AVG 9.0 File Server

Manual do Utilizador

Revisão do documento 90.7 (31. 3. 2010)

Índice

1. Introdução

Este manual do utilizador disponibiliza informações compreensivas para o **AVG 9.0 File Server**.

Parabéns pela sua aquisição do AVG 9.0 File Server!

O **AVG 9.0 File Server** é um entre um leque de premiados produtos AVG desenvolvidos para lhe proporcionar descanso e segurança absoluta para o seu PC. Como todos os produtos AVG, o **AVG 9.0 File Server** foi completamente redesenhado, de raiz, para proporcionar a renomeada e acreditada protecção de segurança de uma forma nova, mais fácil de utilizar e mais eficiente.

O seu novo produto **AVG 9.0 File Server** tem uma interface fácil de utilizar combinada com análises mais agressivas e mais rápidas. Foram automatizadas mais funcionalidades de segurança para a sua conveniência, e foram 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

2.1. Sistemas Operativos Suportados

O **AVG 9.0 File Server** destina-se a proteger estações de trabalho com os seguintes sistemas operativos:

- Windows 2000 Server
- Windows 2003 Server e Windows 2003 Server x64 Edition
- Windows 2008 Server e Windows 2008 Server x64 Edition

(e service packs possivelmente superiores para sistemas operativos específicos)

2.2. Requerimentos de Hardware

Requerimentos mínimos de hardware para o **AVG 9.0 File Server**:

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

Requerimentos recomendados de hardware para o **AVG 9.0 File Server**:

- Intel Pentium CPU 1,8 GHz
- 600 MB de espaço livre no disco rígido (para propósitos de instalação)
- 512 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 (http://www.avg.com).

Antes de iniciar a instalação do AVG, recomenda-se vivamente que visite o website da AVG (http://www.avg.com) para verificar a existência de um novo ficheiro de instalação. Desta forma tem a certeza de que instala a mais recente versão disponível doAVG 9.0 File Server.

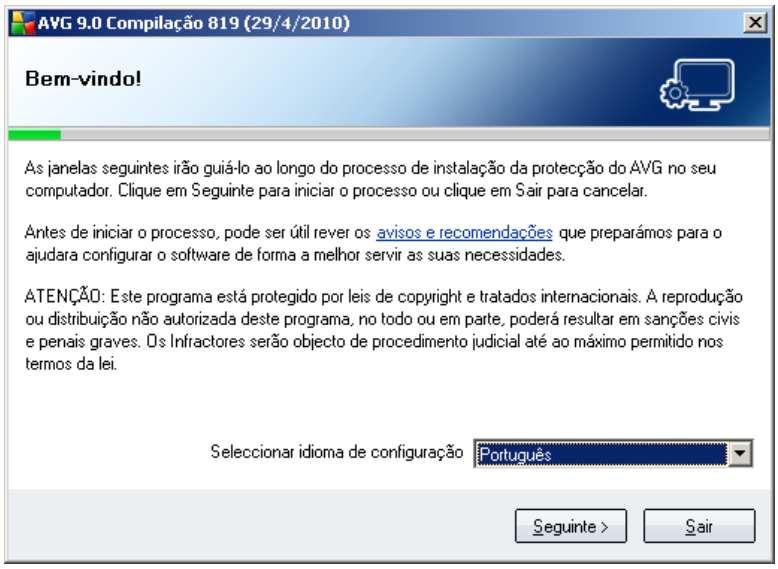
Durante o processo de instalação, ser-lhe-á solicitado o número de licença/venda. Certifique-se de que está disponível antes de iniciar a instalação. O número de venda pode ser encontrado na embalagem do CD. Se tiver adquirido a sua cópia do AVG online, o número de licença foi-lhe enviado por e-mail.

4. Processo de Instalação do AVG

Para instalar o **AVG 9.0 File Server** no seu computador, precisa de transferir o ficheiro de instalação mais recente. Pode utilizar o ficheiro de instalação a partir do CD facultado na caixa da sua edição, mas este ficheiro pode estar desactualizado. Como tal, recomendamos que obtenha o ficheiro de instalação mais recente ficheiro on-line. Pode transferir o ficheiro a partir do website da AVG (http://www.avg.com), secção ***Transferências***.

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

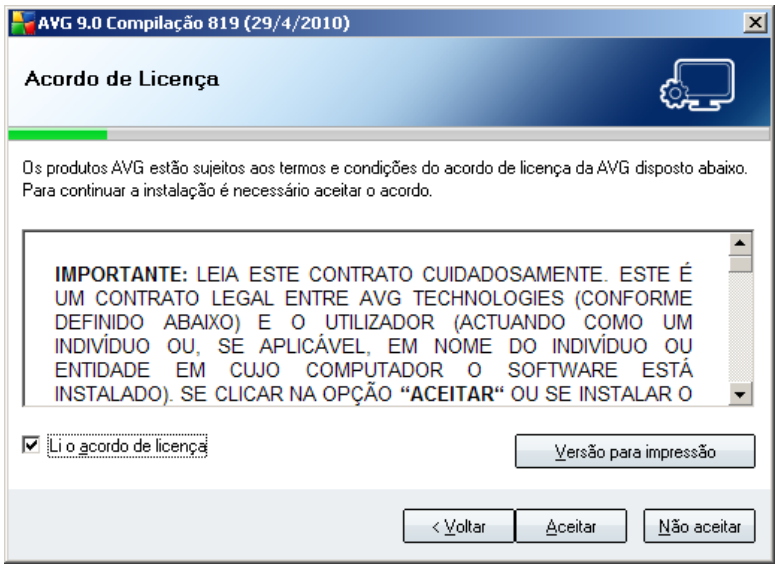
4.1. Execução da Instalação



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: *O idioma que tiver seleccionado no início do processo de instalação será o idioma da aplicação AVG. No entanto, pode alterar esta definição facilmente através dos menus Interface de Utilizador AVG -> Ferramentas -> Definições Avançadas -> Aparência).*

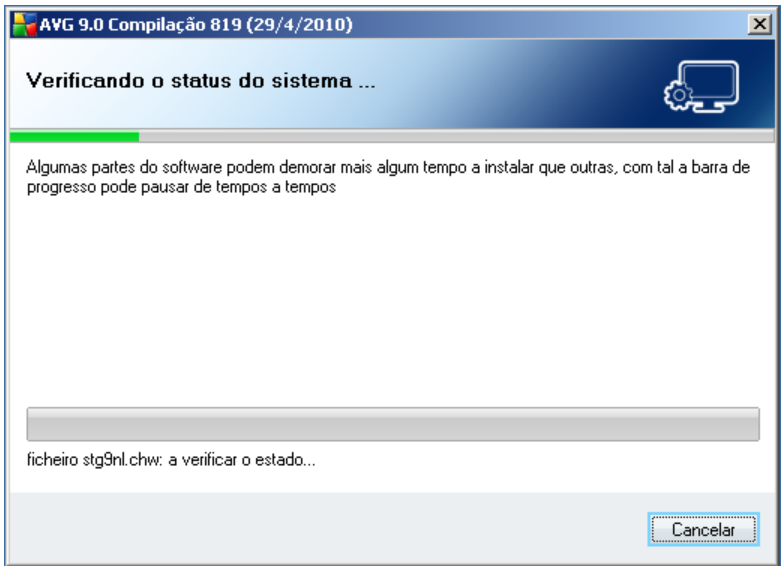
4.2. Contrato de Licença



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

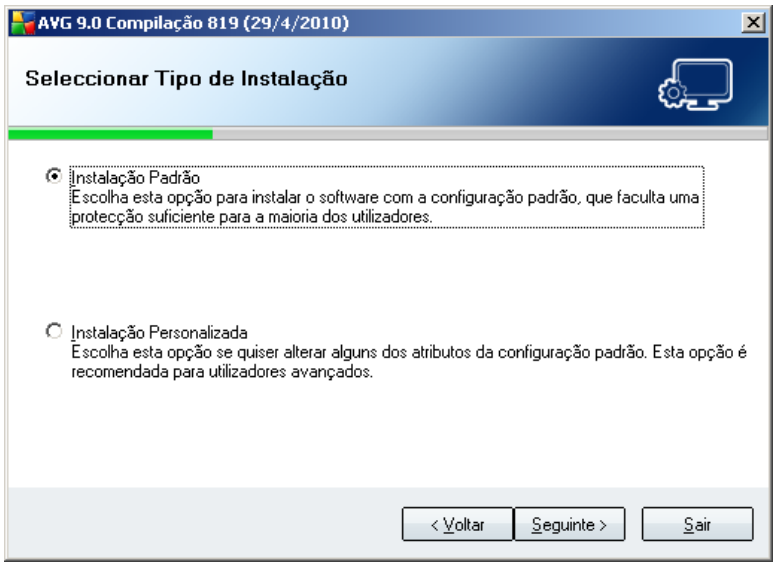
Se não concordar com o acordo de licença clique no botão ***Não aceito*** , e o processo de instalação será abortado imediatamente.

4.3. 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.

4.4. Seleccionar Tipo de Instalação



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

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

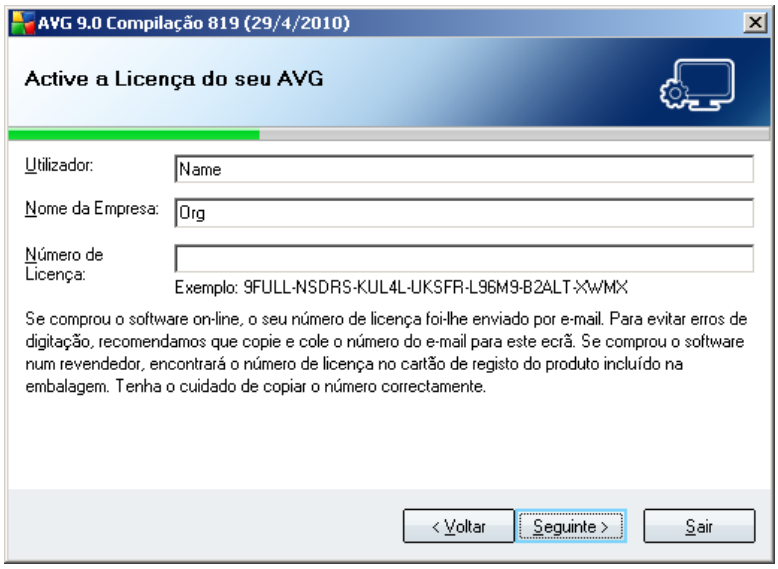
A instalação personalizada só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o AVG com definições que não as padrão. Ex. para corresponder a requisitos de sistema específicos.

4.5. Activar a Licença do seu AVG

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

Depois introduza o seu número de licença/venda no campo de texto ***Número de Licença***. O número de venda pode ser encontrado na caixa do CD do seu **AVG 9.0 File Server**. O número de licença estará na mensagem de e-mail de confirmação que recebeu após comprar o seu **AVG 9.0 File Server** on-line. Tem de digitar o número exactamente conforme apresentado. Se o formato o digital do número de licença

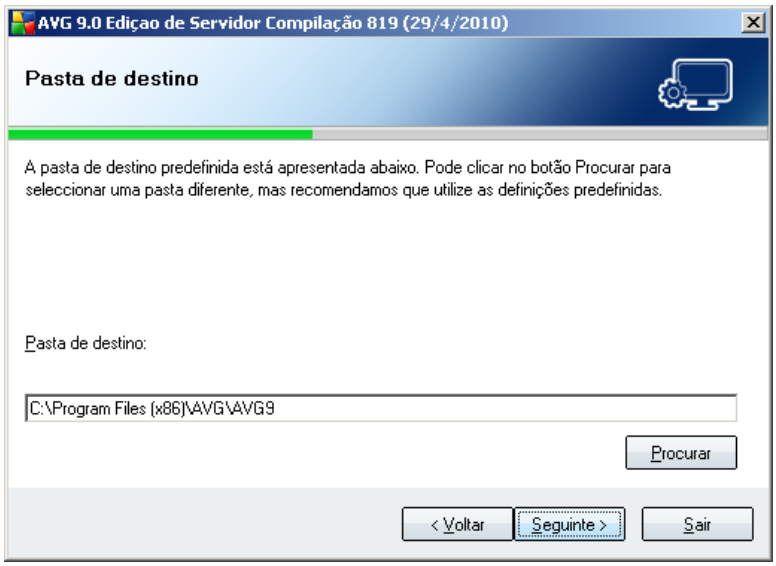
estiver disponível (*no e-mail*), é aconselhável que utilize o método copiar e colar para o inserir.



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

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

4.6. Instalação Personalizada - Pasta de Destino

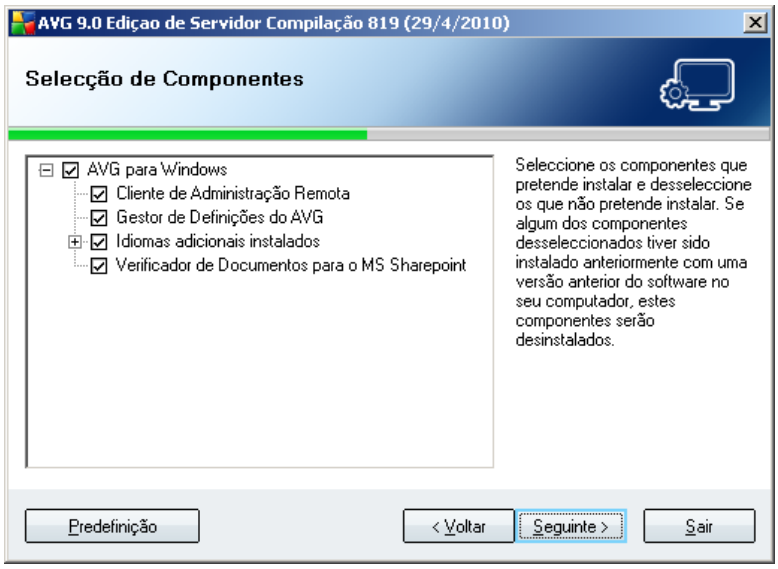


A janela ***Pasta de Destino*** permite-lhe especificar a localização onde o **AVG 9.0 File Server** deve ser instalado. O AVG será instalado por predefinição na pasta de ficheiros de programas localizada na unidade C:. Na eventualidade de a pasta não existir ainda, ser-lhe-á solicitado numa nova janela que confirme que concorda com a criação desta pasta por parte do AVG agora.

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

Prima o botão ***Seguinte*** para confirmar.

4.7. Instalação Personalizada - Selecção de Componentes



A janela ***Selecção de Componentes*** apresenta uma síntese de todos os componentes do **AVG 9.0 File Server** que podem ser instalados. Se as definições predefinidas não forem da sua conveniência, pode remover/adicionar componentes específicos.

- ***Selecção do Idioma***

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

- ***Administração Remota***

  Se tiver intenções de ligar o computador à Administração Remota AVG posteriormente, queira marcar o item respectivo para que este também seja instalado.

- ***Gestor de configurações AVG***

  O Gestor de Definições AVG é uma pequena aplicação que lhe permite configurar de forma simples e rápida as instalações locais do AVG (mesmo as que não estão sujeitas à Administração Remota). Usa os ficheiros de configuração (no formato .pck) que podem ser criados facilmente pelo Gestor de Definições AVG em qualquer computador em que a aplicação AVG esteja instalada. Pode então

copiar estes ficheiros para qualquer dispositivo amovível e usá-los em cada computador. Claro que o mesmo acontece com o Gestor de Definições AVG em si. Para mais informações sobre esta aplicação clique **aqui**.

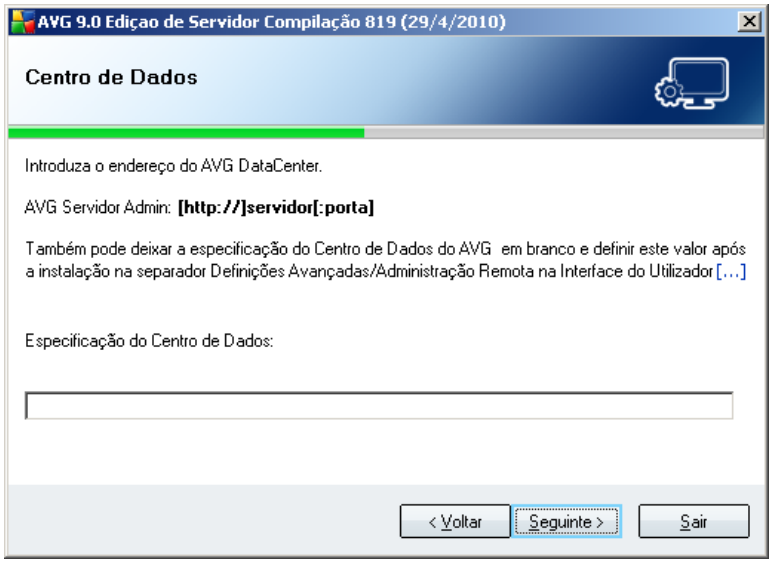
- ***Verificador de Documentos para o MS Sharepoint***

  Este componente analisa ficheiros de documentos guardados no MS Sharepoint e protege contra possíveis ameaças. É uma parte essencial do **AVG 9.0 File Server**, portanto, recomendamos vivamente que o instale.

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

4.8. Centro de Dados AVG

Se estiver a utilizar a licença de rede AVG e se na janela ***Instalação Personalizada - Selecção de Componentes*** anterior tiver marcado o item ***Administração remota*** para instalação, é necessário especificar os parâmetros do ***Centro de Dados AVG***:



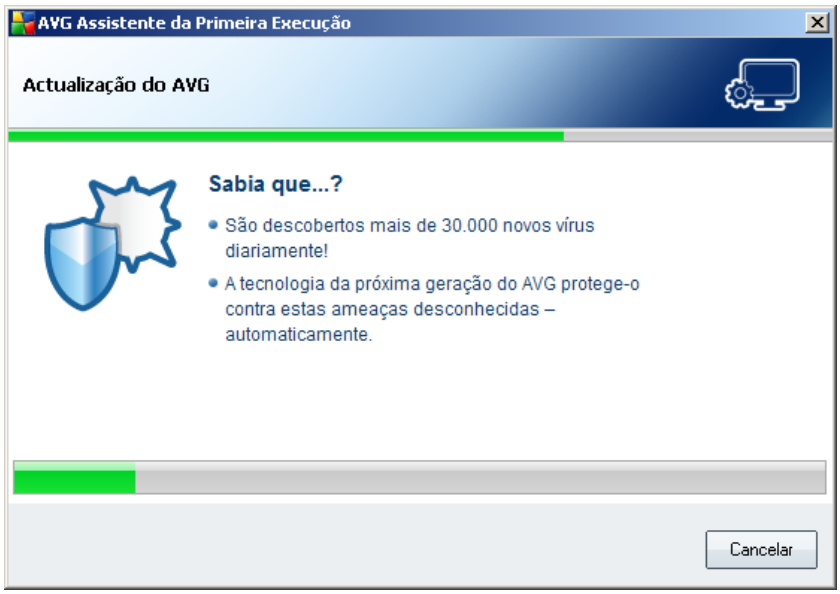
No campo de texto do ***Centro de Dados AVG*** queira introduzir cadeia de caracteres de ligação ao ***Centro de Dados AVG*** no formato *servidor:porta*. Se não dispuser destas informações de momento, deixe o campo em branco e poderá definir a configuração posteriormente na janela ***Definições Avançadas / Administração Remota***.

Nota: *Para informações detalhadas sobre a Administração remota do AVG, queira consultar o manual do utilizador do AVG Network Edition que pode ser transferido a*

partir do Website da AVG (http://www.avg.com).

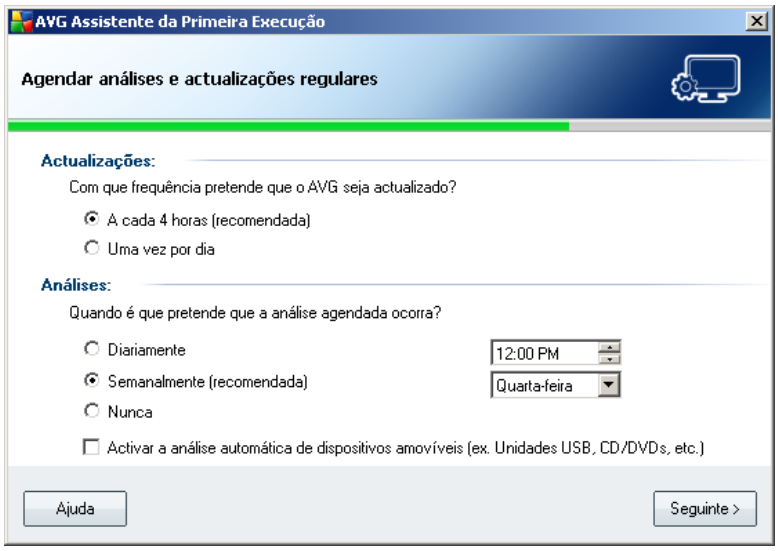
4.9. A instalar o AVG

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



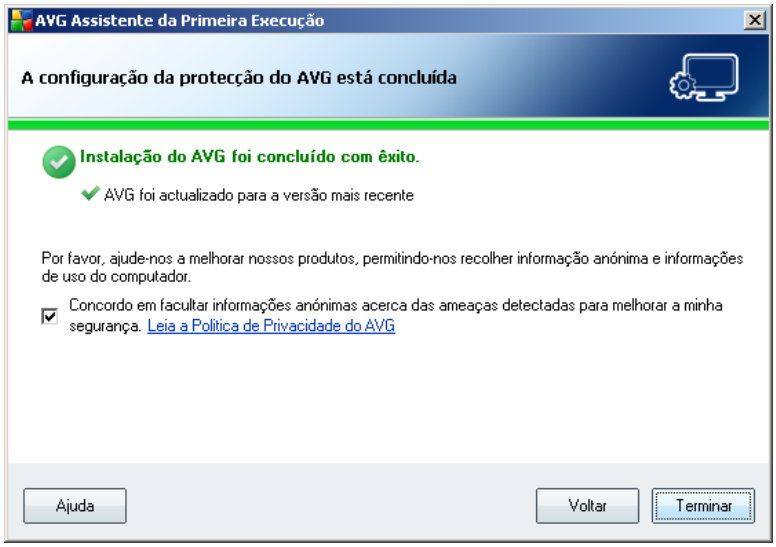
Após a conclusão do processo de instalação, será automaticamente redireccionado para a janela seguinte.

4.10. 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.

4.11. A configuração da protecção do AVG está concluída



Agora, o seu **AVG 9.0 File Server** está configurado.

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

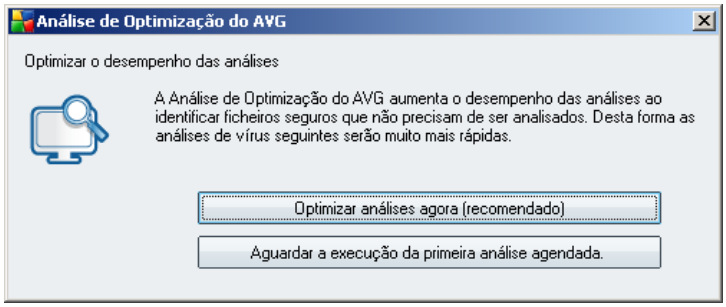
Finalmente, prima o botão ***Concluir***.

5. Após a Instalação

5.1. Optimização da análise

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

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



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

5.2. Registo do Produto

Estando terminada a instalação do **AVG 9.0 File Server**, por favor registe o seu produto on-line no website da AVG (http://www.avg.com), ***Página de registo*** (*siga as instruções facultadas directamente na página*). Após o registo terá acesso total à sua conta de utilizador AVG, o boletim informativo de Actualização da AVG, e outros serviços fornecidos exclusivamente para os utilizadores registados.

5.3. Aceder à Interface do Utilizador

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

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

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

5.4. Análise de todo o computador

Existe um risco potencial de que um vírus informático tenha sido transmitido ao seu computador antes da instalação do **AVG 9.0 File Server**. Por este motivo deve executar uma análise ***Analisar todo o computador***para se certificar de que não existem infecções no seu PC.

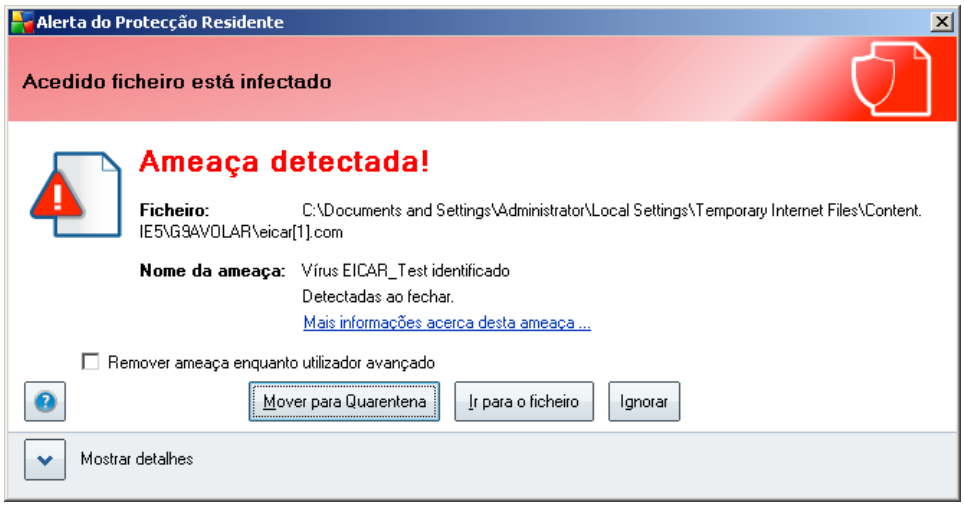
Para instruções relativas à execução de ***Analisar todo o computador*** por favor consulte o capítulo ***Análise do AVG***.

5.5. Teste Eicar

Para confirmar que o **AVG 9.0 File Server** foi devidamente instalado, pode executar o teste EICAR.

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

Tente transferir o ficheiro ***eicar.com***e guardá-lo no disco local. Imediatamente após a confirmação da transferência do ficheiro de teste, a***Protecção Residente*** ***reagirá com um aviso.*** Este aviso da ***Protecção Residente******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!

5.6. Configuração Predefinida do AVG

A configuração predefinida (*ou seja, a forma como a aplicação está configurada imediatamente após a instalação*) do **AVG 9.0 File Server** 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.

6. Interface de Utilizador AVG

O **AVG 9.0 File Server** abre na janela principal:

A janela principal está dividida em várias secções:

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

- ***Síntese de Componentes*** *(secção central da janela)* faculta uma síntese de todos os componentes instalados do AVG - detalhes >>

- ***Estatísticas****(secção inferior esquerda da janela)*fornece-lhe todos os dados estatísticos relativos ao funcionamento do programa - detalhes >>

- ***Ícone da Barra de Notificação do Sistema****(canto inferior direito do monitor, na barra de notificação do sistema)* indica o estado actual do AVG - detalhes >>

6.1. Menu de Sistema

O***menu de sistema*** é a navegação padrão utilizada em todas as aplicações do Wndows. Está localizado na parte superior da janela principal do **AVG 9.0 File Server**. Utilize o menu de sistema para aceder a compoentes, funcionalidades e serviços específicos do AVG.

O menu de sistema está dividido em cinco secções principais:

6.1.1. Ficheiro

- ***Sair*** - fecha a interface do utilizador do**AVG 9.0 File Server**. No entanto, a aplicação AVG continuará a ser executada em segundo plano e o seu computador continuará protegido!

6.1.2. Componentes

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

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

- ***Componentes do servidor*** - muda para a interface predefinida do utilizador com a síntese de todos os componentes do servidor e os estados respectivos

- ***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***

- ***Administração Remota*** - abre a página predefinida do componente ***Administração Remota*** (este componente conecta o seu AVG à

Administração Remota AVG, permitindo que o administrador de rede accione algumas acções de aplicações remotamente). O componente Administração só estará disponível se tiver optado pela sua instalação no passo de ***Selecção de Componentes*** do ***Processo de Instalação***).

- ***SharePoint*** - abre a página predefinida do componente do servidor ***Verificador de Documentos para o MS Sharepoint***
- ***Licença*** - abre a página predefinida do componente ***Licença***
- ***Protecção Residente*** - abre a página predefinida do componente ***Protecção Residente***
- ***Actualizações*** - abre a página predefinida do componente ***Actualizações***

6.1.3. Histórico

- ***Resultados da análise***- muda para a interface de teste do AVG, mais especificamente para a janela ***Síntese de Resultados de Análise***
- ***Detecção da Protecção Residente***- abre uma janela com a síntese das ameaças detectadas pela ***Protecção Residente***
- ***Quarentena de Vírus*** - abre a interface do espaço de quarentena (***Quarentena de Vírus***) para onde o AVG remove todas as infecções detectadas que por alguma razão não podem ser recuperadas automaticamente. Nesta quarentena, os ficheiros infectados são isolados e a segurança do seu computador está assegurada, enquanto que os ficheiros infectados são armazenados para possíveis reparações futuras.
- ***Registo do Histórico de Eventos*** - abre a interface de registo do histórico com uma síntese de todas as acções registadas **AVG 9.0 File Server**.

6.1.4. Ferramentas

- ***Análise do computador*** - muda para a Interface de análise do AVGe inicia uma análise de todo o computador
- ***Análise de pasta seleccionada*** - muda para ainterface de análise do AVGe permite-lhe definir na estrutura em árvore do seu computador quais os ficheiros e pastas que devem ser analisados
- ***Analisar ficheiro*** - permite-lhe executar um teste manual de um único ficheiro seleccionado da estrutura em árvore do seu disco

- ***Actualizar***inicia automaticamente o processo de actualização do **AVG 9.0 File Server**

- ***Actualizar a partir de directório*** -executa o processo de actualização a partir dos ficheiros de actualização localizados numa pasta específica no seu disco local. No entanto, esta opção só é recomendada como emergência, ex. em situações em que não está disponível uma ligação à Internet (*por exemplo, o seu computador está infectado e desconectado da Internet; o seu computador está conectado a uma rede sem acesso à Internet, etc.*). Na nova janela seleccione a pasta onde colocou anteriormente o ficheiro de actualização, e inicie o processo de actualização.

- ***Definições avançadas*** - abre a janela ***Definições avançadas do AVG***onde pode editar a configuração do **AVG 9.0 File Server** . Regra geral, é recomendável que mantenha as definições da aplicação conforme definidas pelo vendedor do software.

6.1.5. Ajuda

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

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

- ***Web do AVG*** - abre o website da AVG (http://www.avg.com)

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

- ***Transferir o CD de Recuperação AVG*** - abre o browser no Website da AVG na página de ***Centro de Suporte/Transferências***. Introduza o seu número de licença no campo de texto disponibilizado para transferir a versão mais recente do CD de Recuperação AVG (*versão portátil do AVG destinada à recuperação do sistema operativo em situações em que não seja possível carregar o sistema operativo normalmente - por exemplo, devido a infecções de vírus substanciais*).

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

- ***Registar agora*** - conecta à página de registo do website da AVG (http://www.avg.com). Por favor preencha os seus dados de registo; somente os

clientes que registem o seu produto AVG podem receber suporte técnico gratuito.

- ***Acerca do AVG*** - abre a janela ***Informações*** com cinco separadores que facultam dados sobre o nome do programa, versão do programa e da base de dados de vírus, informação de sistema, acordo de licenciamento e informações de contacto da ***AVG Technologies CZ***.

