AVG 9 Anti-Virus plus Firewall

Manual do Usuário

Revisão do documento 90.21 (3.2.2010)

Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.
Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

Este produto usa o RSA Data Security, Inc. Algoritmo de Compilador de Mensagem MD5, Copyright (C) 1991-2, RSA Data Security, Inc. Criado em 1991.
Este produto usa o código da biblioteca C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).
Este produto usa a biblioteca de compactação zlib, Copyright (c) 1995-2002 Jean-loup Gailly e Mark Adler.
Este produto usa a biblioteca de compactação libbzip2, Copyright (c) 1996-2002 Julian R. Seward.

Conteúdo

AVG 9 Anti-Virus plus Firewall © 2010 Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.

AVG 9 Anti-Virus plus Firewall © 2010 Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.

AVG 9 Anti-Virus plus Firewall © 2010 Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.

1. Introdução

Este manual do usuário fornece documentação abrangente para **AVG 9 Anti-Virus plus Firewall**.

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

O AVG 9 Anti-Virus plus Firewall**é um dos vários produtos AVG premiados criados para fornecer a você paz de espírito e total segurança para o seu computador.** Como ocorreu com todos os produtos do AVG, o **AVG 9 Anti-Virus plus Firewall** foi completamente reprojetado para fornecer a proteção e a segurança certificada e renomada do AVG em uma nova forma, mais eficiente e amigável.

Seu novo produto AVG 9 Anti-Virus plus Firewall **tem uma interface simples combinada com uma verificação mais agressiva e rápida.** Mais recursos de segurança foram automatizados para sua conveniência e novas e inteligentes opçõespara o usuário foram incluídas, de forma que você possa adequar nossos recursos de segurança à sua forma de vida. A utilização não será mais comprometida em função da segurança!

O AVG foi projetado e desenvolvido para proteger seu computador e sua atividade de rede. Aproveite a experiência da proteção completa com o AVG.

AVG 9 Anti-Virus plus Firewall © 2010 Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais com suporte

O **AVG 9 Anti-Virus plus Firewall** destina-se à proteção de estações de trabalho com os seguintes sistemas operacionais.

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64,todas as edições)
- Windows 7 (x86 e x64, todas as edições)

(e possíveis service packs posteriores para sistemas operacionais específicos)

2.2. Requisitos de HW mínimos e recomendados

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

- CPU Intel Pentium 1,5 GHz
- 512 MB de memória RAM
- 390 MB de espaço livre em disco rígido (para fins de instalação)

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

- CPU Intel Pentium 1,8 GHz
- 512 MB de memória RAM
- 510 MB de espaço livre em disco rígido (para fins de instalação)

3. Opções de instalação do AVG

O AVG pode ser instalado a partir do arquivo de instalação disponível no CD de instalação, ou você pode baixar o arquivo de instalação mais recente no site da AVG (http://www.avgbrasil.com.br).

Antes de começar a instalar o AVG, é altamente recomendável que você visite o site da AVG (http://www.avgbrasil.com.br) para verificar se há um novo arquivo de instalação. Desta forma você pode ter certeza de instalar a versão mais recente disponível de AVG 9 Anti-Virus plus Firewall.

Recomendamos que você experimente a nossa nova ferramentaAVG Download Managerque ajudará a configurar o arquivo de instalação no idioma exigido!

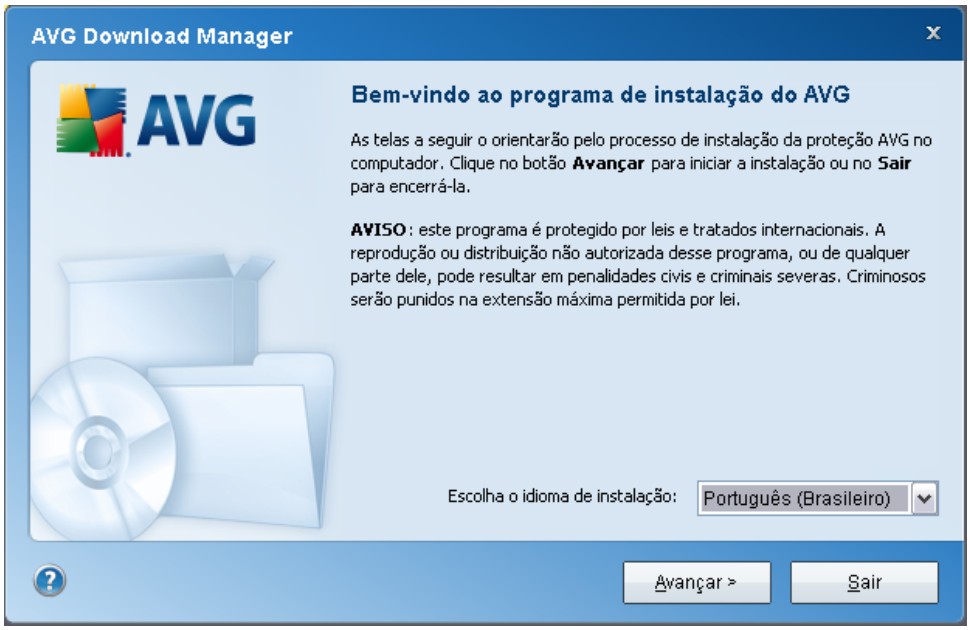
Durante o processo de instalação será solicitado o seu número de venda/licença. Certifique-se de tê-lo disponível antes de iniciar a instalação. O número de venda pode ser encontrado na embalagem do CD. Se você adquiriu a sua cópia do AVG on-line, o número da licença foi enviado para você por e-mail.

4. AVG Download Manager

O **<%AVG__DOWNLOAD_MANAGER%>** é uma ferramenta simples que ajuda você a selecionar o arquivo de instalação apropriado para o seu produto AVG. Com base nos dados inseridos, o gerenciador selecionará o produto específico, o tipo da licença, os componentes adequados e o idioma. Por fim, o download AVG Download Manager continuará e o processo de instalação apropriado será ativado.

Aviso: *observe que o AVG Download Manager não é adequado para o download das edições de rede e SBS. Além disso, que apenas os sistemas operacionais a seguir são suportados: Windows 2000 (SP4 + acumulação SRP), Windows XP, Windows Vista e Windows 7.***AVG Download Manager**<%está disponível para download no site da AVG (http://www.avgbrasil.com.br). Veja a seguir uma descrição breve de cada etapa que você precisará seguir no%>:**AVG Download Manager**

4.1. Seleção de Idioma



Nesta primeira etapa do **AVG Download Manager**, selecione o idioma da instalação no menu suspenso. Observe que a sua seleção de idioma se aplica somente ao processo de instalação; após a instalação, você poderá alterar o idioma diretamente das configurações do programa. Em seguida, pressione o botão ***Avançar***para continuar.

4.2. Verificação de conectividade

Na etapa seguinte o **AVG Download Manager tentará estabelecer uma conexão de Internet, de maneira que as atualizações possam ser localizadas.** Você não poderá continuar com o processo de download até que o AVG Download Manager possa concluir o teste de conectividade.

- Se o teste não mostrar conectividade, certifique-se de estar realmente conectado à Internet. Em seguida, clique no botão ***Repetir***.

- Se estiver usando uma conexão de Proxy para a Internet, clique no botão ***Configurações de Proxy*** para especificar suas informações de proxy:

- Se a verificação foi bem-sucedida, pressione o botão ***Avançar*** para continuar.

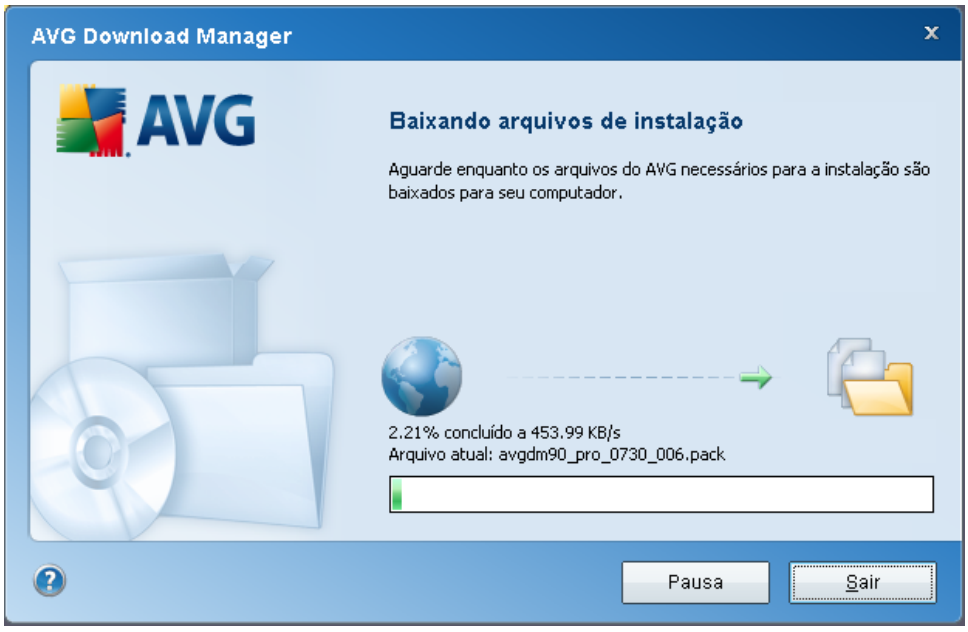
4.3. Configurações de Proxy

Se o AVG Download Manager **não conseguir identificar suas configurações de Proxy, você precisará especifica-las manualmente.** Forneça os seguintes dados:

- ***Servidor*** - insira um nome de servidor proxy ou endereço IP válidos
- ***Porta*** - forneça o respectivo número de porta
- ***Usar autenticação de proxy*** - se o seu servidor proxy exigir autenticação, marque esta caixa de seleção.
- ***Selecionar autenticação*** - no menu suspenso, selecione o tipo de autenticação. É altamente recomendável manter o valor padrão (*em seguida, o servidor de proxy transmitirá automaticamente os requisitos a você*). Entretanto, se você for um usuário experiente, poderá selecionar a opção Básico (*exigida por alguns servidores*) ou NTLM (*exigida por todos os servidores ISA*). Em seguida, insira um ***nome de usuário*** e ***senha*** (opcional) válidos.

Confirme as suas configurações pressionando o botão ***Aplicar***para seguir a próxima etapa de AVG Download Manager.

4.4. Arquivos de download para instalação



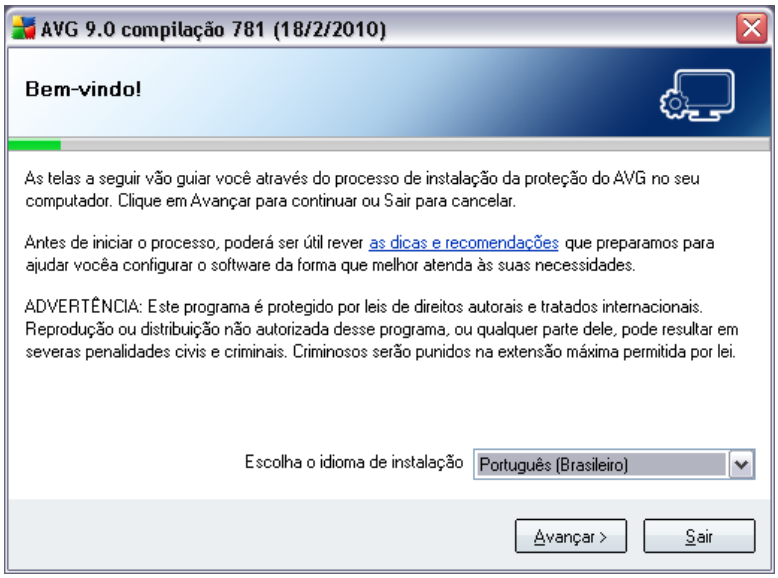
Agora, você forneceu todas as informações necessárias para o **AVG Download Manager** iniciar o download do pacote de instalação e lançar o processo de instalação. Você avançará para o Processo de Instalação do AVG.

