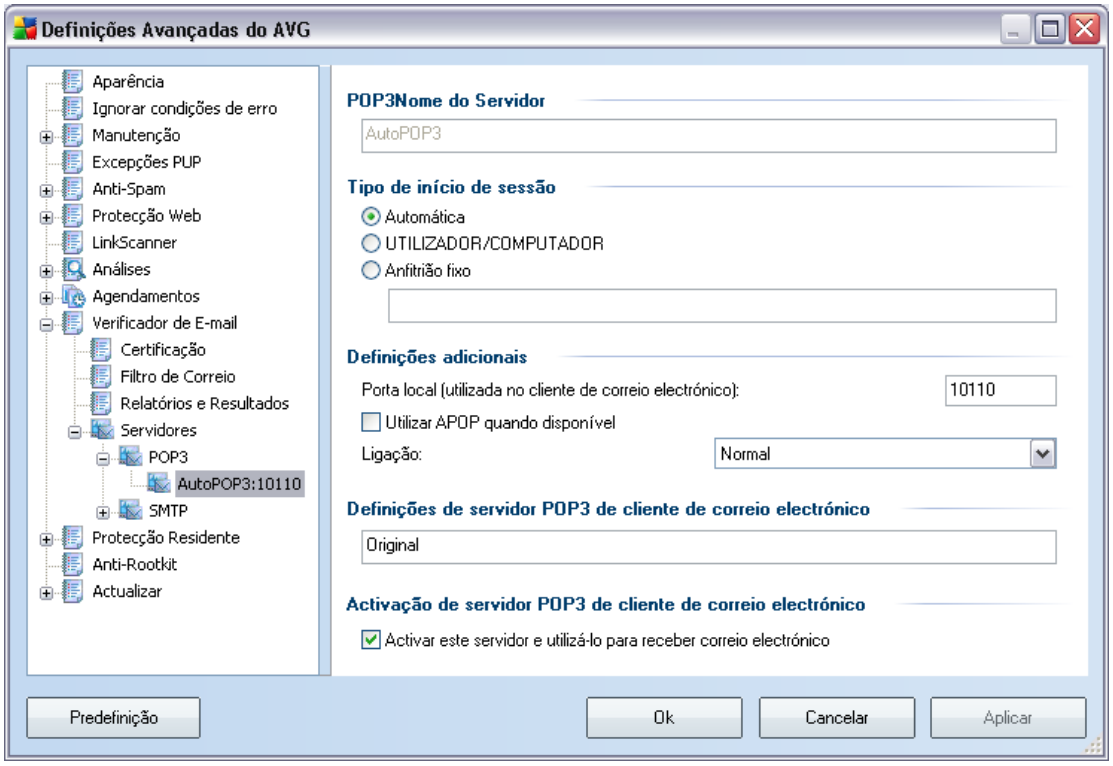


A janela aberta através do item de navegação ***Relatórios e Resultados*** permite-lhe especificar parâmetros para a manutenção dos resultados de análise de e-mail. A janela de diálogo está dividida em várias secções:

- ***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

10.9.4. 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 inicio de sessão***- define o método para determinar o servidor de e-mail utilizado para e-mail a receber:
    - Automático- o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
    - UTILIZADOR/COMPUTADOR- O método mais simples e mais utilizado para determinar o servidor de e-mail 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.

- Anfitriões fixos- Neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. O nome de início de sessão permanece inalterado. Para um nome, pode utilizar um nome de domínio (por exemplo, pop.acme.com) e um endereço IP (por exemplo, 123.45.67.89). Se o servidor de e-mail utilizar uma porta não padrão, pode especificar esta porta a seguir ao nome do servidor, utilizando uma vírgula como delimitador (por exemplo, pop.acme.com:8200). A porta padrão para comunicação POP3 é 110.

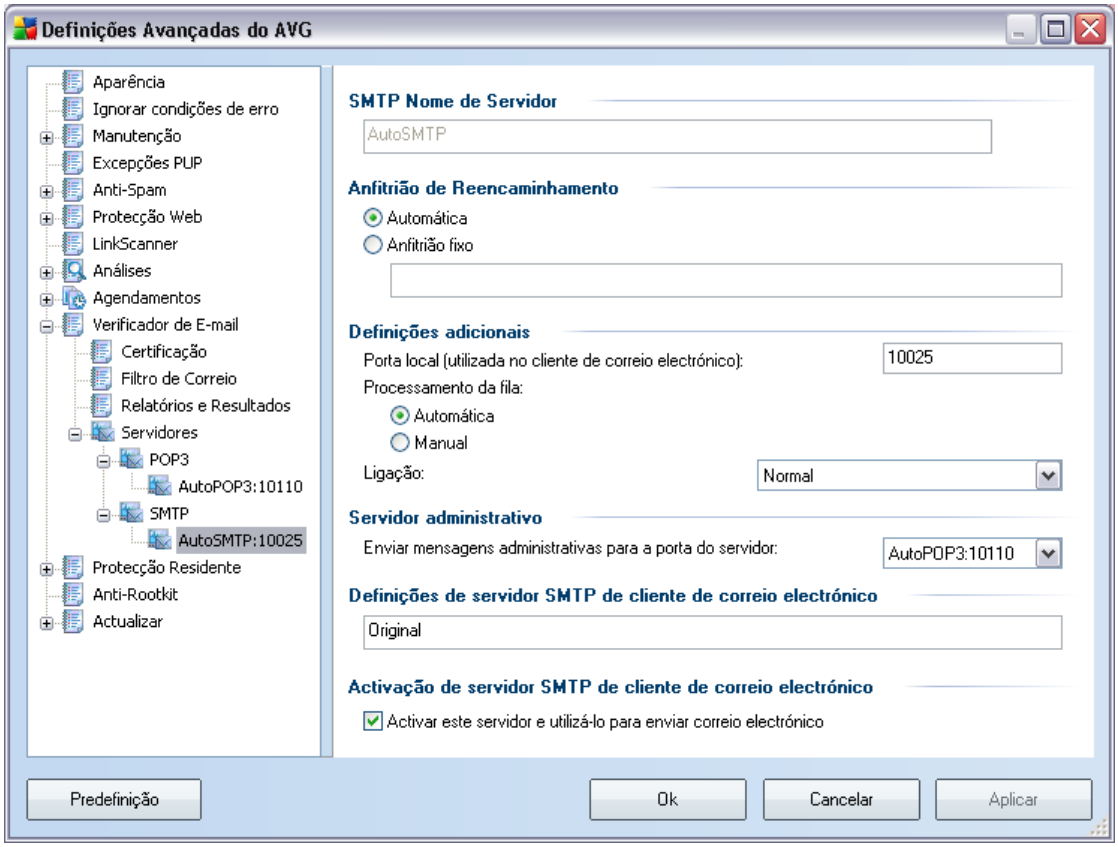
- ***Definições adicionais*** - especifica parâmetros mais detalhados:

  - Porta local - especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação POP3.

  - Utilizar APOP quando disponível - esta opção proporciona um inicio de sessão no servidor de e-mail 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.

  - 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 estará disponível se o servidor de e-mail de destino a suportar.

- ***Activação de servidor POP3 de 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.



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 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 Fixed host - 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 de fila -determina o comportamento do ***Verificador de E-mail*** aquando do processamento dos requisitos para o envio de mensagens de e-mail:

☼ 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

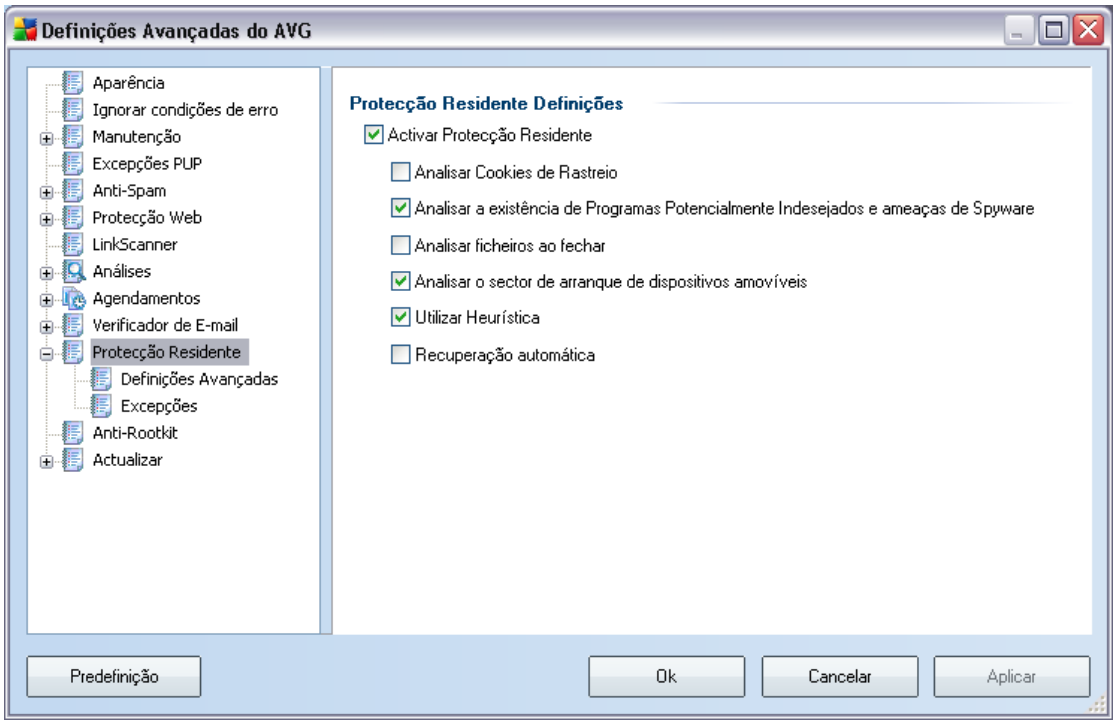
o Ligação - na lista de opções pode especificar que tipo de ligação utilizar (normal/SSL/SSL predefinida). Se seleccionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só está disponível se o servidor de e-mail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

10.10. 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 cookies*** - 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*)

- ***Analisar Programas Potencialmente Indesejados*** - (*activado por predefinição*) analisar pela existência de programas potencialmente indesejados (*aplicações executáveis que podem comportar-se como vários tipos de spyware ou adware*)

- ***Analisar ao fechar processos*** - análise ao fechar processos 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