6.2. Informação de Estado de Segurança

A secção ***Informação de Estado de Segurança*** está localizada na parte superior da janela principal do AVG. Nesta secção encontra sempre informações relativas ao estado de segurança actual do seu **AVG 9.0 File Server**. Por favor veja uma síntese dos ícones possivelmente apresentados, e a respectiva descrição:

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

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

Este ícone também é apresentado se por alguma razão tiver decidido ignorar o estado de erro de um componente (a opção "*Ignorar estado do componente" está disponível a partir do menu de contexto aberto com um clique direito do rato sobre o ícone do componente respectivo na síntese de componentes da janela principal do AVG*). Pode ter de usar esta opção numa situação específica mas é especialmente recomendado desactivar a opção ***Ignorar estado do componente*** assim que possível.

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

de suporte técnico da AVG.

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

Nota:*A informação de estado do AVG também pode ser obtida a qualquer momento a partir doícone da barra de notificação.*

6.3. Links Rápidos

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

- ***Componentes*** - utilize este link para alternar entre a interface do AVG actualmente aberta para a interface padrão com uma síntese de todos os componentes instalados - consulte o capítulo ***Síntese de Componentes >>***
- ***Verificador do computador*** - utilize este link para abrir a interface de análise do AVG onde pode executar testes directamente, agendar análises ou editar os seus parâmetros - consulte o capitulo ***Análises do AVG >>***
- ***Actualizar agora*** - este link abre a interface de actualização, e inicia o processo de actualização do AVG - consulte o capítulo ***Actualizações do AVG >>***
- ***Componentes do servidor***- utilize este link para alternar entre qualquer interface do AVG actualmente aberta para a interface padrão com uma síntese dos componentes do servidor - consulte o capítulo ***Componentes do servidor >>***

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.

6.4. Síntese de Componentes

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

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

No **AVG 9.0 File Server** , a secção ***Síntese de Componentes*** contém informações sobre os seguintes componentes:

- ***Anti-Vírus*** assegura que o seu computador está protegido contra vírus que tentam aceder ao seu computador - detalhes >>
- ***Anti-Spyware*** analisa as suas aplicações em segundo plano à medida que as

executa - detalhes >>

- ***Administração Remota*** - conecta o seu AVG à Administração Remota AVG, permitindo que o administrador de rede accione algumas acções de aplicações remotamente. O componente Administração só estará disponível se tiver optado pela sua instalação no passo de ***Selecção de Componentes*** do ***Processo de Instalação***).

- ***Anti-Rootkit*** detecta programas e tecnologias que tentam camuflar malware - detalhes >>

- ***Licença*** faculta o texto integral do Acordo de Licença AVG - detalhes >>

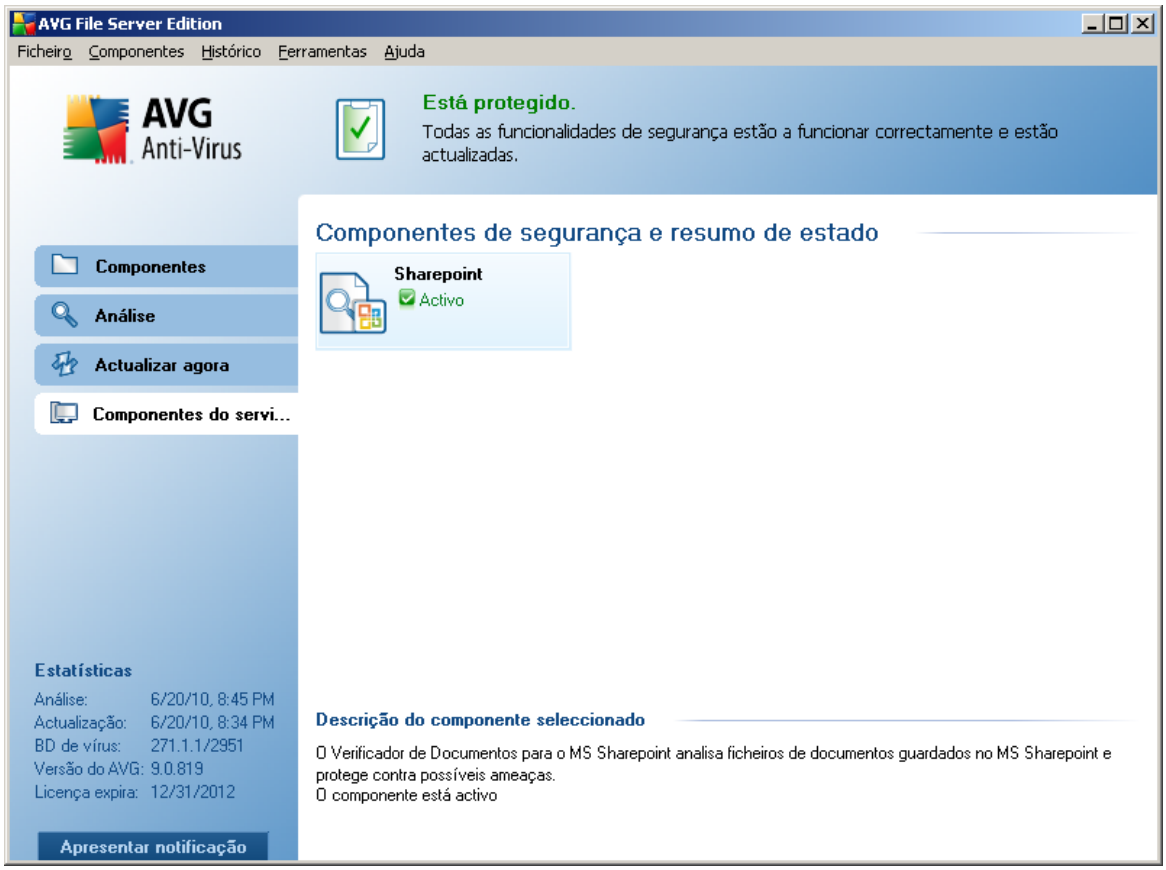
- ***Protecção Residente*** é executada em segundo plano e analisa ficheiros à medida que estes são copiados, abertos ou guardados - detalhes >>

- ***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 através do ícone da barra de notificação.

6.5. Componentes do servidor



A secção ***Componentes do Servidor*** está localizada na parte central da Interface do Utilizador do AVG. A secção está dividida em duas partes:

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

No **AVG 9.0 File Server** , a secção ***Componentes do Servidor*** contém informações sobre os seguintes componentes:

- ***Verificador de Documentos para o MS Sharepoint*** - analisa ficheiros de documentos guardados no MS SharePoint e protege contra possíveis ameaças - informações >>

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 através do ícone da barra de notificação.

6.6. Estatísticas

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

- ***Última análise***- faculta a data em que a última análise foi efectuada
- ***Última actualização***- faculta a data em que a última actualização foi executada
- ***BD de vírus***- informa-o acerca da versão da base de dados de vírus actualmente instalada
- ***Versão do AVG*** - informa-o acerca da versão do AVG instalada*(o número está no formato de 9.0.xx, em que 9.0 é a versão da linha do produto, e xx representa o número de compilação)*
- ***A licença expira*** - faculta a data de expiração da licença do seu AVG

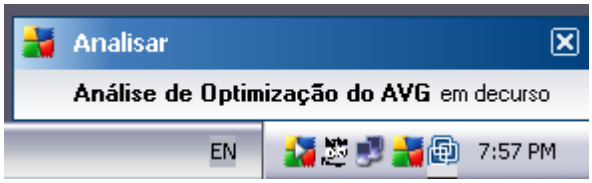
6.7. Ícone da barra de tarefas

Ícone da Barra de Notificação (*na barra de tarefas do Windows*) indica o estado actual do seu **AVG 9.0 File Server**. É visível constantemente na sua barra de notificação, independentemente de a janela principal do AVG estar aberta ou fechada.

Se apresentar a cor preenchida , o ***Ícone da Barra de Notificação*** indica que todos os componentes do AVG estão activos e perfeitamente funcionais. Além disso, o ícone da barra de notificação do AVG pode ser apresentado em cor cheia se o AVG tiver um estado de erro mas o utilizador tiver plena consciência e tiver decidido deliberadamente ***Ignorar o estado do componente***.

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

O ícone da barra de notificação informa 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 ***Ícone da Barra de Notificação*** abre um pequeno menu de contexto com as seguintes opções:

- ***Abrir a Interface do Utilizador do AVG*** - clique para abrir a Interface do Utilizador do AVG
- ***Análises*** - clique para abrir o menu de contexto das análises predefinidas (*Análise de todo o computador*, *Análise de Ficheiros ou Pastas Específicos*, *Análise anti-Rootkit* e seleccione a análise pretendida, que será iniciada imediatamente.
- ***Actualizar agora*** - inicia imediatamente uma actualização
- ***Ajuda*** - abre o ficheiro de ajuda na página inicial

7. Componentes do AVG

7.1. Anti-Vírus

7.1.1. Princípios de Anti-Vírus

O componente de análise do software anti-vírus analisa todos os ficheiros e actividades de ficheiros (abrir/fechar ficheiros, etc.) pela existência de vírus conhecidos. Quaisquer vírus detectados serão impedidos de tomarem qualquer acção e serão eliminados ou 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 significa que o verificador anti-vírus consegue detectar um novo vírus, desconhecido, se o vírus tiver algumas das características habituais dos vírus existentes.

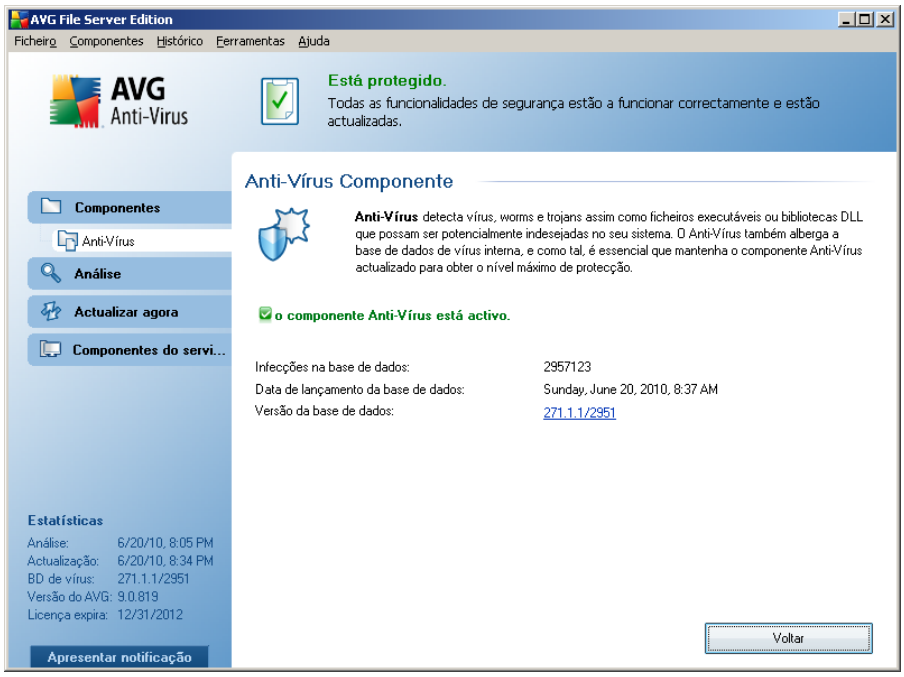
A característica mais importante da protecção anti-vírus é que nenhum vírus conhecido pode ser executado no computador!

Nos casos em que uma única tecnologia pode não ser suficiente para detectar ou identificar um vírus, o ***Anti-Vírus*** combina várias tecnologias para assegurar que o seu computador está protegido contra vírus:

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

O AVG possui ainda a capacidade de analisar e detectar aplicações executáveis ou bibliotecas DLL que poderão ser potencialmente indesejadas no sistema. Tais ameaças são apelidadas de Programas Potencialmente Indesejados (vários tipos de Spyware, adware, etc.). Para além disso, o AVG analisa o registo do sistema para verificar a existência de entradas suspeitas, ficheiros temporários da Internet e cookies de rastreio, permitindo tratar todos os itens potencialmente prejudiciais da mesma forma que qualquer outra infecção.

7.1.2. Interface do Anti-vírus



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

- ***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.*

7.2. Anti-Spyware

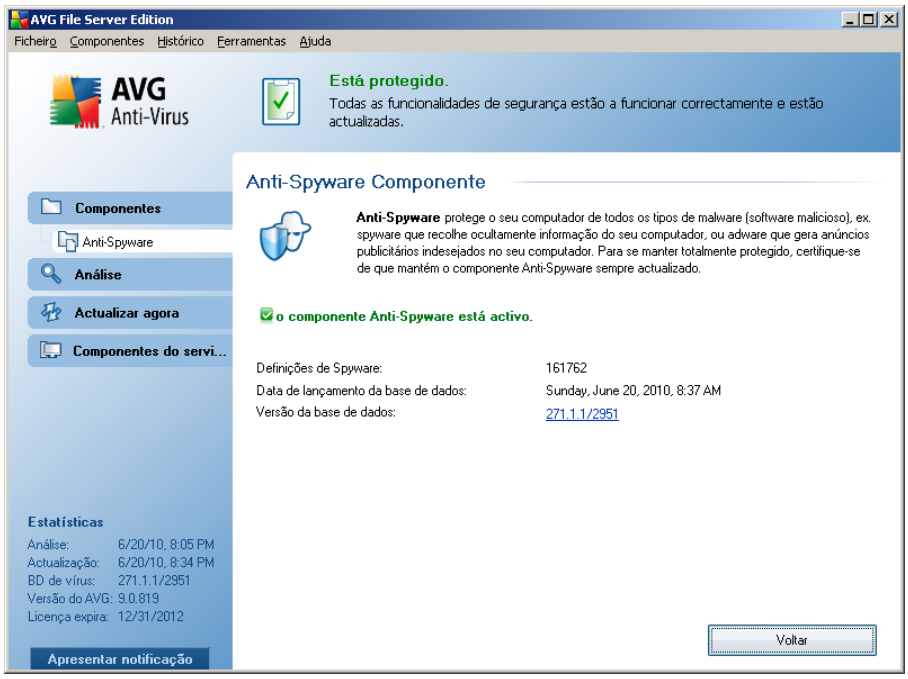
7.2.1. Princípios de Anti-Spyware

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

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

Existe igualmente o risco potencial de ter sido transmitido malware ao computador antes da instalação do AVG, ou que tenha negligenciado as actualizações do **AVG 9.0 File Server**com as bases de dados e actualizações do programa mais recentes. Por este motivo, o AVG permite a verificação completa da existência de malware/spyware no computador, através da funcionalidade de análise. Detecta também malware latente e inactivo, isto é, malware que foi transferido mas ainda não foi activado.

7.2.2. Interface do Anti-Spyware



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.*

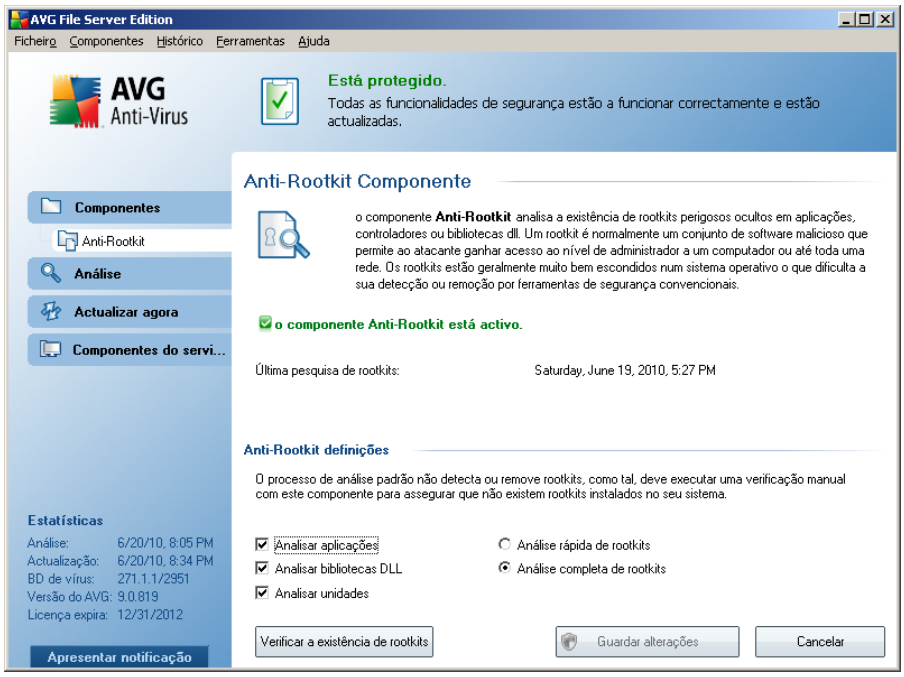
7.3. Anti-Rootkit

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

7.3.1. Princípios do Anti-Rootkit

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

7.3.2. 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:

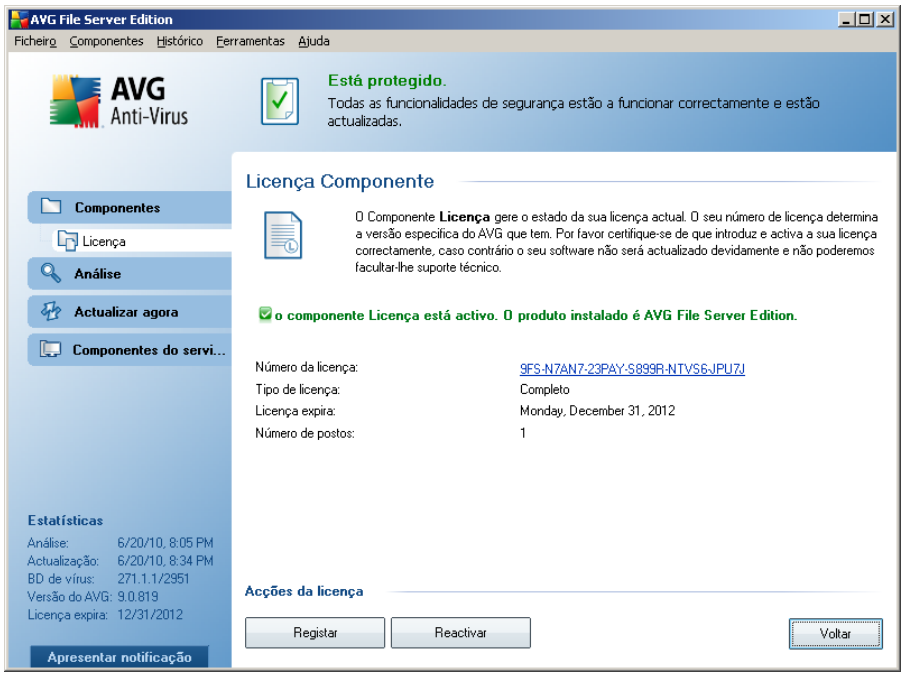
- ***Análise rápida de rootkits*** - analisa somente a pasta sistema *regra geral localizada em c:\Windows*)

- ***Análise completa de rootkits*** - analisa todos os discos acessíveis com a excepção de A: e B:

Botões de controlo disponíveis:

- ***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

7.4. 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. Como tal, recomendamos vivamente que utilize sempre o método "copiar e colar" para qualquer manuseamento do número de licença.

- ***Tipo de licença*** - especifica o tipo de produto instalado.

- ***A licença expira*** - esta data determina o período de validade da sua licença. Se quiser continuar a utilizar o**AVG 9.0 File Server** após esta data terá de renovar a sua licença. A renovação da licença pode ser efectuada on-line no website da AVG (http://www.avg.com).

- ***Número de postos de trabalho*** - quantos postos de trabalho nas quais pode instalar o seu **AVG 9.0 File Server**.

Botões de controlo

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

- ***Reactivar*** - abre a janela ***Activar AVG***com os dados que introduziu na janela ***Personalizar AVG***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*).

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

7.5. Protecção Residente

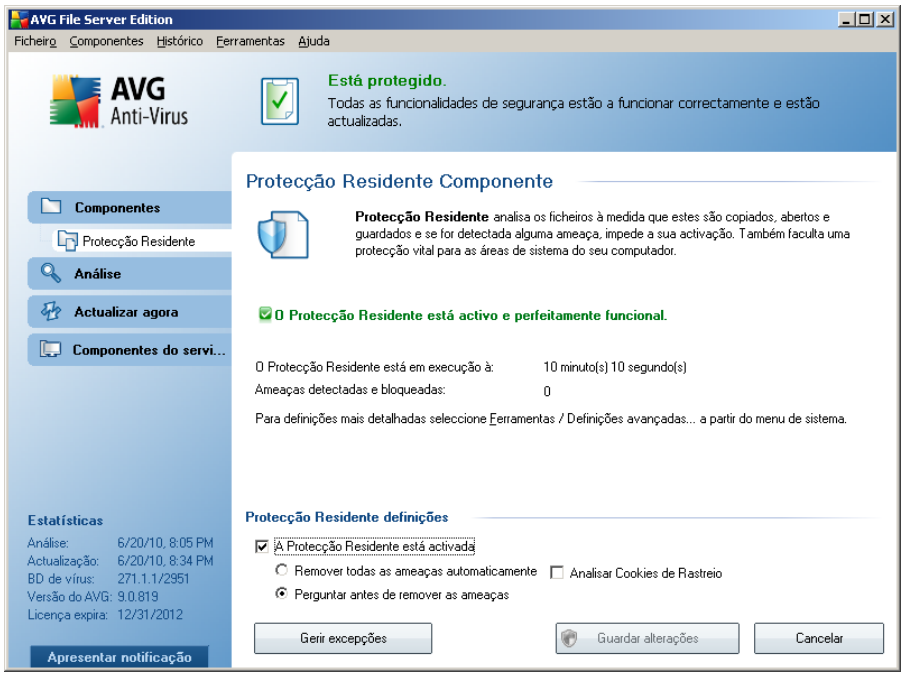
7.5.1. Princípios da Protecção Residente

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

ameaça e remove-a. A ***Protecção Residente*** é carregada na memória do seu computador durante o arranque do sistema.

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

7.5.2. Interface da Protecção Residente



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

- ***A Protecção Residente está activa há*** - faculta o tempo decorrido desde a inicialização do componente

- ***Ameaças detectadas e bloqueadas*** - número de infecções detectadas que foram impedidas de executar/abrir (*se necessário, este valor pode ser restaurado; ex. para propósitos estatísticos - Restaurar valor*)

Configuração básica do componente

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

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

- 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.*

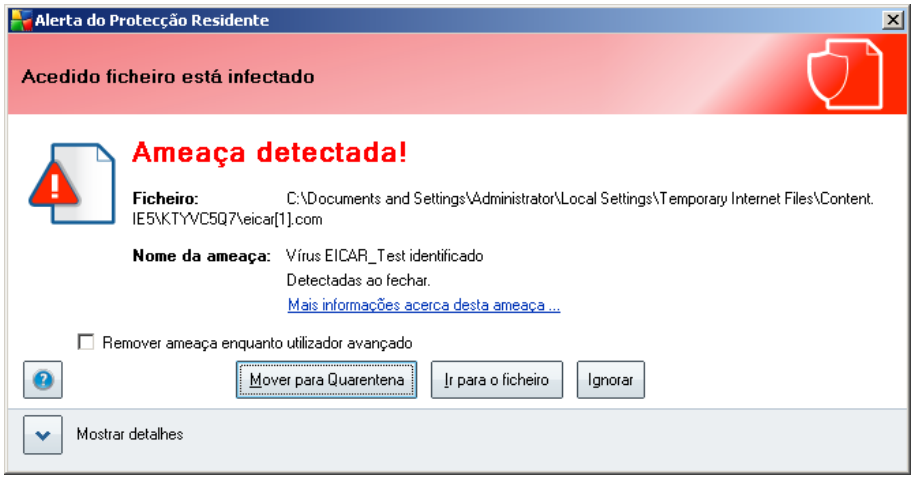
Botões de controlo

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

- ***Gerir excepções*** - abre uma nova janela onde pode definir as pastas/ficheiros que deverão ser ignoradas da análise da ***Protecção Residente*** (para mais informações sobre esta janela, consulte os capítulos ***Exclusões de Directório*** e/ou ***Ficheiros Excluídos***).
- ***Guardar alterações*** - clique neste botão para guardar e aplicar quaisquer alterações efectuadas nesta janela
- ***Cancelar*** - clique neste botão para retroceder para a ***Interface do utilizador do AVG***padrão (síntese dos componentes)

7.5.3. 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:

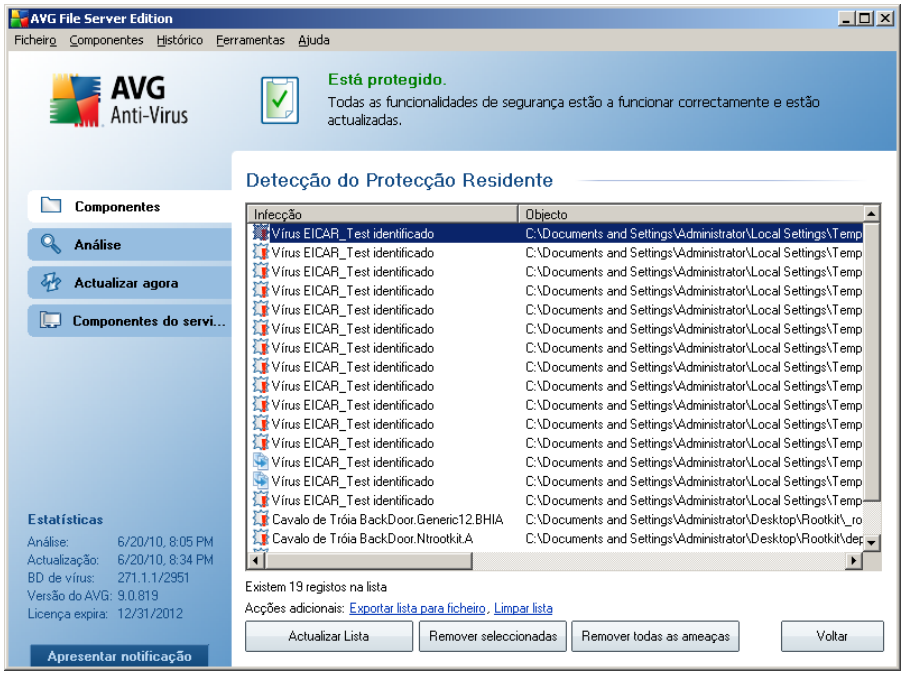
- ***Restaurar*** - se houver uma cura disponível, o AVG restaurará o ficheiro infectado automaticamente; esta opção é a acção recomendada

- ***Mover para a Quarentena*** - o vírus será movido para a ***Quarentena de Vírus do AVG***

- ***Ir para o ficheiro*** - esta opção redirecciona-o para a localização exacta do objecto suspeito (*abre uma nova janela do Explorador do Windows*)

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

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



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

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

- ***Objecto***- localização do objecto

- ***Resultado***- acção efectuada com o objecto detectado

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

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

7.6. Actualizações

7.6.1. Princípios de Actualizações

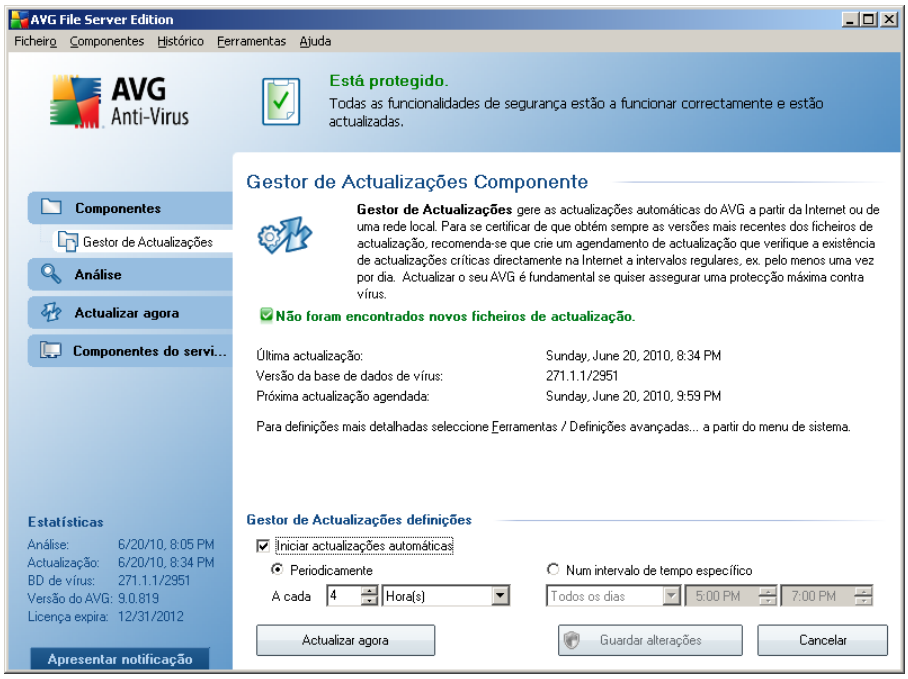
Nenhum software de segurança pode garantir uma protecção efectiva de vários tipos de ameaças a menos que seja actualizado regularmente! Os criadores de vírus estão constantemente à espreita de novas falhas que possam explorar tanto em software como nos sistemas operativos. Novos vírus, novo malware, novos ataques de intrusão surgem todos os dias. Por isso, os vendedores de software estão constantemente a lançar actualizações e correcções, para solucionar quaisquer falhas de segurança que sejam descobertas.

É essencial actualizar o seu AVG regularmente!

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

Nota: *Por favor preste atenção ao capítulo Actualizações do AVG para mais informações relativas a tipos de actualizações e níveis!*

7.6.2. 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
- ***Próxima actualização agendada*** - especifica para quando e a que hora a próxima actualização da base de dados está agendada

Configuração básica do componente

Na parte inferior da janela pode encontrar a secção ***Definições de Actualizações*** onde pode proceder a algumas alterações às regras de execução do processo de actualização. Pode definir se pretende que os ficheiros de actualização sejam transferidos automaticamente (***Iniciar actualizações automáticas*** ou somente

manualmente. Por predefinição, a opção***Iniciar actualizações automáticas*** está activada e recomendamos que a mantenha neste estado! A transferência regular dos mais recentes ficheiros de actualização é essencial para o funcionamento apropriado de qualquer software de segurança!