5. Processo de instalação do AVG

Para instalar o **AVG 9 Anti-Virus plus Firewall** em seu computador, você precisa obter o arquivo de instalação mais recente. Você pode usar o arquivo de instalação do CD que é parte da edição, mas o arquivo pode estar desatualizado. Dessa forma, é recomendável obter a versão mais recente do arquivo de instalação on-line. Você pode fazer download do arquivo no site da AVG http://www.avgbrasil.com.br), seção ***Suporte e Download***. Se preferir, você pode usar a nossa nova ferramenta ***AVG Download Manager***, que ajuda a criar e baixar o pacote de instalação necessário e ativa o processo de instalação.

A instalação é uma seqüência de janelas de caixa de diálogo com uma descrição resumida do que fazer em cada etapa. A seguir, oferecemos uma explicação de cada janela da caixa de diálogo:

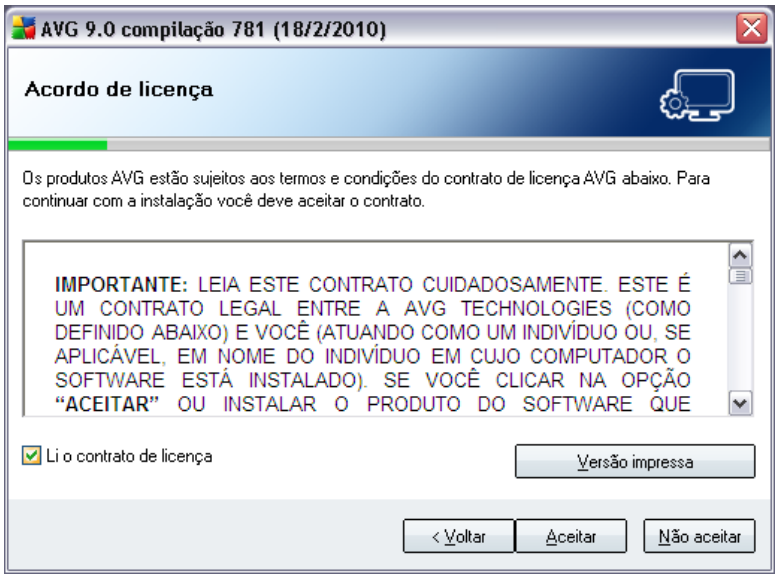
5.1. Início da instalação



O processo de instalação começa com a janela ***Bem-vindos ao Programa de Instalação do AVG*** . Nela você seleciona o idioma usado na instalação. Na parte inferior da janela da caixa de diálogo, localize o item ***Selecionar seu idioma da instalação*** e selecione o idioma desejado no menu suspenso. Em seguida, pressione o botão ***Avançar*** para confirmar e continuar para a próxima caixa de diálogo.

Atenção: *aqui você está selecionando o idioma somente para o processo de instalação. Você não está selecionando o idioma do aplicativo AVG. Isso poderá ser especificado posteriormente, durante o processo de instalação.*

5.2. Contrato de licença



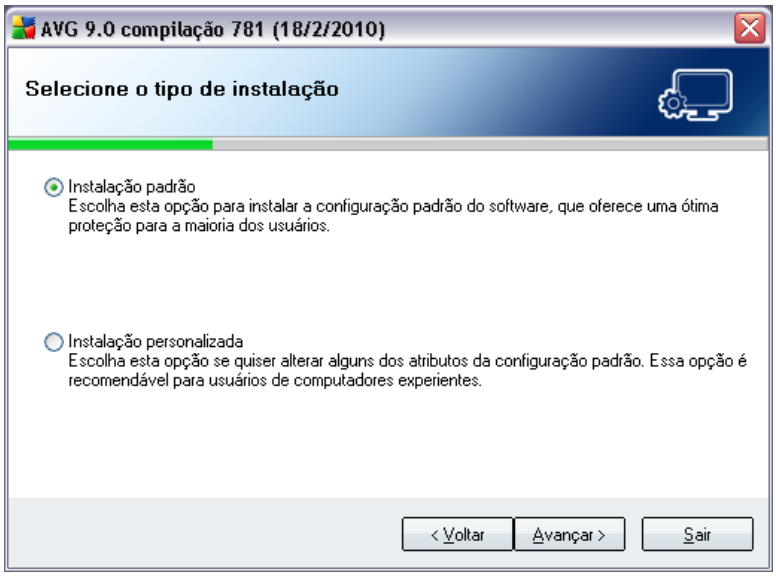
A caixa de diálogo ***Contrato de Licença*** indica o texto completo do contrato de licença do AVG. Leia-o cuidadosamente e confirme se leu, compreendeu e aceitou o contrato, marcando a caixa de seleção ***Li o contrato de licença*** e pressionando o botão ***Aceitar***.

Se você não concordar com o contrato de licença, pressione o botão ***Não aceito*** e o processo de instalação será encerrado imediatamente.

5.3. Verificando o status do sistema

Depois de confirmar o contrato de licença, você será redirecionado para a caixa de diálogo ***Verificação do Status do Sistema***. Essa caixa de diálogo não requer nenhuma intervenção; o sistema está sendo verificado antes da inicialização da instalação do AVG. Aguarde a conclusão do processo e continue automaticamente para a caixa de diálogo seguinte.

5.4. Selecionar o tipo de instalação



A caixa de diálogo ***Selecionar Tipo de Instalação*** oferece duas opções de instalação como alternativa: ***padrão*** e ***personalizada.***

Para a maioria dos usuários, é altamente recomendável manter a ***instalação padrão*** que instala o AVG no modo totalmente automático, com configurações predefinidas pelo fornecedor do programa. Essa configuração fornece o máximo de segurança combinado com o uso ideal dos recursos. No futuro, se houver necessidade de alterar a configuração, você sempre terá a possibilidade de fazer isso diretamente no aplicativo AVG.

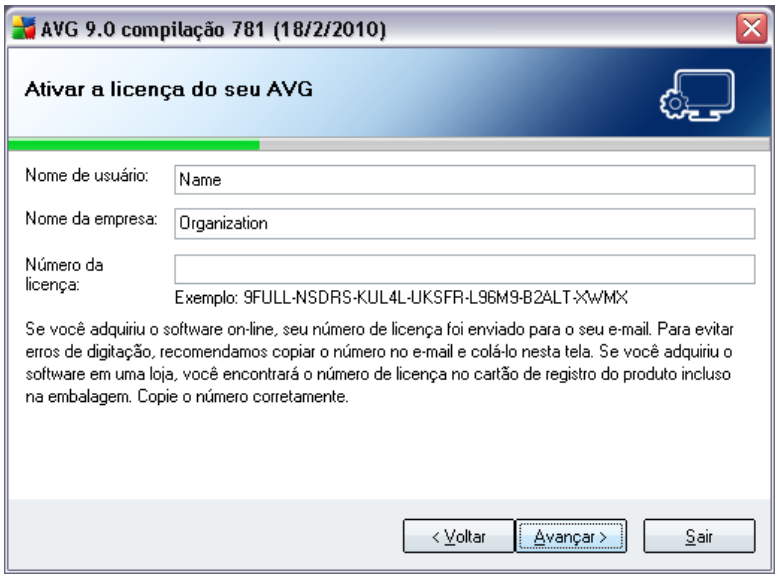
A instalação personalizada só deve ser usada por usuários experientes que tenham um motivo válido para instalar o AVG com configurações diferentes das padrão, ou seja, para se ajustar aos requisitos específicos do sistema.

5.5. Ative a sua Licença AVG

Na caixa de diálogo ***Ativar sua Licença do AVG*** , você deverá preencher o registro. Digite seu nome (campo ***Nome do Usuário***) e o nome da sua empresa (***Nome da Empresa).***

Em seguida, digite seu número de licença/vendas no campo de texto ***Número da Licença*** . O número de vendas pode ser encontrado no CD fornecido na embalagem do **AVG 9 Anti-Virus plus Firewall**. O número da licença está no e-mail de confirmação

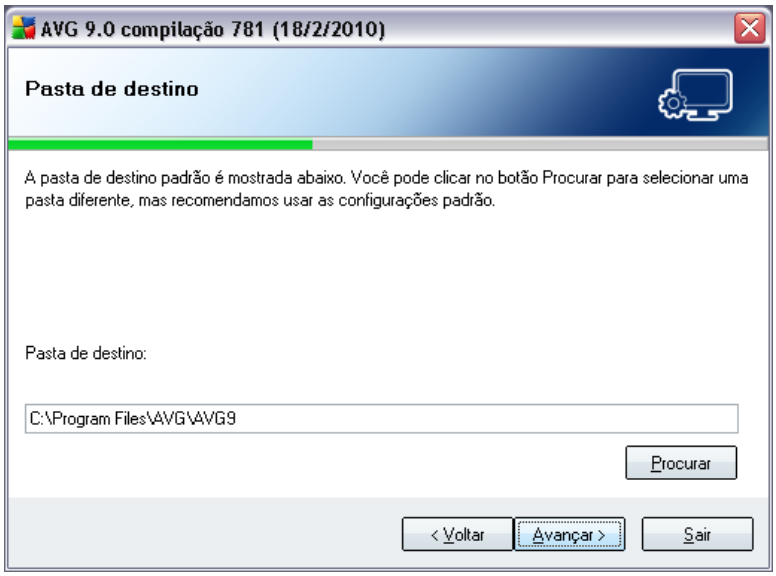
recebido depois da aquisição do AVG 9 Anti-Virus plus Firewall **on-line.** Digite o número exatamente como mostrado. Se o formulário digital do número de licença estiver disponível (*no e-mail*), é recomendável usar o método de copiar e colar para inseri-lo.



Pressione o botão ***Avançar*** para continuar o processo de instalação.

Se na etapa anterior você tiver selecionado a instalação padrão, será redirecionado para a caixa de diálogo ***Barra de Ferramentas de Segurança AVG*** **.** Se a instalação personalizada tiver sido selecionada, você continuará na caixa de diálogo ***Pasta de Destino***.

5.6. Instalação personalizada - Pasta de destino

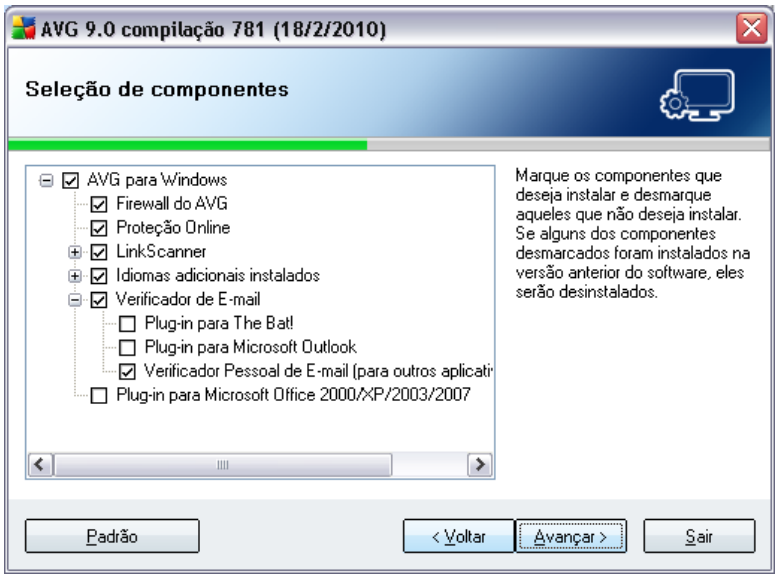


A caixa de diálogo ***Pasta de destino*** **permite especificar o local de instalação do AVG 9 Anti-Virus plus Firewall**. Por padrão, o AVG será instalado na pasta Arquivos de Programas da unidade C:. Se a pasta ainda não existir, uma nova caixa de diálogo solicitará que você confirme se deseja que o AVG a crie agora.