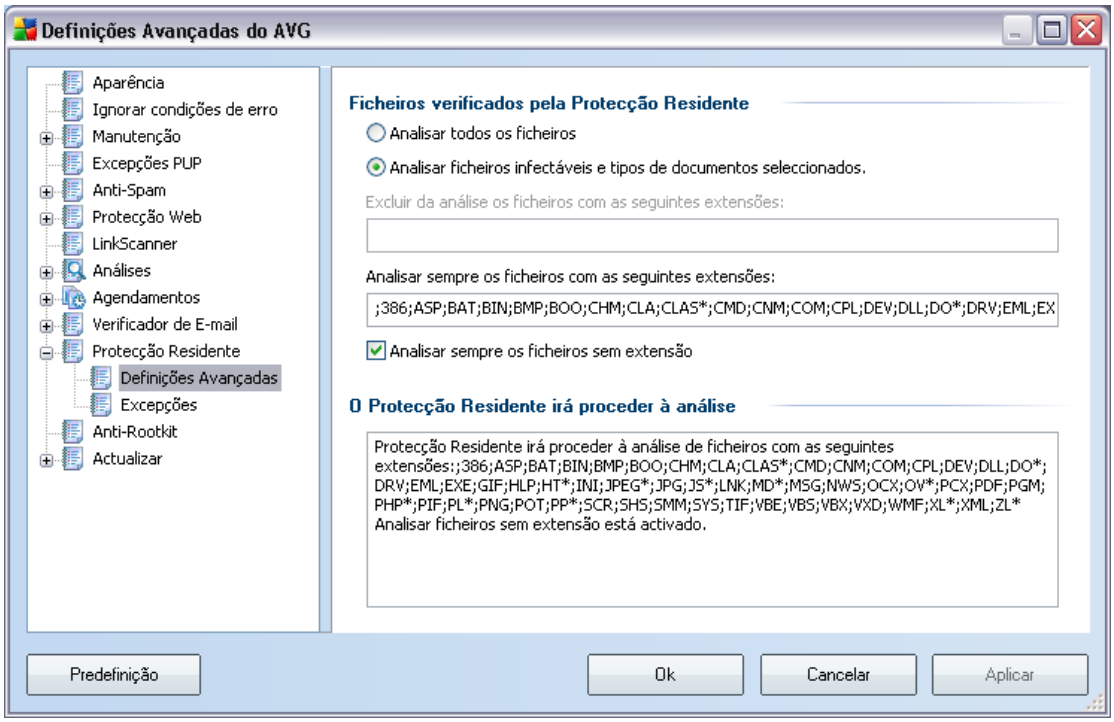
- ***Analisar o sector de arranque de discos amovíveis***- (*activado por predefinição*)

- ***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

10.10.1. Definições Avançadas

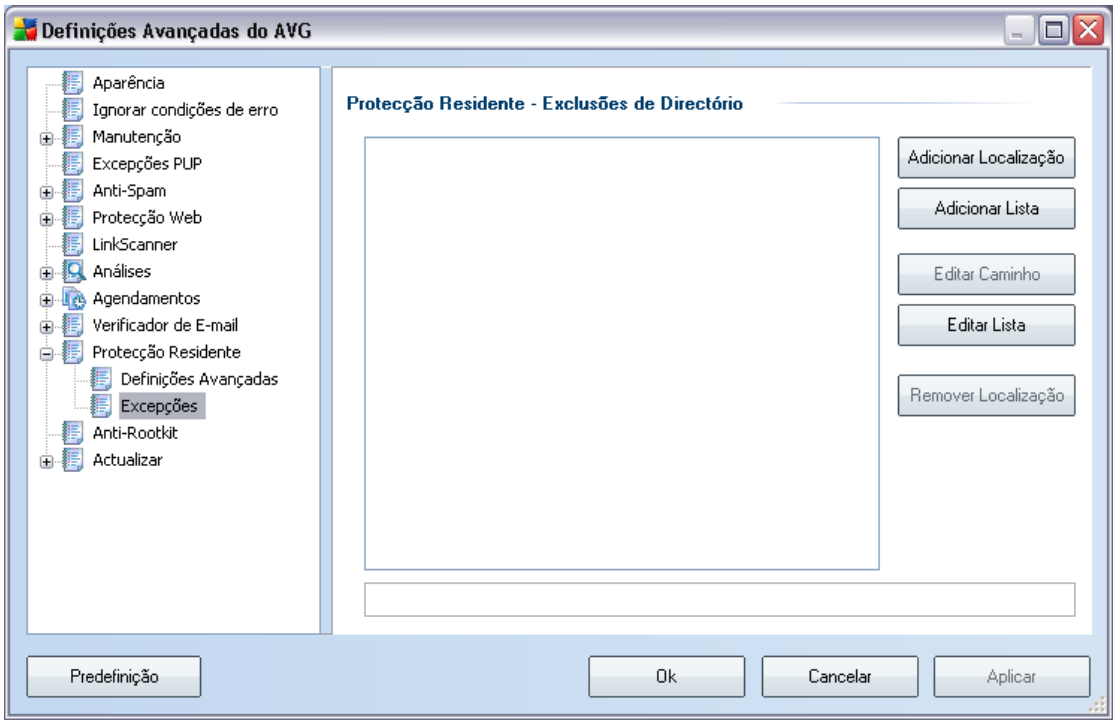
Na janela ***Ficheiros verificados pela Protecção Residente*** é possível configurar os ficheiros a analisar*em termos de extensões*):



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.

10.10.2. Excepções



A janela ***Protecção Residente - Exclusões de Directórios*** oferece a possibilidade de definir as pastas que devem ser excluidas da análise do ***Protecção Residente***. Se não for estritamente necessário, recomenda-se vivamente que não exclua directórios!

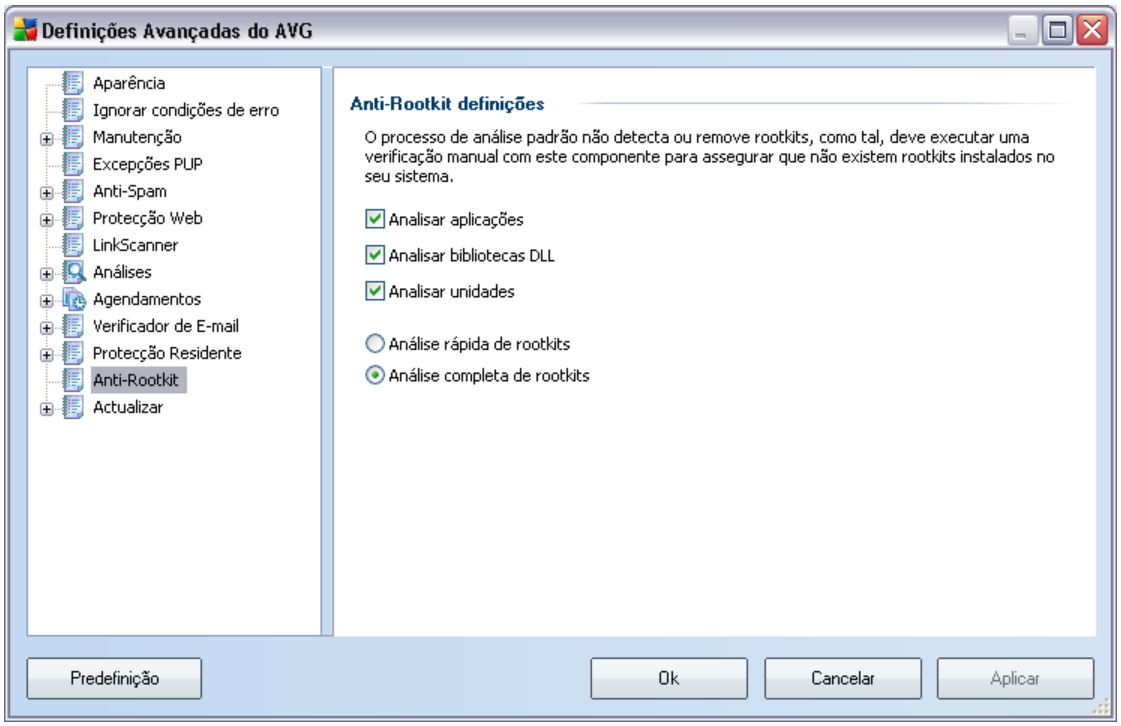
A janela inclui os seguintes botões de controlo:

- ***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. Anti-Rootkit

Nesta janela pode editar a configuração do componente ***Anti-Rootkit***:



Editar todas as funções do componente ***Anti-Rootkit conforme dispostas nesta janela também é acessível directamente a partir da interface do componente Anti-Rootkit*** .

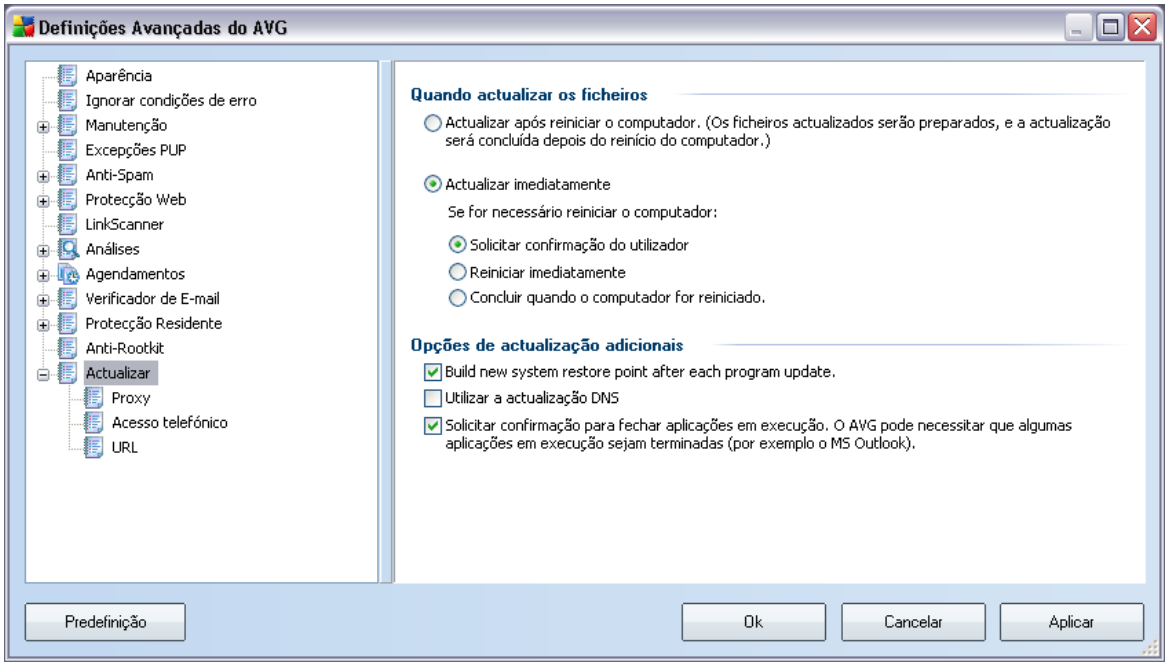
Primeiro, seleccione as caixas de verificação respectivas para especificar objectos que devem ser analisados:

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

Posteriormente pode escolher o modo de análise de rootkits:

- ***Análise rápida de rootkits*** - analisa somente a pasta sistema *regra geral localizada em c:\Windows*)
- ***Análise completa de rootkits*** - analisa todos os ciscos acessíveis com a excepção de A: e B:

10.12. 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 actualizaçãopode 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.