Pode ainda definir quando a actualização deve ser executada:

- ***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)

8. Componentes do Servidor AVG

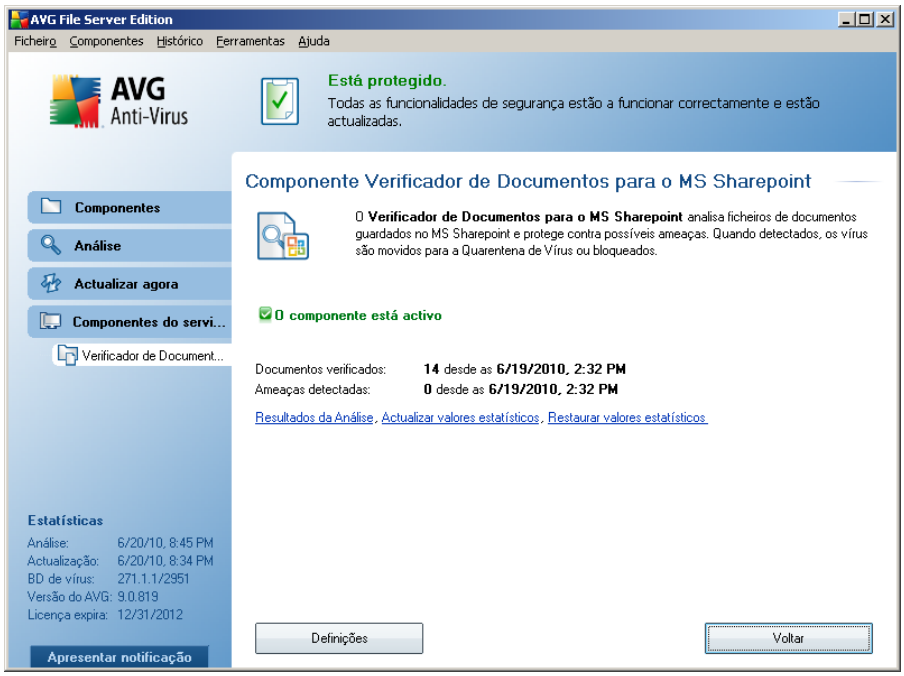
8.1. Verificador de Documentos para o MS Sharepoint

8.1.1. Princípios do Verificador de Documentos

O propósito do componente ***Verificador de documentos para o MS SharePoint*** é analisar documentos guardados no MS SharePoint. Se for detectado algum vírus, será movido para a Quarentena de Vírus ou removido na totalidade.

O Microsoft SharePoint é um conjunto de produtos e elementos de software que inclui, entre uma crescente variedade de componentes, funções de colaboração baseadas no Internet Explorer, módulos de gestão de processos, módulos de pesquisa e uma plataforma de gestão de documentos. O SharePoint pode ser usado para alojar websites que permitem o acesso a espaços de trabalho partilhado, espaços informativos e documentos.

8.1.2. Interface do Verificador de Documentos



Para além de uma síntese dos dados estatísticos mais importantes e das informações relativas ao estado do componente (*O componente está activo*), a interface do

Verificador de documentos para o MS SharePoint disponibiliza uma breve síntese das estatísticas do componente:

- ***Documentos analisados*** - número de documentos analisados desde uma determinada data
- ***Ameaças detectadas*** . número de infecções detectadas desde uma determinada data

O utilizador pode actualizar estas estatísticas em qualquer altura ao clicar na ligação ***Actualizar valores estatísticos***. Os novos dados serão apresentados quase imediatamente. Se quiser restaurar todos os valores estatísticos para zero, clique na ligação ***Restaurar valores estatísticos***. Finalmente, clicar na ligação ***Resultados da Análise*** activará uma nova janela com uma listagem dos resultados da análise. Ordene os dados na listagem por meio dos botões disponibilizados e/ou os separadores.

Botões de controlo

Os botões de controlo disponíveis na interface do ***Verificador de Documentos para o MS SharePoint***são os seguintes:

- ***Definições*** - abre uma nova janela onde pode ajustar vários parâmetros relacionados o desempenho de análise de vírus em documentos do ***Verificador de Documentos para o MS Sharepoint*** (para mais informações sobre esta janela, consulte as secções ***Definições Avançadas do Verificador de Documentos para o MS Sharepoint*** e/ou ***Acções de detecção***).
- ***Retroceder - prima esta botão para regressar à*** Síntese de componentes do servidor*** predefinida.

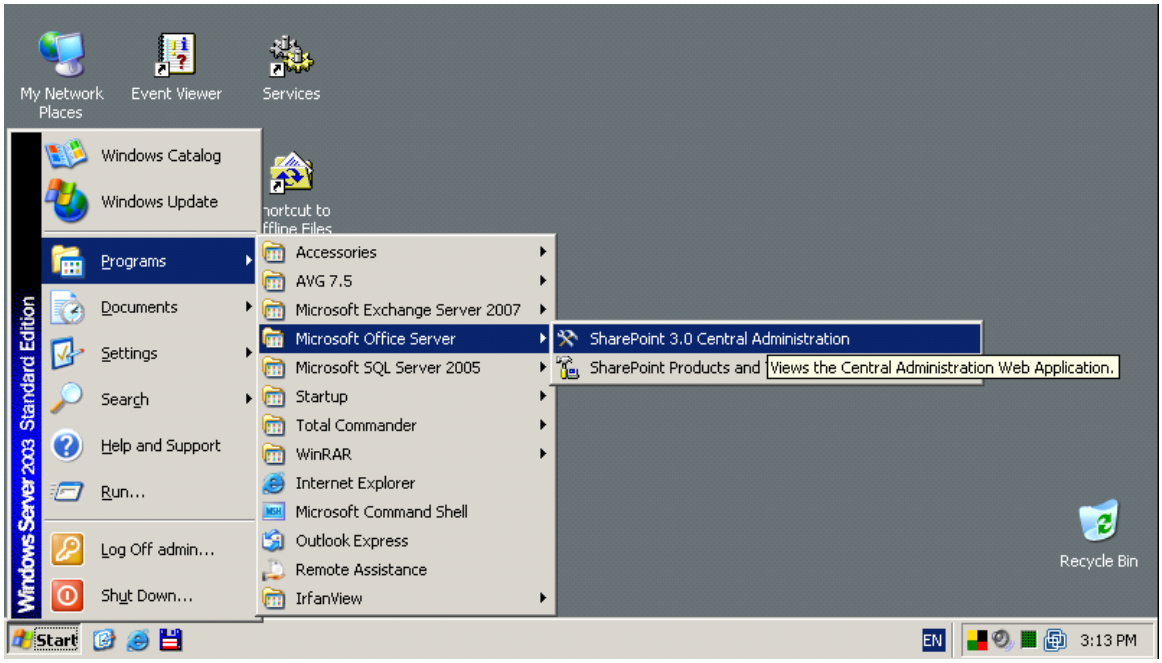
9. AVG para SharePoint Portal Server

Esta secção trata da manutenção do AVG num ***MS SharePoint Portal Server*** que pode ser considerado um tipo especial de servidor de ficheiros.

9.1. Manutenção do Programa

O **AVG for SharePoint Portal Server** usa a interface de análise de vírus Microsoft SP VSAPI 1.4 para protecção do seu servidor contra possíveis infecções de vírus. Os objectos no servidor são analisados pela presença de malware aquando da sua transferência e/ou carregamento de ou para o servidor pelos utilizadores. A configuração da protecção anti-vírus pode ser configurada na interface da ***Administração Central*** do seu SharePoint Portal Server. Na ***Administração Central***, também pode consultar e gerir o ficheiro de registo do **AVG for SharePoint Portal Server**.

Pode iniciar a ***Administração Central do SharePoint Portal Server*** quando tiver sessão iniciada no computador que tem o servidor instalado. A interface de administração é baseada na Internet (*assim como a interface do utilizador do SharePoint Portal Server*) e o utilizador pode aceder à mesma através da opção ***SharePoint (3.0) Central Administration*** na pasta ***Programas/Microsoft Office Server*** ou menu Iniciar do Windows/***SharePoint Portal Server***):

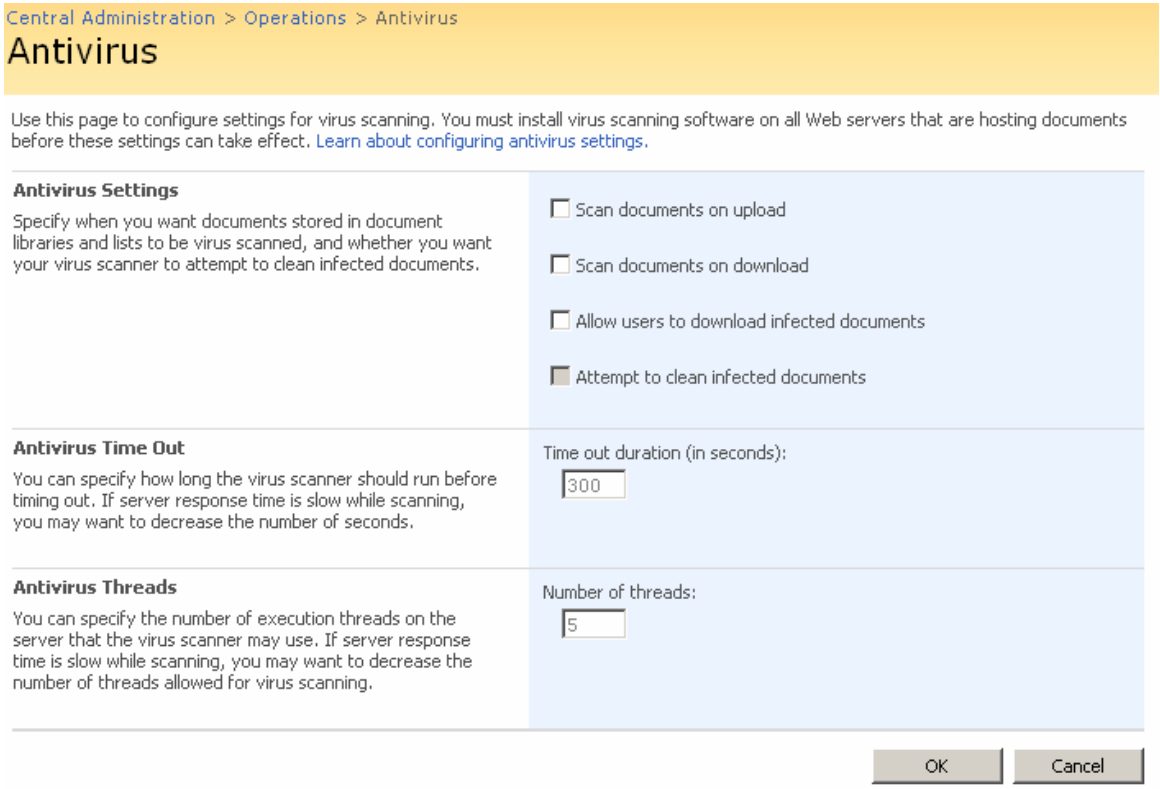


Também pode aceder à página Web da ***Administração Central do SharePoint Portal Server*** remotamente usando os direitos de acesso e URL correctos.

9.2. Configuração do AVG para SPPS - SharePoint 2007

Na interface ***SharePoint 3.0 Central Administration*** pode configurar facilmente os parâmetros de desempenho e as acções do verificador **AVG for SharePoint Portal Server**. Escolha a opção ***Operações*** na secção ***Administração Central***. Será apresentada uma nova janela. Seleccione o item ***Anti-vírus*** na ***Configuração da Segurança***.

Será apresentada a seguinte janela:



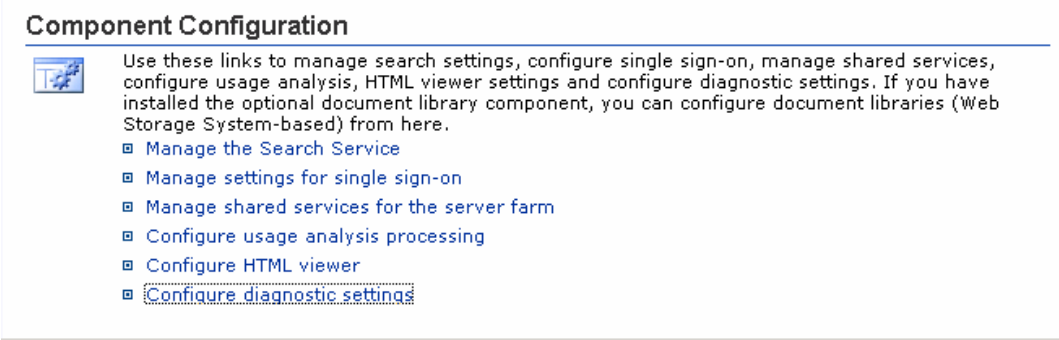
Pode configurar várias funcionalidades relativas a desempenho e acções de análise do anti-vírus do **AVG for SharePoint Portal Server** aqui:

- ***Analisar documentos aquando do carregamento*** - activar/desactivar a análise de documentos em fase de carregamento
- ***Analisar documentos aquando da transferência*** - activar/desactivar a análise de documentos em fase de transferência
- ***Permitir que os utilizadores transfiram documentos infectados*** - permitir/impedir a transferência de documentos infectados pelos utilizadores
- ***Tentar limpar os documentos infectados*** - activar/desactivar o restauro automático dos documentos infectados
- ***Duração do tempo limite*** *em segundos*- o número máximo de segundos que o processo de análise de vírus demorará após uma execução (diminua o valor quando a resposta do servidor parecer muito lenta devido a análise dos documentos)

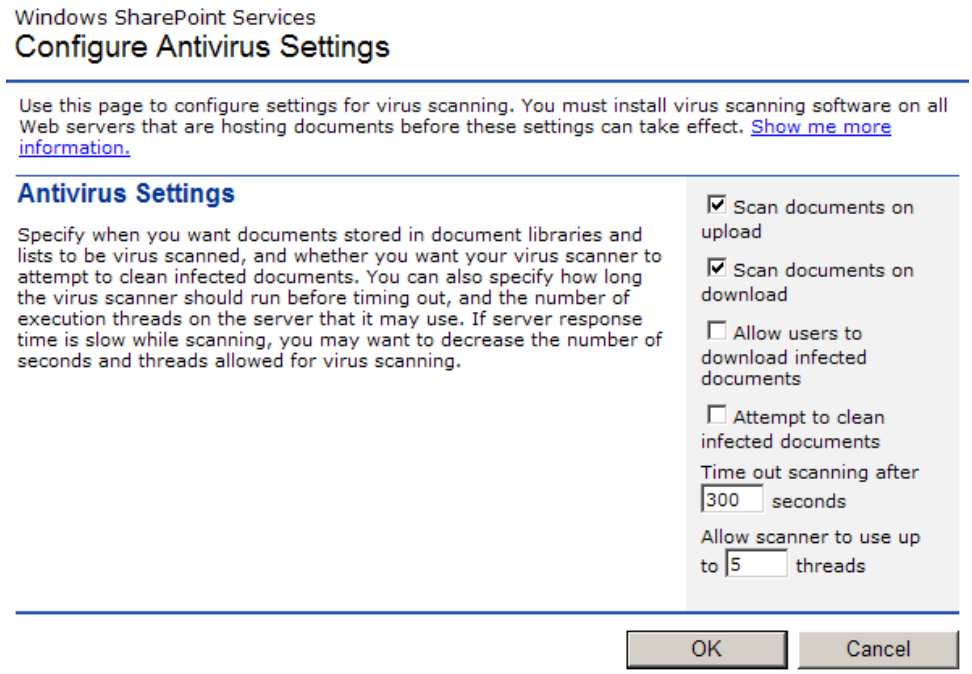
- ***Número de tópicos***- pode especificar o número de tópicos de análise de vírus que podem ser executados em simultâneo; o aumento deste número pode aumentar a velocidade da análise devido ao maior nível de paralelismo, mas, por outro lado, pode aumentar o tempo de resposta do servidor.

9.3. Configuração do AVG para SPPS - SharePoint 2003

Na interface ***SharePoint Portal Server Central Administration*** pode configurar facilmente os parâmetros de desempenho e as acções do verificador **AVG for SharePoint Portal Server**. Escolha a opção ***Configuração das Acções do Anti-vírus*** na secção ***Configuração da Segurança***:



Será apresentada a seguinte janela:



Pode configurar várias funcionalidades relativas a desempenho e acções de análise do anti-vírus do **AVG for SharePoint Portal Server** aqui:

- ***Analisar documentos aquando do carregamento*** - activar/desactivar a análise de documentos em fase de carregamento
- ***Analisar documentos aquando da transferência*** - activar/desactivar a análise de documentos em fase de transferência
- ***Permitir que os utilizadores transfiram documentos infectados*** - permitir/impedir que os utilizadores transfiram documentos infectados
- ***Tentar limpar os documentos infectados*** - activar/desactivar o restauro automático dos documentos infectados
- ***Tempo limite da análise*** - o número máximo de segundos que o processo de análise de vírus demorará após uma execução (*diminua o valor quando a resposta do servidor parecer muito lenta devido a análise dos documentos*)
- ***Usar número máximo de processos X secundários aquando da análise de documentos*** - o X especifica o número de tópicos de análise de vírus que podem ser executados em simultâneo; o aumento deste número pode aumentar

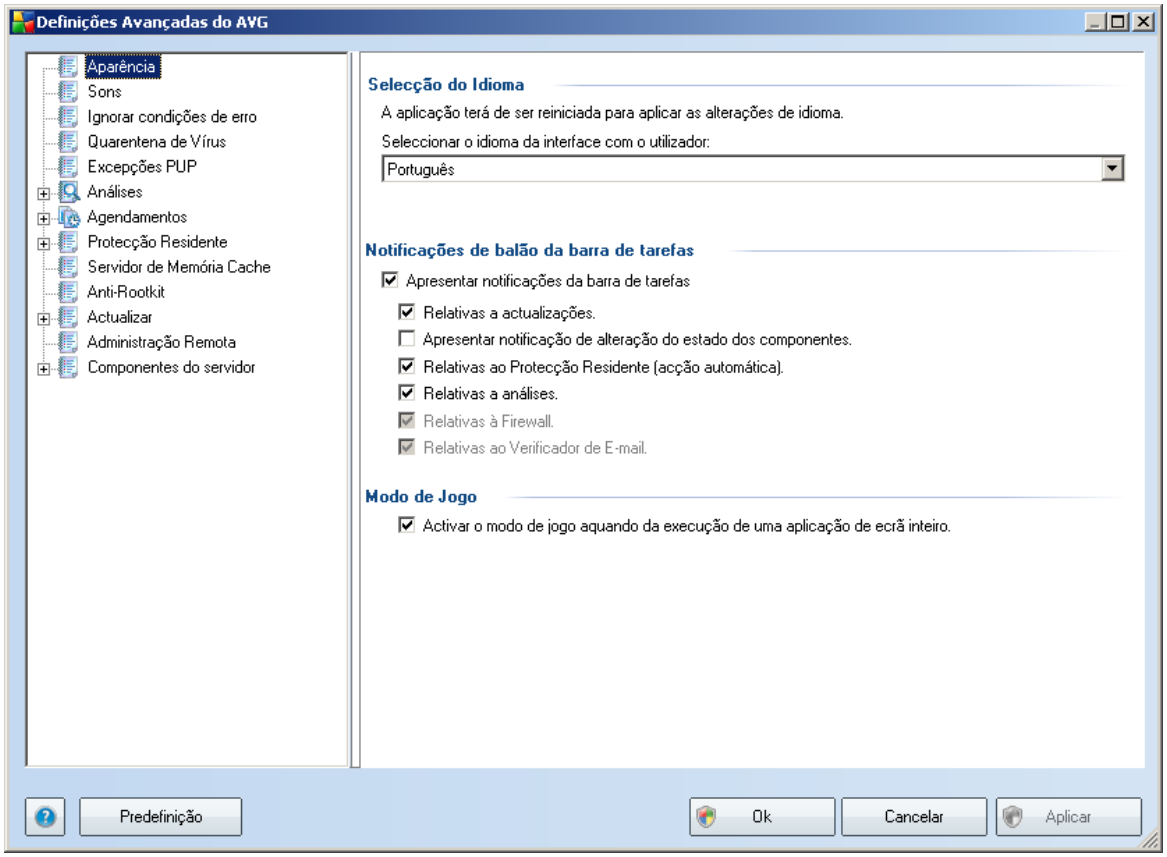
a velocidade da análise devido ao maior nível de paralelismo, mas, por outro lado, pode aumentar o tempo de resposta do servidor.

10. Definições Avançadas do AVG

A janela de configuração avançada do **AVG 9.0 File Server** abre numa nova janela com a identificação***Definições Avançadas do AVG***. A janela está dividida em duas secções: a parte esquerda disponibiliza uma navegação esquematizada em árvore às opções de configuração do programa. Seleccione o componente ao qual pretende alterar a configuração (*ou a parte especifica deste*) para abrir a janela de edição na janela na secção do lado direito.

10.1. Aparência

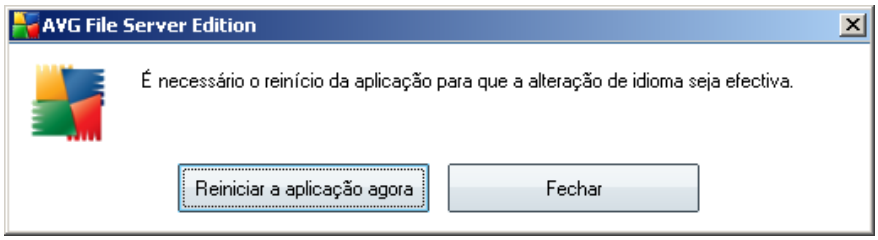
O primeiro item da árvore de navegação, ***Aparência***, refere-se às definições gerais da Interface do utilizador do AVG e a algumas opções elementares do comportamento da aplicação:



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)
- Prima o botão ***OK*** para confirmar
- É apresentada uma nova janela a informá-lo de que a alteração do idioma da interface do utilizador do AVG requer a reinicialização da aplicação:



Notificações de balão da barra de tarefas

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

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

- ***Apresentar notificações da barra de notificações do sistema*** - este item está seleccionado por predefinição (*activado*), e as notificações são apresentadas. Desmarque este item para desactivar por completo a apresentação de balões de notificação. Quando activado, pode ainda especificar quais as notificações específicas que devem ser apresentadas.

- ***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 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 *(esta opção é a única desactivada por predefinição)*.

- ***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;

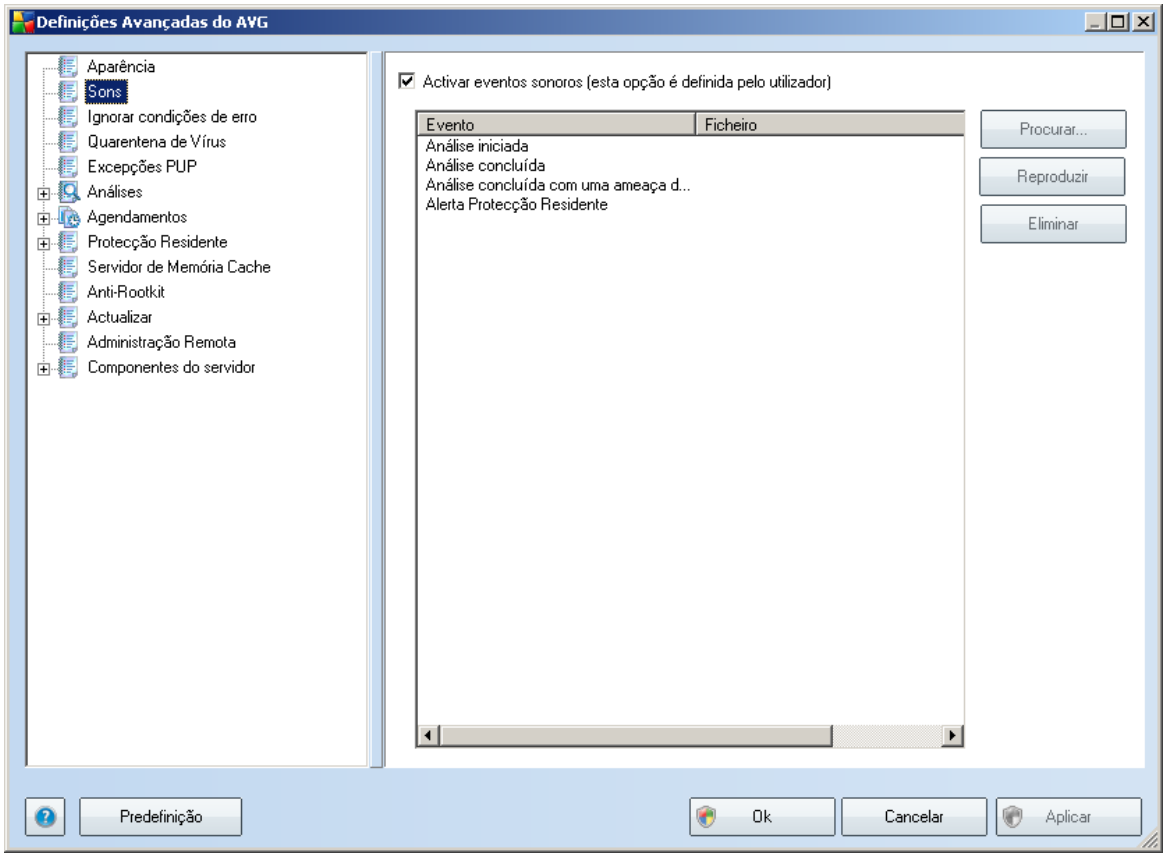
- ***Apresentar notificações da barra de notificação relativas a análises*** - decida se as informações relativas ao início automático da análise agendada, o seu progresso e resultados deverão ser apresentadas.

Modo de Jogo

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

10.2. Sons

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

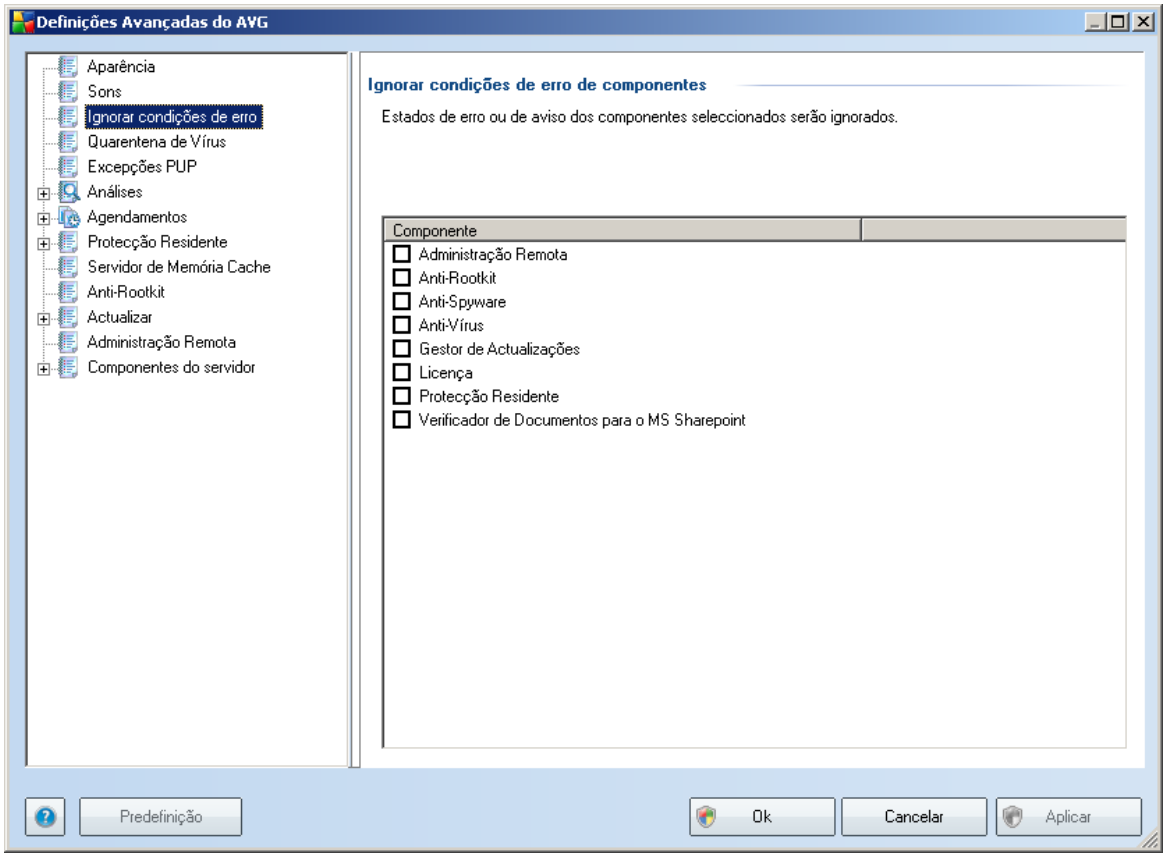


Depois, seleccione o evento respectivo a partir da lista procure (***Procurar***) no seu disco um som adequado que pretenda atribuir a este evento. Para ouvir o som seleccionado, realce o evento na lista e prima o botão ***Reproduzir*** . Use o botão ***Eliminar*** para remover o som atribuído a um evento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

Nota: *Só são suportados sons *.wav!*

10.3. Ignorar Condições de Erro

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



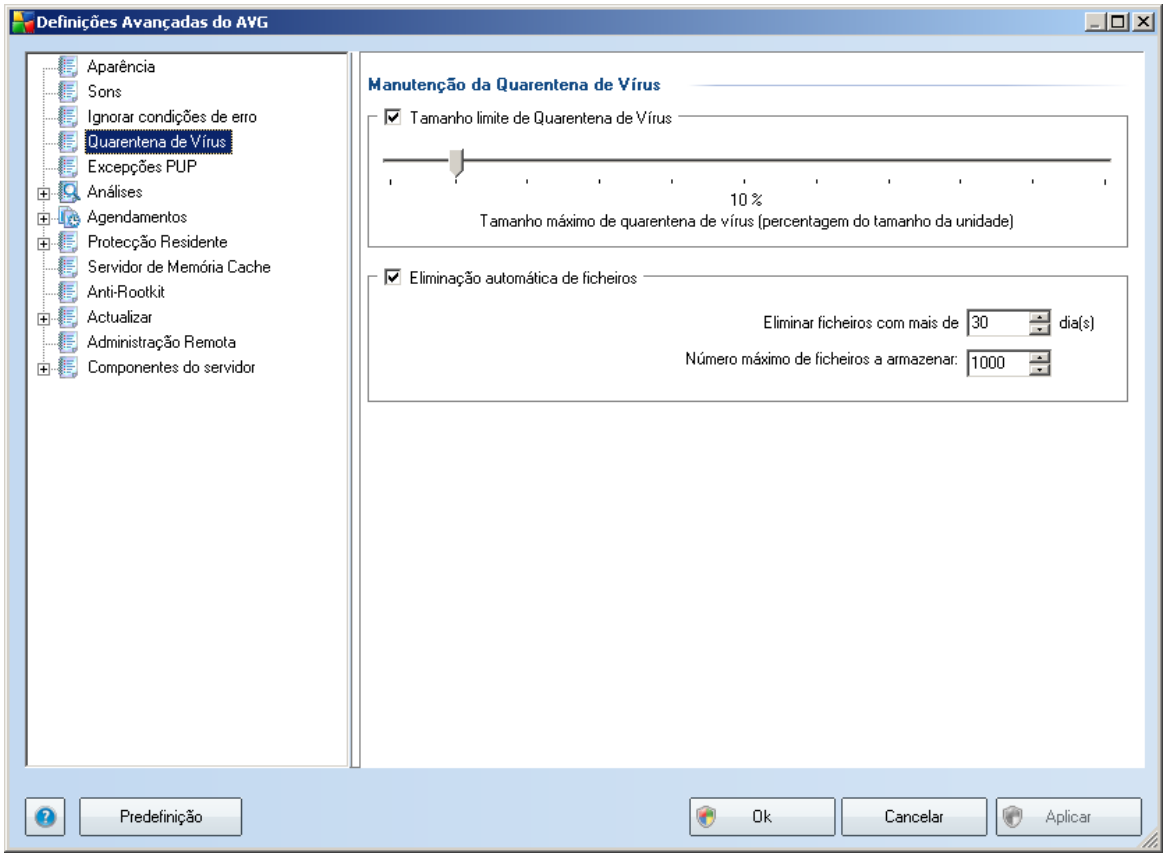
Por predefinição, nenhum dos componentes na lista está seleccionado. O que significa que se algum componente obtiver um estado de erro, será informado imediatamente dessa situação através:

- ***ícone da barra de notificação*** - enquanto todos os componentes do AVG estiverem a funcionar devidamente, o ícone é apresentado com quatro cores; no entanto, se ocorrer um erro, o ícone será apresentado 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 com o ponto de exclamação, o ícone não poderá apresentar quaisquer outros erros que possam surgir.