Se você desejar alterar esse local, use o botão ***Procurar*** para exibir a estrutura da unidade e selecionar a pasta respectiva.

Pressione o botão ***Avançar*** para confirmar.

5.7. Instalação personalizada - Seleção de componentes



A caixa de diálogo ***Seleção do componente*** **exibe uma visão geral de todos AVG 9 Anti-Virus plus Firewall os componentes do AVG 9 Anti-Virus plus Firewall que podem ser instalados.** Se as configurações padrão não forem adequadas a você, será possível remover/adicionar componentes específicos.

Entretanto, só é possível selecionar os componentes incluídos na edição do AVG que você adquiriu. Somente esses componentes serão oferecidos para a instalação na caixa de diálogo Seleção do Componente.

- ***Seleção de Idioma***

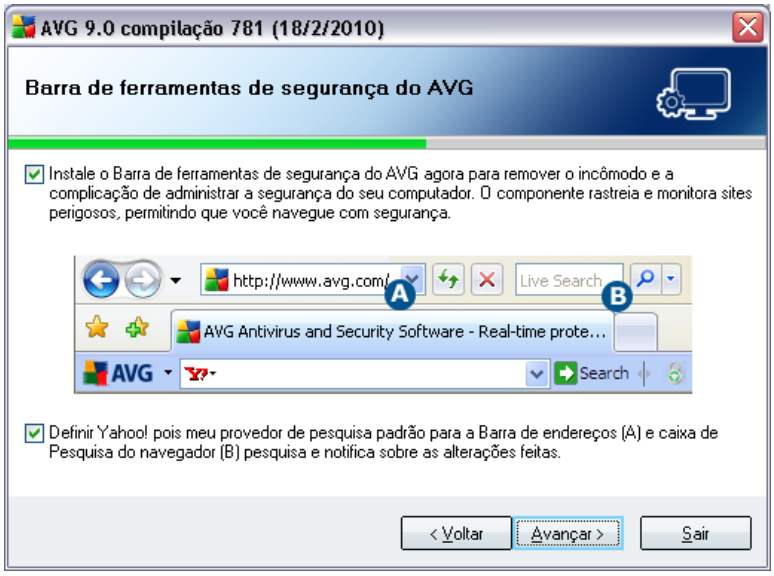
  Na lista de componentes a serem instalados, você poderá definir em que idioma (s) o AVG deverá ser instalado. Marque o item ***Idiomas adicionais instalados*** e selecione os idiomas desejados no respectivo menu.

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

  Clique no item ***Verificador de E-mail*** parar abrir e decidir que plug-in deverá ser instalado para garantir a segurança de sua correspondência eletrônica. Por padrão, o ***Plug-in para Microsoft Outlook*** será instalado. Outra opção específica é o ***Plug-in para The Bat!*** Se você utiliza qualquer outro cliente de e-mail (*MS Exchange, Qualcomm Eudora, ...*), escolha a opção ***Verificador Pessoal de E-mail*** para proteger suas comunicações de e-mail automaticamente, seja qual for o programa executado.

Continue pressionando o botão ***Avançar***.

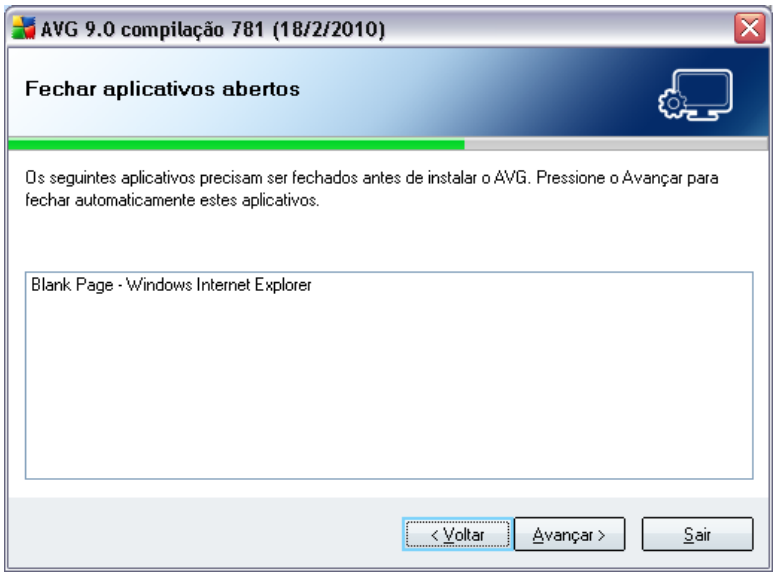
5.8. Barra de Ferramentas de Segurança do AVG



Na caixa de diálogo da ***Barra de Ferramentas de Segurança do AVG***, decida se você deseja instalar a ***Barra de Ferramentas de Segurança do AVG*** (*verificação dos resultados de pesquisa para mecanismos de pesquisa da Internet suportados*). Se você não alterar as configurações padrão, esse componente será instalado automaticamente no navegador da Internet (navegadores atualmente suportados são Internet Explorer da Microsoft v. 6.0 ou superior, e Mozilla Firefox v. 2.0 ou superior), para lhe fornecer proteção on-line abrangente enquanto estiver navegando pela Internet.

Além disso, você tem a opção de decidir se quer escolher o Yahoo! como o provedor de pesquisa padrão. Em caso afirmativo, marque a caixa de seleção respectiva.

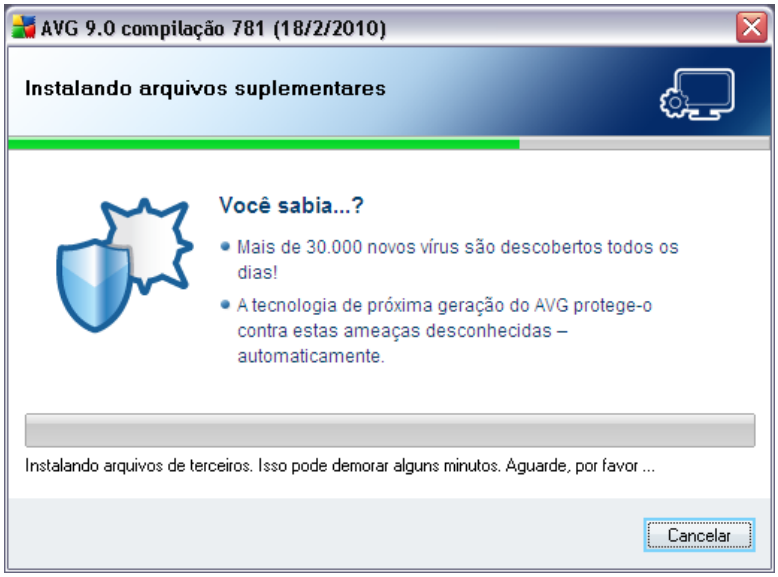
5.9. Fechar aplicativos abertos



A caixa de diálogo ***Feche os aplicativos abertos*** aparece durante o processo de instalação apenas no caso de existirem alguns programas em conflito em execução no computador neste momento. Será fornecida a lista de programas que precisam ser fechados a fim de concluir o processo de instalação. Pressione o botão ***Avançar*** para confirmar que você concorda em fechar os respectivos aplicativos e em continuar para a etapa seguinte.

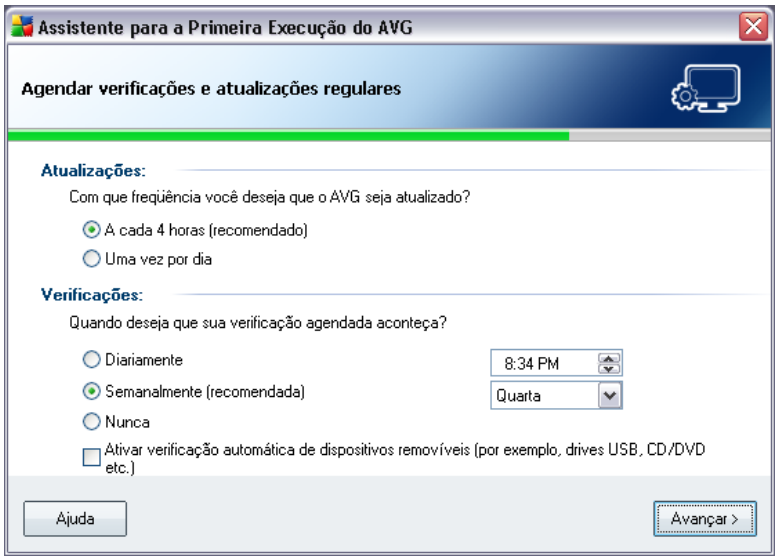
5.10. Instalando o AVG

A caixa de diálogo ***Instalar o AVG*** mostra o andamento do processo de instalação e não requer intervenção:



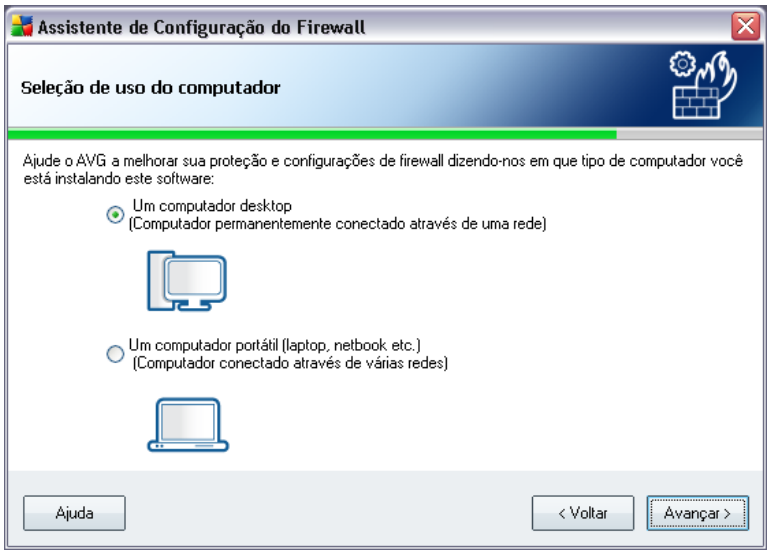
Após a conclusão do processo de instalação, você será redirecionado à próxima caixa de diálogo automaticamente.

5.11. Agendar verificações e atualizações regulares



Na caixa de diálogo ***Agendar verificações e atualizações regulares***, defina o intervalo para a verificação de acessibilidade dos novos arquivos de atualização e o horário em que a verificação agendada deve ser iniciada. É recomendável manter os valores padrão. Pressione o botão ***Avançar*** para continuar.

5.12. Seleção de uso do computador



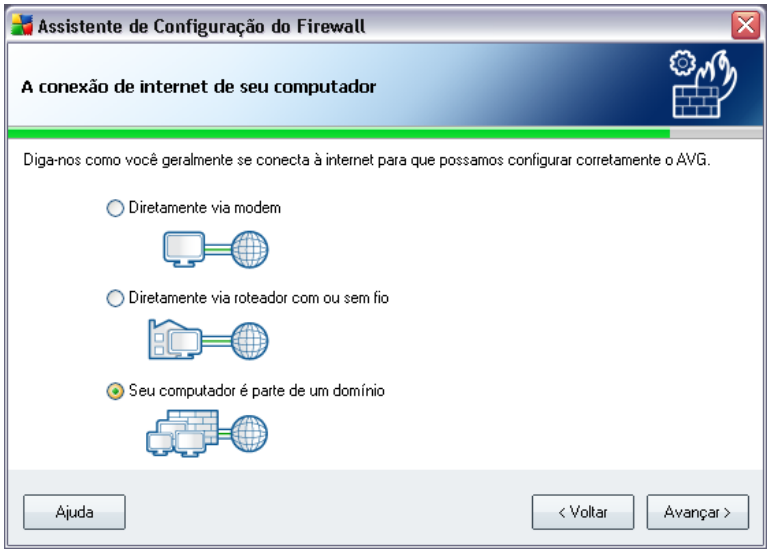
Nessa caixa de diálogo, o ***Assistente de configuração de firewall*** solicita o tipo de computador que você está usando. Por exemplo, seu notebook, que se conecta à Internet de diferentes locais *(aeroportos, quartos de hotel etc.)*) requer regras de segurança mais rigorosas do que as regras de um computador em um domínio *(rede empresarial etc.*). Com base no tipo de uso do computador selecionado, as regras padrão do ***Firewall*** serão definidas com um nível de segurança diferente.