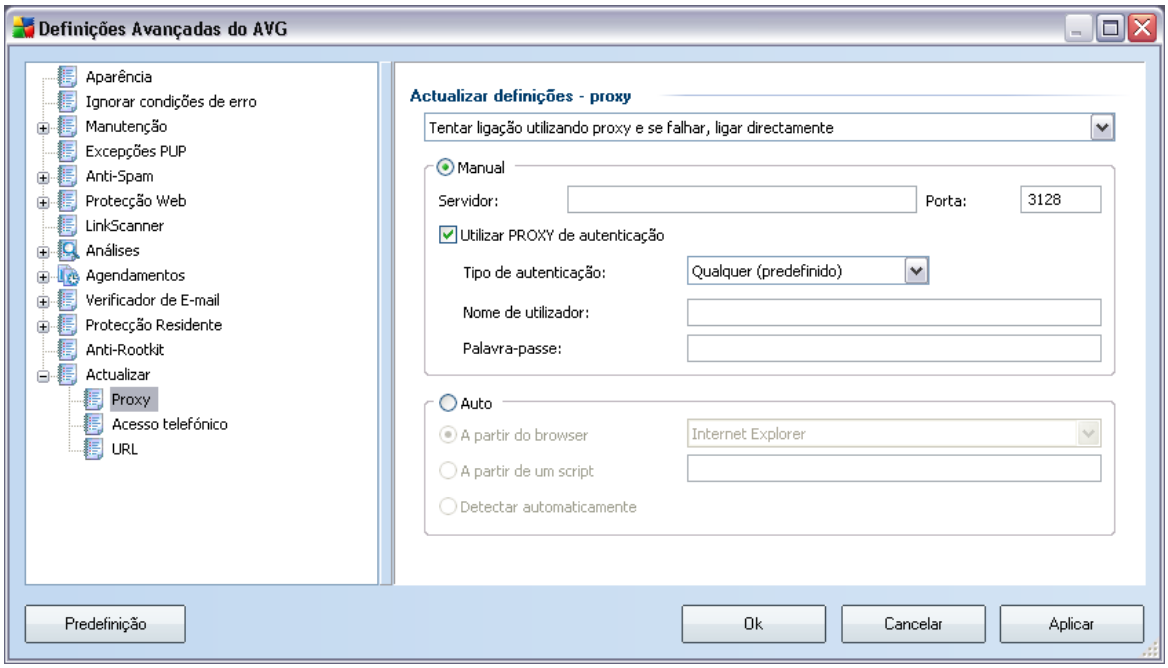
Se decidir manter a configuração predefinida e executar o processo de actualização imediatamente, pode especificar as circunstâncias em que um possível reinicio deverá ser efectuado:

- ***Requerer confirmação ao utilizador*** - ser-lhe-á pedido que aprove um reinicio do PC necessário para finalizar o processo de actualização
- ***Reiniciar imediatamente*** - o computador será reiniciado automaticamente após oprocesso 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

Opções de actualização adicionais

- ***Criar un 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.

10.12.1. 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 utilizar servidor proxy***
- ***Tentar ligação utilizando proxy e se falhar, ligar directamente*** - definições padrão

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

Configuração manual

Se selecionar 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*)

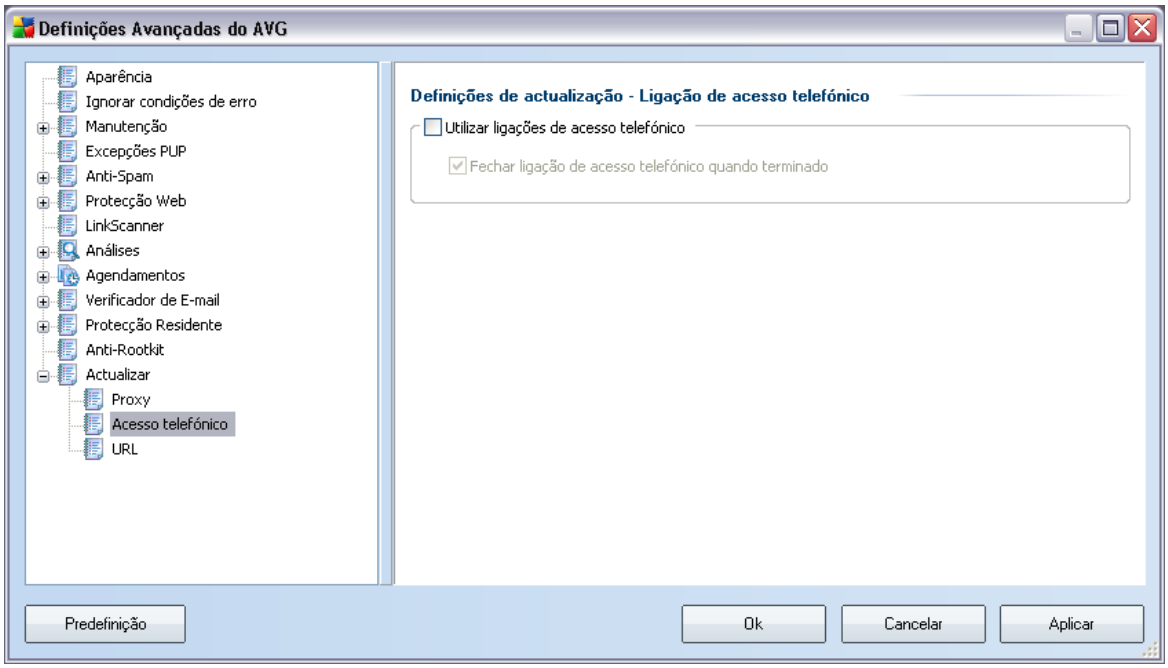
O servidor proxy também pode ter regras específicas configuradas para cada utilizador. Se o seu servidor proxy estiver configurado desta forma, seleccione a opção ***Utilizar PROXY de autenticação*** para verificar se o seu nome de utilizador e palavra-passe são válidos para estabelecer ligação à Internet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

Configuração automática

Se seleccionar a configuração automática (*seleccione 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

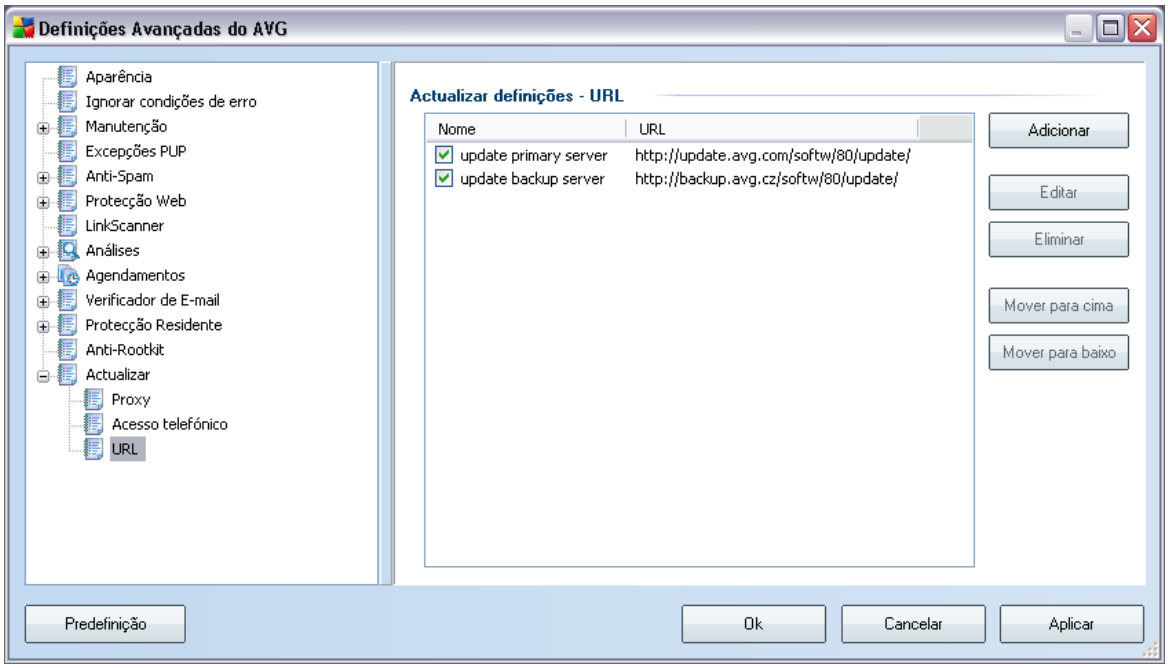
10.12.2. Acesso telefónico



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***).