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

10.4. Quarentena de Vírus



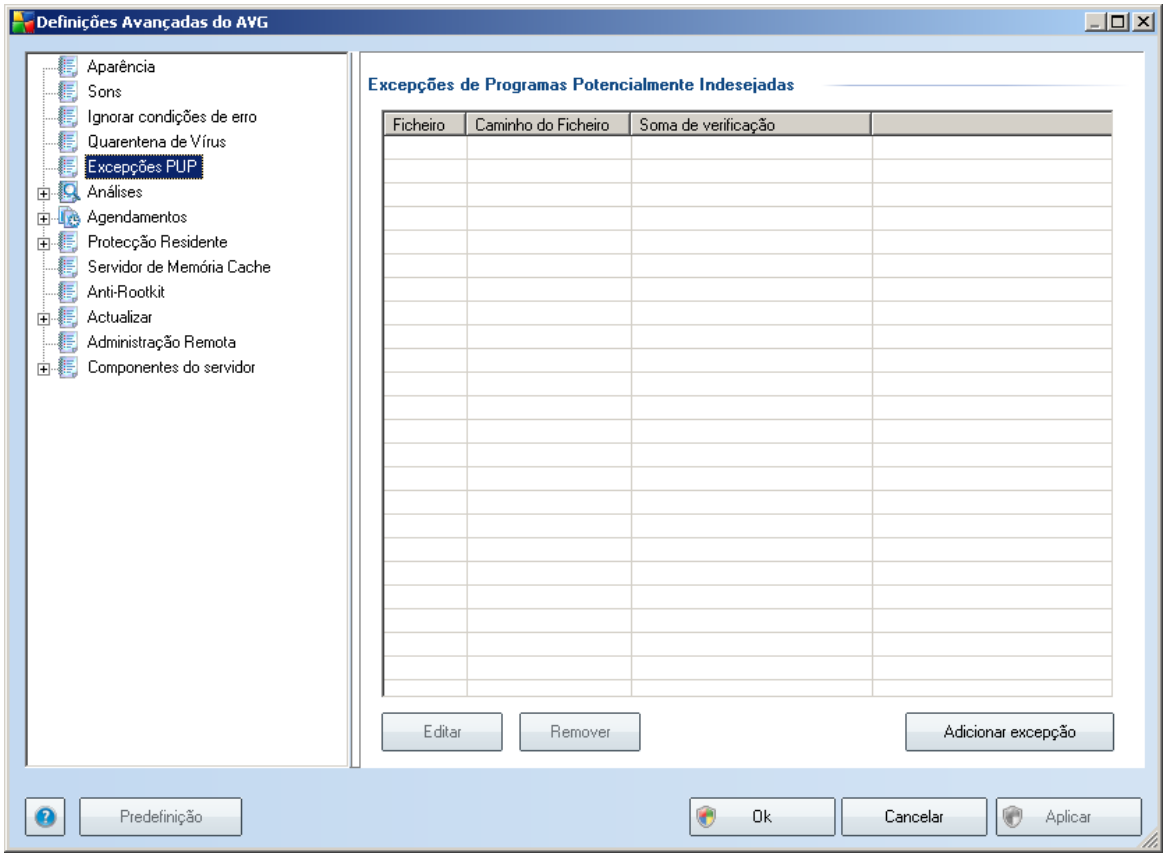
A janela ***Manutenção da Quarentena de Vírus*** permite-lhe definir vários parâmetros em relação à administração dos objectos armazenados na***Quarentena de Vírus***:

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

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

10.5. Excepções PUP

O **AVG 9.0 File Server** 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 a lista, eliminar itens existentes, ou adicionar novas excepções. As seguintes informações podem ser encontradas na lista para todas as excepções:

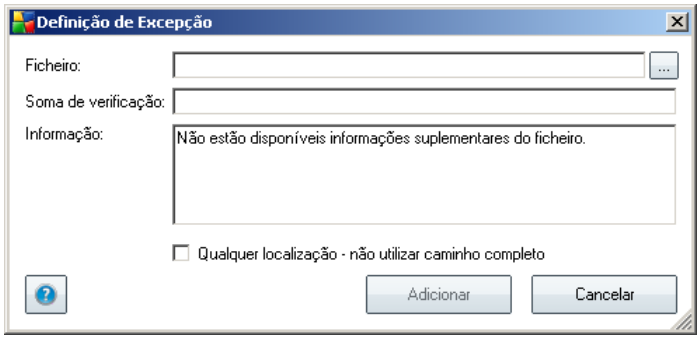
- ***Ficheiro*** - faculta o nome da aplicação respectiva
- ***Localização do Ficheiro*** - apresenta a localização da aplicação
- ***Soma de verificação***- apresenta a 'assinatura' única do ficheiro seleccionado. Esta soma de verificação é uma cadeia de caracteres gerada automaticamente, que permite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

Botões de controlo

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

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

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



  - ***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.

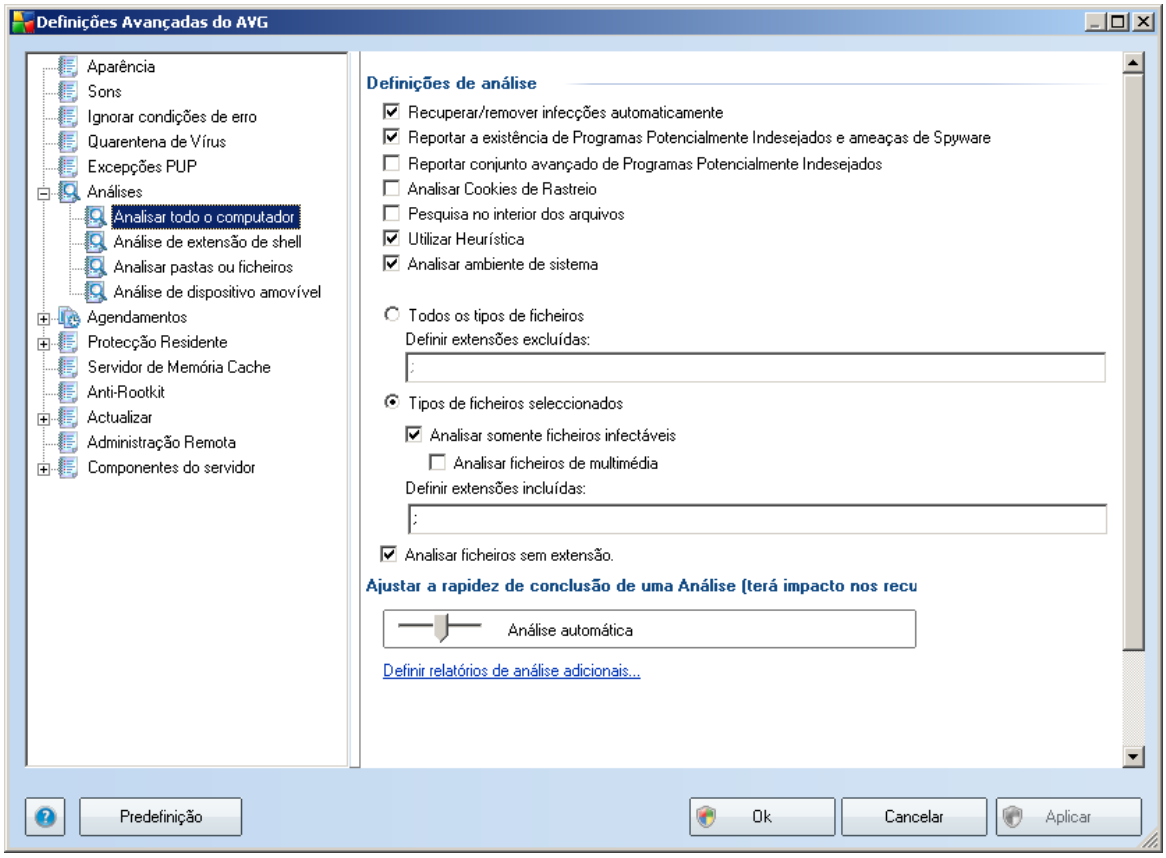
10.6. Análises

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

- ***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

10.6.1. 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.

- ***Reportar Programas Potencialmente Indesejados e Ameaças de Spyware*** - 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;

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

- ***Analisar a Existência de Cookies de Rastreio*** este parâmetro do componente Anti-Spyware define que as cookies deverão ser detectadas; (*cookies HTTP são utilizadas para autenticação, rastreio, e manutenção de informação 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.

Além disso deve decidir se pretende que sejam analisados

- ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

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

reduzirá o tempo de análise ainda mais uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infectados por vírus). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser analisados.

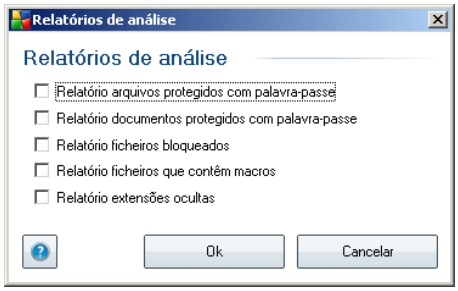
- Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** - esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

Prioridade do processo de análise

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

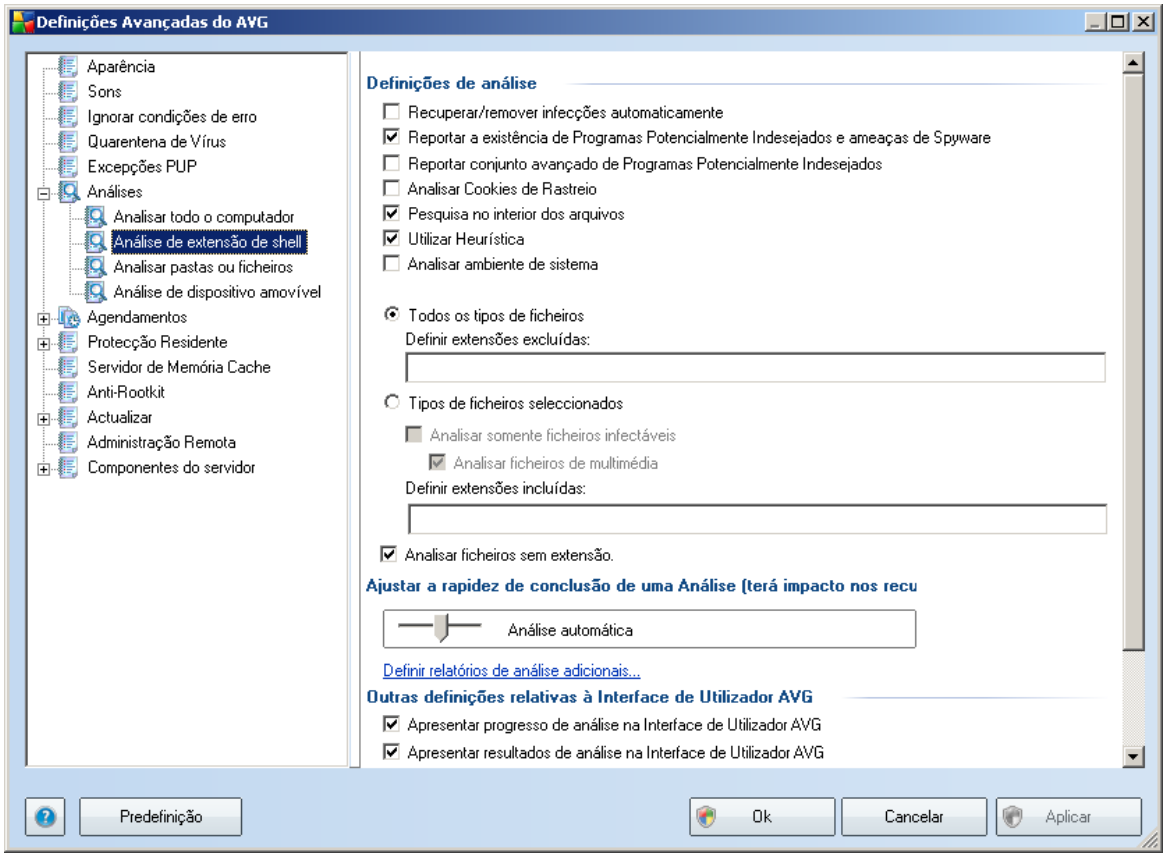
Definir relatórios de análise adicionais...

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



10.6.2. Análise em contexto

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



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

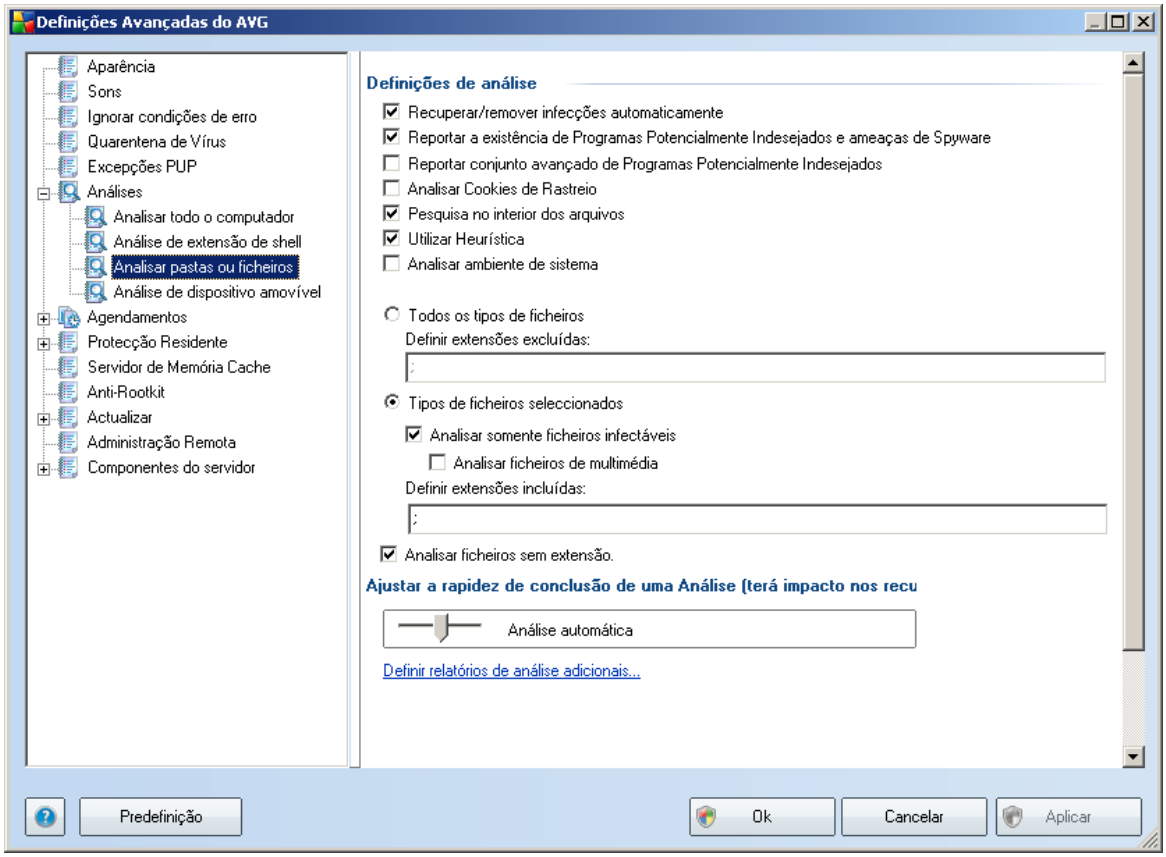
Nota:*Para uma descrição de parâmetros específicos, por favor consulte o capítulo* ***Definições Avançadas do AVG / Análises / Analisar Todo o Computador*** *.*

No entanto, há alguns parâmetros que só são apresentados na Análise da extensão de shell. Pode encontrar estes parâmetros na secção **Outras definições relativas à Interface do Utilizador do AVG**:

- ***Apresentar progresso da análise na Interface do Utilizador do AVG*** - se esta caixa estiver marcada, será notificado sobre cada início/conclusão de uma Análise da extensão de shell (será apresentada uma pequena janela de informação no canto inferior do ecrã).
- ***Apresentar resultado da análise na Interface do Utilizador do AVG*** - se esta caixa estiver marcada, sempre que a Análise da extensão de shell terminar, a Interface do Utilizador do AVG é aberta e será apresentada a janela ***Detalhes dos Resultados da Análise*** padrão (o número de separadores dependerá dos resultados de análise).
    - ***Só se a análise detectar alguma ameaça*** - esta caixa só estará activa se a anterior tiver sido marcada. Se a marcar, a janela ***Detalhes dos Resultados da Análise*** será apresentada se tiverem sido detectadas ameaças durante a Análise da extensão de shell.

10.6.3. Analisar pastas ou ficheiros específicos

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

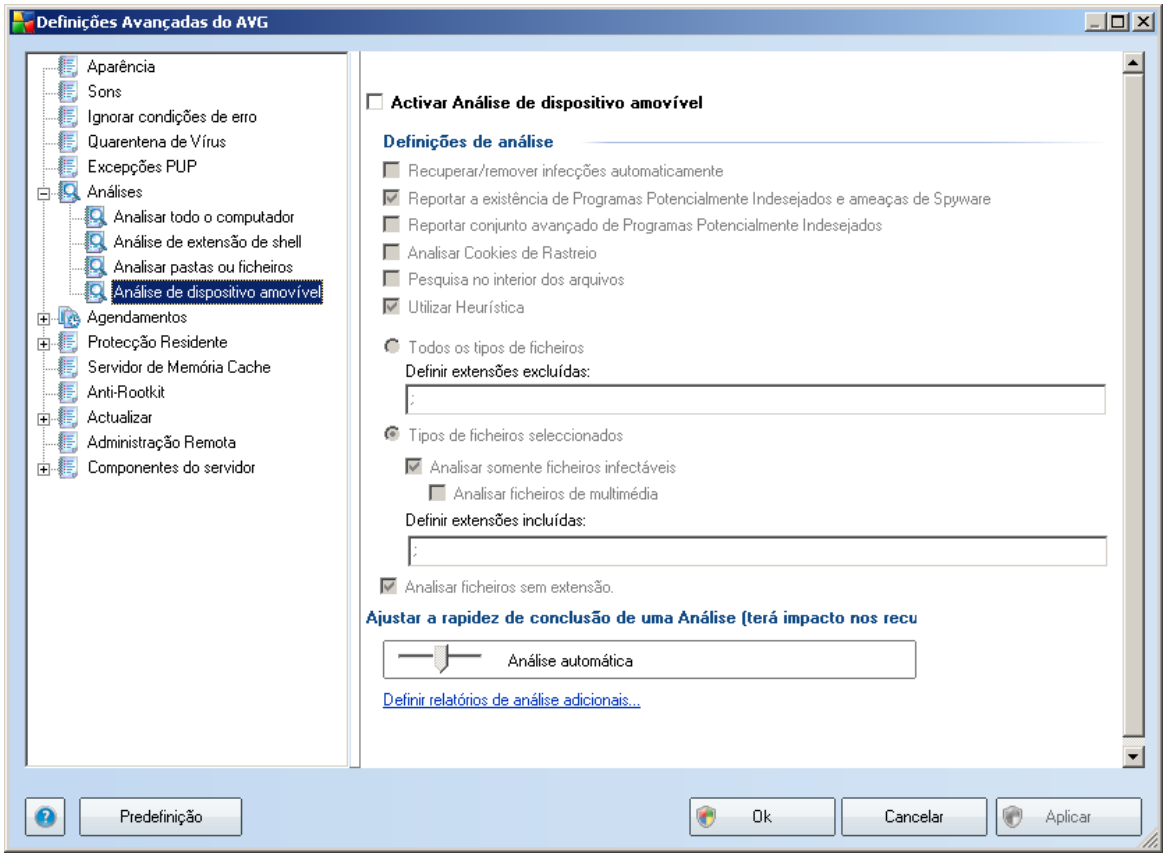


Todos os parâmetros definidos nesta janela de configuração aplicam-se apenas às áreas seleccionadas para análise com a ***Análise de ficheiros e pastas específicos***!

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

10.6.4. 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*** .

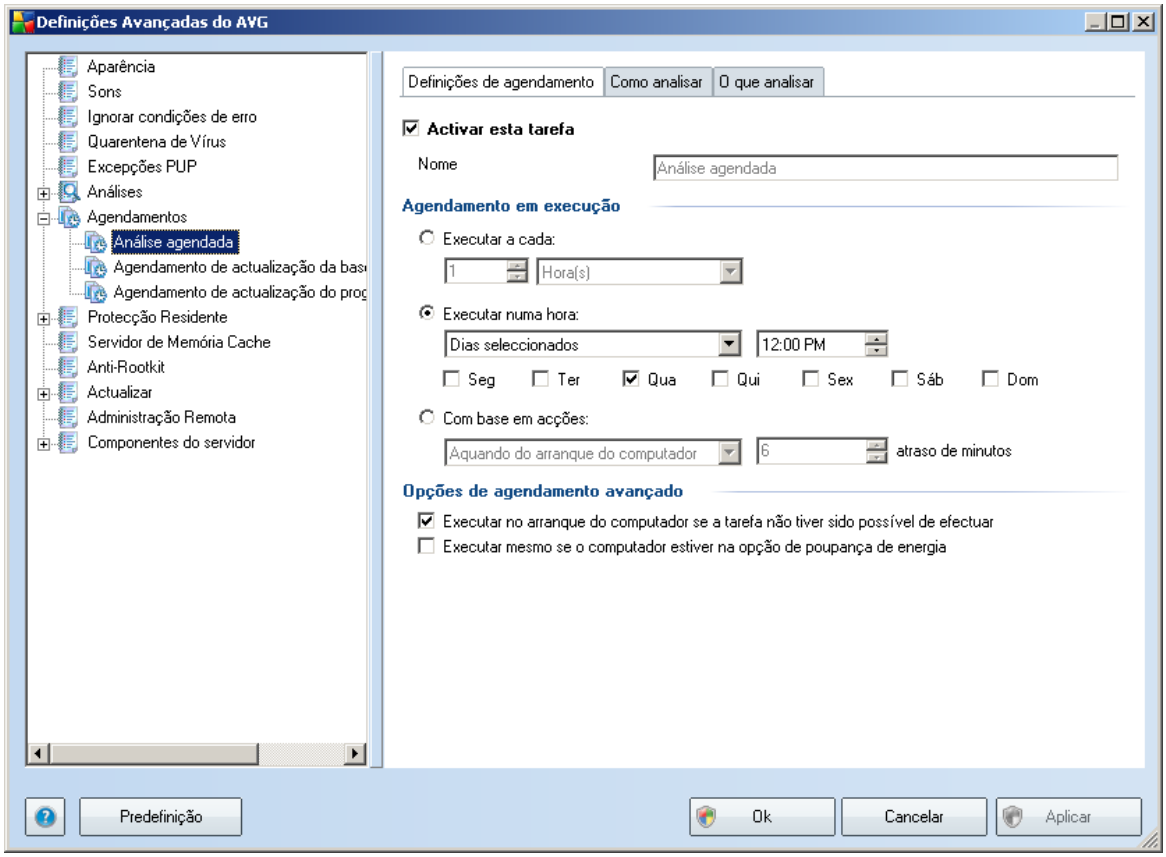
10.7. Agendamentos

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

- Agendamento de análise a todo o computador
- Agendamento de actualização da base de dados de vírus
- Agendamento de actualização do programa

10.7.1. Análise agendada

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



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

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

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

Nesta janela pode ainda definir os seguintes parâmetros de análise:

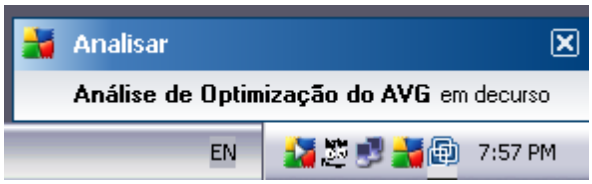
Agendamento em execução

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

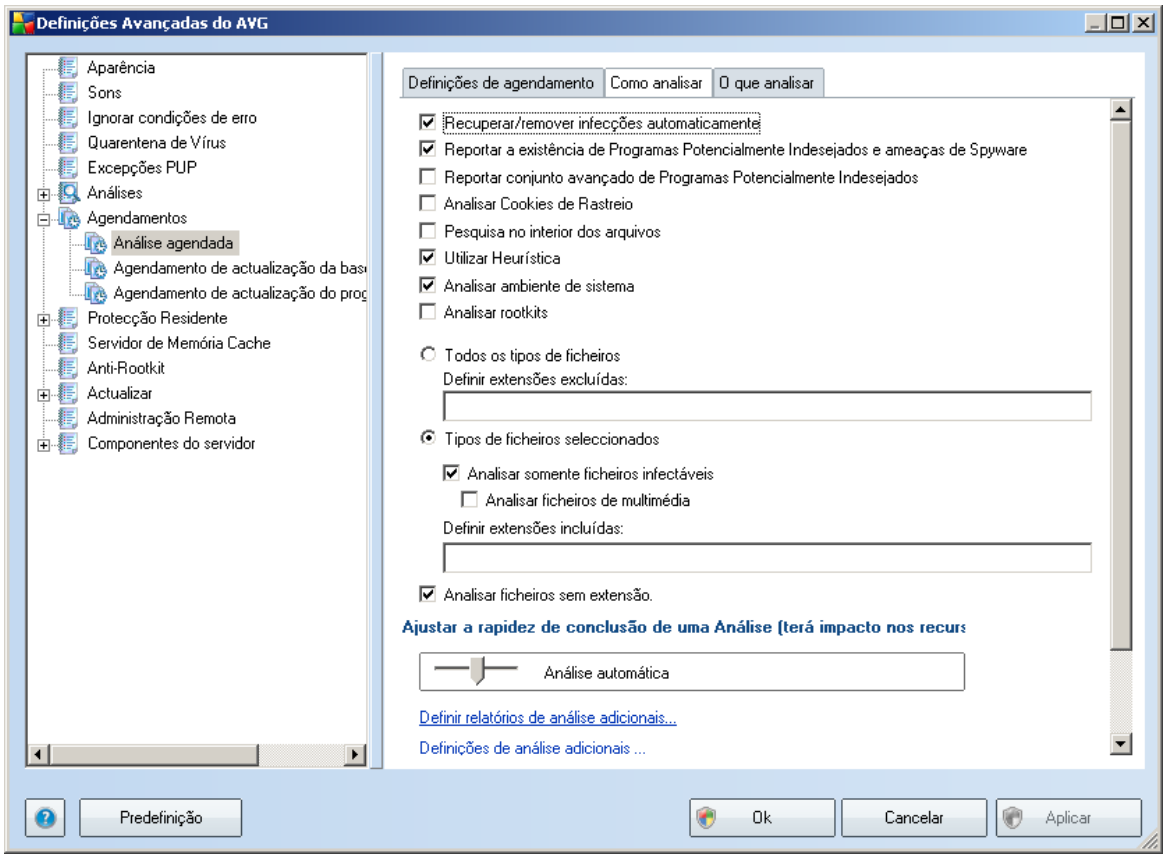
Opções de agendamento avançado

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.