Existem duas opções alternativas para seleção:

- ***Um computador desktop***
- ***Um computador portátil***

Confirme a seleção pressionando o botão ***Avançar*** e passe para a próxima caixa de diálogo.

5.13. A conexão de internet de seu computador



Nesta caixa de diálogo, o ***Assistente de Configuração do Firewall*** pergunta de que modo o computador está conectado à Internet. Com base no tipo de conexão selecionado, as regras padrão do ***Firewall*** serão definidas com um nível de segurança diferente.

Existem três opções alternativas para seleção:

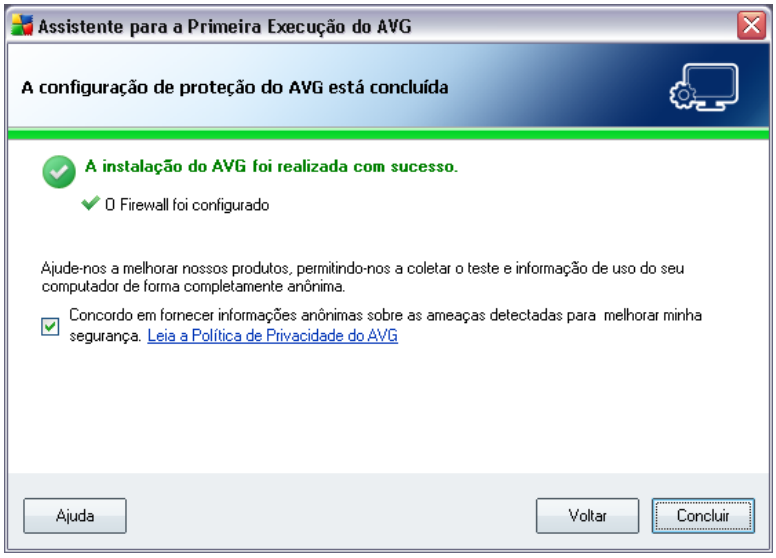
- ***Diretamente via modem***

- ***Diretamente via roteador com ou sem fio***
- ***Seu computador é parte de um domínio***

Selecione o tipo de conexão que melhor descreve a conexão do seu computador com a Internet.

Confirme a seleção pressionando o botão ***Avançar*** e passe para a próxima caixa de diálogo.

5.14. A configuração da proteção do AVG está concluída



Agora seu **AVG 9 Anti-Virus plus Firewall** foi configurado.

Nessa caixa de diálogo, você decide se deseja ativar a opção de relatórios anônimos sobre explorações e sites mal-intencionados para o AVG Virus Lab. Em caso positivo, marque a opção ***Concordo em fornecer informações ANÔNIMAS sobre ameaças detectadas para aumentar a minha segurança***.

Por fim, pressione o botão ***Concluir.*** Será necessário reiniciar o computador para que você possa começar a trabalhar com o AVG.

6. Após a instalação

6.1. Otimização da verificação

A funcionalidade de otimização da verificação pesquisa as pastas *Windows* e *Arquivos de programas* onde detecta arquivos apropriados (*no momento em que esses são arquivos *.exe, *.dll e *.sys*) e salva as informações nestes arquivos. No próximo acesso estes arquivos não serão verificados novamente e isso reduz o tempo de verificação de forma significativa.

Assim que o processo de instalação terminar você será convidado por meio de uma nova janela de diálogo a otimizar a verificação:

Recomendamos usar esta opção e executar o processo de otimização da verificação pressionando o botão ***Otimizar a verificação agora***.

6.2. Registro do produto

Ao concluir a instalação do **AVG 9 Anti-Virus plus Firewall**, registre o produto online no site do AVG (http://www.avgbrasil.com.br), página ***Registro*** *(siga as instruções fornecidas diretamente na página*). Depois do registro, você terá acesso completo à sua conta de usuário do AVG, ao boletim informativo de atualização do AVG e a outros serviços fornecidos exclusivamente para usuários registrados.

6.3. Acesso à interface do usuário

A ***Interface do Usuário do AVG*** pode ser acessada de várias formas:

- clique duas vezes no ícone do AVG na bandeja do sistema
- clique duas vezes no ícone do AVG na área de trabalho

AVG 9 Anti-Virus plus Firewall © 2010 Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.

- no menu ***Iniciar/Programas/AVG 9.0/Interface do Usuário do AVG***

6.4. Verificação de todo o computador

Existe um risco potencial de um vírus de computador ter sido transmitido ao seu computador antes da instalação do **AVG 9 Anti-Virus plus Firewall** . Por esse motivo, você deve executar uma ***verificação de todo o computador*** para assegurar que seu PC não esteja infectado.

Para obter instruções sobre a ***Verificação em todo o computador,*** consulte o capítulo ***Verificação do AVG***.

6.5. Teste Eicar

Para confirmar que **AVG 9 Anti-Virus plus Firewall** foi instalado corretamente, você pode executar o teste EICAR.

O teste EICAR é um método padrão e absolutamente seguro usado para testar o funcionamento do sistema antivírus. É seguro usá-lo, pois não se trata de um vírus real e não inclui fragmentos de código de vírus. A maioria dos produtos reage a este como se fosse um vírus (*embora sempre se refiram a ele com um nome óbvio, como "EICAR-AV-Test"*). É possível baixar o vírus EICAR no site www.eicar.com, onde você encontrará também todas as informações necessárias sobre o teste EICAR.

Tente baixar o arquivo ***eicar.com*** e salve-o em seu disco local. Logo após a confirmação do download do arquivo de teste, o***On-line Shield***reagirá a ele com um aviso. Esse aviso demonstra que o AVG está instalado corretamente em seu computador.

A partir do sitehttp://www.eicar.com você também pode fazer o download da versão compactada do 'vírus' EICAR (*por exemplo, na forma de eicar_com.zip* ***Proteção Online*** permite que você baixe este arquivo e salve-o no disco local, mas a ***Proteção Residente*** detecta o 'vírus' conforme tenta descompactá-lo. **Se o AVG falhar na identificação do teste EICAR como sendo um vírus, você deverá verificar novamente a configuração do programa.**

6.6. Configuração padrão do AVG

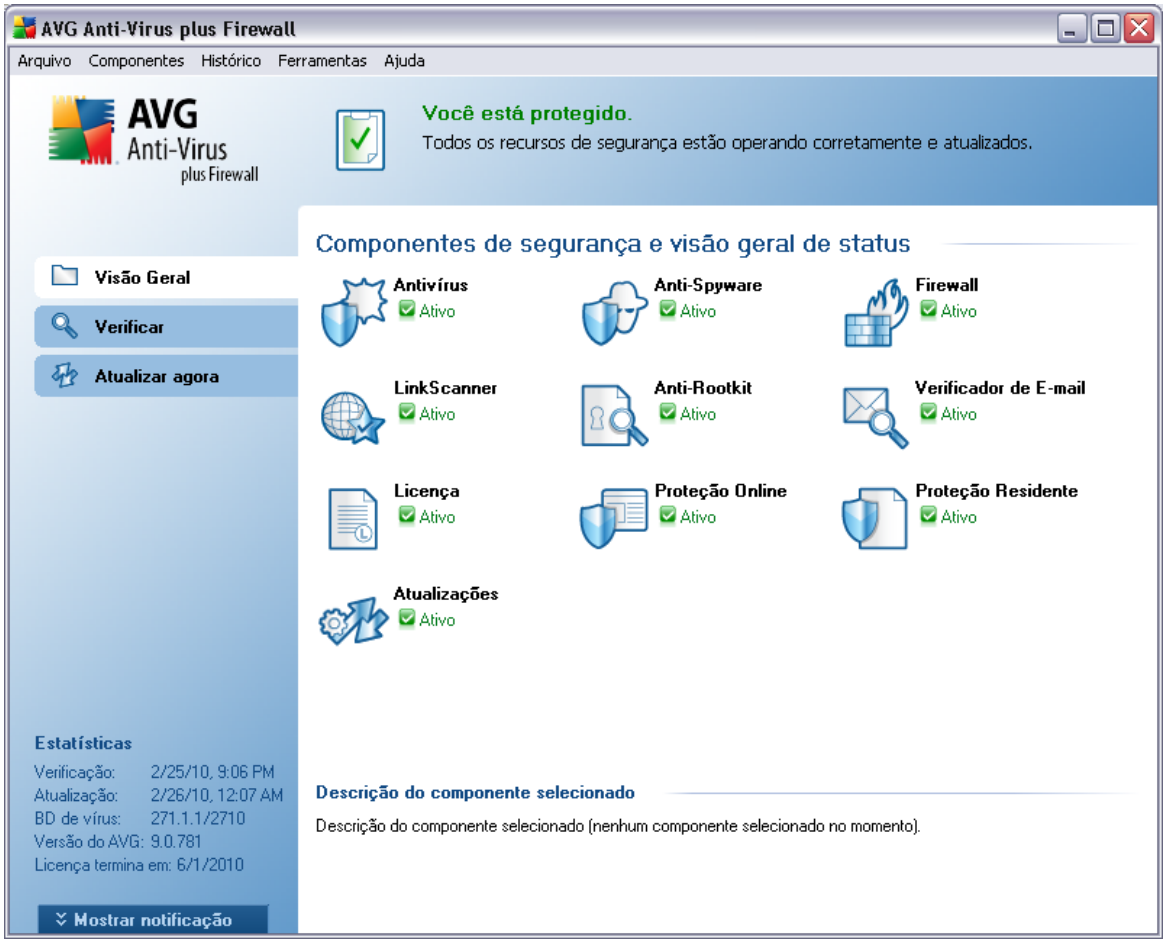
A configuração padrão (*isto é, como o aplicativo é configurado logo após a instalação*) de **AVG 9 Anti-Virus plus Firewall**é definida pelo fornecedor do software, de forma que todos os componentes e funções sejam ajustados para obter um desempenho ideal.

A menos que você tenha um motivo real para isso, não mude as configurações do AVG! Alterações nas configurações devem ser realizadas somente por um usuário experiente.

É possível acessar algumas edições menos importantes das configurações dos componentes do AVG diretamente na interface do usuário do componente específico. Se você tiver necessidade de alterar a configuração do AVG de acordo com suas necessidades, vá para ***Configurações Avançadas do AVG***: selecione o item de menu do sistema ***Ferramentas/Configurações avançadas*** e edite a configuração do AVG na nova caixa de diálogo aberta, a ***Configurações avançadas do AVG***.

7. Interface de usuário do AVG

O **AVG 9 Anti-Virus plus Firewall** é aberto com a janela principal:



A janela principal é dividida em várias seções:

- ***Menu do Sistema*** *(linha do sistema superior da janela)* é a navegação padrão que permite acessar todos os componentes, serviços e recursos do AVG - detalhes >>
- ***Informações do Status de Segurança*** *(seção inferior da janela)* fornece informações sobre o status atual do programa AVG - detalhes >>
- ***Links Rápidos*** *(seção esquerda da janela)* permite acessar rapidamente as tarefas mais importantes e mais utilizadas do AVG - detalhes >>

- ***Visão Geral dos Componentes*** *(seção central da janela)* oferece uma visão geral de todos os componentes AVG instalados - detalhes >>

- ***Estatísticas*** *(seção inferior esquerda da janela)* fornece todos os dados estatísticos referentes à operação dos programas - detalhes >>

- ***Ícone da Bandeja do Sistema*** *(canto inferior direito do monitor, na bandeja do sistema)* indica o status atual do AVG - detalhes >>

7.1. Menu do sistema

O ***Menu do sistema*** é a navegação padrão usada em todos os aplicativos Windows. Está localizado horizontalmente, na parte superior da janela principal do AVG 9 Anti-Virus plus Firewall**.** Use o menu do sistema para acessar os componentes específicos do AVG, recursos e serviços.