10.12.3. 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
- ***Predefinição***-repõe a lista predefinida de URLs
- ***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

10.12.4. Gerir

A janela ***Gerir*** faculta duas opções acessíveis via dois botões:

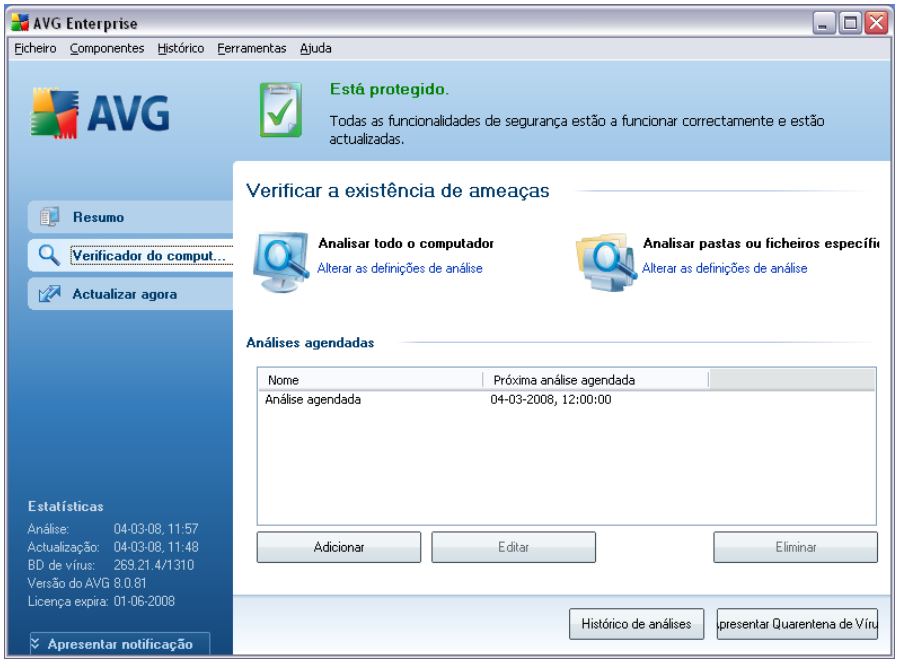
- ***Eliminar os ficheiros de actualização temporários*** - prima este botão para eliminar todos os ficheiros de actualização redundantes do seu disco rígido (*por predefinição, estes ficheiros são guardados durante 30 dias*)

- ***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 seguinte actualização*)

11. Análise do AVG

A análise é uma parte crucial da funcionalidade do**AVG 8.5 Anti-Vírus** Pode executar testes a pedido ou agendá-los para serem executados periodicamente em alturas convenientes.

11.1. Interface de Análise



A interface de análise do AVG é acessível via ***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 dois tipos de testes (definidos pelo fornecedor do software) prontos a serem utilizados imediatamente seja manualmente ou agendado;
- secção agendamento de análise - onde pode definir novos testes e criar novos agendamentos consoante necessário.

Botões de controlo

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

- ***Histórico de análises*** - apresenta a janela Síntese dos resultados da análise com todos o históricos de análises

- ***Apresentar Quarentena de Vírus*** - abre uma nova janela com a Quarentena de Vírus - um espaço onde as infecções detectadas são colocadas em quarentena

11.2. Análises Predefinidas

Uma das principais funcionalidades do AVG é a análise mediante solicitação. 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.

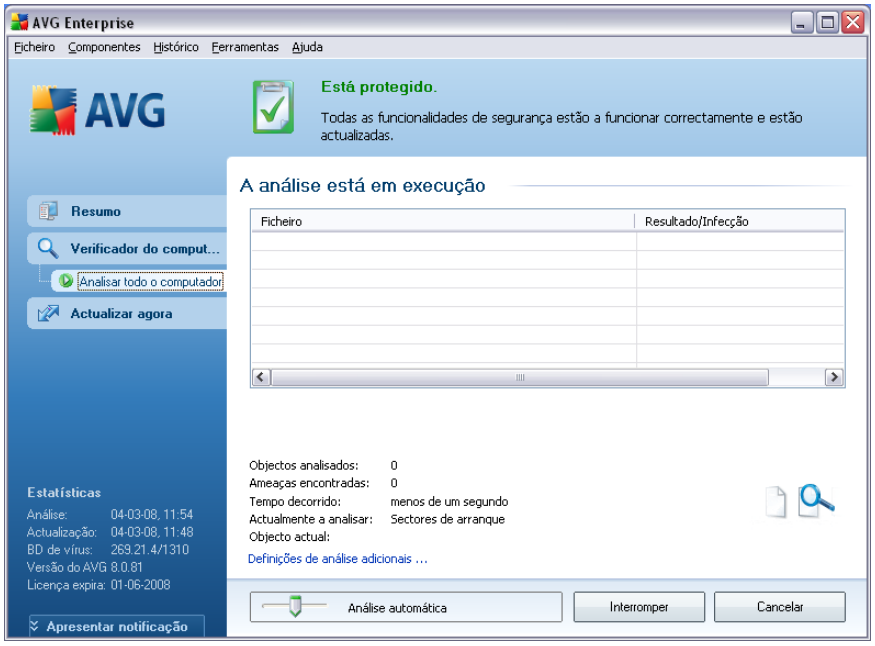
No **AVG 8.5 Anti-Vírus**encontrará dois tipos de análises predefinidas pelo fornecedor do software:

11.2.1. 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.

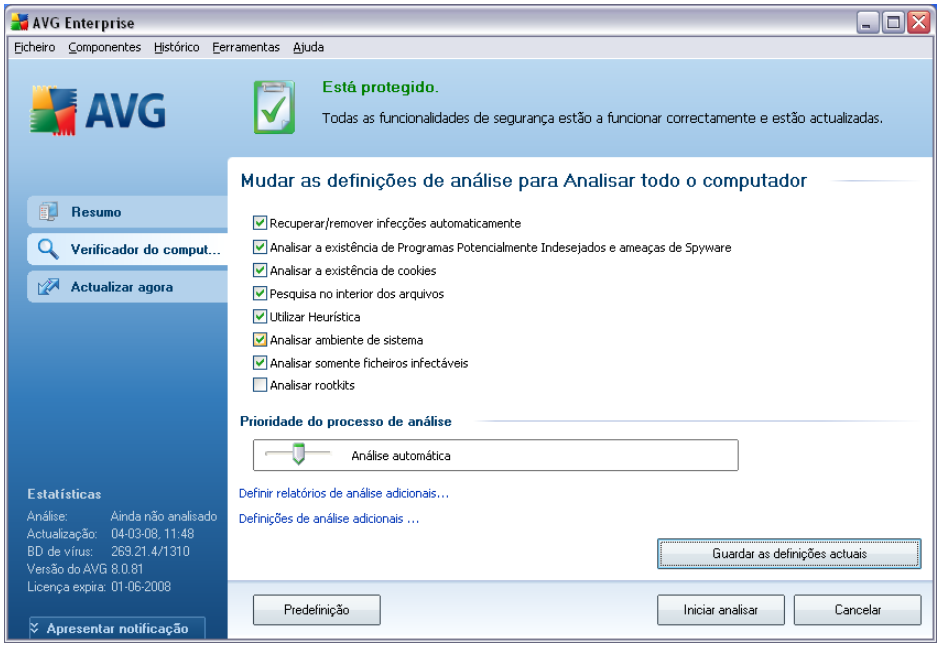
Início de análise

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

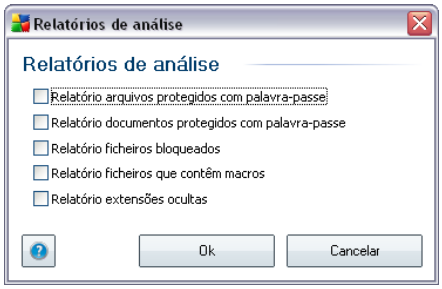
Tem a opção de editar as definições padrão predefinidas da análise ***Analisar todo o computador***. Clique no link ***Alterar definições de análise*** para ir para a janela ***Alterar definições de análise para a Análise de todo o computador***. ***É recomendável que mantenha das definições padrão a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



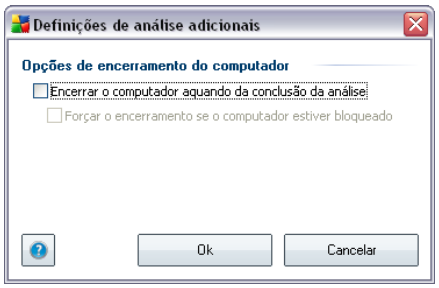
- ***Parâmetros de análise*** - na lista de parâmetros de análise pode activar/ desactivar parâmetros específicos consoante necessário. A maioria dos parâmetros estão activados por predefinição e serão utilizados automaticamente durante a análise.

- ***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:



- ***Definições de análise adicionais*** - o link abre 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***).



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

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

11.2.2. Analisar pastas ou ficheiros específicos

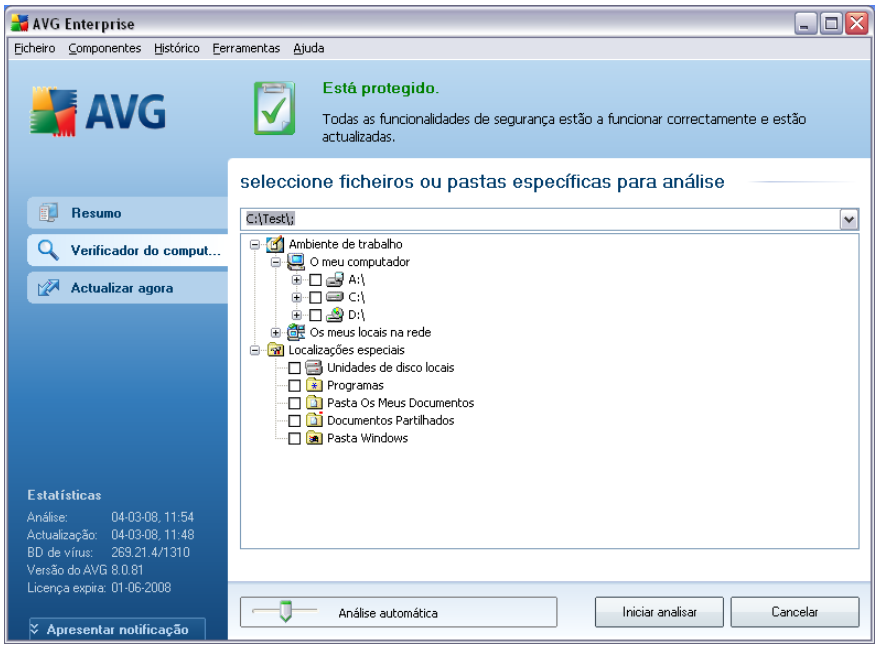
Analisar pastas ou ficheiros específicos - analisa apenas as áreas do seu computador que tiver seleccionado para o efeito (pastas seleccionadas, discos rígidos, unidades de disquetes, CDs, etc.). O progresso da análise na eventualidade da detecção de vírus e o seu tratamento é o mesmo que o da análise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