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

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

- ***Reportar Programas Potencialmente Indesejados e Ameaças de Spyware*** - (*activado por predefinição*): 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;

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

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

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

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

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

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

Além disso deve decidir se pretende que sejam analisados

- ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

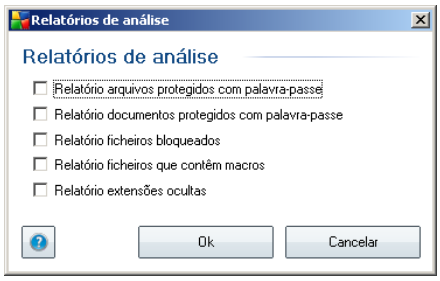
- ***Tipos de ficheiros seleccionados*** - pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros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

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

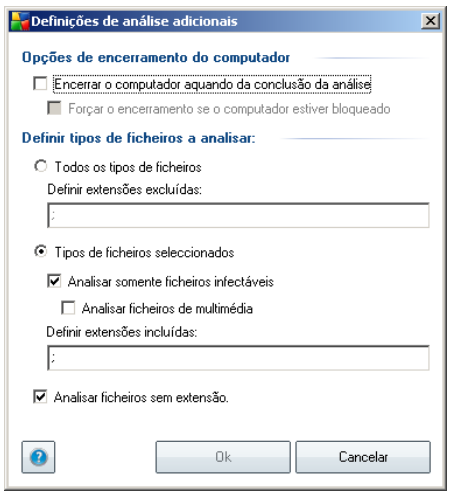
Prioridade do processo de análise

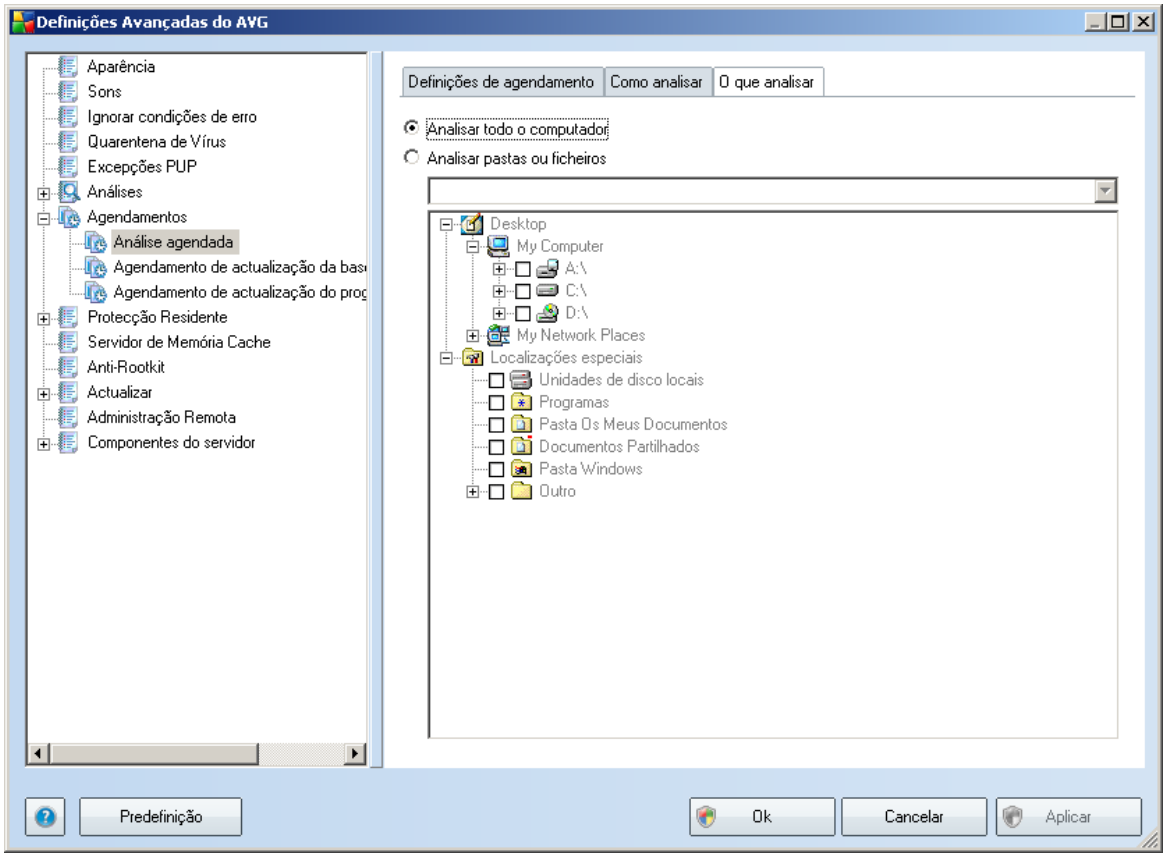
Na secção ***Prioridade do processo de análise*** pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. O valor desta opção está por predefinição definido para o nível médio de utilização automática de recursos. Se quiser que a análise seja executada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



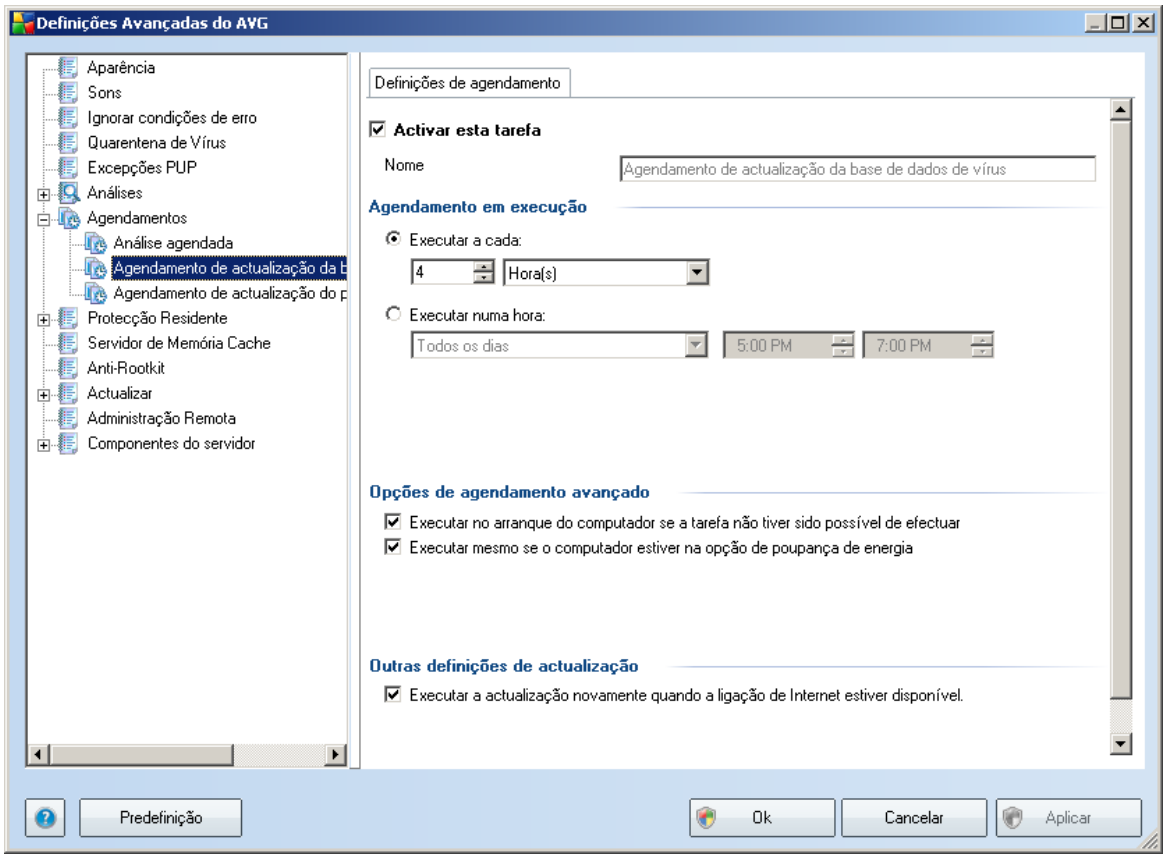
Clique nas ***Definições de análise adicionais...***para abrir uma nova janela de ***Opções de encerramento do computador*** onde pode decidir se o computador deve ser encerrado automaticamente aquando do término do processo de análise. Tendo confirmado esta opção (***Encerrar o computador aquando do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

10.7.2. 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:

No campo de texto ***Nome*** (*desactivado para todos os agendamentos predefinidos*) encontra o nome atribuído ao agendamento actual pelo fornecedor do software. Para agendamentos novos (*o utilizador pode adicionar novos agendamentos ao clicar com o botão direito do rato sobre o item* ***Agendamento de actualização da base de dados de vírus*** *na árvore de navegação à esquerda*) o utilizador pode especificar um nome da sua preferência, e nessas situações o campo de texto estará aberto para edição. Tente utilizar sempre nomes descritivos e adequados para os seus

agendamentos para facilitar o reconhecimento dos mesmos.

Agendamento em execução

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

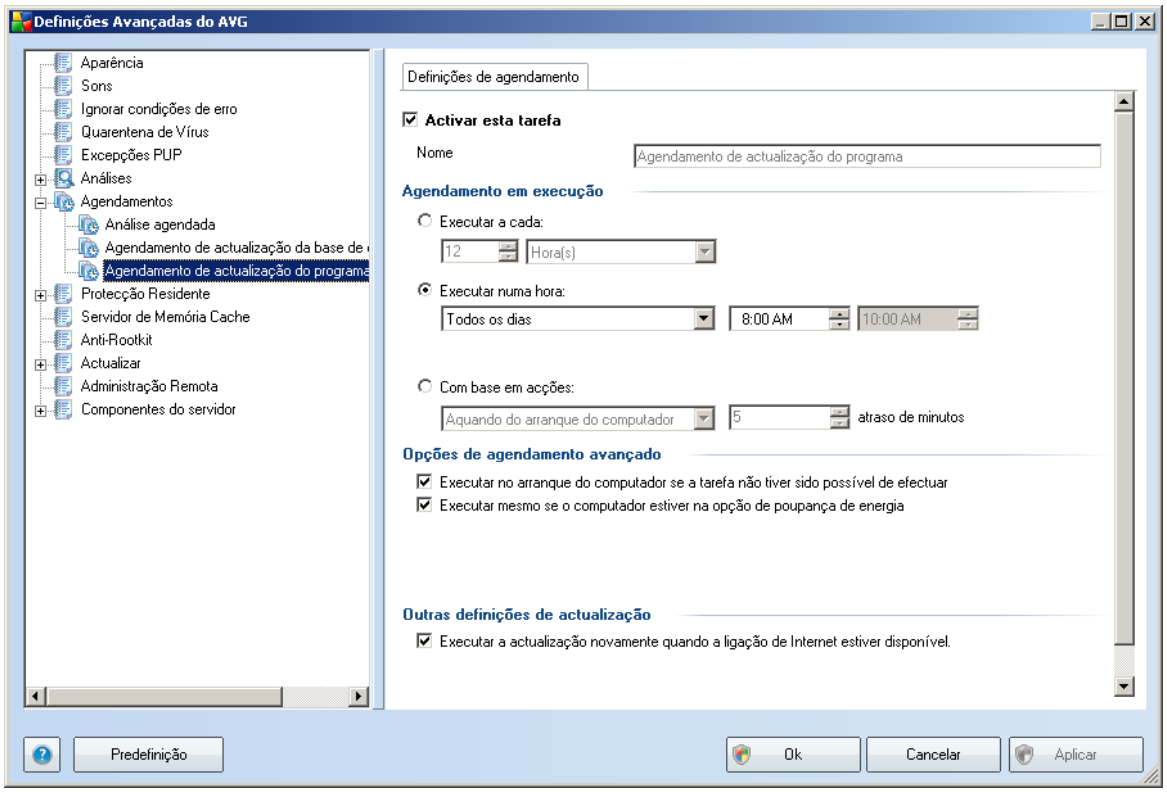
Esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de bateria fraca ou desligado.

Outras definições de actualização

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

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

10.7.3. 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.

No campo de texto ***Nome*** (*desactivado para todos os agendamentos predefinidos*) encontra o nome atribuído ao agendamento actual pelo fornecedor do software. Para agendamentos novos (*o utilizador pode adicionar novos agendamentos ao clicar com o botão direito do rato sobre o item* ***Agendamento de actualização do programa*** *na árvore de navegação à esquerda*) o utilizador pode especificar um nome da sua preferência, e nessas situações o campo de texto estará aberto para edição. Tente utilizar sempre nomes descritivos e adequados para os seus agendamentos para facilitar o reconhecimento dos mesmos.

Agendamento em execução

Aqui, especifique os intervalos de tempo para a execução do novo agendamento de

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

Opções de agendamento avançado

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

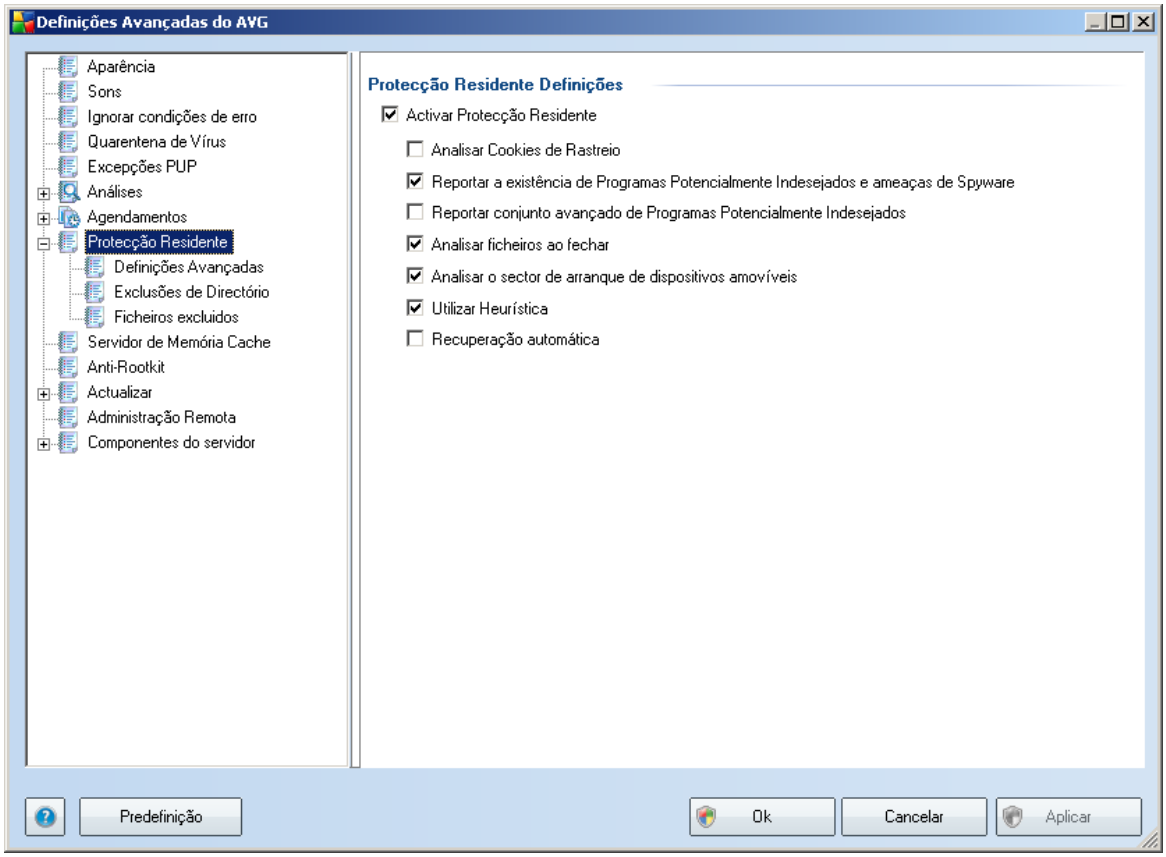
Outras definições de actualização

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

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

10.8. Protecção Residente

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



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

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

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

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

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

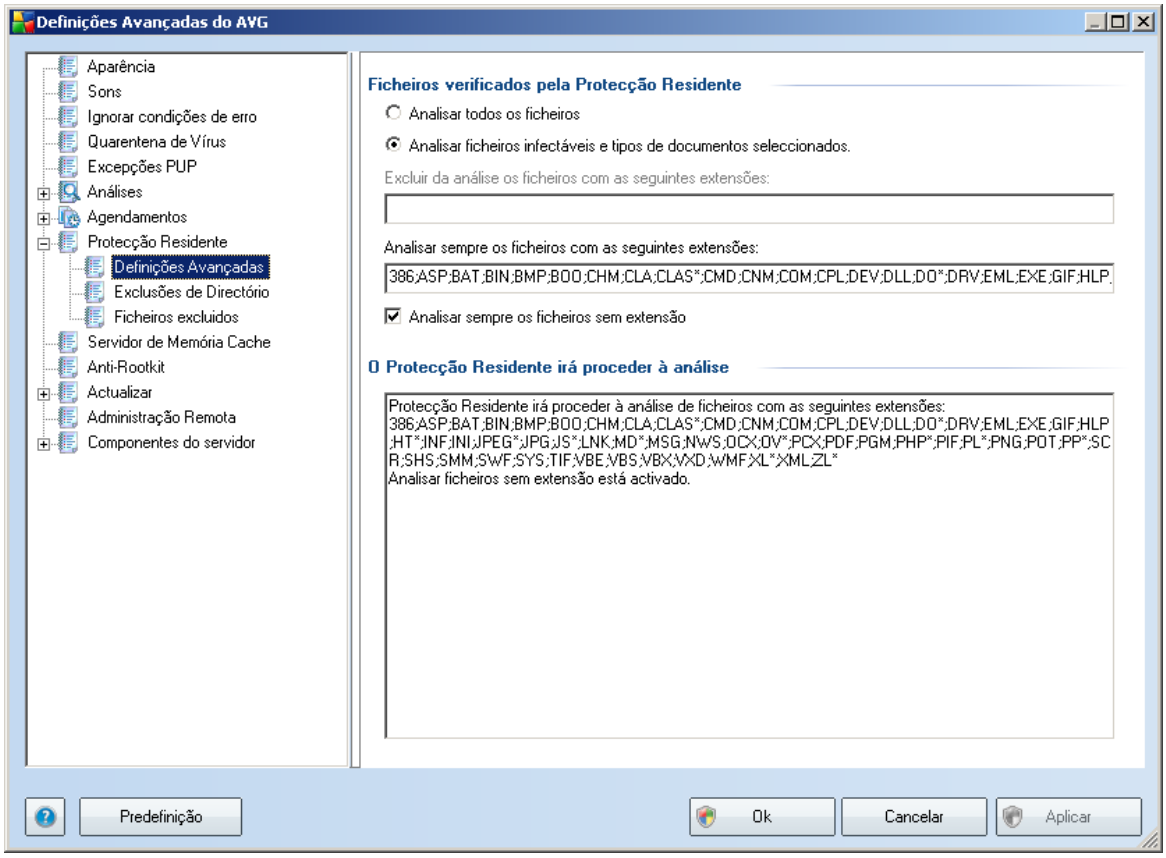
- ***Analisar o sector de arranque de discos amovíveis***- (*activado por predefinição*)

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

- ***Recuperação Automática*** - quaisquer infecções detectadas serão recuperadas automaticamente se houver uma cura disponível

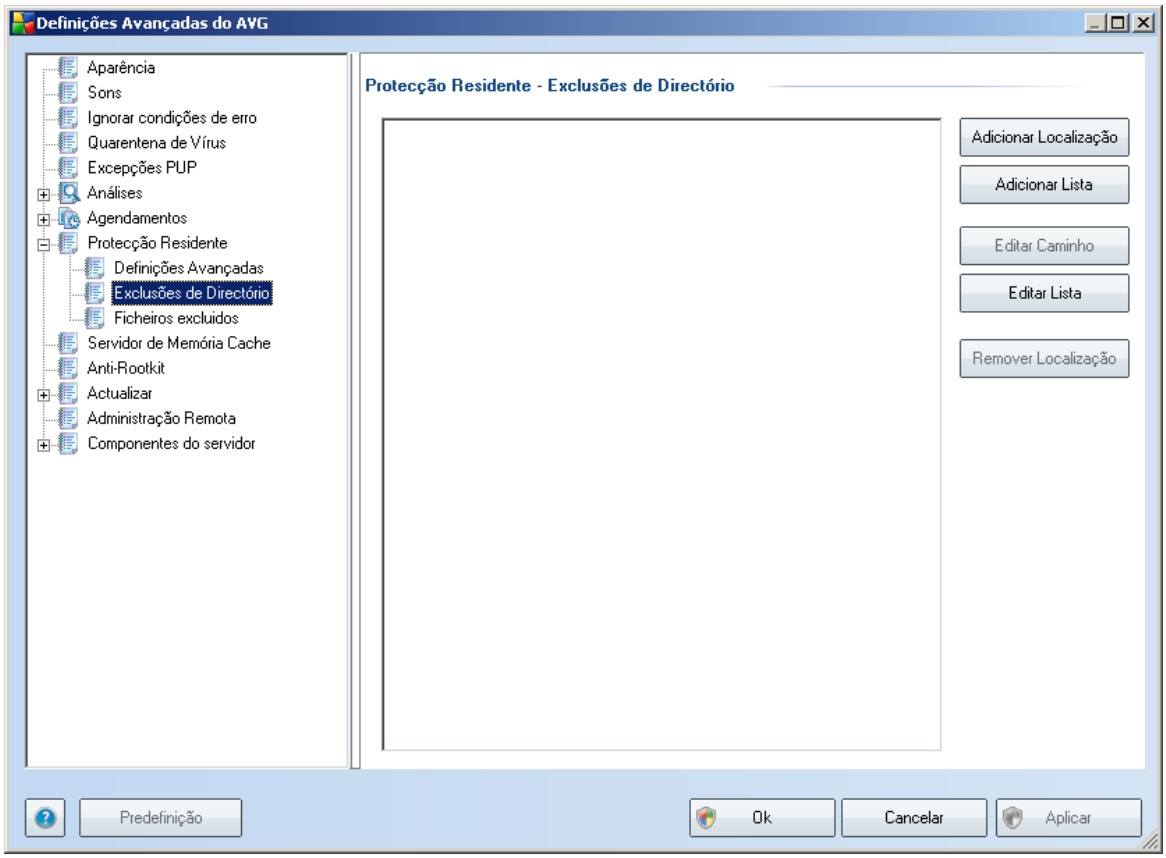
10.8.1. Definições Avançadas

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.

10.8.2. Exclusões de Directórios



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

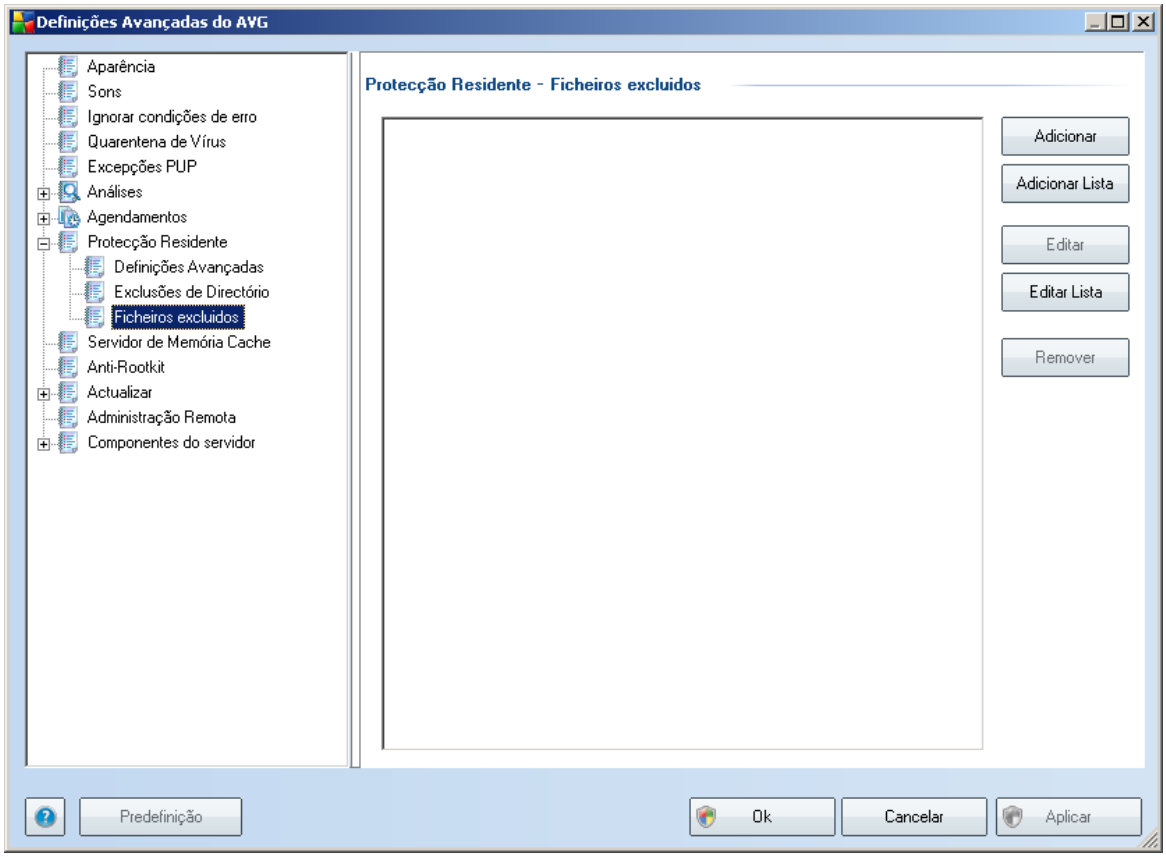
Se não for estritamente necessário, recomenda-se vivamente que não exclua directórios!

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

10.8.3. Ficheiros Excluídos



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

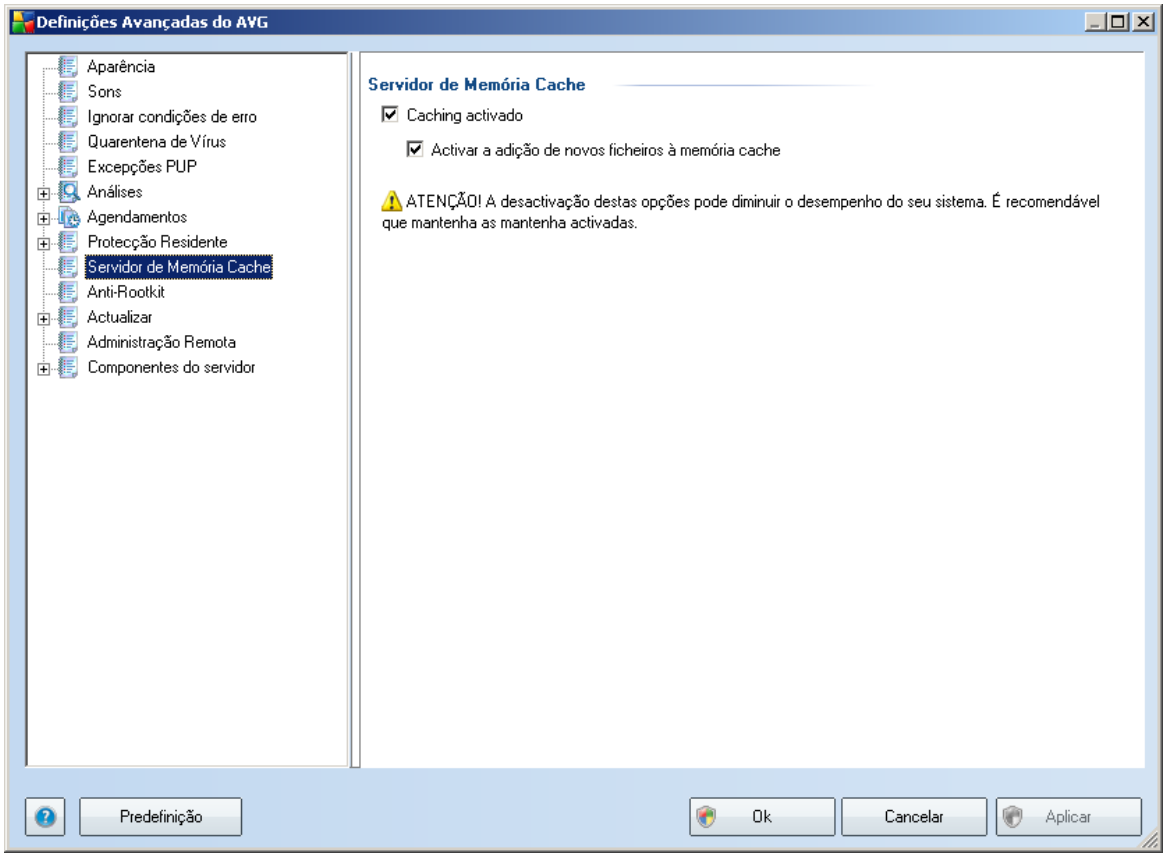
Se não for estritamente necessário, recomenda-se vivamente que não exclua quaisquer ficheiros!

A janela inclui os seguintes botões de controlo:

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

10.9. Servidor de Memória Cache

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



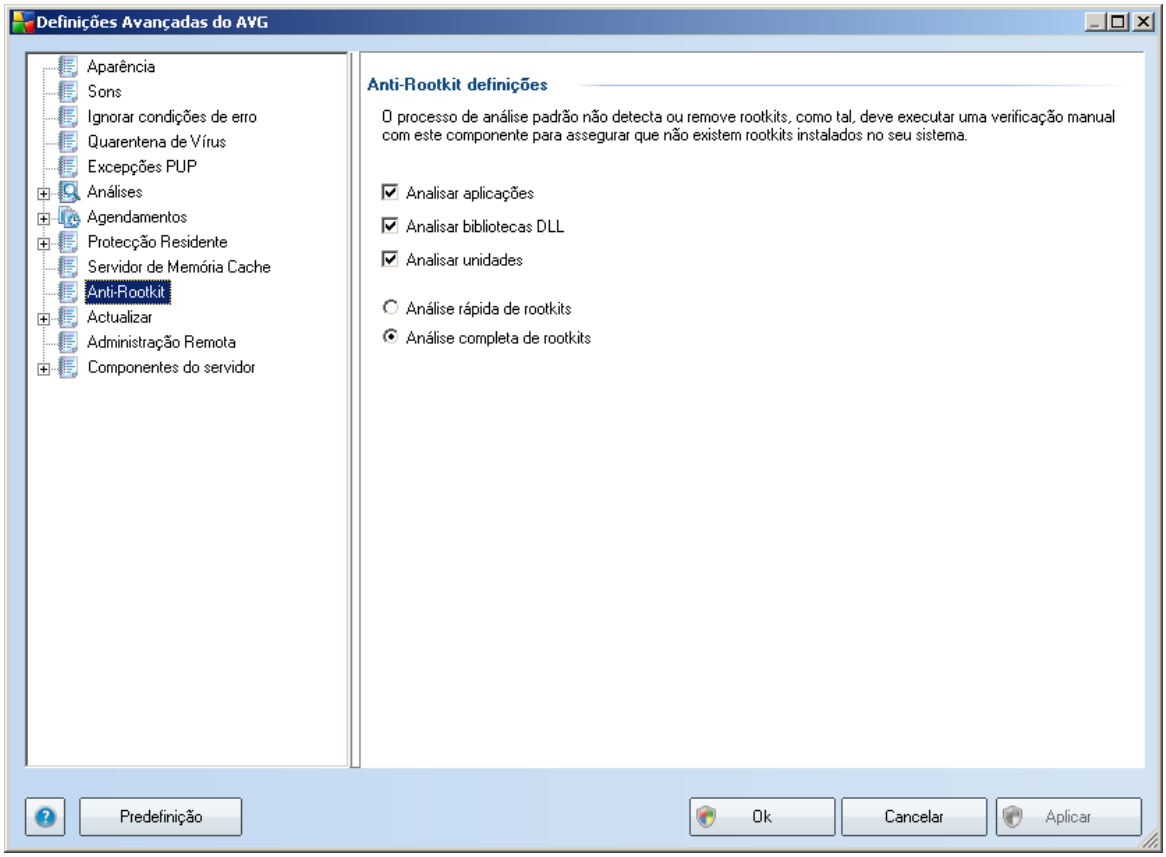
A janela de definições disponibiliza duas opções:

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

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

10.10. Anti-Rootkit

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



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

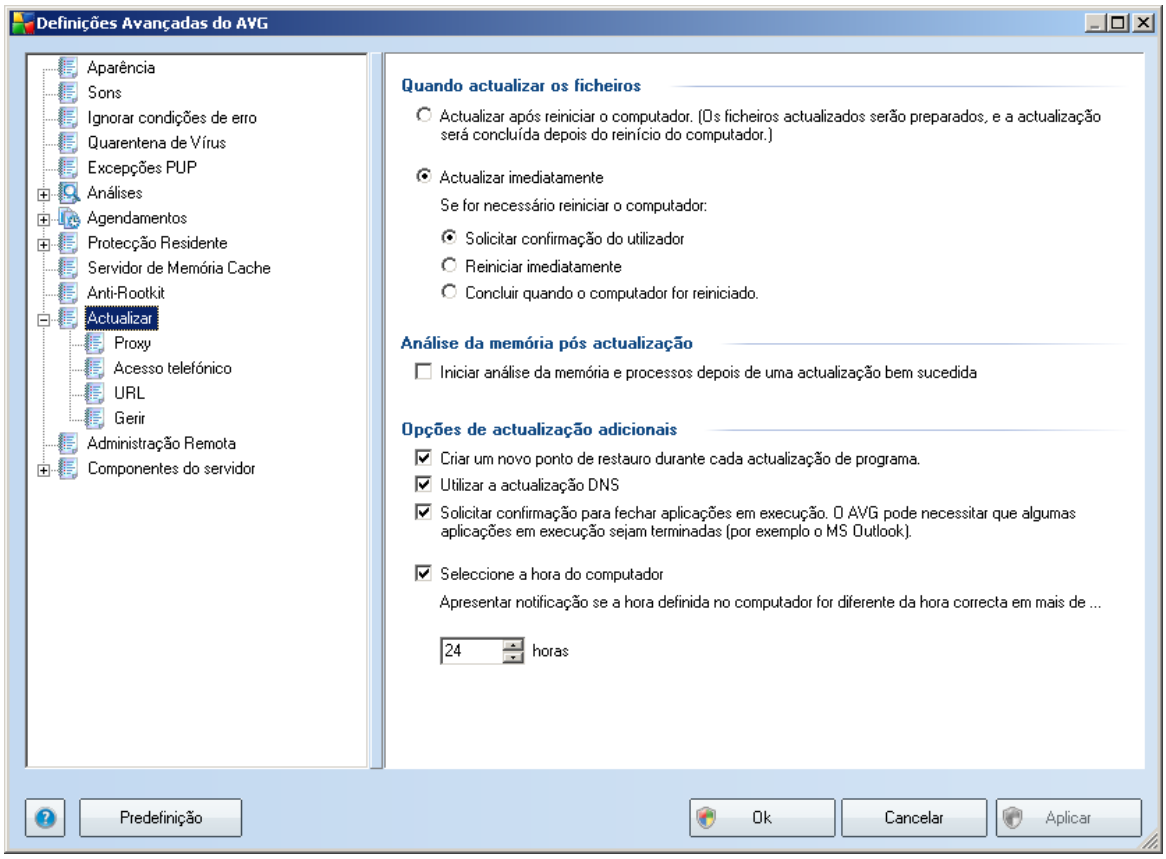
Primeiro, seleccione as caixas de verificação respectivas para especificar objectos que devem ser analisados:

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

Posteriormente pode escolher o modo de análise de rootkits:

- ***Análise rápida de rootkits*** - analisa 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:

10.11. 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

Análise da memória pós actualização

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

Opções de actualização adicionais

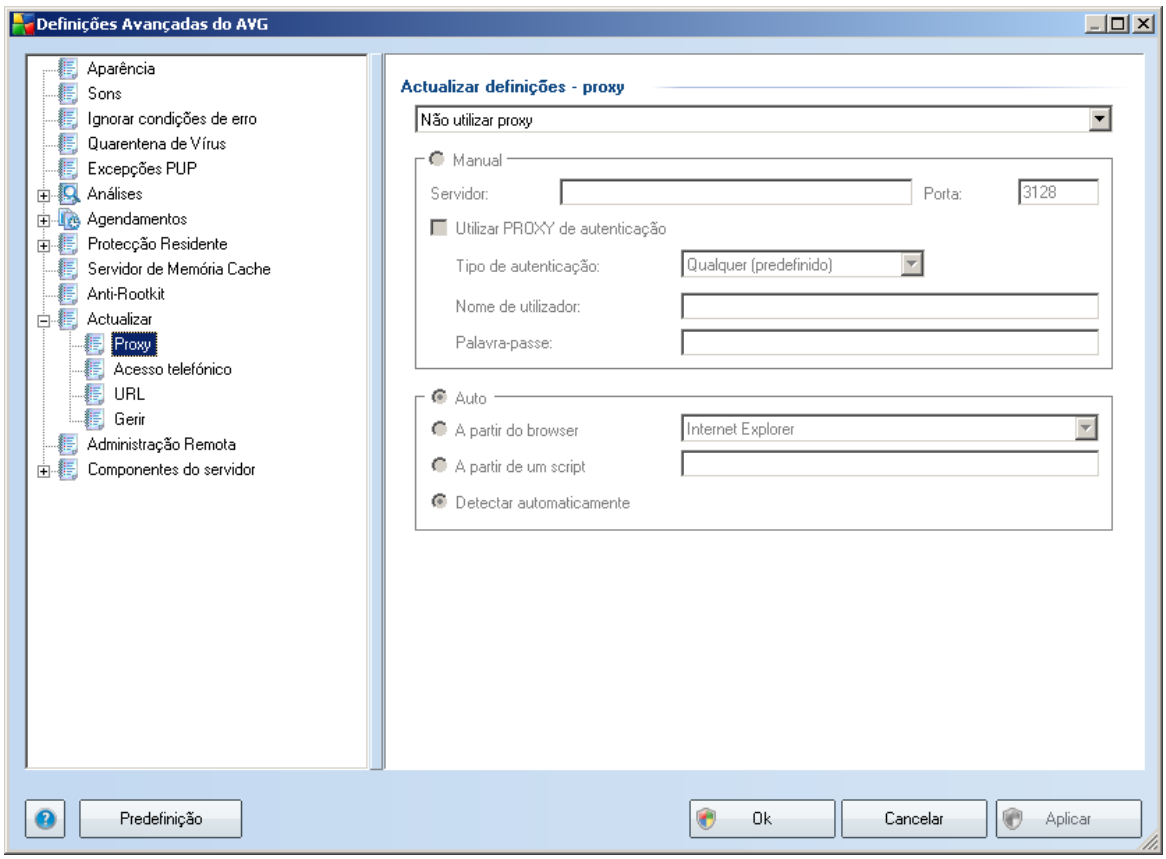
- ***Criar um novo ponto de restauro do sistema após cada actualização de programa*** - antes da execução de cada actualização de Programa do AVG, o sistema criará um ponto de restauro do sistema. Na eventualidade do processo de actualização falhar e o seu sistema operativo falhar pode sempre restaurar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

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

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

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

10.11.1. Proxy



O servidor proxy é um servidor autónomo ou um serviço executado no computador que

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

- ***Utilizar proxy***
- ***Não usar o servidor proxy***- definições predefinidas
- ***Tentar ligação utilizando proxy e se falhar, ligar directamente***

Se seleccionar qualquer opção utilizando o servidor proxy, terá de 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.