O menu do sistema é dividido em cinco seções principais:

7.1.1. Arquivo

- ***Sair*** - fecha a interface do usuário do **AVG 9 Anti-Virus plus Firewall**. Entretanto, o aplicativo AVG continuará sendo executado em segundo plano e seu computador continuará protegido.

7.1.2. Componentes

O item ***Componentes*** do menu do sistema inclui links para todos os componentes do AVG instalados, abrindo sua caixa de diálogo padrão na interface do usuário:

- ***Visão geral do sistema*** - muda para a caixa de diálogo da interface padrão do usuário com a visão geral de todos os componentes instalados e seu status

- ***Antivírus*** - abre a página padrão do componente ***Antivírus***

- ***Anti-rootkit*** - abre a página padrão do componente ***Anti-Rootkit***

- ***Anti-spyware*** - abre a página padrão do componente ***Anti-spyware***

- ***Firewall*** - abre a página padrão do componente ***Firewall***

- ***Link Scanner -*** abre a página padrão do componente***Link Scanner***

- ***Verificador de E-mail*** - abre a página padrão do componente ***Verificador de E-mail***

- ***Licença*** - abre a página padrão do componente ***Licença***
- ***On-line Shield*** - abre a página padrão do componente***Proteção Online***
- ***Proteção Residente*** - abre a página padrão do componente ***Proteção Residente***
- ***Gerenciador de Atualizações*** - abre a página padrão do componente ***Gerenciador de Atualizações***

7.1.3. Histórico

- ***Resultados da verificação*** - alterna para a interface de teste do AVG, especificamente para a caixa de diálogo ***Visão Geral dos Resultados da Verificação***
- ***Detecção da Proteção Residente*** - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela ***Proteção Residente***
- ***Detecção do Verificador de E-mail*-** abre uma caixa de diálogo com uma visão geral dos anexos de mensagens de e-mail detectados como perigosos pelo componente ***Verificador de E-mail***
- ***Detecção da Proteção Online*** - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pelo ***Proteção Online***
- ***Quarentena de Vírus*** - abre a interface do espaço de quarentena (***Quarentena de Vírus***) no qual o AVG remove todas as infecções detectadas que, por algum motivo, não podem ser resolvidas automaticamente. No espaço de quarentena, os arquivos infectados são isolados e a segurança do computador é preservada, e, ao mesmo tempo, os arquivos infectados são armazenados para possível reparo futuro.
- ***Log de Histórico de Eventos*** - abre a interface do log de eventos com uma visão geral de todas as ações registradas do **AVG 9 Anti-Virus plus Firewall** .
- ***Firewall*** - abre a interface de configurações do firewall na guia ***Logs*** com uma visão geral detalhada de todas as ações do firewall

7.1.4. Ferramentas

- ***Verificar computador*** - alterna para a interface de verificação do AVG e inicializa a verificação em todo o computador
- ***Verificar pasta selecionada*** - alterna para a interface de verificação do AVG

e permite definir, na estrutura de árvore do computador, quais arquivos e pastas devem ser verificados

- ***Verificar arquivo*** - permite executar um teste sob demanda em um único arquivo selecionado na estrutura de árvore do disco

- ***Atualizar*** - inicializa automaticamente o processo de atualização **AVG 9 Anti-Virus plus Firewall**

- ***Atualizar a partir do diretório*** - executa o processo de atualização a partir dos arquivos de atualização localizados em uma pasta específica do disco local. Entretanto, esta opção é recomendada somente como emergência, ou seja, em situações em que não há conexão com a Internet (*por exemplo, seu computador está infectado e desconectado da Internet; seu computador está conectado a uma rede sem acesso à Internet etc.*). Na nova janela aberta, selecione a pasta na qual colocou o arquivo de atualização anteriormente e inicialize o processo de atualização.

- ***Configurações avançadas*** - abre a caixa de diálogo ***Configurações avançadas do AVG***, na qual é possível editar a configuração **AVG 9 Anti-Virus plus Firewall**. Em geral, é recomendável manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.

- ***Configurações do Firewall*** - abre uma caixa de diálogo independente para configuração avançada do componente ***Firewall***

7.1.5. Ajuda

- ***Conteúdo*** - abre os arquivos de ajuda do AVG

- ***Obter ajuda on-line*** - abre o site da AVG (http://www.avgbrasil.com.br) na página de suporte técnico ao cliente

- ***Sua Web AVG*** - abre o site da AVG (http://www.avgbrasil.com.br)

- ***Sobre Vírus e Ameaças*** - abre a ***Enciclopédia de Vírus*** on-line na qual é possível pesquisar por informações sobre o vírus identificado

- ***Reativar*** - abre a caixa de diálogo ***Ativar AVG*** com os dados inseridos na caixa de diálogo ***Personalizar AVG*** do processo de instalação. Nessa caixa de diálogo é possível inserir o número da licença para substituir o número de vendas (*o número com o qual você instalou o AVG*) ou para substituir o número antigo da licença (*por exemplo, durante a atualização de um novo produto AVG*).

- ***Registre-se agora*** - estabelece uma conexão com a página de registro do site da AVG (http://www.avgbrasil.com.br). Informe os dados de registro; somente os clientes que registrarem seus produtos AVG poderão receber suporte técnico gratuito.

Observação**: Se estiver utilizando a versão de teste do* **AVG 9 Anti-Virus plus Firewall, os dois últimos itens aparecem como* ***Comprar agora*** *e* ***Ativar****, permitindo que você compre a versão completa do programa imediatamente. Para* **AVG 9 Anti-Virus plus Firewall** *instalado com um número de vendas, o itens são exibidos como****Registrar*** *e* ***Ativar****. Para obter mais informações, visite a seção Licença deste documento.*

- ***Sobre o AVG*** - abre a caixa de diálogo ***Informações*** com cinco guias que fornecem dados sobre o nome do programa, versão do programa e do banco de dados de vírus, informações do sistema, contrato de licença e informações de contato da ***AVG Technologies CZ***.

7.2. Informações sobre status de segurança

A seção ***Informações sobre Status de Segurança*** está localizada na parte superior da janela principal do AVG. Nessa seção, você encontrará informações sobre o status de segurança atual do **AVG 9 Anti-Virus plus Firewall.** Observe uma visão geral dos ícones possivelmente ocultos dessa seção e seus significados:

 O ícone verde indica que o AVG está totalmente funcional. Seu computador está totalmente protegido, atualizado e todos os componentes instalados estão funcionando corretamente.

 O ícone laranja avisa que um ou mais componentes estão configurados incorretamente e você deverá prestar atenção às propriedades e configurações respectivas. Não há problema crítico no AVG e você provavelmente decidiu desativar alguns componentes por algum motivo. Você ainda está protegido pelo AVG. Entretanto, preste atenção às configurações do componente com problema. Seu nome será fornecido na seção ***Informações sobre*** o Status de Segurança.

Esse ícone também aparece se, por alguma razão, você decidiu ignorar o status de erro de um componente (a opção *"Ignorar estado do componente" está disponível no menu de contexto aberto clicando-se com o botão direito sobre o ícone do componente em questão na visão geral do componente na janela*

principal do AVG). Você pode precisar usar esta opção em uma determinada situação; porém, recomendamos que a opção "***Ignorar estado do componente***" seja desligada o mais rápido possível.


O ícone vermelho indica que o AVG está em estado crítico ! Um ou mais componentes não está funcionando propriamente e o AVG não poderá proteger o seu computador. Preste atenção para reparar imediatamente o problema relatado. Se você não conseguir reparar o erro por conta própria, entre em contato com o Suporte Técnico do AVG .

É altamente recomendável prestar atenção nas Informações sobre Status de Segurança e, caso o relatório indique algum problema, tentar resolvê-lo imediatamente. Caso contrário, seu computador estará sob risco!

Nota: *as informações sobre o status do AVG também podem ser obtidas a qualquer momento no ícone da bandeja do sistema.*

7.3. Links rápidos

Os links rápidos *(na seção esquerda da Interface do Usuário do AVG)* permitem acessar imediatamente os recursos mais importantes e usados com mais frequência no AVG:

- ***Visão Geral*** - use esse link para passar de qualquer interface do AVG aberta no momento para a interface padrão, com uma visão geral de todos os componentes. Consulte o capítulo ***Visão geral dos componentes >>***
- ***Verificador do computador*** - use esse link para abrir a interface de verificação do AVG, onde é possível executar testes diretamente, programar verificações ou editar parâmetros. Consulte o capítulo ***Verificação do AVG >>***
- ***Atualizar agora*** - esse link abre a interface de atualização e inicializa o processo de atualização do AVG imediatamente. Consulte o capítulo

Atualizações do AVG >>

Esses links podem ser acessados da interface do usuário a qualquer momento. Quando você usar um link rápido para executar um processo específico, a GUI será alterada para uma nova caixa de diálogo, mas os links rápidos permanecerão disponíveis. Além disso, o processo de execução será representado graficamente.

7.4. Visão geral dos componentes

A seção ***Visão Geral dos Componentes*** se localiza na parte central da Interface do usuário do AVG. A seção é dividida em duas partes:

- Visão Geral de todos os componentes instalados consistindo de um painel com o ícone do componente e as informações sobre se o respectivo componente está ativo ou inativo.
- Descrição de um componente selecionado

No**AVG 9 Anti-Virus plus Firewall**a seção***Visão geral dos componentes*** contém informações sobre os seguintes componentes:

- ***O Antivírus*** garante que o computador seja protegido de vírus que tentam entrar nele -detalhes >>
- ***O Anti-Spyware*** verifica seus aplicativos em segundo plano enquanto você os executa-detalhes >>
- ***O Firewall*** controla a forma como o computador troca dados com outros computadores na Internet ou na rede local detalhes >>
- ***O LinkScanner*** verifica os resultados de pesquisa exibidos no navegador da Internet - detalhes >>
- ***O Anti-Rootkit*** detecta programas e tecnologias que tentam camuflar malware - detalhes>>
- ***O Verificador de E-mail*** verifica todas as mensagens enviadas e recebidas para procurar vírusdetalhes>>
- ***Licença*** exibe o número da licença, tipo e data de validade - detalhes >>
- ***Proteção Online*** verifica todos os dados baixados por um navegador da Web detalhes>>

- ***A Proteção Residente*** verifica os arquivos em segundo plano, conforme eles são copiados, abertos ou salvosdetalhes>>

- ***O Gerenciador de Atualizações*** controla todas as atualizações do AVG - detalhes>>

Clique no ícone de qualquer um dos componentes para realçá-lo na visão geral dos componentes. A descrição da funcionalidade básica do componente será exibida na parte inferior da interface do usuário. Clique duas vezes no ícone para abrir a interface dos componentes com uma lista de dados estatísticos básicos.

Clique com o botão direito sobre o ícone de um componente para expandir um menu de contexto: além de abrir a interface gráfica do componente, você ainda pode selecionar ***Ignorar estado do componente***. Selecione esta opção para informar que você está ciente do estado de erro do componente mas que, por alguma razão, deseja continuar com o AVG e não quer ser avisado pelo ícone da bandeja do sistema.