Início de análise

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

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

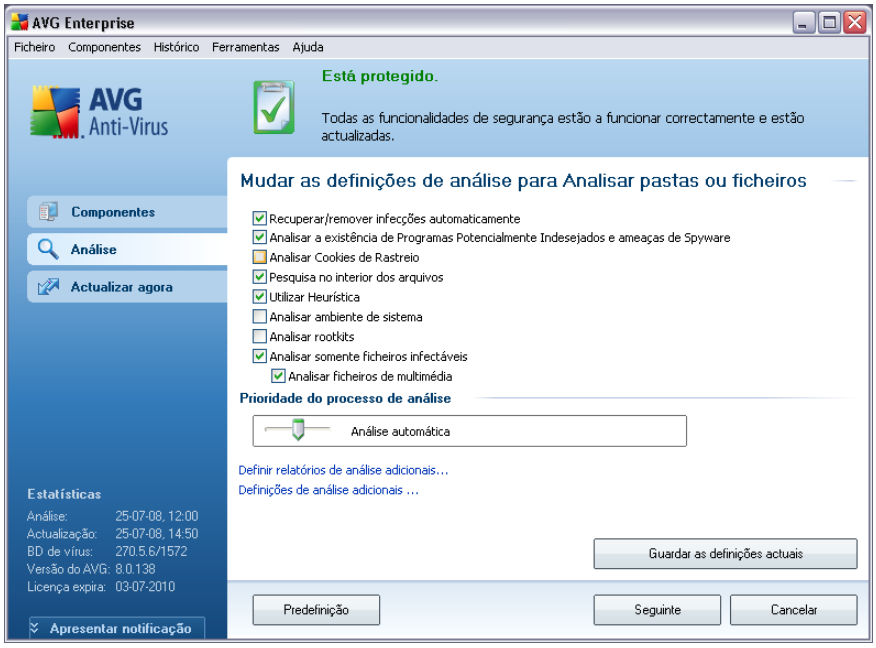
Finalmente, para iniciar a análise, clique no botão ***Iniciar análise***; o processo de análise em si é idêntico ao da análise análise de todo o computador.



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

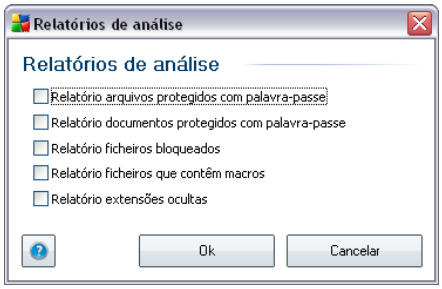
ir para a janela ***alterar definições de análise para a Análise de ficheiros e pastas específicos***. ***É recomendável que mantenha as definições padrão a menos que tenha uma razão válida para as alterar!***



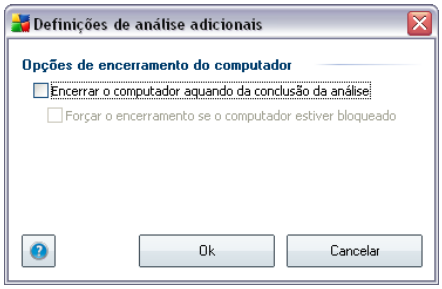
- ***Parâmetros de análise*** - na lista de parâmetros de análise pode activar/ desactivar parâmetros específicos consoante necessário (*para descrições detalhadas destas definições por favor consulte o capítulo Definições Avançadas do AVG / Análises / Análisar Pastas ou Ficheiros*).

- ***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:



- ***Definições de análise adicionais*** - o link abre 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***).



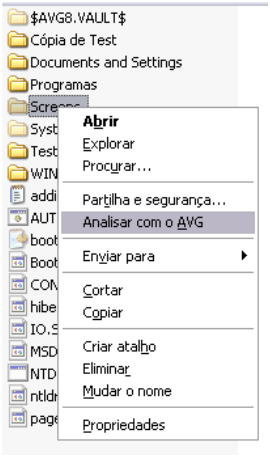
Aviso: *Estas definições de análise são idênticas aos parâmetros de uma análise nova - conforme descrito no capítulo* ***Análise do AVG / Agendamento de análises / Como Analisar*** *.*

Na eventualidade de decidir alterar a configuração padrão da análise ***Analisar pastas ou ficheiros específicos*** pode guardar as suas novas definições como a definição padrão a ser utilizada para todas as análises de ficheiros e pastas específicos. Além disso, esta configuração será utilizada como modelo para todos os novos agendamentos de análise (*todas as análises personalizadas são baseadas na configuração actual da análise Analisar ficheiros e pastas específicos*).

11.3. A analisar no Explorador do Windows

Para além das análises predefinidas executadas para todo o computador ou as suas áreas seleccionadas, o AVG também disponibiliza a opção de análise rápida de um objecto específico directamente no ambiente do Explorador do Windows. Se quiser abrir um ficheiro desconhecido e não estiver seguro do seu conteúdo, pode querer

analisá-lo manualmente. Siga estes passos:



- No Explorador do Windows seleccione o ficheiro (ou pasta) que pretende verificar
- Clique com o botão direito do rato sobre o objecto para abrir o menu de contexto
- Seleccione a opção ***Analisar com o AVG*** para proceder à análise do ficheiro com o AVG

11.4. Análise da Linha de Comandos

Existe no **AVG 8.5 Anti-Vírus** 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 tem de facultar a localização exacta da secção seleccionada), os valores são divididos por vírgulas, por exemplo: ***avgscanx /scan=C:\,D:***

Parâmetros de digitalização

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

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

Análise CMD iniciada a partir da interface gráfica

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

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

11.4.1. Parâmetros da Análise CMD

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

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

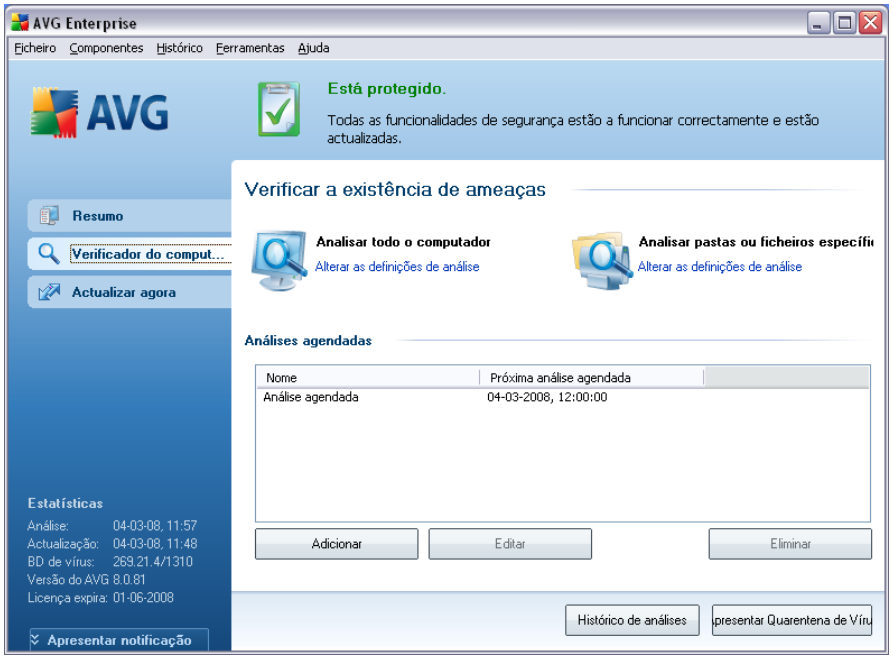
- ***/PUP*** Reportar "Programas potencialmente indesejados"
- ***/REG*** Analisar registo
- ***/COO*** Analisar cookies
- ***/?*** Apresentar ajuda neste tópico
- ***/HELP*** Apresentar ajuda acerca deste tópico
- ***/PRIORITY*** Definir a prioridade de análise /Baixa, Auto, Elevada/ (consulte as Definições 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)

11.5. Agendamento de Análise

Com o **AVG 8.5 Anti-Vírus** pode executar análise 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 posibilidade 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***:



Botões de controlo para o agendamento de análises

Na secção de edição encontrará os seguintes botões de controlo:

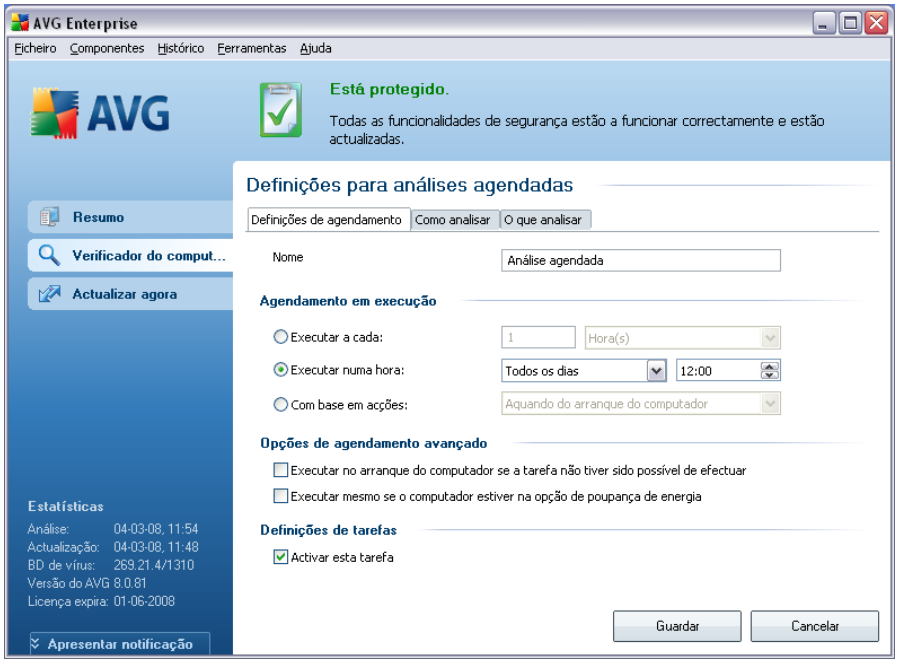
- ***Adicionar agendamento de análise*** - o botão abre a janela ***Definições para agendamento de análises*** , separador***Definições de agendamento***. Nesta janela pode especificar os parâmetros do teste definido.