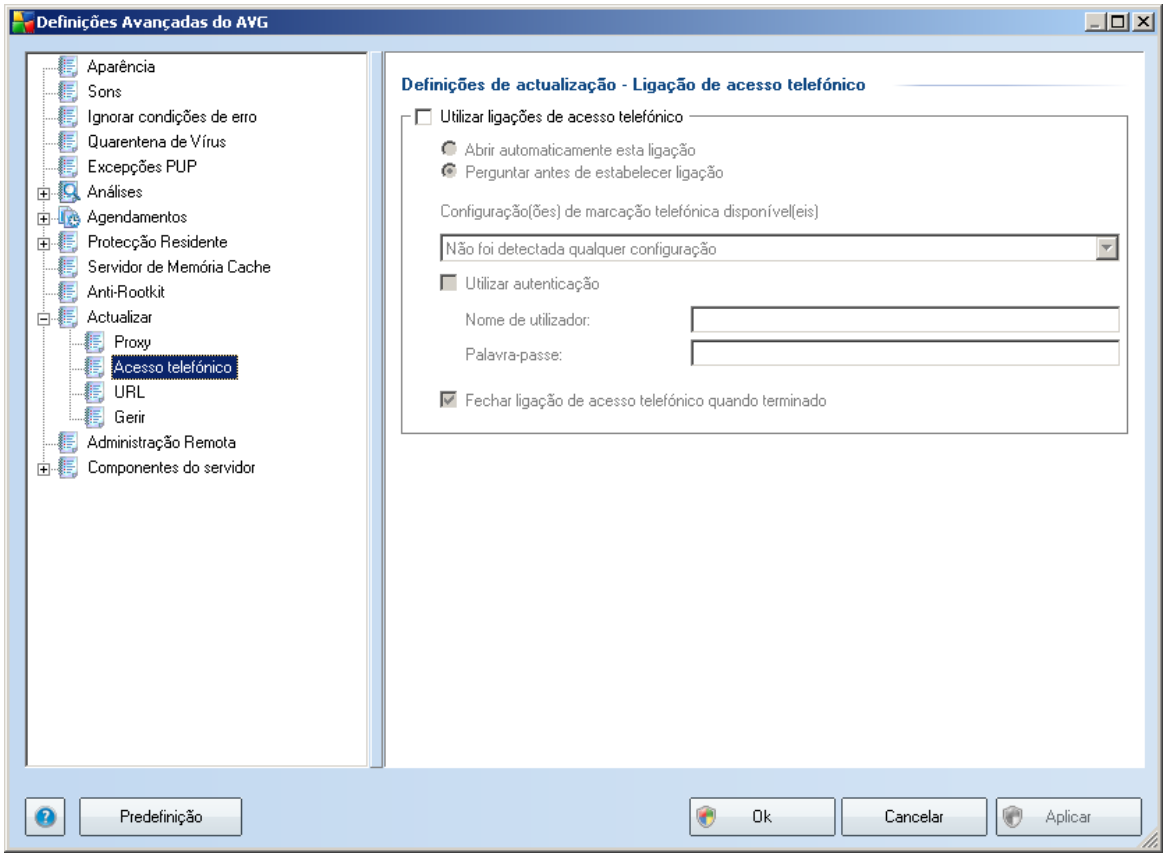
Configuração automática

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

- ***A partir do browser*** - a configuração será lida a partir do seu browser predefinido

- ***Do script*** - a configuração será lida a partir do script transferido com a função a devolver o endereço do proxy
- ***Autodetecção*** - a configuração será detectada automática e directamente a partir do servidor proxy

10.11.2. Acesso telefónico

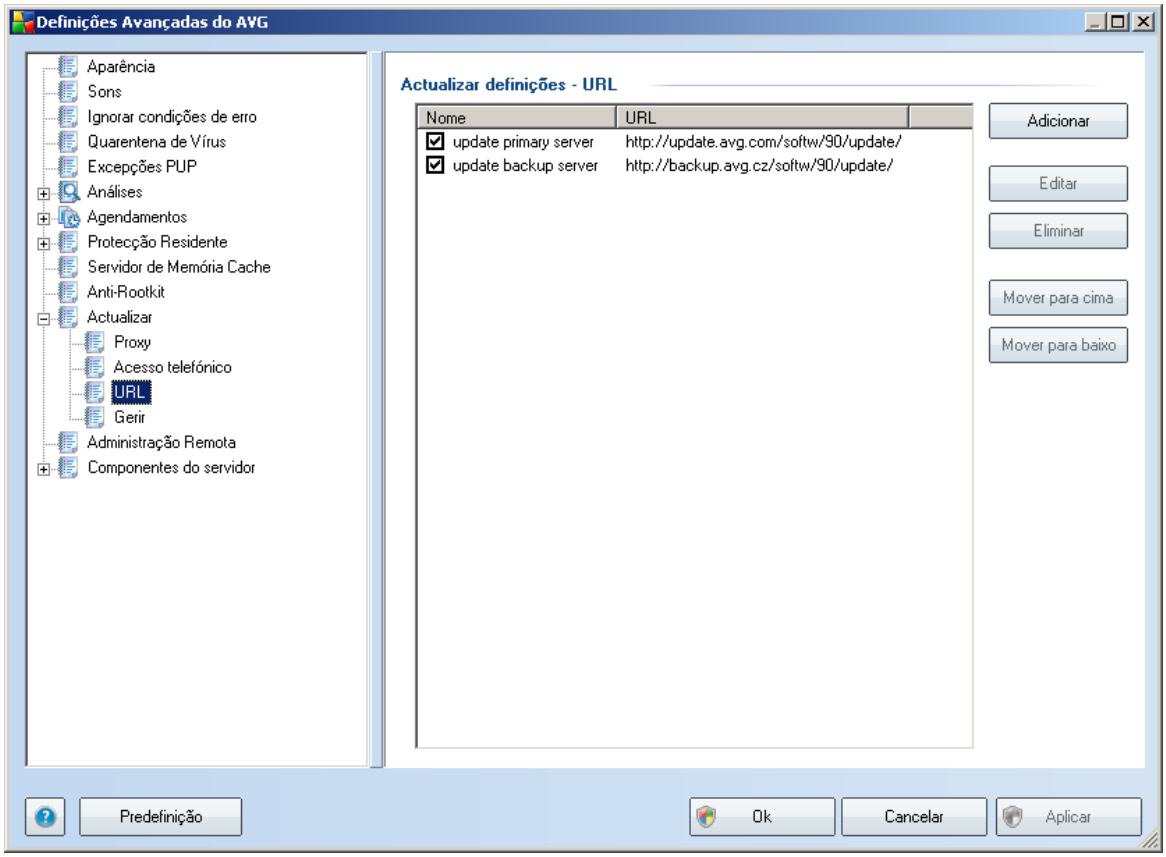


Todos os parâmetros definidos na janela ***Definições de Actualização - Ligação de acesso telefónico*** referem-se à ligação à Internet de Acesso telefónico. Os campos do separador estão inactivos até que seja marcada a opção ***Utilizar ligações de Acesso Telefónico*** que activa os campos.

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).

10.11.3. URL



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

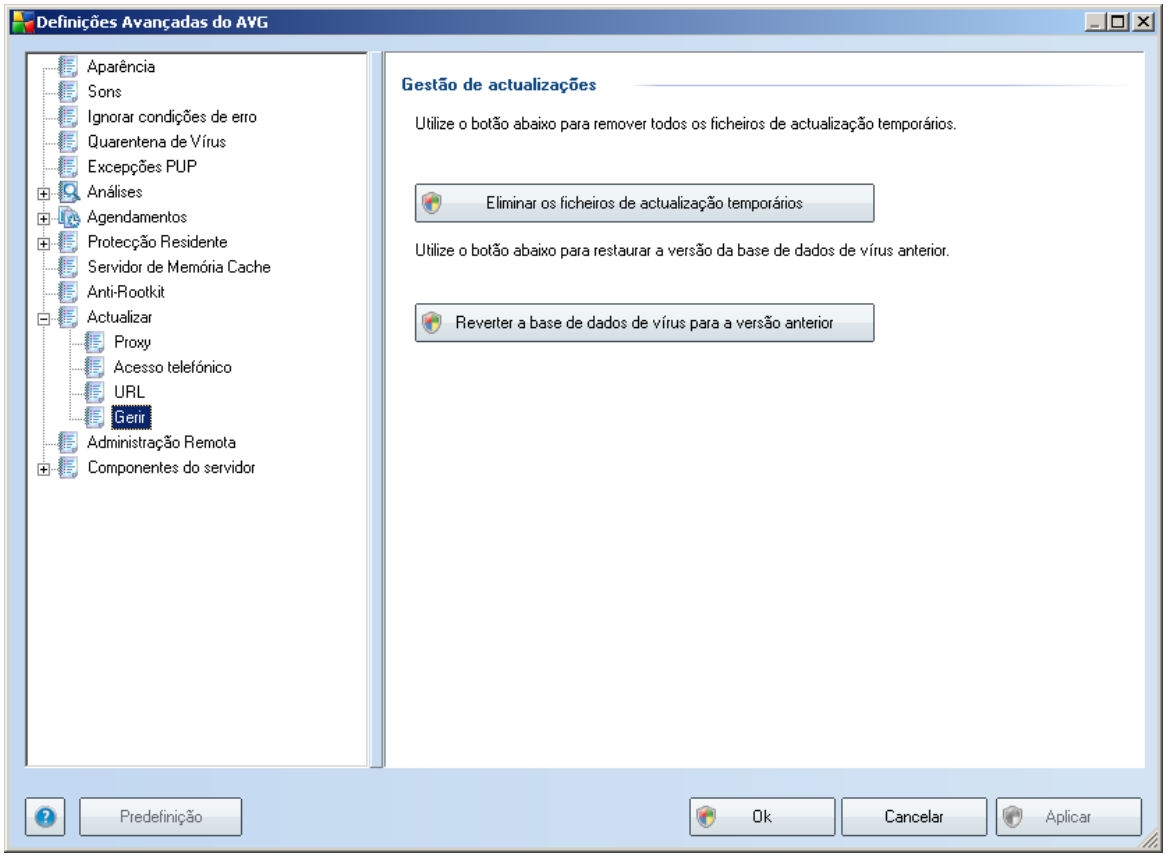
- ***Adicionar*** -abre uma janela onde pode especificar um novo URL a adicionar à lista
- ***Editar*** – abre uma janela onde pode editar os parâmetros do URL seleccionado
- ***Eliminar*** - – elimina o URL seleccionado da lista
- ***Mover para cima/Mover para baixo*** - estes dois botões são muito

importantes. O primeiro servidor da lista é sempre o que será usado durante cada tentativa de actualização. Como tal ao mover os servidores para cima ou para baixo, está na verdade a definir a sua prioridade. O botão ***Mover para cima*** move o URL seleccionado uma posição acima na lista, enquanto que o botão ***Mover para baixo*** move o URL seleccionado uma posição abaixo na lista

A desactivação da caixa junto ao nome do servidor desactiva temporariamente o servidor correspondente (sem necessidade de o eliminar da lista).

10.11.4. Gerir

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

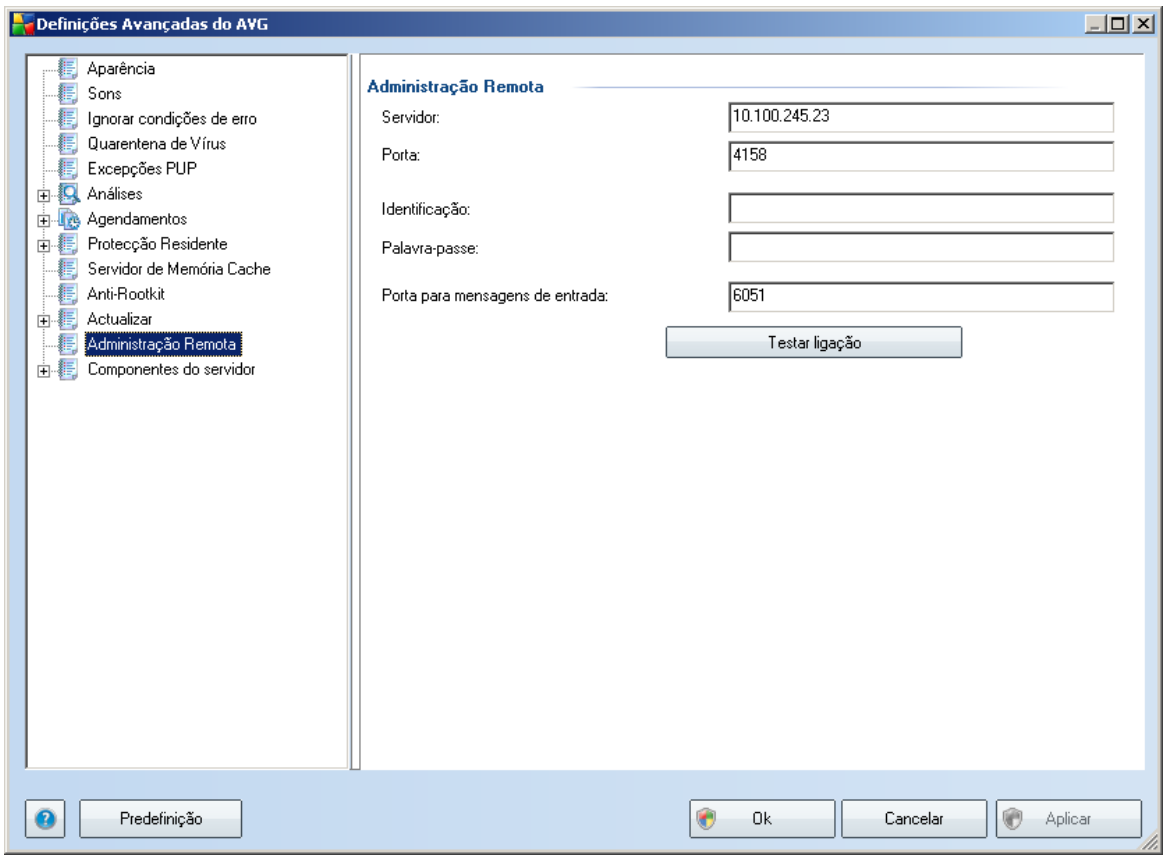


- ***Eliminar os ficheiros de actualização temporários*** - prima este botão para eliminar todos os ficheiros de actualização redundantes do seu disco rígido (*por predefinição, estes ficheiros são guardados durante 30 dias*)

- ***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*)

10.12. Administração Remota

O item ***Administração Remota*** só é apresentado na síntese das ***Definições Avançadas*** se tiver optado anteriormente pela instalação da ***Administração Remota*** , ou seja, se tiver marcado durante o processo de instalação esta opção na janela ***Selecção de Componentes***.



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

- ***Servidor*** - nome do servidor (ou endereço IP do servidor) onde o AVG Admin

Server está instalado

- ***Porta*** - faculte o número da porta através da qual o cliente AVG comunica com o AVG Admin Server (*o número de porta 4158 é considerado padrão - se utilizar este número de porta não tem de especificá-lo explicitamente*)
- ***Inicio de Sessão*** - se a comunicação entre o cliente AVG e o AVG Admin Server estiver definida como segura, faculte o seu nome de utilizador ...
- ***Palavra-passe*** - ....e a sua palavra-passe
- ***Porta para mensagens a receber*** - número da porta onde o cliente AVG aceita mensagens do AVG Admin Server

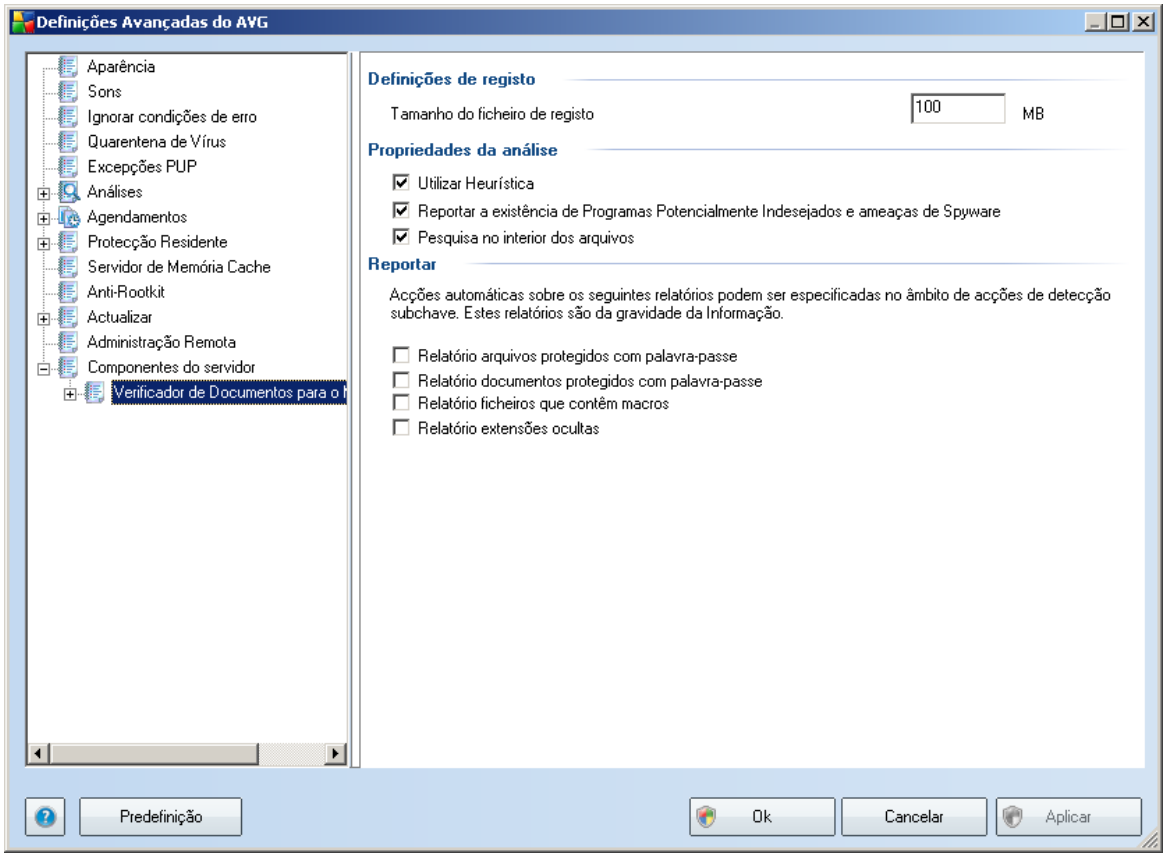
O botão ***Testar ligação*** ajuda-o a verificar se todos os dados especificados acima são válidos e podem ser usados para ligar com sucesso ao Centro de Dados

Nota: *Para uma descrição detalhada da administração remota por favor consulte a documentação do AVG Business Edition.*

10.13. Componentes do servidor

10.13.1. Verificador de Documentos para o MS Sharepoint

Nesta janela encontrará várias definições predefinidas relativas ao desempenho do ***Verificador de Documentos para o MS SharePoint*** em termos de análise de vírus nos documentos. A janela está dividida em várias secções:



Definições de registo

Tamanho do ficheiro de registo - o ficheiro de registo contém o registo vários eventos relacionados com o ***Verificador de Documentos para o MS SharePoint***, tais como notas de carregamento de bibliotecas de programas, eventos de detecção de vírus, avisos de resolução de problemas, etc. Use o campo de texto para definir o tamanho máximo deste ficheiro.

Propriedades da análise

- ***Utilizar a heurística*** - marque a caixa para utilizar o método de detecção da análise heurística durante a análise de documentos. Quando esta opção está activada, pode filtrar documentos não só por extensão mas também serão considerados os conteúdos do documento.

- ***Reportar Programas Potencialmente Indesejados e ameaças de Spyware*** – marque a caixa para utilizar o componente Anti-Spyware, ou seja, detectar e reportar programas suspeitos e potencialmente indesejados ao analisar documentos.

- ***Analisar no interior de arquivos*** - marque a caixa para analisar os conteúdos de arquivos.

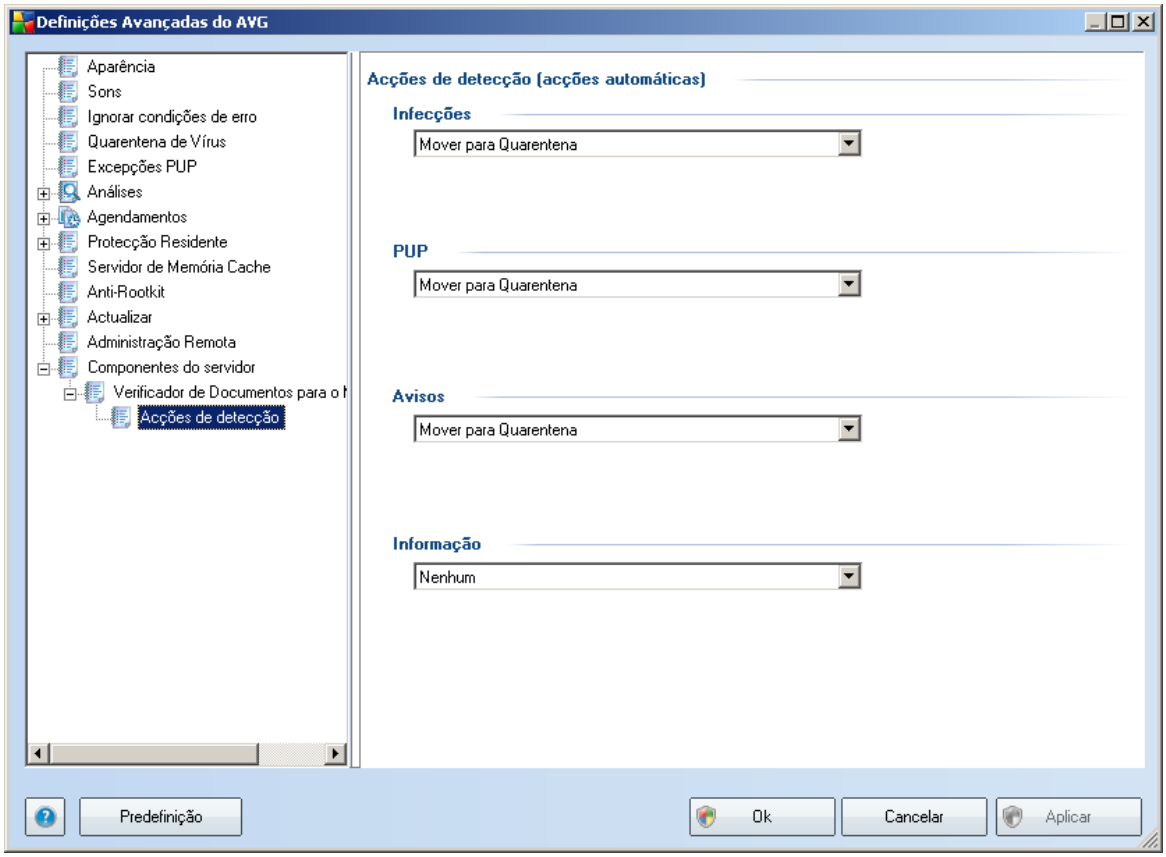
Reportar

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

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

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

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



Nesta janela pode configurar a forma como o componente ***Verificador de documentos para MS SharePoint*** se deve comportar quando detecta uma ameaça. As ameaças estão divididas em várias categorias:

- ***Infecções*** - códigos maliciosos que se copiam e disseminam, normalmente despercebidos até o mal estar feito.
- ***PUP (Programas Potencialmente Indesejados)*** - programas que, regra geral, variam de positivamente graves para meras ameaças potenciais para a sua privacidade.
- ***Avisos*** - objectos detectados que não podem ser analisados.
- ***Informações*** – incluem todas as potenciais ameaças detectadas que não podem ser classificadas em nenhuma das categorias acima.

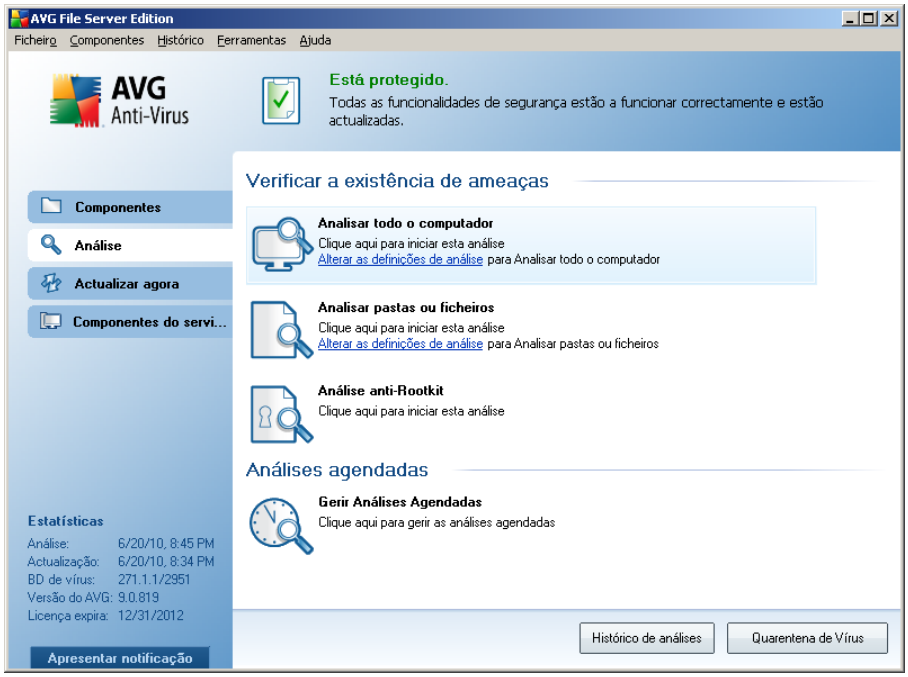
Use o menu pendente para seleccionar uma acção automática para cada uma destas:

- ***Nenhuma*** - um documento que contenha uma destas ameaças não será corrigido.
- ***Mover para a Quarentena de Vírus****** - todos os documentos infectados serão movidos para a Quarentena de Vírus.
- ***Remover*** - um documento no qual seja detectado um vírus será eliminado.

11. Análise do AVG

A análise é uma parte crucial do funcionamento do **AVG 9.0 File Server**. 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 três tipos de análises definidas pelo fornecedor do software e que estão prontas a serem utilizadas imediatamente seja manualmente ou por agendamento:
  - ***Analisar todo o computador***
  - ***Analisar pastas ou ficheiros específicos***
  - ***Análise anti-Rootkit***

- secção agendamento de análise - onde pode definir novos testes e criar novos agendamentos consoante necessário.

Botões de controlo

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

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

11.2. Análises Predefinidas

Uma das principais funcionalidades do **AVG 9.0 File Server** é a análise manual. Os testes a pedido são concebidos para analisar várias partes do computador sempre que existam suspeitas de uma possível infecção por vírus. De qualquer modo, recomenda-se vivamente que esses testes sejam efectuados regularmente, mesmo que considere que não serão detectados vírus no computador.