7.5. Estatísticas

A seção ***Estatísticas***se localiza na parte inferior esquerda da Interface do usuário do AVG. Ela oferece uma lista de informações relativas à operação do programa:

- ***Última verificação*** - fornece a data da última verificação

- ***Última atualização*** - fornece a data da inicialização da última atualização

- ***Banco de Dados de Vírus*** - informa sobre a versão do banco de dados de vírus instalada no momento

- ***Versão do AVG*** - informa sobre a versão do AVG instalada *(o número está na forma de 9.0.xx, onde 9.0 é a versão da linha do produto, e xx indica o número da compilação)*

- ***Vencimento da licença*** - fornece a data de vencimento da licença do AVG

7.6. Ícone da bandeja do sistema

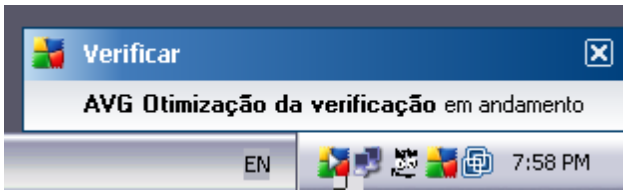
O Ícone da Bandeja do Sistema (*na barra de tarefas do Windows*) indica o status atual doAVG 9 Anti-Virus plus Firewall. Ele fica visível sempre na bandeja do sistema, independentemente de a janela principal do AVG estar aberta ou fechada.

Se colorido, o ***Ícone da Bandeja do Sistema*** indica que todos os componentes do AVG estão ativos e completamente funcionais. Da mesma forma, o ícone AVG na bandeja do sistema pode ser exibido em sua cor normal caso o AVG esteja em estado

de erro mas que você esteja completamente ciente desta situação e tenha deliberadamente decidido ***Ignorar o estado do componente***.

Um ícone com um sinal de exclamação indica um problema (componente inativo, status de erro, etc.). Clique duas vezes no ***Ícone da Bandeja do Sistema*** para abrir a tela principal e editar um componente.

O ícone da bandeja do sistema também informa sobre atividades atuais do AVG e possíveis mudanças de status no programa (*por ex., início automático de uma verificação ou atualização agendada,mudança de perfil do Firewall, alteração do status do componente, ocorrência de status de erro, ...*) por uma janela pop-up aberta pelo ícone AVG na bandeja do sistema:



O ***Ícone da Bandeja do Sistema*** também pode ser usado como um link rápido para acessar uma janela principal do AVG a qualquer momento (basta clicar duas vezes no ícone). Ao clicar com o botão direito do mouse no ***Ícone da Bandeja do Sistema*** , você abre um menu de contexto breve com as opções a seguir:

- ***Abrir Interface do Usuário do AVG*** - clique para abrir a Interface do Usuário do AVG
- ***Atualizar*** - inicia uma atualização imediata

8. Componentes do AVG

8.1. Antivírus

8.1.1. Princípios do Antivírus

O mecanismo de verificação do software antivírus verifica se há vírus conhecidos em todos os arquivos e atividades de arquivo (abertura/fechamento de arquivos etc.) Qualquer vírus detectado será bloqueado e não poderá realizar nenhuma ação. Ele também será limpo e colocado em quarentena. A maioria dos softwares antivírus usa a verificação heurística, onde os arquivos são verificados no que diz respeito às características normais de vírus, as chamadas assinaturas virais. Isso significa que o verificador antivírus pode detectar um novo e desconhecido vírus se este contiver algumas características típicas dos vírus existentes.

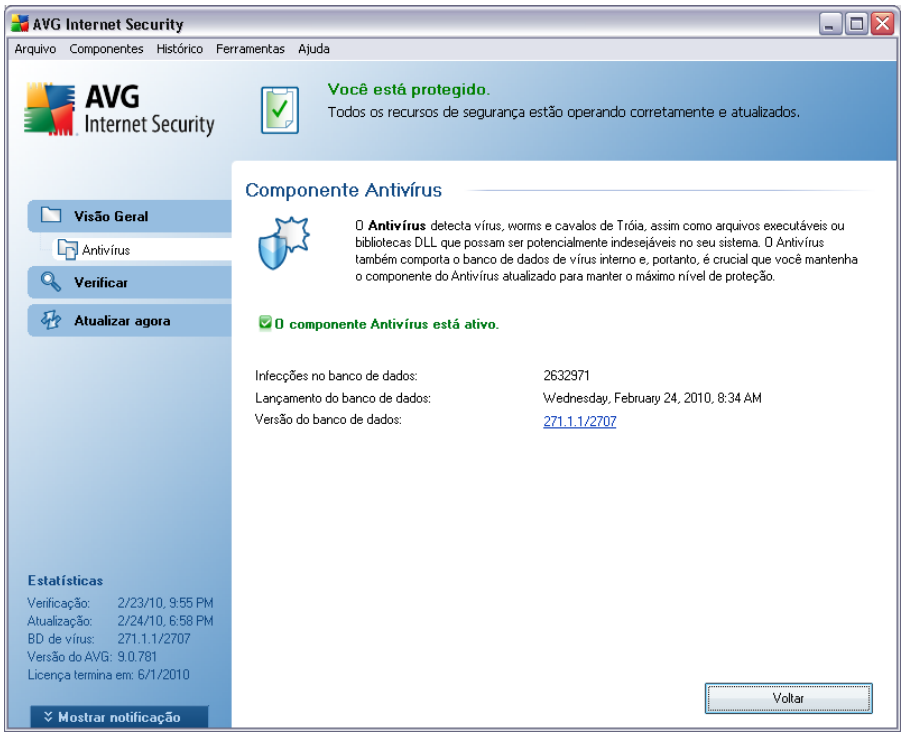
O recurso importante da proteção antivírus é que nenhum vírus conhecido pode ser executado no computador!

Nas situações em que uma única tecnologia poderia falhar na detecção ou identificação de um vírus, o ***Antivírus*** combina várias tecnologias para assegurar que o computador fique protegido:

- Verificação - procura seqüências de caracteres características de um determinado vírus.
- Análise heurística - emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual
- Detecção genérica - detecção de instruções características de um determinado vírus ou grupo de vírus

O AVG também é capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL potencialmente indesejáveis no sistema. Chamamos essas ameaças de Programas Potencialmente Indesejáveis (vários tipos de spyware, adware etc). Além disso, o AVG verifica o registro do sistema em busca de entradas suspeitas, arquivos temporários da Internet e cookies de rastreamento, e permite tratar todos os itens potencialmente prejudiciais da mesma maneira que qualquer outra infecção.

8.1.2. Interface do Antivírus



A interface do componente do ***Antivírus*** apresenta informações básicas sobre a funcionalidade do componente, informações sobre o status atual do componente (*O Antivírus está ativo.*) e uma breve visão geral das ***estatísticas do*** Antivírus:

- ***Definições de infecção*** - o número fornece a contagem de vírus definidos na versão atualizada do banco de dados de vírus.
- ***Atualização mais recente do banco de dados*** - especifica quando e a que horas o banco de dados de vírus foi atualizado
- ***Versão do banco de dados*** - define o número da versão mais recente do banco de dados. Esse número aumenta a cada atualização da base de vírus

Existe apenas um botão de operação disponível na interface deste componente (***Voltar***) - pressione o botão para retornar para a interface do usuário do AVG padrão (visão geral dos componentes).

Nota: *o fornecedor do software configurou todos os componentes do AVG para proporcionar um desempenho ideal. A menos que você tenha um motivo real para*

isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema ***Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

8.2. Anti-Spyware

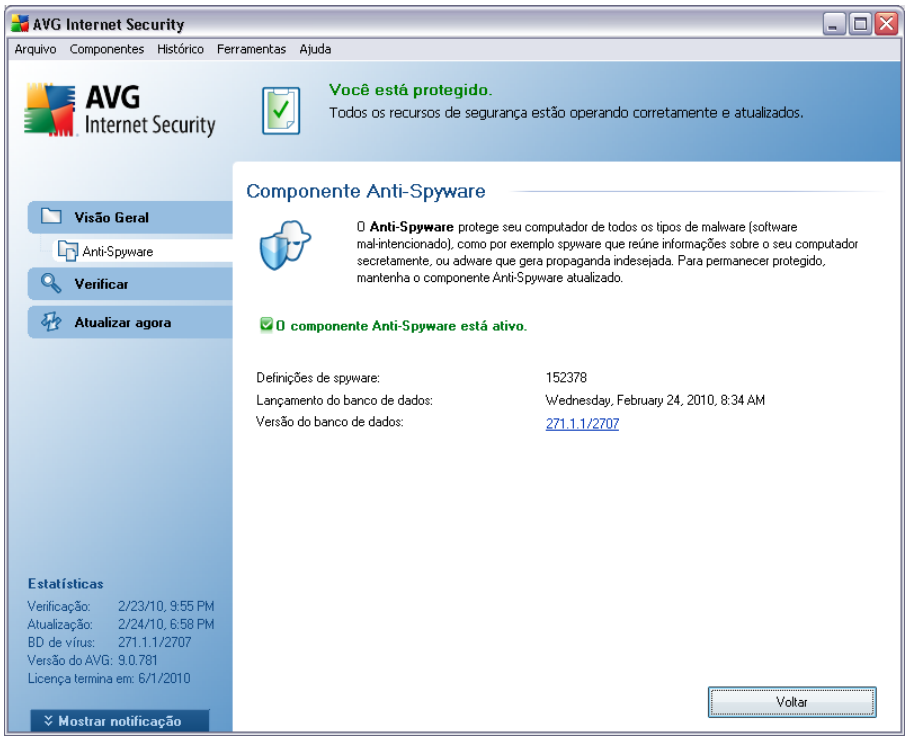
8.2.1. Princípios do Anti-Spyware

A definição comum de spyware é um tipo de malware, ou seja, softwares que coletam informações a partir do computador do usuário sem o conhecimento ou consentimento deste. Alguns aplicativos de spyware também podem ser instalados propositalmente e, geralmente, contêm anúncios, janelas pop-up ou tipos diferentes de softwares inoportunos.

Atualmente, a fonte mais comum de infecção são sites com conteúdo potencialmente perigoso. Outros métodos de transmissão, como email ou transmissão por worms e vírus, são também predominantes. A proteção mais importante é o uso de um verificador de segundo plano sempre ativo, o ***Anti-Spyware***, que funciona como uma proteção residente e verifica seus aplicativos em segundo plano, à medida que são executados.

Também é possível que algum malware tenha sido transmitido ao seu computador antes da instalação do AVG ou que você tenha esquecido de baixar as últimasAVG 9 Anti-Virus plus Firewall atualizações de banco de dados e programas . Por esta razão, o AVG permite verificar totalmente o computador em busca de malware ou spyware, usando o recurso de verificação. Ele também detecta malwares inativos e não perigosos, ou seja, baixados mas ainda não ativados.

8.2.2. Interface do Anti-Spyware



A interface do componente do ***Anti-Spyware*** fornece uma breve visão geral da funcionalidade do componente, informações sobre o status atual do componente (*O Anti-Spyware está ativo.*) e algumas estatísticas sobre o ***Anti-Spyware***:

- ***Definições de spyware*** - o número fornece a contagem de amostras de spyware definidas na versão do banco de dados de spyware mais recente.
- ***Atualização mais recente do banco de dados*** - especifica quando e a que horas o banco de dados do spyware foi atualizado
- ***Versão do banco de dados*** - define o número da versão mais recente do spyware. Esse número aumenta a cada atualização da base de vírus.

Existe apenas um botão de operação disponível na interface deste componente (***Voltar***) - pressione o botão para retornar para a interface do usuário do AVG padrão (visão geral dos componentes).

Nota: o *fornecedor do software configurou todos os componentes do AVG para propiciar um desempenho ideal. A menos que você tenha um motivo real para isso,*

não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema ***Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

8.3. Anti-Rootkit

Um rootkit é um programa criado para assumir o controle fundamental de um sistema de computador, sem autorização dos proprietários do sistema e gerentes legítimos. O acesso ao hardware é realmente necessário, pois um rootkit tem o objetivo de executar o controle do sistema operacional executado no hardware. Geralmente, os rootkits atuam para obscurecer sua presença no sistema por meio de subversão ou evasão de mecanismos de segurança padrão do sistema operacional. Freqüentemente, eles também são Cavalos de Tróia, levando os usuários a acreditarem que é confiável executá-los no sistema. As técnicas usadas para conseguir isso podem incluir ocultar processos em execução de programas de monitoramento ou ocultar arquivos ou dados do sistema operacional.