- ***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.

11.5.1. Definições de agendamento

Se quiser agendar um novo teste e a sua execução regular, aceda à janela ***Definições para testes agendados***. 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 o agendamento de actualização do Anti-Spam, e voltar a activá-lo conforme necessário.

De seguida atribua um nome à análise que está em vias de criar e agendar. Digite o nome no campo de texto ao lado do item ***Nome***. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir.

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

Nesta janela pode ainda definir os seguintes parâmetros de análise:

- ***Agendamento em execução*** - especifique os intervalos de tempo para a execução do novo agendamento de análise. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (***Executar a cada ...***ou definindo uma data e hora precisas (***Executar a uma hora específica ...***), ou ainda definindo um evento ao qual a execução da actualização esteja associada (***Acção baseada no arranque do computador***).

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

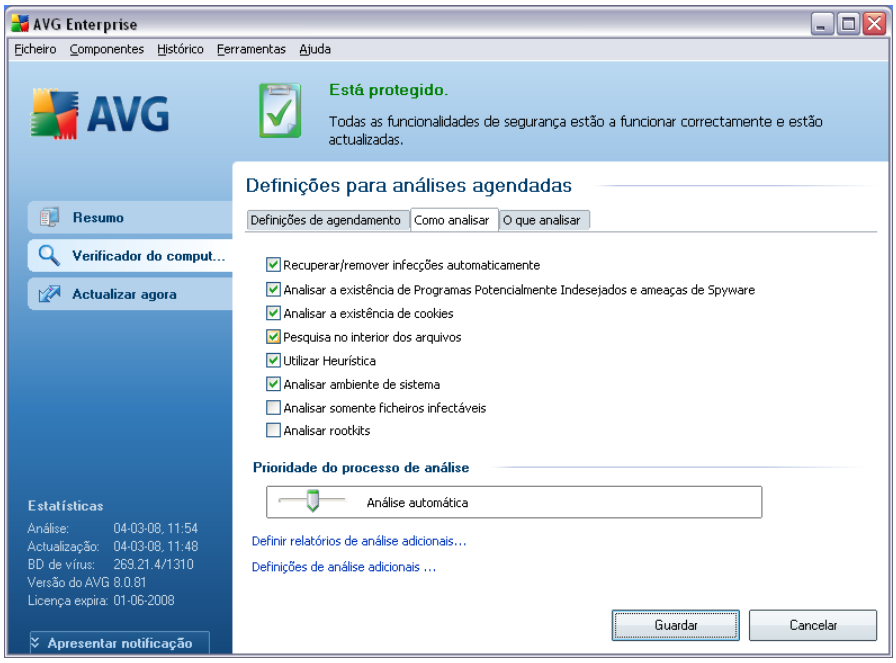
Botões de controlo da janela de Definições para análises agendadas

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

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

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

11.5.2. Como Analisar



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

- ***Reparação automática/remover infecção*** - (*activado por predefinição*): se um vírus for detectado durante a análise pode ser reparado 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.

- ***Analisar Programas Potencialmente Indesejados*** - (*activado por predefinição*): este parâmetro controla a funcionalidade Anti-Vírus que permite a detecção de programas potencialmente indesejados (*ficheiros executáveis que podem ser executados como spyware ou adware* e que podem ser bloqueados, ou removidos;

- ***Analisar a existência de Cookies de Rastreio*** - (*activado por predefinição*): este parâmetro do componente Anti-Spyware define que as cookies deverão

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

- ***Analisar no interior de arquivos*** - (*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***;

    - ***Analisar somente ficheiros infectáveis*** - (*desactivado por predefinição*): com esta opção activada, a análise não será aplicada a ficheiros que não podem ser infectados. Estes podem ser por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis.

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 desejar que a análise seja executada mais rapidamente, 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.

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.*

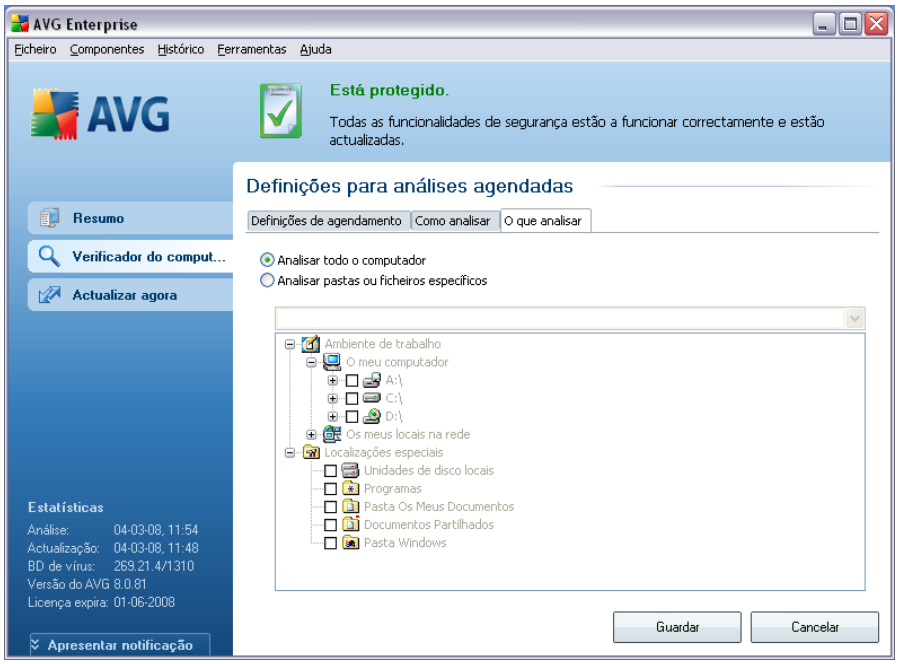
Botões de controlo da janela de Definições para análises agendadas

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 em que esteja:

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

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

11.5.3. O que Analisar



No separador ***O que analisar*** pode definir se pretende agendar uma análise a todo o computador ou analisar ficheiros e pastas específicos. Na eventualidade de seleccionar a análise de ficheiros e pastas específicos, na parte inferior desta janela é

activada a estrutura da árvore apresentada e pode especificar pastas a serem analisadas.

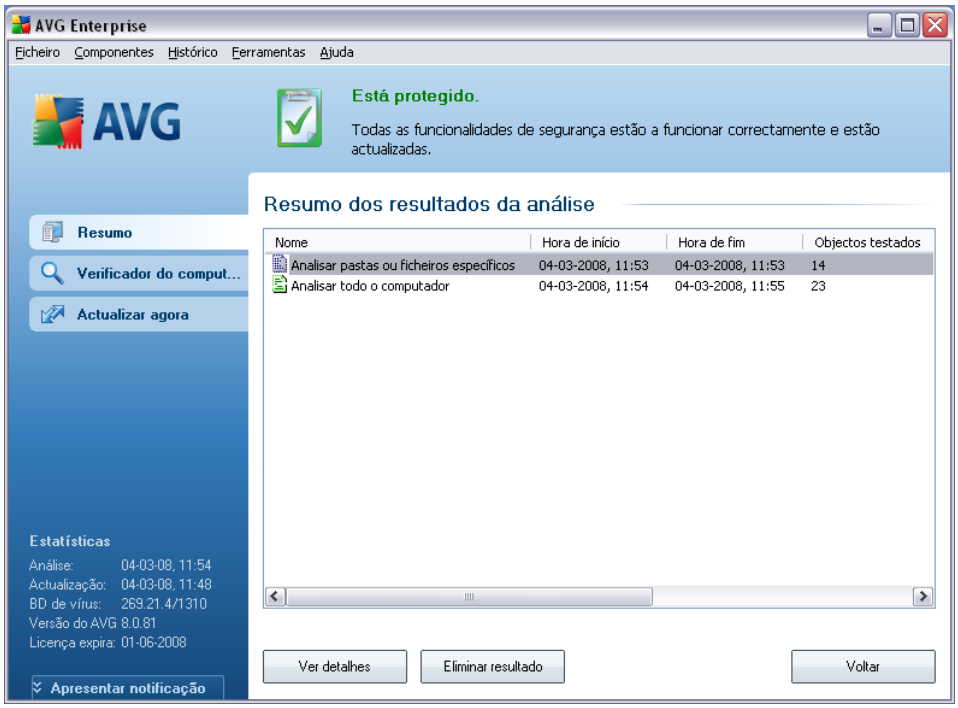
Botões de controlo da janela de Definições para análises agendadas

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 em que esteja:

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

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

11.6. Resumo dos Resultados da Análise



A janela ***Síntese dos resultados da análise*** é acessível a partir dainterface 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 atribuido 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 concluida 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 inicio*** - data e hora em que a análise foi iniciada
- ***Hora de término*** - data e hora em que a análise foi terminada
- ***Objectos testados*** - número de objectos que foram verificados durante a análise
- ***Infecções*** - número de infecções de vírus detectadas / removidas
- ***Spyware*** - número de spyware detectado / removido
- ***Informação de registo de análise***- informações relativas ao decurso da análise e resultados (normalmente sobre a sua finalização ou interrupção)

Botões de controlo

Os botões de controlo para a janela ***Resumo dos resultados da análise***são:

- ***Ver detalhes*** - este botão só estará activo se estiver seleccionada uma análise específica na síntese acima; clique nele para alternar para a janela ***Resultados da Análise*** e visualizar dados relativos à análise seleccionada
- ***Eliminar resultado*** - este botão só estará activo se estiver seleccionada uma análise específica na síntese acima, clique nele para remover o item seleccionado da síntese de resultados de análise
- ***Retroceder*** - alterna para a janela padrão da interface de análise do AVG