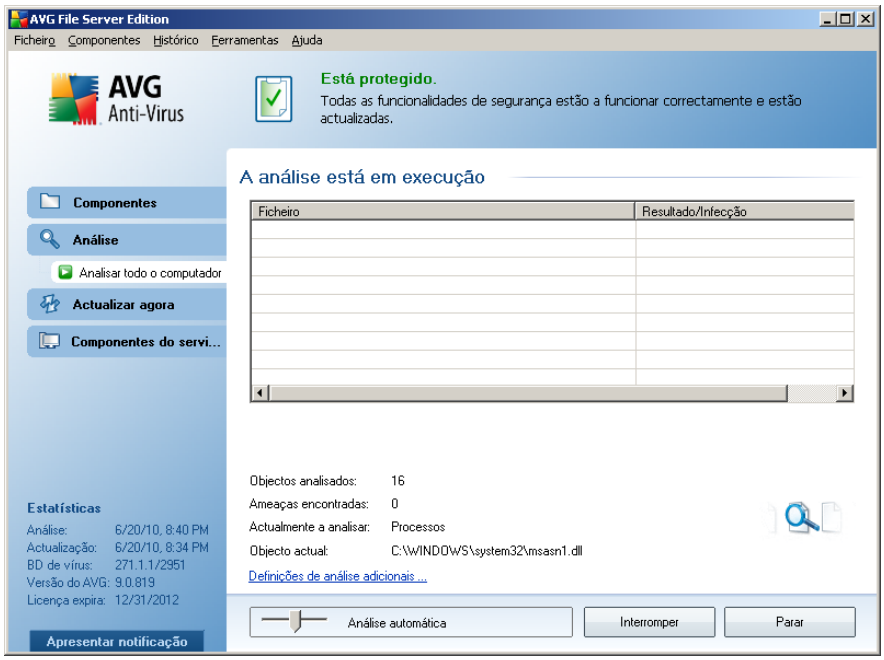
No **AVG 9.0 File Server** encontrará os seguintes tipos de análises predefinidas pelo fornecedor do software:

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.

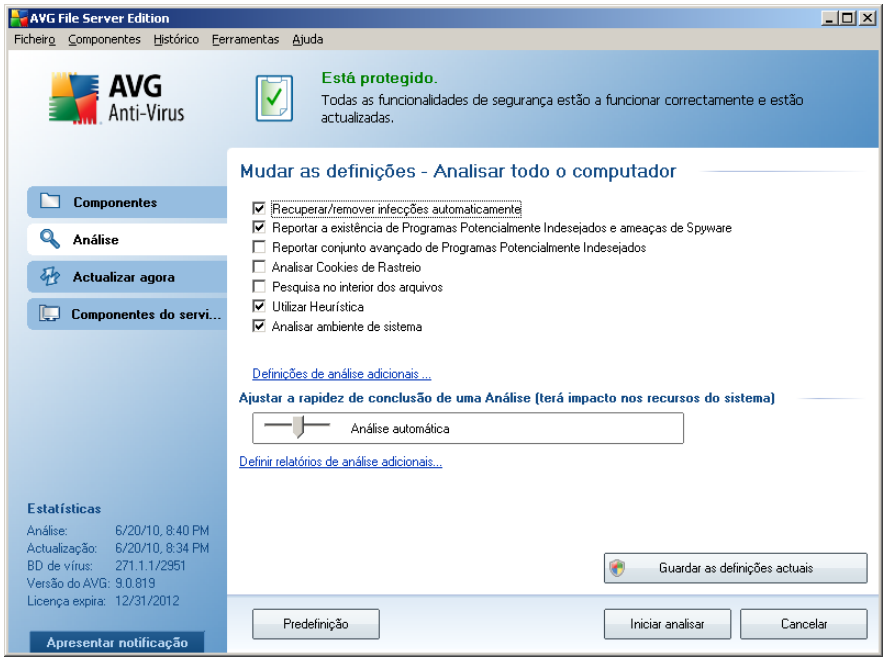
Início de análise

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.



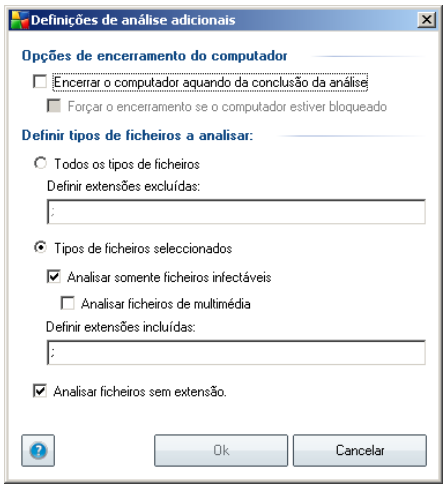
Edição da configuração de análise

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.

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



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

- ***Definir tipos de ficheiros para análise*** - deve decidir ainda se pretende que sejam analisados:

  - ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

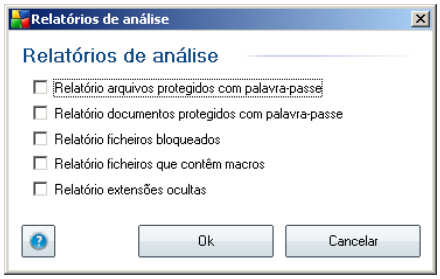
  - ***Tipos de ficheiros seleccionados*** - pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros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

  - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** - esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão

válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

- ***Prioridade do processo de análise*** - pode usar o cursor para alterar a prioridade do processo de análise. Por predefinição, a prioridade está definida para um nível médio (*Análise automática*) que optimiza a velocidade do processo de análise e a utilização dos recursos do sistema. Alternativamente, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*ex. quando o computador não está a ser utilizado*).

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



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

11.2.2. Analisar pastas ou ficheiros específicos

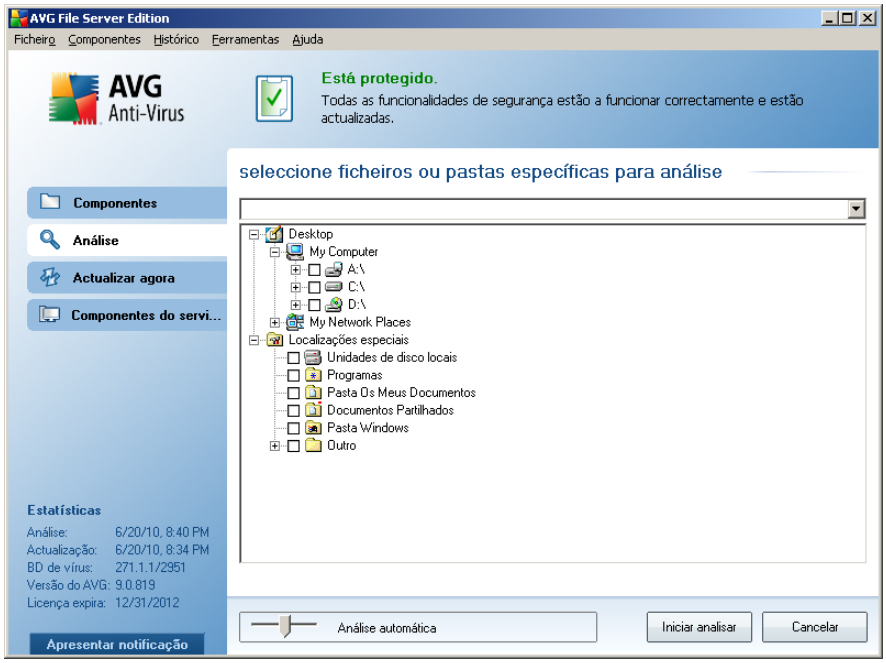
Analisar pastas ou ficheiros específicos - analisa apenas as áreas do seu computador que tiver seleccionado para o efeito (*pastas seleccionadas, discos rígidos, unidades de disquetes, CDs, etc.*). O progresso da análise na eventualidade da detecção de vírus e o seu tratamento é o mesmo que o da análise 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. Para excluir toda a pasta da análise utilize o "!" parâmetro.

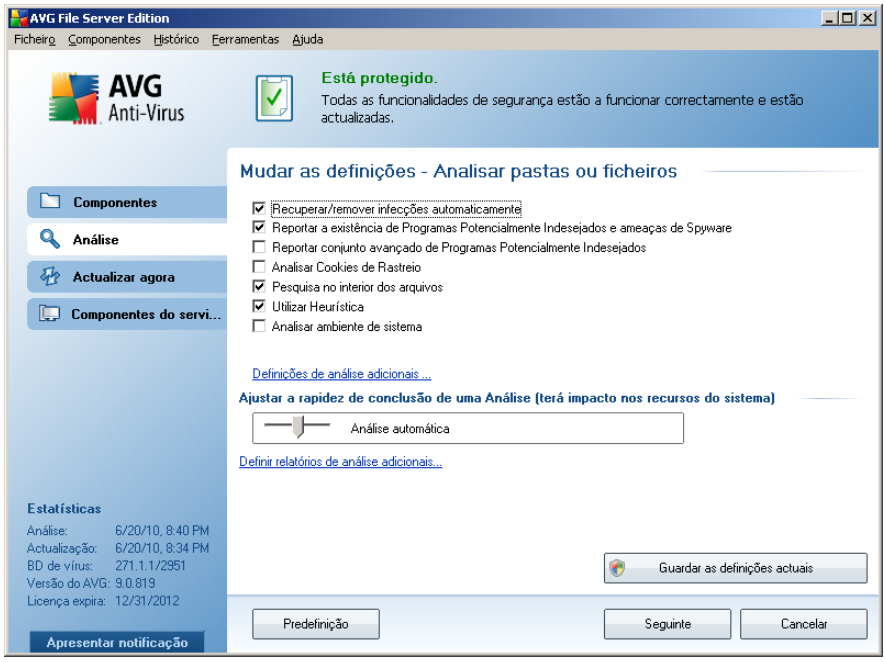
Finalmente, para iniciar a análise, clique no botão ***Iniciar análise***; o processo de análise em si é idêntico ao da análise análise de todo o computador.



Edição da configuração de análise

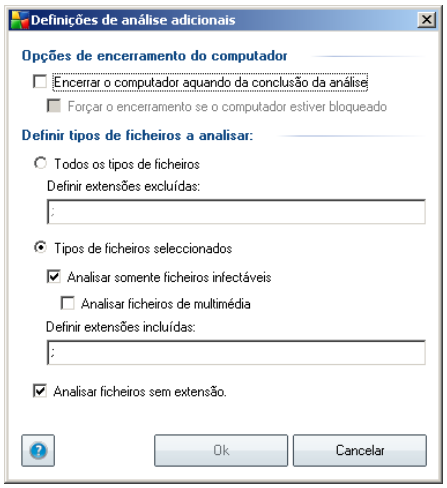
Tem a opção de editar as definições padrão predefinidas da análise ***Analisar ficheiros e pastas específicos***. Clique no link ***Alterar definições de análise*** para ir para a

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



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

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



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

- ***Definir tipos de ficheiros para análise*** - deve decidir ainda se pretende que sejam analisados:

  - ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

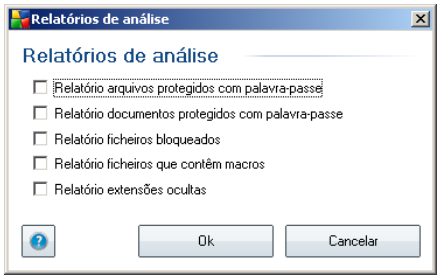
  - ***Tipos de ficheiros seleccionados*** - pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros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

  - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** - esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão

válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

- ***Prioridade do processo de análise*** - pode usar o cursor para alterar a prioridade do processo de análise. Por predefinição, a prioridade está definida para um nível médio (*Análise automática*) que optimiza a velocidade do processo de análise e a utilização dos recursos do sistema. Alternativamente, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*ex. quando o computador não está a ser utilizado*).

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



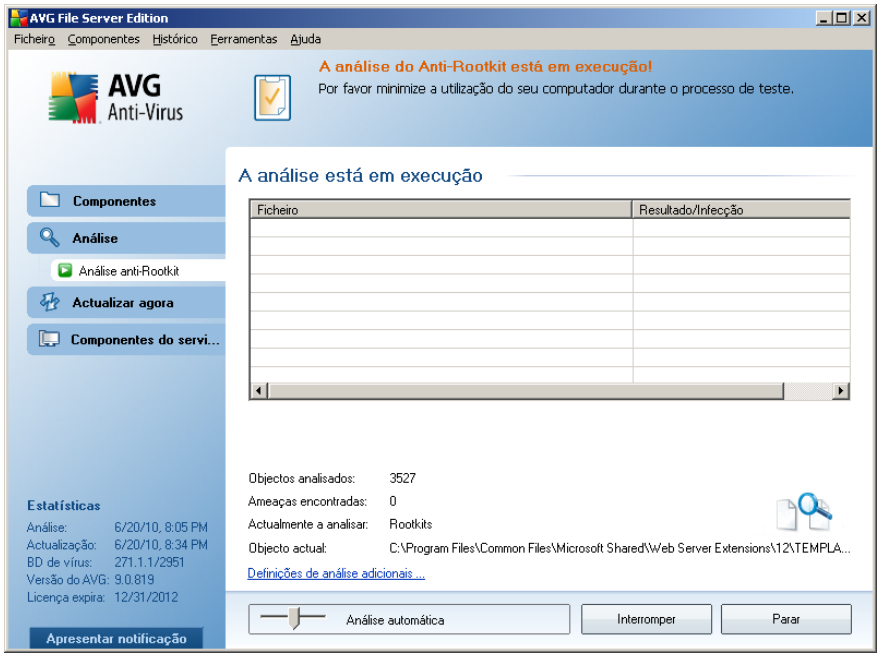
Aviso: *Estas definições de análise são idênticas aos parâmetros de uma análise nova - conforme descrito no capítulo* ***Análise do AVG / Agendamento de análises / Como Analisar*** *. Na eventualidade de decidir alterar a configuração padrão da análise* ***Analisar pastas ou ficheiros específicos***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

11.2.3. Análise Anti-Rootkit

A análise anti-Rootkit analisar o seu computador pela existência de eventuais rootkits (*programas e tecnologias que podem ocultar actividade de malware no seu computador*). Se for detectado um rootkit, isto não significa necessariamente que o computador esteja infectado. Em alguns casos, podem ser erroneamente detectados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Início de análise

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



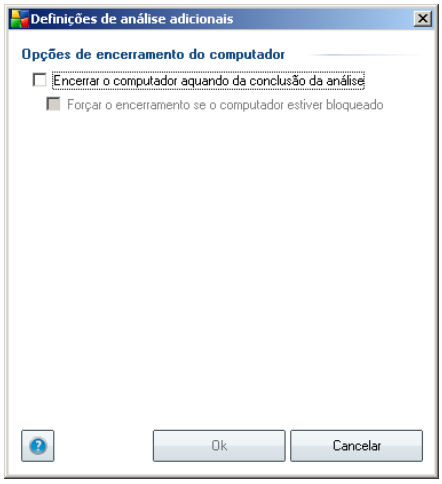
Edição da configuração de análise

A análise Anti-Rootkit é sempre iniciada a partir das predefinições, e a edição dos parâmetros de análise só é acessível na janela ***Definições Avançadas do AVG / Anti-Rootkit***. Na interface de análise só estão disponíveis as seguintes configurações:

- ***Análise automática*** - 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

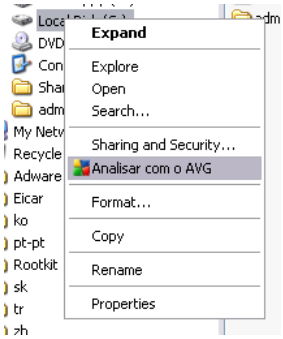
mais elevados (*ex. quando o computador não está a ser utilizado*).

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



11.3. A analisar no Explorador do Windows

Para além das análises predefinidas executadas para todo o computador ou as suas áreas seleccionadas, o **AVG 9.0 File Server** também disponibiliza a opção de análise rápida de um objecto específico directamente no ambiente do Explorador do Windows. Se quiser abrir um ficheiro desconhecido e não estiver seguro do seu conteúdo, pode querer analisá-lo manualmente. Siga estes passos:



- No Explorador do Windows seleccione o ficheiro (ou pasta) que pretende

verificar

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

11.4. Análise da Linha de Comandos

No **AVG 9.0 File Server** existe ainda a opção de executar a análise a partir da linha de comandos. Pode utilizar esta opção em servidores por exemplo, ou ao criar um batch script a ser executado automaticamente após o arranque do computador. Pode iniciar a análise a partir da linha de comandos com várias parâmetros, como na interface gráfica do utilizador do AVG.

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

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

Sintaxe do comando

A sintaxe do comando é a seguinte:

- ***avgscanx /parâmetro*** ... ex. ***avgscanx /comp*** para analisar todo o computador
- ***avgscanx /parâmetro /parâmetro*** .. com vários parâmetros, estes deverão estar alinhados numa linha e separados por espaço e o símbolo "barra"
- se um parâmetro requerer que seja facultado um valor específico (ex. o parâmetro ***/scan*** que requer informação acerca das áreas seleccionadas do seu computador a serem analisadas, e o utilizador 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

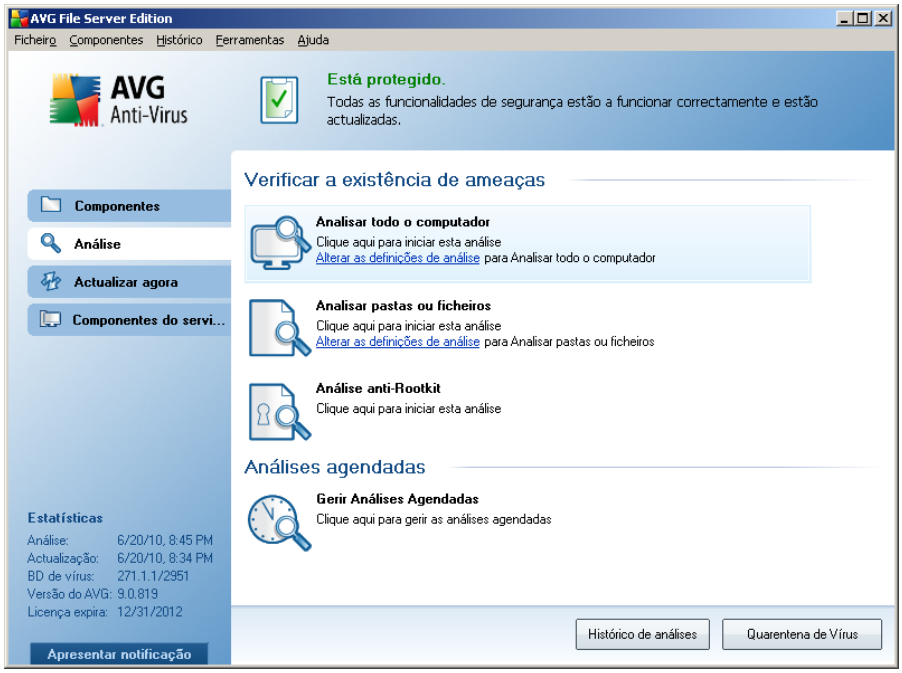
- ***/TRASH*** Mover ficheiros infectados para a Quarentena de Vírus***
- ***/QT*** Teste Rápido
- ***/MACROW*** Reportar macros
- ***/PWDW*** Reportar ficheiros protegidos por palavra-passe
- ***/IGNLOCKED*** Ignorar ficheiros bloqueados
- ***/REPORT*** Reportar para ficheiro /nome de ficheiro/
- ***/REPAPPEND*** 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*** Defina a prioridade de análise /Baixa, Auto, Elevada/ (consulte a secção Definições avançadas / Análises)
- ***/SHUTDOWN*** Encerrar o computador aquando da conclusão da análise
- ***/FORCESHUTDOWN*** Forçar o encerramento do computador após o término da análise
- ***/ADS*** Analisar Fluxos de Dados Alternados (somente NTFS)
- ***/ARCBOMBSW*** Reportar "arquivos bomba" (arquivos repetidamente comprimidos)

11.5. Agendamento de Análise

Com o **AVG 9.0 File Server** pode executar análises manualmente (por exemplo quando suspeita que uma infecção contagiou o seu computador) ou baseado num agendamento planeado. É vivamente recomendável que execute as análises baseado num agendamento: desta forma pode assegurar que o seu computador está protegido de quaisquer possibilidade de ser infectado, e não terá de se preocupar com quando e se iniciar uma análise.

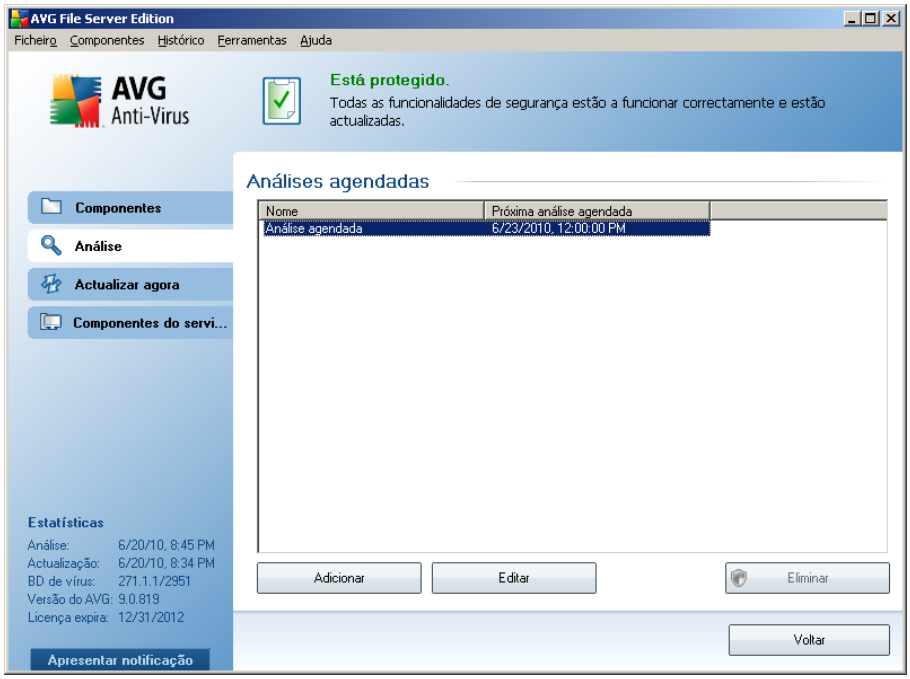
Deve executar a análise ***Analisar todo o computador*** regularmente, pelo menos uma vez por semana. No entanto, se possível, execute a análise de todo computador diariamente - conforme configurado na configuração de agendamento de análise predefinida. Se o computador estiver "sempre ligado" então pode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

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



Análises agendadas

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



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

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

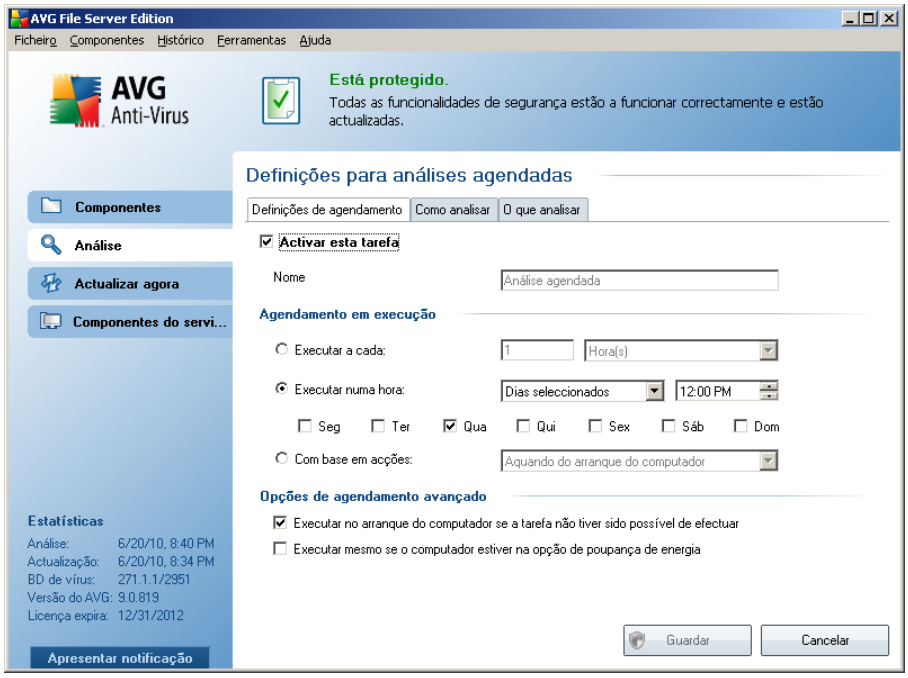
- ***Editar agendamento de análise*** - este botão só pode ser utilizado se já tiver seleccionado um teste existente a partir da lista de testes agendados. Nesse caso o botão aparece como activo e pode clicar nele para alternar para a janela ***Definições para análise agendada*** , separador ***Definições de agendamento***. Os parâmetros do teste seleccionado já estão especificados e podem ser editados.

- ***Eliminar agendamento de análise*** - este botão só pode ser utilizado se já tiver seleccionado um teste existente a partir da lista de testes agendados. Este teste pode então ser eliminado da lista clicando no botão de controlo. No entanto, só pode remover os teste que tiver criado; o ***Agendamento de análise a todo o computador*** predefinido nas configurações padrão nunca pode ser eliminado.

- ***Retroceder*** - regressar à interface de análise do AVG

11.5.1. Definições de agendamento

Se quiser agendar um novo teste e a sua execução regular, aceda à janela ***Definições para teste agendado*** ((*clique no botão* ***Adicionar agendamento de análise*** *na janela* ***Análises agendadas***). A janela está dividida em três separadores: ***Definições de agendamento*** - *consulte a imagem abaixo* (*o separador predefinido para o qual será automaticamente redireccionado*), ***Como analisar*** e ***O que analisar***.



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

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

Exemplo:*Não é adequado nomear uma análise com o nome "Nova análise" ou "A minha análise" uma vez que estes nomes não referem o que a análise efectivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc. Também não é necessário especificar no nome da análise se*

é a análise de todo o computador ou somente de ficheiros e pastas seleccionados - as suas próprias análises serão sempre uma versão específica da análise de ficheiros e pastas seleccionados.

Nesta janela pode ainda definir os seguintes parâmetros de análise:

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

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

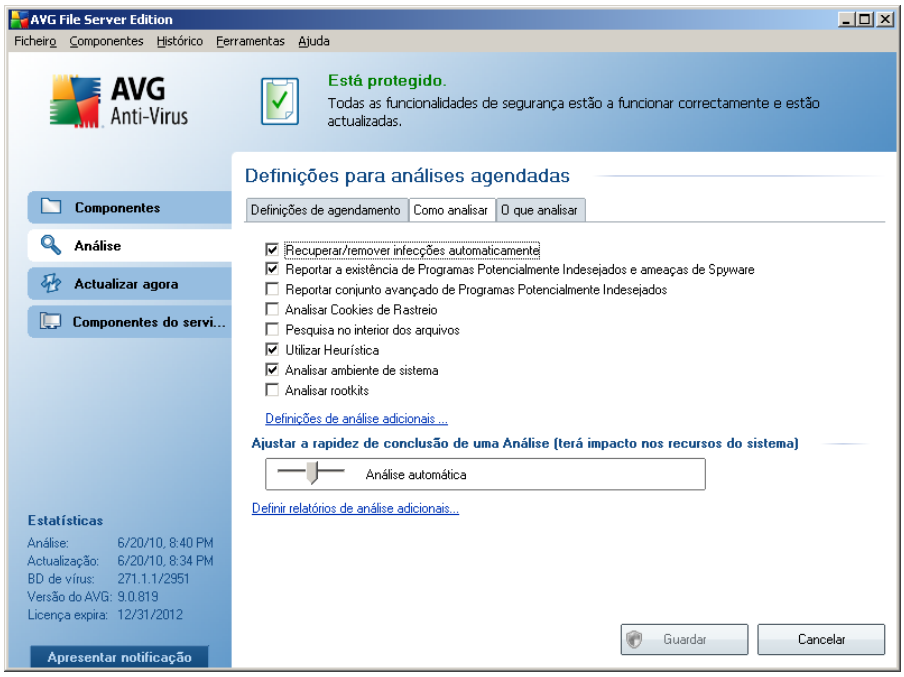
Botões de controlo da janela de Definições para análises agendadas

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

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

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

11.5.2. Como Analisar



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

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

- ***Reportar Programas Potencialmente Indesejados e Ameaças de Spyware*** - 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;

- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** - detecção de pacotes expandidos de spyware: programas que são

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

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

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

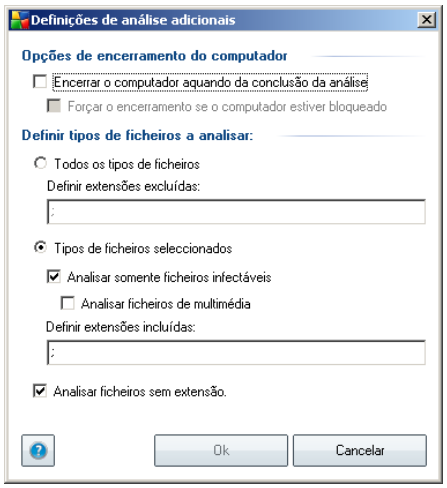
- ***Utilizar Heurística*** - análise heurística (*a emulação dinâmica das instruções do objecto analisado num ambiente de computador virtual* será um dos métodos utilizados para a detecção de vírus durante a análise;

- ***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 apenas de rootkits está disponível no componente ***Anti-Rootkit***;

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

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



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

- ***Definir tipos de ficheiros para análise*** - deve decidir ainda se pretende que sejam analisados:

  - ***Todos os tipos de ficheiros*** com a possibilidade de definir excepções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

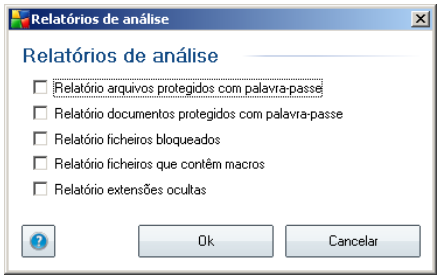
  - ***Tipos de ficheiros seleccionados*** - pode especificar que pretende analisar apenas ficheiros que sejam potencialmente infectáveis (*ficheiros que não possam ser infectados não serão analisados, por exemplo alguns ficheiros de texto simples, ou outros ficheiros não executáveis*), incluindo ficheiros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

  - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** - esta opção está activada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão

válida para a alterar. Os ficheiros sem extensão são bastante suspeitos e devem ser sempre analisados.

- ***Prioridade do processo de análise*** - pode usar o cursor para alterar a prioridade do processo de análise. Por predefinição, a prioridade está definida para um nível médio (*Análise automática*) que optimiza a velocidade do processo de análise e a utilização dos recursos do sistema. Alternativamente, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*ex. quando o computador não está a ser utilizado*).