8.4. Firewall

O firewall é um sistema que impõe uma política de controle de acesso entre duas ou mais redes, bloqueando ou permitindo o tráfego. Todo firewall contém um conjunto de regras que protegem a rede interna de ataques originados externos (normalmente da Internet) e controlam toda a comunicação em cada porta da rede. A comunicação é avaliada de acordo com as regras definidas e, então, são permitidas ou proibidas. Se o firewall reconhece uma tentativa de invasão, ele "bloqueia" a tentativa e não permite que o invasor acesse o computador.

O firewall é configurado para permitir ou recusar a comunicação interna/externa (de saída ou entrada) por meio de portas definidas e para aplicativos definidos. Por exemplo, o firewall pode ser configurado para permitir que os dados da Web entrem e saiam usando apenas o Microsoft Explorer. Qualquer tentativa de transmitir dados da Web por outro navegador seria bloqueada.

O firewall protege as informações identificadas como pessoais, não permitindo que elas sejam enviadas do seu computador sem permissão. Ele controla a forma como o computador troca dados com outros computadores na Internet ou na rede local. Dentro de uma organização, o Firewall também protege um único computador de ataques iniciados por usuários internos em outros computadores da rede.

Recomendação: *geralmente, não é recomendável usar mais de um firewall em um computador individual. A segurança do computador não é aumentada se você instalar mais firewalls. É mais provável que ocorram alguns conflitos entre esses dois*

aplicativos. Por isso recomendamos que você use somente um firewall no seu computador e desative todos os outros, eliminando assim o risco de possível conflito e de problemas relacionados.

8.4.1. Princípios do Firewall

No AVG, o componente do ***Firewall*** controla todo o tráfego em cada porta de rede do seu computador. Com base nas regras definidas, o ***Firewall*** avalia os aplicativos em execução (e que pretendem se conectar à rede Internet ou local) ou aplicativos que abordam o computador externamente, tentando estabelecer conexão com o PC. Para cada um desses aplicativos, o ***Firewall*** permitirá ou impedirá a comunicação nas portas da rede. Por padrão, se o aplicativo for desconhecido, (isto é, se não tiver regras definidas de ***Firewall*** o ***Firewall*** perguntará se você deseja permitir ou bloquear a tentativa de comunicação.

Observação: o *Firewall do AVG não se destina a plataformas de servidores!*

O que o AVG Firewall pode fazer:

- Permitir ou bloquear tentativas de comunicação de aplicativos automaticamente ou pedir sua confirmação
- Usar perfis completos com regras predefinidas, de acordo com as suas necessidades
- Alternar os perfis automaticamente ao se conectar a várias redes ou usar vários adaptadores de rede

8.4.2. Perfis do Firewall

O Firewall permite que você defina regras específicas de segurança com base no fato de o seu computador estar localizado em um domínio, ou ser um computador isolado, ou até mesmo um notebook. *** Cada uma dessas opções requer um nível diferente de proteção, e os níveis são abordados pelos respectivos perfis. Em suma, um perfil do ***Firewall***é uma configuração específica do componente ***Firewall*** e você pode usar várias dessas configurações predefinidas.

Perfis disponíveis

- ***Permitir tudo -***um perfil do sistema de ***Firewall*** que foi predefinido pelo fabricante e está sempre presente. Quando esse perfil é ativado, toda a comunicação de rede é permitida e não se aplicam as regras da política de

segurança, como se a proteção do ***Firewall*** estivesse desativada *(isto é, todos os aplicativos são permitidos, mas os pacotes ainda estão sendo verificados; para desabilitar completamente qualquer filtragem, é preciso desabilitar o firewall)*. Esse perfil do sistema não pode ser duplicado, excluído e suas configurações não podem ser modificadas.

- ***Bloquear tudo -*** um perfil do sistema de ***Firewall*** predefinido pelo fabricante e que está sempre presente. Quando o perfil é ativado, toda a comunicação de rede é bloqueada e o computador não fica acessível para redes externas, nem pode se comunicar com ambientes externos. Esse perfil do sistema não pode ser duplicado, excluído e suas configurações não podem ser modificadas.

- ***Perfis personalizados***:

  - ***Conectado diretamente à Internet*** – adequada para PCs comuns conectados diretamente à Internet ou notebooks conectando-se à Internet fora da rede segura da empresa. Selecione essa opção se estiver se conectando de casa ou se estiver em uma rede de pequena empresa sem controle central. Além disso, selecione essa opção quando estiver viajando e conectando seu notebook a partir de vários locais possivelmente perigosos (*internet café, quarto de hotel, etc.*). Serão criadas regras mais restritas, pois se parte do princípio que esses computadores não possuem proteção adicional e, portanto, requerem proteção máxima.

  - ***Computador no domínio*** – adequado para computadores em uma rede local, como rede de uma empresa ou escola. Presume-se que a rede esteja protegida por algumas medidas adicionais, de modo que o nível de segurança pode ser inferior para um computador isolado.

  - ***Rede doméstica ou corporativa pequena*** – adequado para computadores em uma rede pequena, como uma rede doméstica ou de uma pequena empresa, geralmente vários computadores conectados entre si, sem um administrador "central".

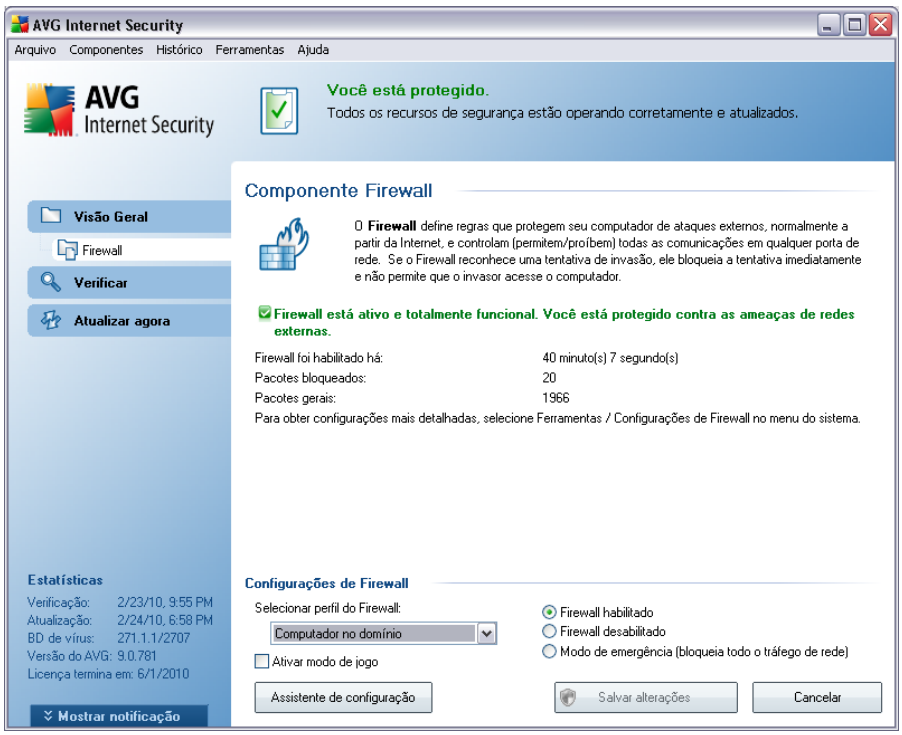
Alternância de perfil

O recurso Alternância de perfil permite que o ***Firewall*** alterne automaticamente para o perfil definido ao usar um determinado adaptador de rede, ou ao se conectar a um determinado tipo de rede. Se nenhum perfil tiver sido atribuído a uma área de rede ainda, durante a próxima conexão com essa área, o ***Firewall*** exibirá uma caixa de diálogo solicitando que você atribua um perfil

Você pode atribuir perfis para todas as interfaces da rede local ou áreas e especificar futuras configurações na janela ***Perfis de Áreas e Adaptadores***, onde você também pode desabilitar essa função, caso você não deseja utilizá-la (*dessa forma, qualquer tipo de conexão, o perfil padrão será utilizado*).

Geralmente, os usuários que possuem um notebook e usam vários tipos de conexão acharão esse recurso útil. Se você tiver um computador desktop e usar somente um tipo de conexão (*como conexão cabeada à Internet*), não será preciso se preocupar com a alternância de perfil, pois, provavelmente, você nunca a utilizará.

8.4.3. Interface do Firewall



A interface do ***Firewall*** oferece algumas informações básicas sobre a funcionalidade do componente, além de uma visão geral resumida das estatísticas do ***Firewall***:

- ***Firewall ficou habilitado por*** - tempo decorrido desde que o Firewall foi iniciado
- ***Pacotes bloqueados*** - número de pacotes bloqueados do volume total de pacotes verificados

- ***Pacotes gerais*** - número de todos os pacotes verificados durante a execução do Firewall

Configuração básica do componente

- ***Selecionar perfil do Firewall*** - no menu suspenso, selecione um dos perfis definidos - dois perfis estão disponíveis sempre (os *perfis padrão denominados* ***Permitir tudo*** *e* ***Bloquear tudo***), outros perfis foram adicionados manualmente por meio da edição do perfil na caixa de diálogo ***Perfis*** em ***Configurações do Firewall***.

- ***Ativar modo de jogo -*** Marque esta opção para garantir que, ao executar aplicativos em tela cheia (jogos, apresentações no PowerPoint, etc.), o ***Firewall*** não exiba caixas de diálogo perguntando se você deseja permitir ou bloquear a comunicação para aplicativos desconhecidos. No caso de um aplicativo desconhecido tentar comunicar-se pela rede neste momento, o ***Firewall*** permitirá ou bloqueará a tentativa automaticamente, de acordo com as configurações no perfil atual.

- ***Status do Firewall***:

  - ***Firewall ativado -*** selecione esta opção para permitir a comunicação nesses aplicativos considerados 'permitidos' no conjunto de regras definidas no perfil de ***Firewall*** selecionado

  - ***Firewall desativado -*** esta opção desativa totalmente o ***Firewall***, todo o tráfego da rede é permitido mas não verificado!

  - ***Modo de emergência (bloquear todo o tráfego de Internet)*** - selecione esta opção para bloquear todo o tráfego em toda porta de rede; o ***Firewall*** ainda está em execução, mas todo o tráfego da rede é interrompido

Nota: *o fornecedor do software configurou todos os componentes do AVG para proporcionar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. As alterações nas configurações só devem ser feitas por um usuário experiente. Se você precisar alterar a configuração do Firewall, selecione o item de menu do sistema****Ferramentas/Configurações avançadas*** *e edite a configuração do Firewall na caixa de diálogo recém-aberta* ***Configurações do Firewall****.*

Botões de controle

- ***Assistente de configuração*** - pressione o botão para acessar a respectiva caixa de diálogo (*usada no processo de instalação*) denominada ***Seleção do uso do computador***, na qual é possível especificar a configuração do componente ***Firewall***

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo

- ***Cancelar*** - pressione este botão para retornar à interface do usuário do AVG padrão (*visão geral dos componentes*)

8.5. Verificador de E-mail

O e-mail é uma das fontes mais comuns de vírus e cavalos de tróia. O phishing e o spam tornam o e-mail uma fonte de riscos ainda maior. Contas gratuitas de e-mail são as que têm maior probabilidade de receber mensagens de e-mail mal-intencionadas (*já que raramente adotam tecnologias anti-spam*), e os usuários domésticos confiam demais nesse tipo de conta de e-mail. Além dos usuários domésticos, sites desconhecidos e formulários de preenchimento on-line com dados pessoais (*como endereço de e-mail*) aumentam a exposição a ataques via e-mail. Em geral, as empresas usam contas de e-mail corporativo e adotam filtros anti-spam, etc., para reduzir o risco.