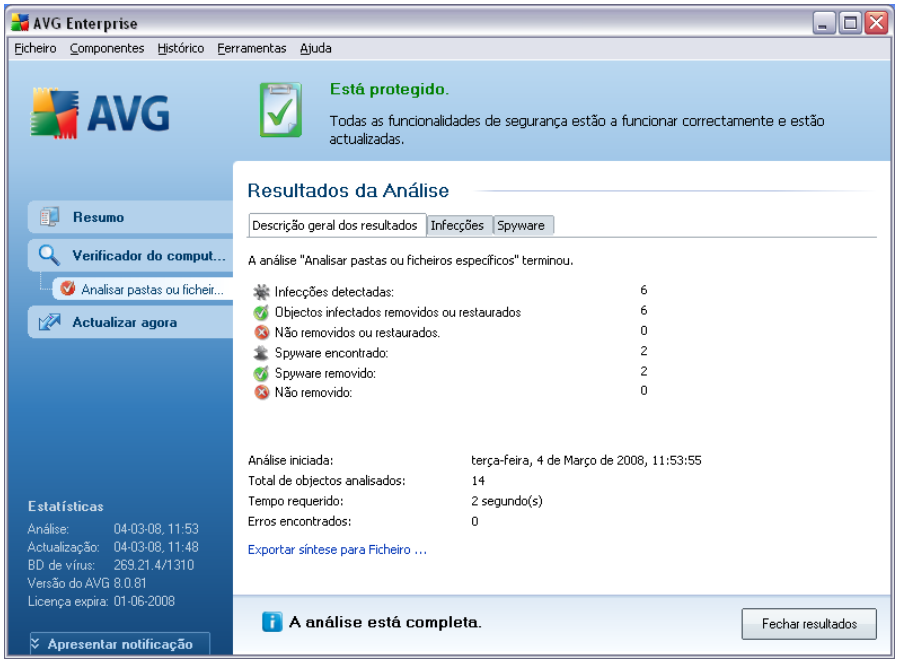
11.7. Detalhes dos Resultados da Análise

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

A janela de diálogo está dividida em vários separadores:

- ***Síntese de Resultados*** - este separador é apresentado constantemente e faculta dados estatísticos que descrevem o progresso da análise
- ***Infecções*** - este separador só é apresentado se tiver sido detectada alguma infecção de vírusdurante a análise
- ***Spyware*** - este separador só é apresentado se tiver sido detectado algum spywaredurante a análise
- ***Avisos*** - este separador só é apresentado se tiverem sido detectados durante a análise alguns objectos que não podem ser analisados
- ***Rootkits*** - este separador só é apresentado se tiver sido detectado algum rootkitdurante 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

11.7.1. Separador Resumo dos Resultados



No separador ***Resultados da Análise*** pode encontrar estatísticas detalhadas com

informação relativa a:

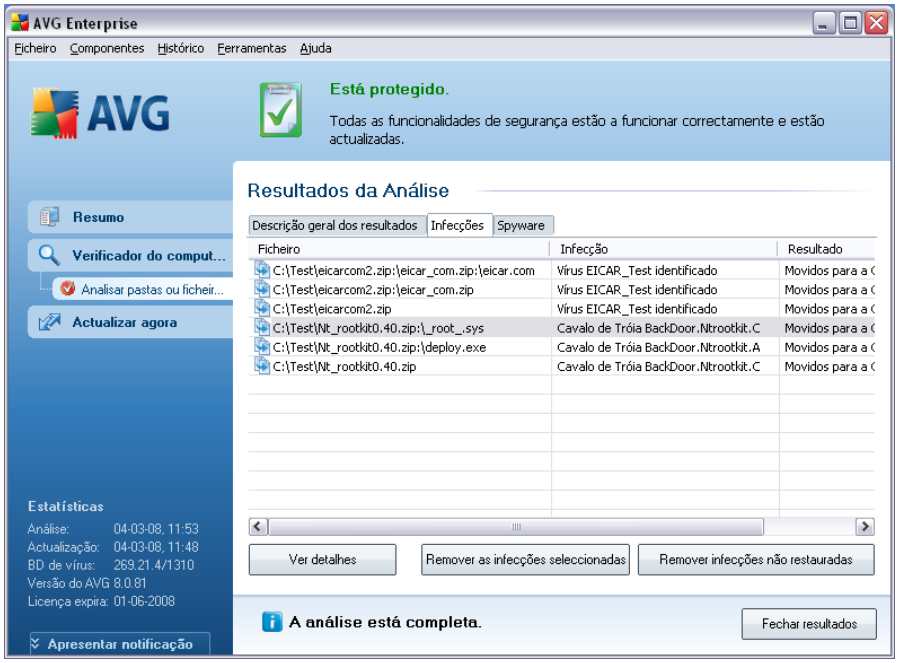
- infecções de vírus/spyware detectadas
- infecções de vírus/spyware removidas
- o número de infecções de vírus / spyware que não podem ser removidas ou recuperadas

Adicionalmente, encontrará informações relativas à data e hora exacta do inicio da análise, ao número total de objectos analisados, à duração da análise e ao número de erros que tenham ocorrido durante a análise.

Botões de controlo

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

11.7.2. Separador Infecções



O separador ***Infecções*** só é apresentado na janela ***Resultados da Análise*** se tiver sido detectada alguma infecçãodurante a análise. O separador está dividido em três

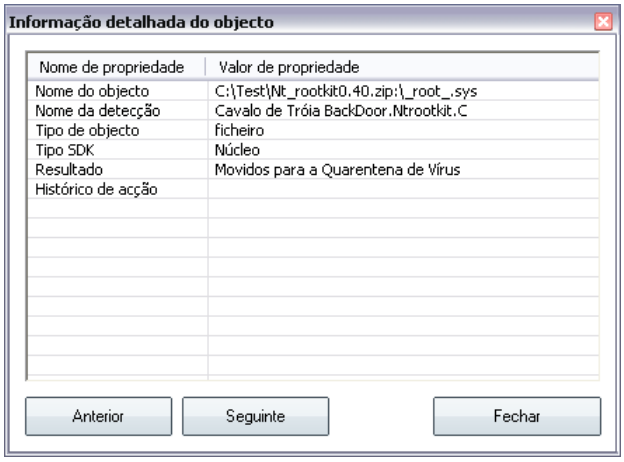
secções que facultam a seguinte informação:

- ***Ficheiro*** - localização original completa do objecto infectado
- ***Infecções*** - nome do vírus detectado (*para detalhes específicos relativos a vírus por favor consulte a Enciclopédia de vírus on-line*)
- ***Resultado*** - define o estado actual do objecto infectado que foi detectado durante a análise:
  - ***Infectado*** - o objecto infectado foi detectado e mantido na sua localização original (*por exemplo se tiver desactivado a opção de recuperação automática nas definições de uma análise específica*)
  - ***Recuperado*** - o objecto infectado foi recuperado automaticamente e mantido na sua localização original
  - ***Movido para a Quarentena de Vírus*** - o objecto infectado foi movido para a ***Quarentena de Vírus***
  - ***Eliminado*** - o objecto infectado foi eliminado
  - ***Adicionado às excepções PUP*** - a detecção foi avaliada como sendo uma excepção e adicionada à lista de excepções PUP (*configurada na janela* ***Excepções PUP*** *das definições avançadas*)
  - ***Ficheiro bloqueado - não testado*** - o objecto detectado está bloqueado e o AVG não o consegue analisar
  - ***Objecto potencialmente perigoso*** - o objecto foi detectado como sendo potencialmente perigoso mas não infectado(*pode conter macros, por exemplo*); a informação deverá ser entendida como sendo um aviso
  - ***É necessário reiniciar para concluir a acção*** - o objecto infectado não pode ser removido, para o remover por completo tem de reiniciar o seu computador

Botões de controlo

Existem três botões de controlo disponíveis nesta janela:

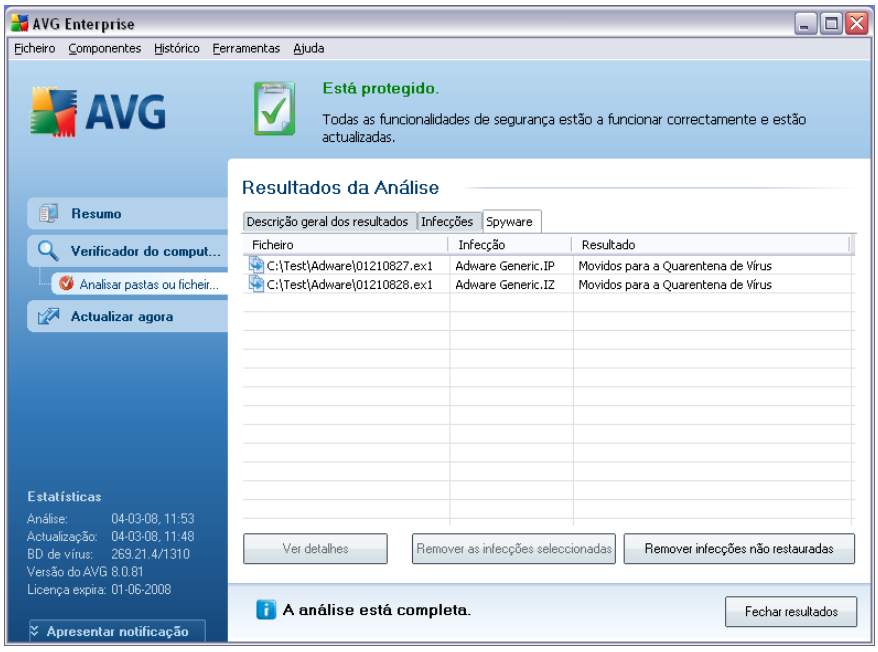
- ***Ver detalhes*** - o botão abre uma nova janela apelidada ***Informação detalhada de resultado de análise***:



Nesta janela pode encontrar informações relativas à localização do objecto infeccioso detectado (***Nome de propriedade***). Ao utilizar os botões ***Anterior*** / ***Seguinte***pode visualizar informações específicas relativas a detecção especifica. 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 sintese de informações detalhadas e retorna à janela ***Resumo dos resultados da análise***

11.7.3. Separador Spyware



O separador ***Spyware*** só é apresentado na janela ***Resultados da Análise*** se tiver sido detectado spywaredurante a análise. O separador está dividido em três secções que facultam a seguinte informação:

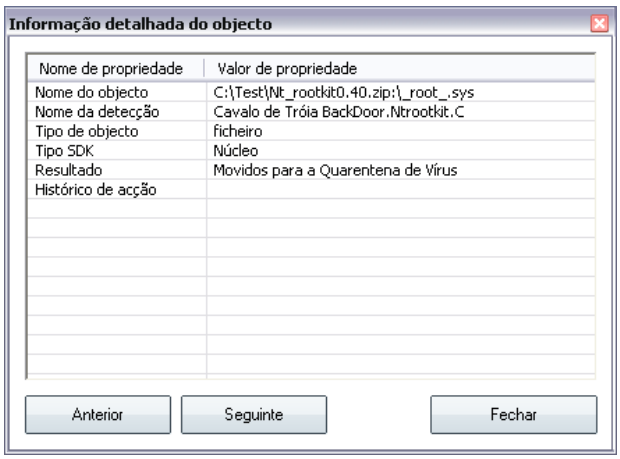
- ***Ficheiro*** - localização original completa do objecto infectado
- ***Infecções*** - nome do spyware detectado (*para detalhes relativos a vírus específicos por favor consulte a* ***Enciclopédia de vírus*** *on-line*)
- ***Resultado*** - define o estado actual do objecto infectado que foi detectado durante a análise:
  - ***Infectado*** - o objecto infectado foi detectado e mantido na sua localização original (por exemplo se tiver desactivado a opção de recuperação automática nas definições de uma análise específica)
  - ***Recuperado*** - o objecto infectado foi recuperado automaticamente e mantido na sua localização original
  - ***Movido para a Quarentena de Vírus*** - o objecto infectado foi movido para a ***Quarentena de Vírus***

- ***Eliminado*** - o objecto infectado foi eliminado
- ***Adicionado às excepções PUP*** - a detecção foi avaliada como sendo uma excepção e adicionada à lista de excepções PUP (*configurada na janela* ***Excepções PUP*** *das definições avançadas*)
- ***Ficheiro bloqueado - não testado*** - o objecto detectado está bloqueado e o AVG não o consegue analisar
- ***Objecto potencialmente perigoso*** - o objecto foi detectado como sendo potencialmente perigoso mas não infectado (pode conter macros, por exemplo); a informação deverá ser entendida como sendo um aviso
- ***É necessário reiniciar para concluir a acção*** - o objecto infectado não pode ser removido, para o remover por completo tem de reiniciar o seu computador

Botões de controlo

Existem três botões de controlo disponíveis nesta janela:

- ***Ver detalhes***- o botão abre uma nova janela apelidada ***Informação detalhada de 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 específicas relativas a detecções especificas. Utilize 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 sintese de informações detalhadas e retorna à janela ***Resumo dos resultados da análise***

11.7.4. Separador Avisos

O separador ***Avisos*** apresenta informações acerca de objectos "suspeitos" (*normalmente ficheiros*) detectados durante as análises. Ao serem detectados pela ***Protecção Residente***, o acesso a estes ficheiros é bloqueado. Exemplo tipicos deste tipo de detecções são: ficheiros ocultos, cookies, chaves de registo suspeitas, documentos ou arquivos protegidos por palavra-passe, etc.

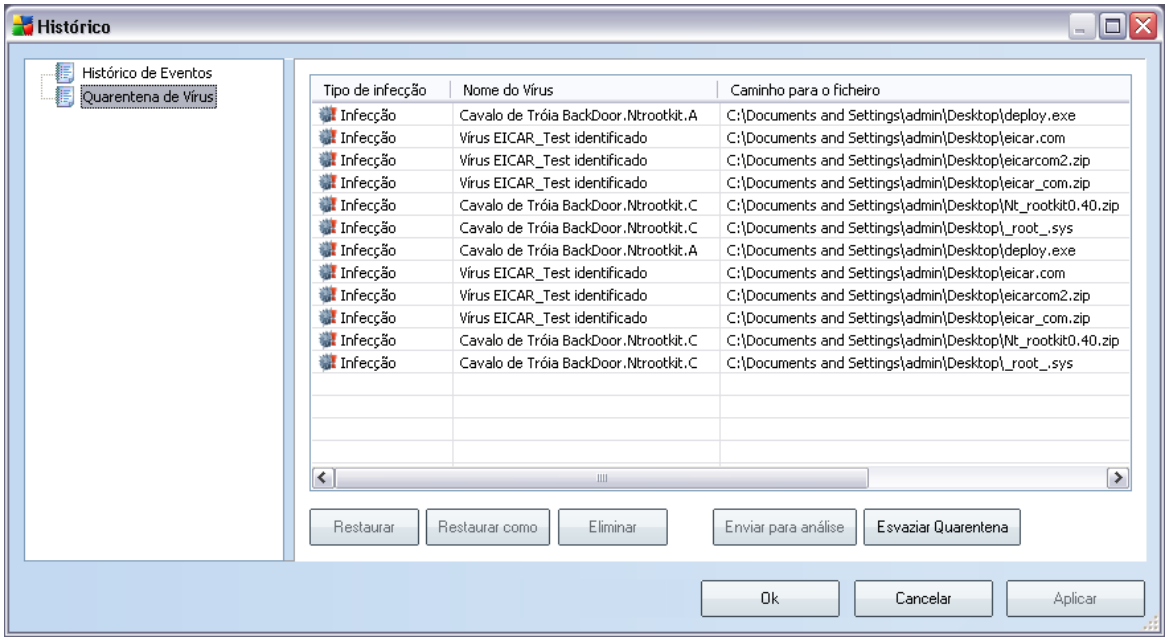
11.7.5. Separador Rootkits

O separador ***Rootkits*** apresenta informações acerca de rootkits detectados durante a análise. A sua estrutura é basicamente a mesma do ***separador Infecções*** ou do ***separador Spyware***.

11.7.6. Separador Informações

O separador ***Informação*** contém dados acerca dessas "detecções" que não podem ser categorizadas como infecções, spyware, etc. Não podem ser positivamente etiquetadas como perigosas mas contudo carecem da sua atenção. Todos os dados neste separador são meramente informativos.

11.8. Quarentena de Vírus



A Quarentena de Vírus é um ambiente seguro para a gestão de objectos suspeitos/ infectados detectados durante os testes AVG. Se um objecto infectado for detectado durante a análise e o AVG não puder recuperá-lo automaticamente, deverá decidir o que fazer com o objecto suspeito. A solução recomendada consiste em mover o objecto para a ***Quarentena de Vírus*** para tratamento futuro.

A interface da ***Quarentena de vírus*** abre numa janela separada e oferece uma síntese da informação dos objectos infectados colocados em quarentena:

- ***Tipo de infecção*** - distingue ao encontrar tipos baseado no nível infeccioso(*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.
- ***Eliminar*** -remove o ficheiro infectado da ***Quarentena de Vírus*** por completo
- ***Enviar para análise*** - envia o ficheiro suspeito para os laboratórios de vírus da AVG para uma profunda análise.
- ***Quarentena vazia*** -remover todos ***Quarentena de Vírus***conteúdo completamente

12. Actualizações do AVG

12.1. Níveis de Actualização

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

- ***Definições de actualização*** contém alterações necessárias para uma protecção anti-vírus e anti-malware fiável. Normalmente, não inclui alterações ao código e apenas actualiza a base de dados de definições. Esta actualização deve ser aplicada logo que esteja disponível.

- ***Actualicação 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.

12.2. Tipos de Actualização

É possível distinguir dois tipos de actualização:

- ***A actualização manual***consiste numa actualização imediata do AVG que pode ser executada sempre que for necessário.

- ***Actualização agendada*** - no AVG, também é possível predefinir um plano de actualização. A actualização programada é então executada periodicamente, de acordo com a configuração definida. Sempre que existem novos ficheiros de actualização na localização especificada, são transferidos directamente a partir da Internet ou de um directório da rede. Quando não existem novas actualizações disponíveis, nada acontece.

12.3. Processo de Actualização

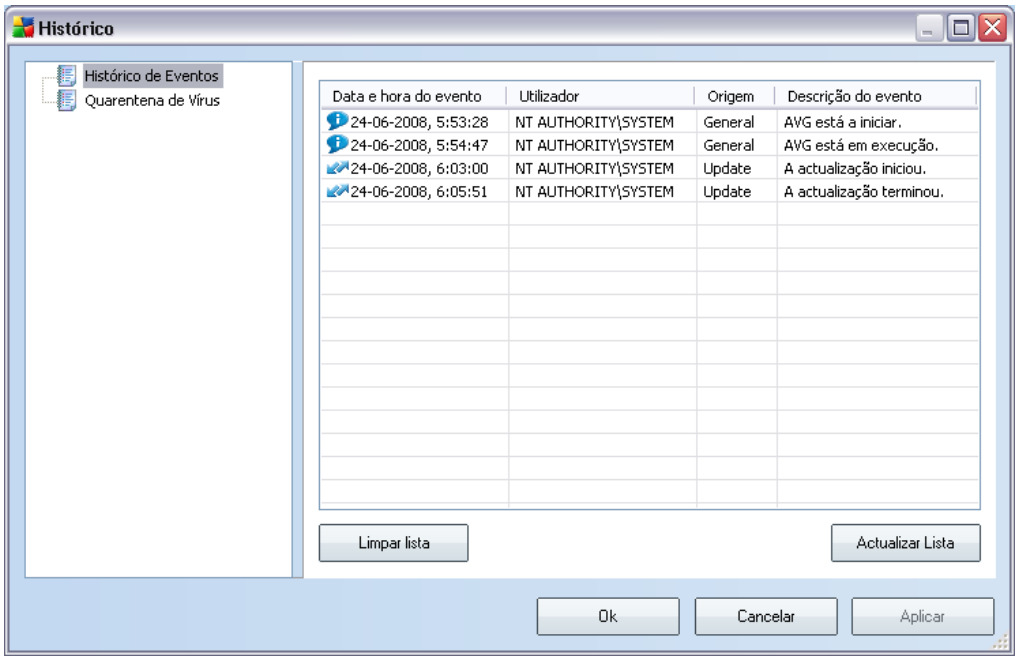
O processo de actualização pode ser executado imediatamente à medida que a necessidade surge via o link rápido ***Actualizar agora*** . Este link está constantemente disponível a partir de qualquer janela daInterface do utilizador do AVG. No entanto, ainda é altamente recomendável efectuar actualizações regularmente conforme expresso no agendamento de actualizações editável no componenteActualizações .

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 através de Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauro do Sistema. Recomendado apenas para utilizadores experientes!*

13. Histórico de Eventos



A janela ***Histórico de Eventos*** é acessível a partir domenu de sistema via o item ***Histórico/Registo do Histórico de Eventos***. Nesta janela poderá encontrar um resumo dos eventos importantes ocorridos durante **AVG 8.5 Anti-Vírus** o funcionamento. ***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 (peloProtecção Residenteou análise) incluindo a localização da ocorrência
- Outros eventos importantes

Botões de controlo

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

14. FAQ e Suporte Técnico

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