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



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

Botões de controlo

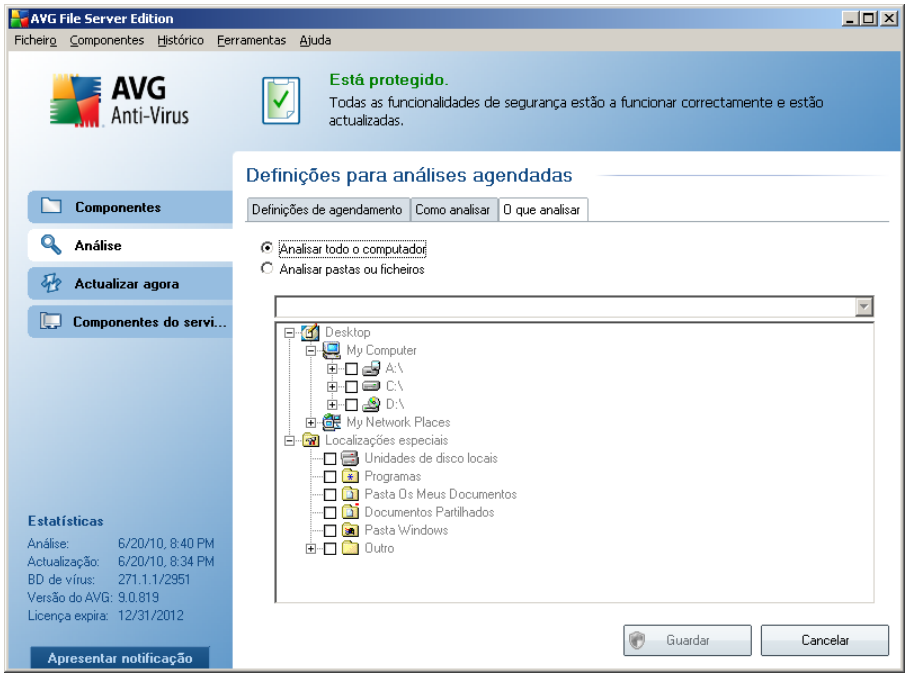
Existem dois botões de controlo disponíveis nos três separadores da janela ***Definições para análises agendadas*** (***Definições de agendamento***, ***Como analisar*** e ***O que analisar***) e estes têm as mesmas funcionalidades independentemente do separador activo:

- ***Guardar*** - guarda todas as alterações que tenha efectuado neste ou em qualquer outro separador desta janela e retorna para a interface padrão de análise do AVG. Como tal, se pretender configurar os parâmetros de teste em

todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos

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

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.

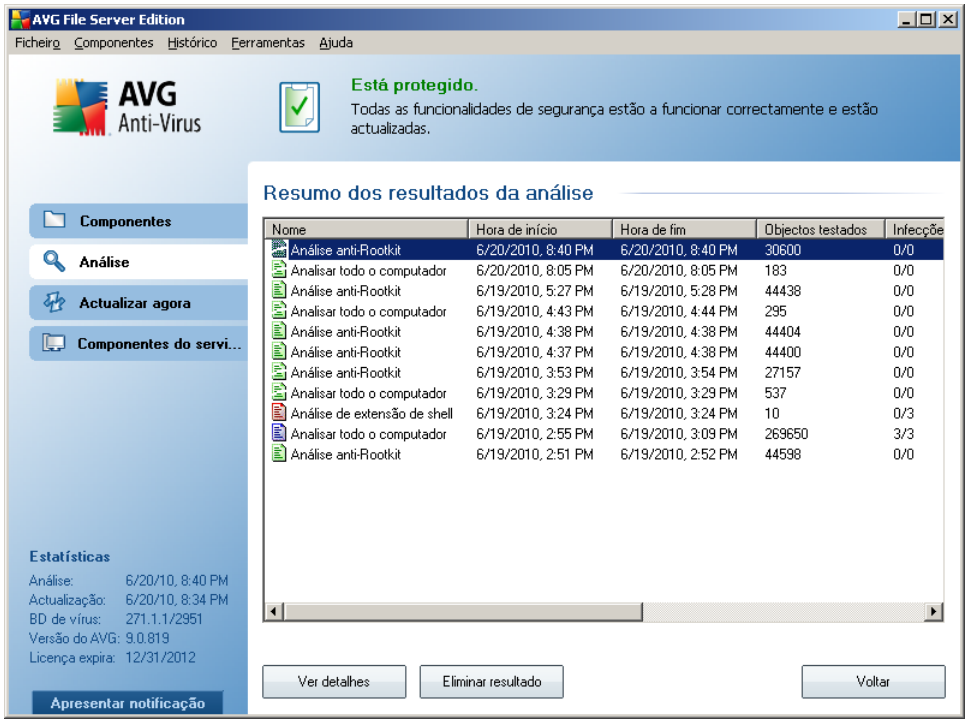
Botões de controlo da janela de Definições para análises agendadas

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 activo:

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

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

11.6. Resumo dos Resultados da Análise



A janela ***Síntese dos resultados da análise*** é acessível a partir 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

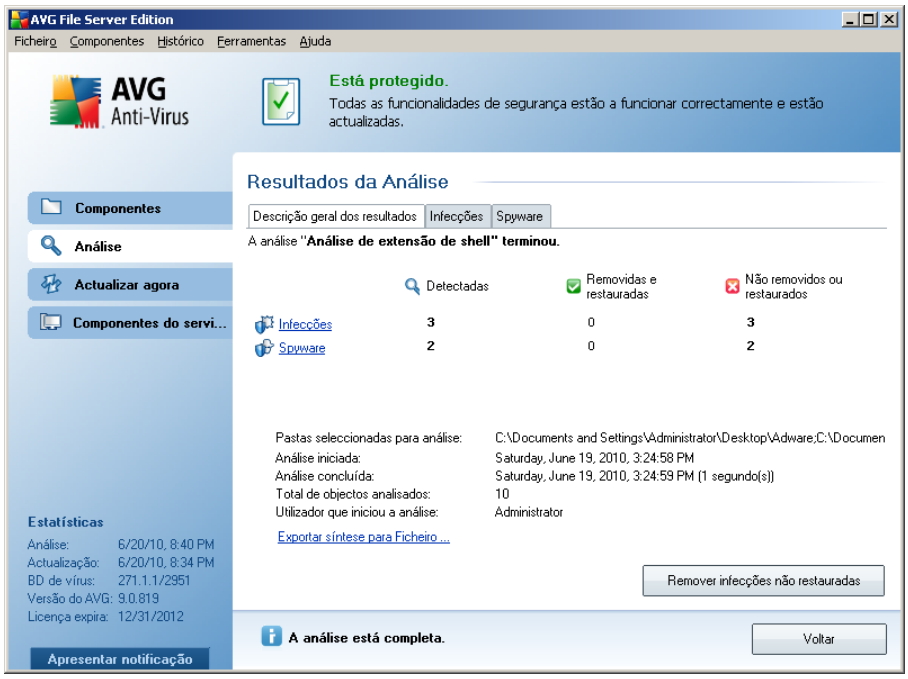
11.7. Detalhes dos Resultados da Análise

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 / avisos / rootkits / informações
- infecções de vírus/spyware removidas / avisos / rootkits
- o número de infecções de vírus / spyware / avisos / rootkits que não podem ser removidos ou recuperados

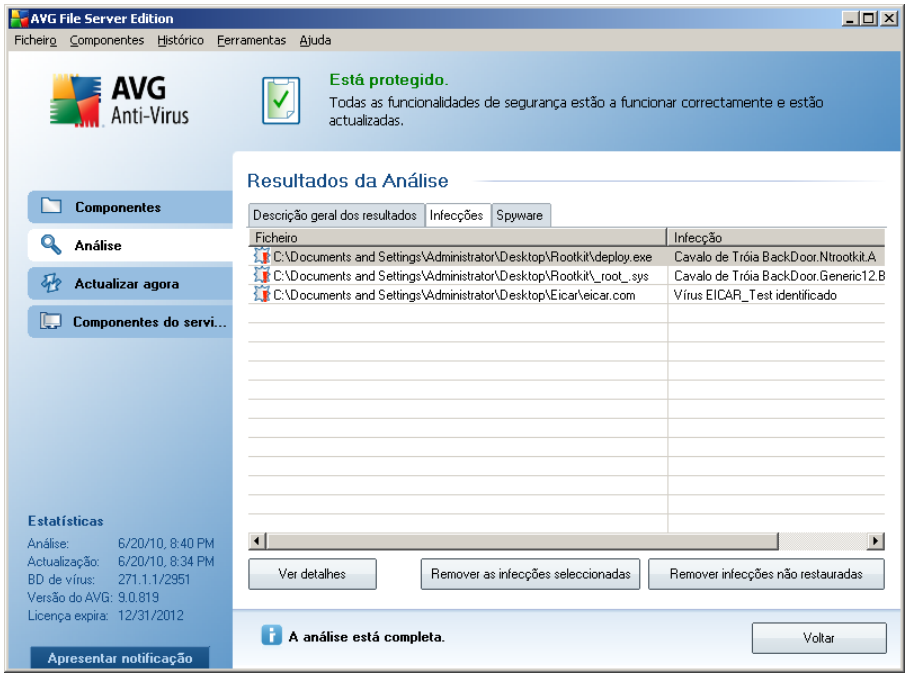
Adicionalmente, encontrará informações relativas à data e hora exacta do inicio da análise, ao número total de objectos analisados, à duração da análise, ao número de erros que tenham ocorrido durante a análise e o utilizador que iniciou a análise.

Botões de controlo

Só existem dois botões de controlo disponíveis nesta janela. O botão ***Fechar resultados*** remete para a janela ***Resumo dos resultados da análise***. O botão ***Remover todas as infecções não restauradas*** só é apresentado se a análise tiver detectado alguma ameaça que não tenha sido removida automaticamente. Se clicar

nele, move essas ameaças para a ***Quarentena de Vírus***.

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:

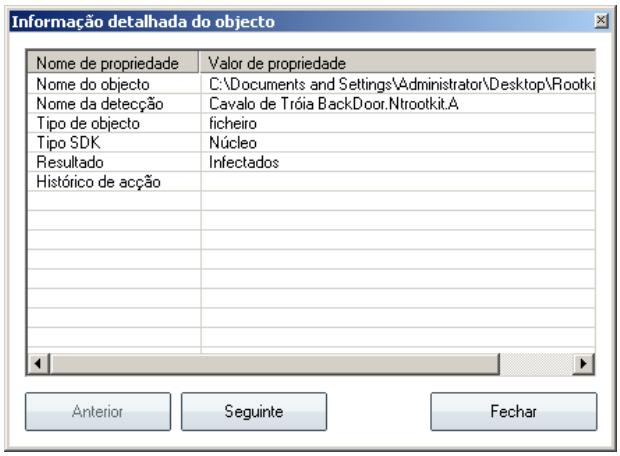
- ***Ficheiro*** - localização original completa do objecto infectado
- ***Infecções*** - nome do vírus detectado (*para detalhes específicos relativos a vírus por favor consulte a Enciclopédia de vírus on-line*)
- ***Resultado*** - define o estado actual do objecto infectado que foi detectado durante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

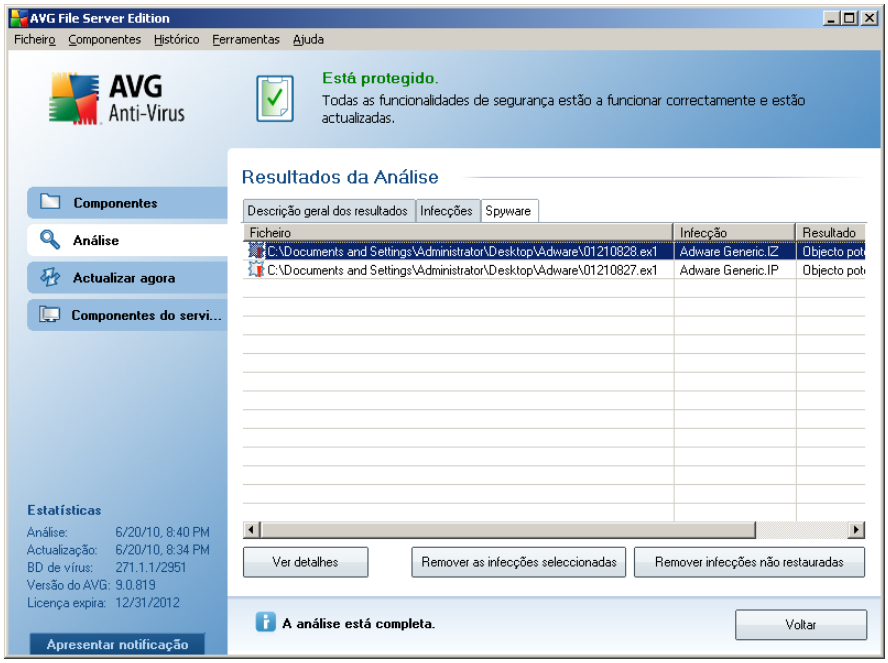


Nesta janela pode encontrar informações relativas à localização do objecto

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

- ***Remover as infecções seleccionadas*** - use o botão para restaurar as detecções seleccionadas, ou para as mover para a ***Quarentena de Vírus*** (se não for possível restaurá-las)
- ***Remover as infecções não restauradas*** - use o botão para restaurar as detecções seleccionadas, ou para as mover para a ***Quarentena de Vírus*** (se não for possível restaurá-las)
- ***Fechar resultados*** conclui a síntese de informações detalhadas e retorna à janela ***Resumo dos resultados da análise***

11.7.3. Separador Spyware



O separador ***Spyware*** só é apresentado na janela ***Resultados da Análise*** se tiver sido detectado 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

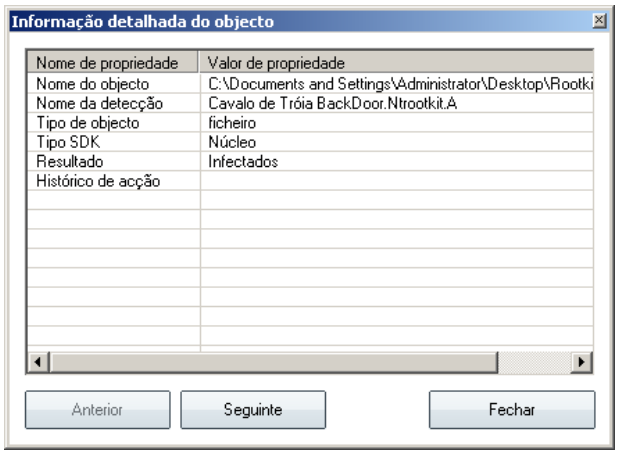
    - ***Objecto potencialmente perigoso*** - o objecto foi detectado como sendo potencialmente perigoso mas não infectado (pode conter macros, por exemplo); a informação deverá ser entendida como sendo um aviso

    - ***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 relativas a detecções especificas. Utilize o botão ***Fechar*** para fechar esta janela.

- ***Remover as infecções seleccionadas*** - use o botão para restaurar as detecções seleccionadas, ou para as mover para a ***Quarentena de Vírus*** (se não for possível restaurá-las)
- ***Remover as infecções não restauradas*** - use o botão para restaurar as detecções seleccionadas, ou para as mover para a ***Quarentena de Vírus*** (se não for possível restaurá-las)
- ***Fechar resultados*** conclui a síntese de informações detalhadas e retorna à janela ***Resumo dos resultados da análise***

11.7.4. Separador Avisos

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

Esta é uma breve descrição dos exemplos mais comuns desses objectos:

- ***Ficheiros ocultos*** - Os ficheiros ocultos não são, por predefinição, visíveis no Windows, e alguns vírus ou outras ameaças podem evitar a sua detecção ao guardarem os seus ficheiros com este atributo. Se o AVG reportar um ficheiro oculto que o utilizador suspeite ser malicioso, pode movê-lo para a ***Quarentena de Vírus*** do AVG.

- ***Cookies*** - As cookies são ficheiros de texto simples que são usados pelos websites para guardar informações específicas relativas ao utilizador e que são posteriormente usadas para carregar esquemas de página predefinidos, preenchimento do nome de utilizador, etc.

- ***Chaves de registo suspeitas***- Algum malware guarda as suas informações no Registo do Windows para assegurar que é carregado no arranque ou para alargar o seu efeito sobre o sistema operativo.

11.7.5. Separador Rootkits

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

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

A estrutura deste separador é basicamente a mesma do ***separador Infecções*** ou do ***separador Spyware***.

11.7.6. Separador Informações

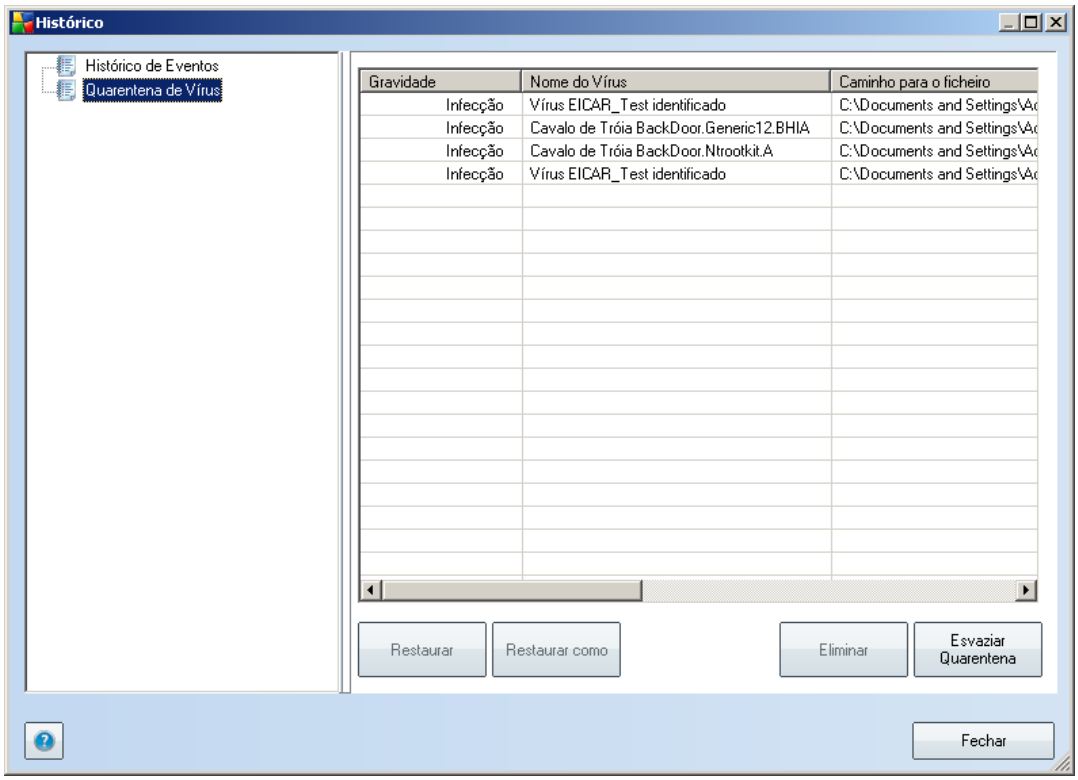
O separador ***Informação*** contém dados acerca dessas "detecções" que não podem ser categorizadas como infecções, spyware, etc. Não podem ser positivamente etiquetadas como perigosas mas contudo carecem da sua atenção. A análise do AVG pode detectar ficheiros que podem não estar infectados, mas que são suspeitos. Estes

ficheiros são reportados como ***Aviso***, ou como ***Informação***.

O nível de gravidade ***Informação*** pode ser reportado por uma das seguintes razões.

- ***Executável compilado*** - O ficheiro foi compilado com um dos compiladores de executáveis menos comuns, o que pode indicar uma tentativa de evitar a análise desse ficheiro. No entanto, nem todas as reportações desse ficheiro indicam um vírus.
- ***Executável compilado recursivo*** - semelhante ao anterior, no entanto menos frequente entre o software comum. Tais ficheiros são suspeitos e deve ser considerada a sua remoção ou submissão para análise.
- ***Arquivo ou documento protegidos por palavra-passe*** - Os ficheiros protegidos por palavra-passe não podem ser analisados pelo AVG (*ou qualquer outros programa anti-malware*).
- ***Documentos com macros*** - o documento contém macros, que podem ser maliciosas.
- ***Extensão oculta*** - Ficheiros com extensão oculta podem aparentar ser, por exemplo, imagens, mas serem na verdade ficheiros executáveis (*ex. imagem. jpg.exe*). A segunda extensão não é visível no Windows por predefinição, e o AVG reporta esses ficheiros para evitar a abertura acidental dos mesmos.
- ***Localização do ficheiro inadequada***- Se algum ficheiro de sistema importante estiver a ser executado a partir de outra localização que não a predefinida (*ex. winlogon.exe a ser executado de outra pasta que não a pasta Windows*), o AVG reporta esta discrepância. Em alguns casos, os vírus usam nomes de processos do sistema tradicionais para tornarem a sua presença menos evidente no sistema.
- ***Ficheiro bloqueado***- O ficheiro está bloqueado e, como tal, não pode ser analisado pelo AVG. Isto normalmente significa que existe um ficheiro que está constantemente a ser usado pelo sistema (*ex. ficheiro swap*).

11.8. Quarentena de Vírus



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

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

- ***Gravidade*** - providencia identificação do tipo e gravidade da detecção respectiva
- ***Tipo de infecção*** - distingue os tipos de detecção com base 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
- ***Quarentena vazia*** -remover todos ***Quarentena de Vírus***conteúdo completamente

12. Actualizações do AVG

Manter o seu AVG actualizado é essencial para assegurar que todos os vírus recém descobertos serão detectados assim que possível. Uma vez que as actualizações do AVG não são lançadas em conformidade com qualquer período pré-determinado, mas antes em função da quantidade e gravidade das novas ameaças, é recomendável que verifique a existência de novas actualizações pelo menos uma vez por dia. Efectuar uma verificação a cada 4 horas garantirá que a base de dados de Vírus do AVG se mantém actualizada também durante o dia.

12.1. Níveis de Actualização

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

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

- ***Actualização do programa***contém várias alterações do programa, soluções e melhorias.

Aquando do agendamento de uma actualização, é possível seleccionar o nível de prioridade que deve ser transferido e aplicado.

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

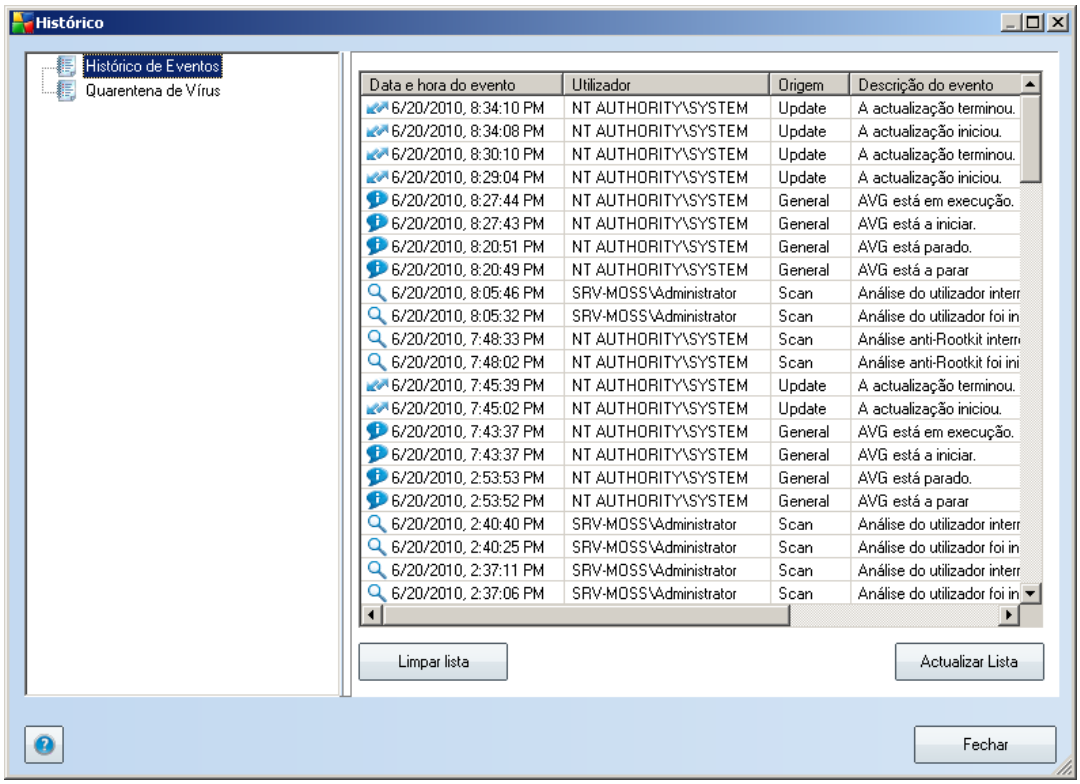
O processo de actualização pode ser executado imediatamente à medida que a necessidade surge via o link rápido ***Actualizar agora*** ***. Este link está constantemente disponível a partir de qualquer janela daInterface do utilizador do AVG . No entanto, ainda é altamente recomendável efectuar actualizações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

conforme expresso no agendamento de actualizações editável no componente Actualizações .

Assim que inicia a actualização, o AVG verifica a existência de novos ficheiros de actualização disponíveis. Se assim for, o AVG inicia a transferência e executa o processo de actualização autonomamente. Durante o processo de actualização será redireccionado para a interface de ***Actualização*** onde pode ver o progresso do processo na sua representação gráfica, assim como numa síntese de parâmetros estatísticos relevantes (*tamanho do ficheiro de actualização, dados recebidos, velocidade de transferência, tempo decorrido, ...*).

***Nota**: Antes da iniciação da actualização do programa AVG será criado um ponto de restauro. Na eventualidade do processo de actualização falhar e o seu sistema operativo falhar pode sempre restaurar o seu SO para a configuração original a partir deste ponto. Esta opção é acessível via Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauro do Sistema. Recomendado apenas a utilizadores avançados!*

13. Histórico de Eventos



A janela ***Histórico 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 o funcionamento do **AVG 9.0 File Server**. ***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

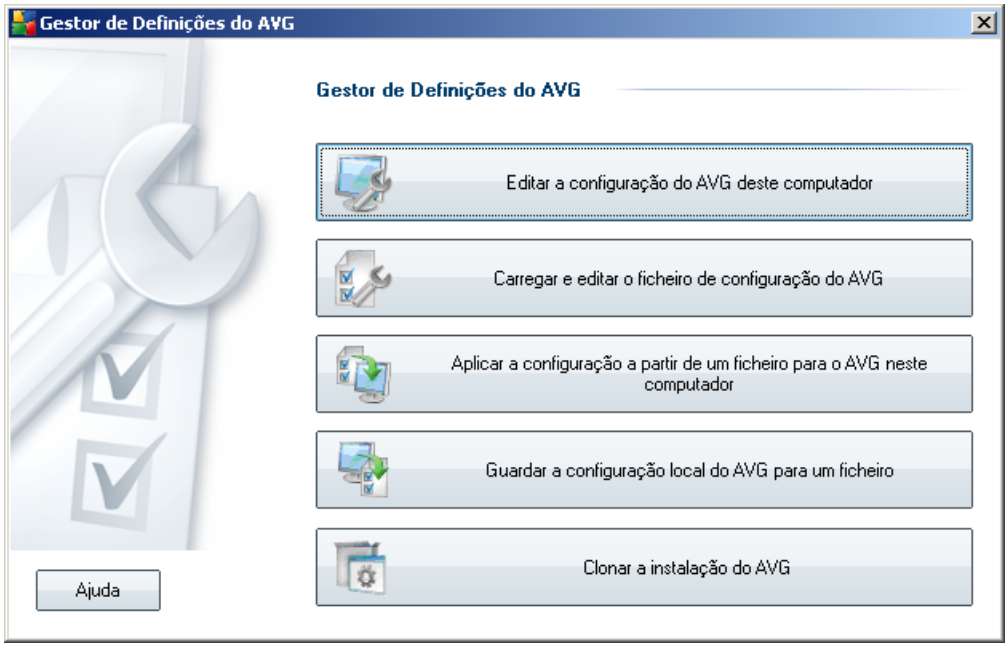
- ***Limpar Lista***- eliminar todas as entradas na lista de eventos
- ***Actualizar Lista*** - actualizar todas as entradas na lista de eventos

14. Gestor de Definições AVG

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

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

Todos os programas/AVG 9.0/Gestor de Definições AVG



- ***Editar a configuração do AVG neste computador***

  Use este botão para abrir uma janela com definições avançadas do AVG local. Todas as alterações efectuadas aqui serão reflectidas na instalação local do AVG.

- ***Carregar e editar o ficheiro de configuração do AVG***

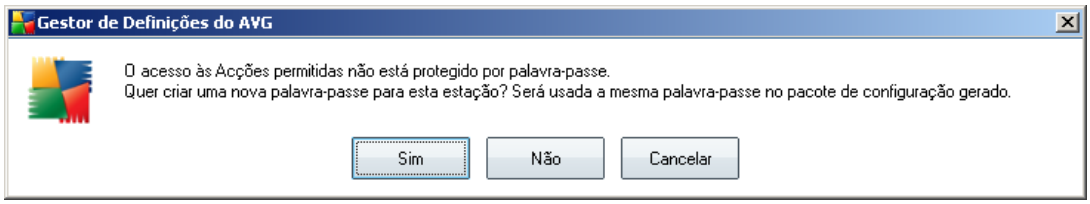
  Se já possui um ficheiro de configuração AVG (.pck), use este botão para o abrir e editar. Depois de confirmar as alterações através do botão ***OK*** ou ***Aplicar***, o ficheiro será substituído pelas novas definições!

- ***Aplicar configuração ao AVG neste computador a partir de ficheiro***

  Use este botão para abrir um ficheiro de configuração do AVG (.pck) e aplicá-lo à instalação local do AVG.

- ***Guardar a configuração do AVG local num ficheiro***

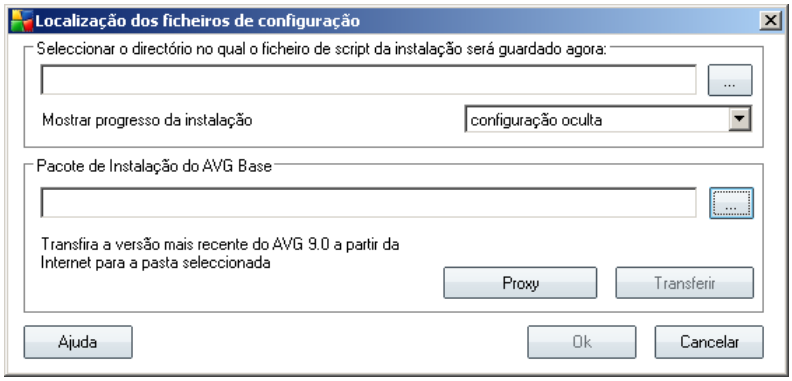
  Use este botão para guardar o ficheiro de configuração do AVG (.pck) da instalação local do AVG. Se não tiver definido uma palavra-passe para as Acções permitidas, pode ser apresentada a seguinte janela:



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

- ***Clonar instalação do AVG***

  Esta opção permite-lhe fazer uma cópia exacta da instalação local do AVG através da criação de um pacote de instalação com opções personalizadas. Para o efeito, primeiro seleccione a pasta onde o script de instalação deve ser guardado.



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

- ***Instalação oculta*** - não serão apresentadas quaisquer informações durante o processo de configuração.

- ***Mostrar apenas o progresso da instalação*** - a instalação não necessitará de qualquer intervenção do utilizador, mas o progresso será perfeitamente visível.

- ***Mostrar o assistente de instalação*** - a instalação será visível e o utilizador terá de confirmar todos os passos manualmente.

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

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

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

15. FAQ e Suporte Técnico

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

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