8.5.1. Princípios do Verificador de E-mail

O componente ***Verificador de e-mail*** verifica e-mails de entrada/saída automaticamente. Você pode usá-lo com clientes de e-mail que não possuem um plug-in próprio no AVG (*por exemplo, Outlook Express, Mozilla, Incredimail, etc.*).

Durante a instalação do AVG, existem servidores automáticos criados para controle de e-mails: um para verificar e-mails de entrada e o segundo para verificar e-mails de saída. Utilizando esses dois servidores, os e-mails são automaticamente verificados nas portas 110 e 25 (*portas padrão para o recebimento e envio de e-mails*).

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

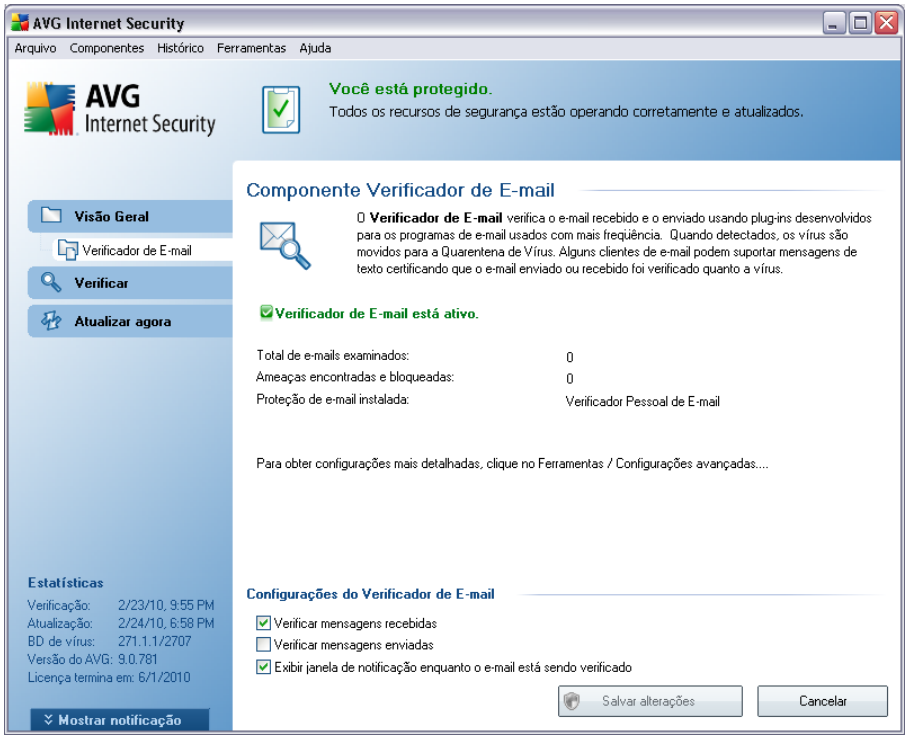
- ***E-mails de entrada:*** ao receber uma mensagem do servidor, o componente ***Verificador de e-mail*** a testa em busca de vírus, remove anexos infectados e adiciona uma certificação. Quando detectados, os vírus são movidos para a ***Quarentena de Vírus***imediatamente. Então a mensagem é passada para o cliente de e-mail.

- ***E-mails de saída:*** a mensagem é enviada a partir do cliente de e-mail para o

Verificador de e-mail; ele testa essa mensagem e seus anexos em busca de vírus e, em seguida, envia a mensagem ao servidor SMTP (*a verificação de e-mails de saída está desativada por padrão e pode ser configurada manualmente*).

Observação: *o Verificador de E-mail do AVG não se destina a plataformas de servidores!*

8.5.2. Interface do Verificador de E-mail



Na caixa de diálogo do componente***Verificador de E-mail*** , você pode encontrar um breve texto descrevendo a funcionalidade do componente, informações sobre o status atual (*Verificador de E-mail está ativo.*) e as seguintes estatísticas:

- ***Total de e-mails verificados***- quantas mensagens de e-mail foram verificadas desde que foi lançado o ***Verificador de E-mail*** mais recente (*se necessário, este valor pode ser redefinido; para fins de estatística, por exemplo - Redefinir valor*)

- ***Ameaças encontradas e bloqueadas*** - fornece o número de infecções detectadas nas mensagens de e-mail desde que o ***Verificador de E-mail*** foi

iniciado pela última vez.

- ***Proteção de e-mail instalada*** - informações sobre um plug-in de proteção de e-mail específico referente ao seu cliente de e-mail padrão instalado.

Configuração básica do componente

Na parte inferior da caixa de diálogo, você pode encontrar a seção ***Configurações do Verificador de E-mail*** , onde é possível editar alguns recursos básicos da funcionalidade do componente.

- ***Verificar mensagens de entrada*** - marque esse item para especificar que todos os e-mails enviados à sua conta devem ser verificados em busca de vírus. Esse item está ativado por padrão e não convém alterar essa configuração!

- ***Verificar mensagens de saída*** - marque o item para confirmar a verificação de vírus em todos os e-mails enviados a partir da sua conta. Esse item está desativado por padrão.

- ***Exibir ícone de notificação enquanto o e-mail for verificado*** – marque o item para confirmar que deseja ser informador através da caixa de diálogo de notificação exibida sobre o ícone AVG na bandeja do sistema durante a verificação de seu e-mail através do componente ***Verificador de E-mail***. Esse item está ativado por padrão e não convém alterar essa configuração!

A configuração avançada do componente ***Verificador de E-mail*** pode ser acessada pelo item ***Ferramentas/Configurações avançadas*** do menu do sistema. Entretanto, a configuração avançada é recomendada somente para usuários experientes.

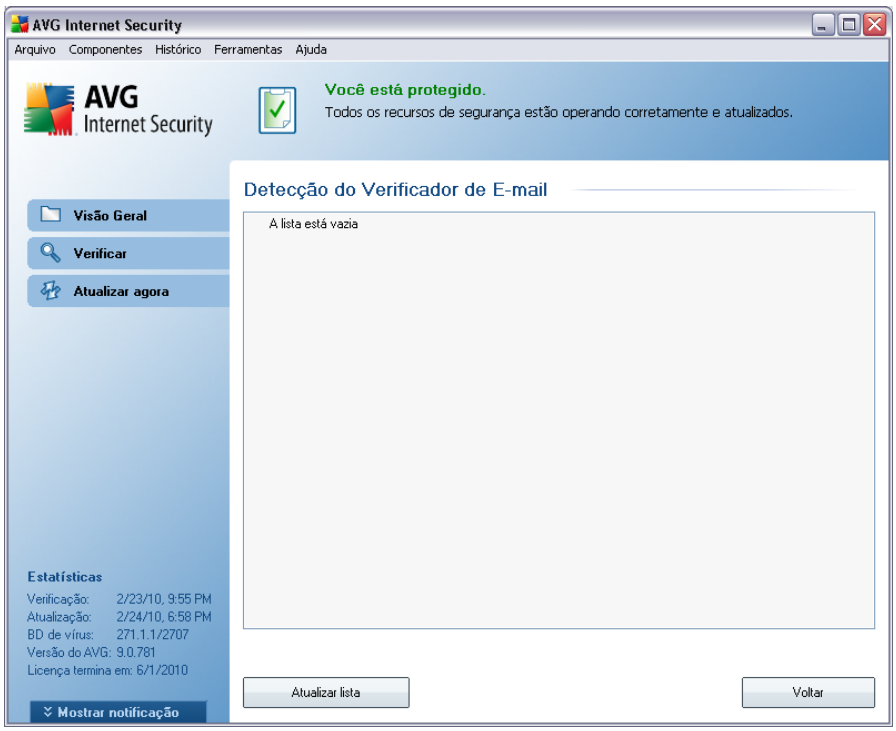
Nota: *o fornecedor do software configurou todos os componentes do AVG para proporcionar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema****Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

Botões de controle

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

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione esse botão para voltar para a interface do usuário do AVG padrão (visão geral dos componentes).

8.5.3. Detecção de Verificador de E-mail



Na caixa de diálogo ***Detecção do verificador de e-mail*** (*acessível através da opção do menu do sistema Detecção de histórico/verificador de e-mail*), será possível ver uma lista de todas as detecções do componente ***Verificador de e-mail*** . Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção*** - descrição (possivelmente até o nome) do objeto detectado
- ***Objeto*** - localização do objeto
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que o objeto suspeito foi detectado

- ***Tipo de Objeto*** - tipo de objeto detectado

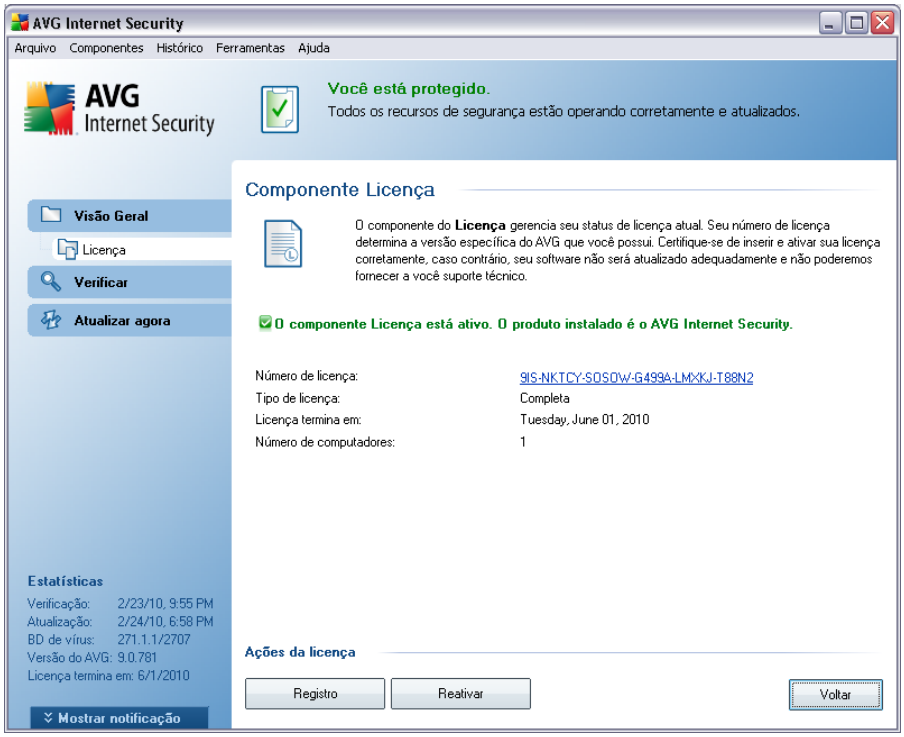
Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir todas as entradas de objetos detectados (***Lista vazia***).

Botões de controle

Os botões de controle disponíveis na interface de ***Detecção do verificador de e-mail*** são os seguintes:

- ***Atualizar listas*** - atualiza a lista de ameaças detectadas
- ***Voltar*** - leva você de volta à ***interface do usuário do AVG*** padrão (visão geral dos componentes)

8.6. Licença



Na caixa de diálogo do componente ***Licença*** , você encontrará um texto curto descrevendo a funcionalidade do componente, informações sobre seu status atual (*componente Licença está ativo.*) e as seguintes informações:

- ***Número da licença*** - fornece a forma exata do número de licença. Ao digitar o número da licença, você deve ser totalmente preciso e inseri-lo como mostrado. Portanto, convém sempre usar o método "copiar e colar" para qualquer manipulação com o número da licença.
- ***Tipo de licença*** - especifica o tipo de produto instalado.
- ***Vencimento da licença*** - essa data determina o período de validade da licença. Se quiser continuar usando o **AVG 9 Anti-Virus plus Firewall** depois dessa data, terá que renovar a licença. A renovação da licença pode ser realizada online, no site da AVG (site da).
- ***Número de computadores*** - a quantidade de estações de trabalho em que você tem permissão para instalar o **AVG 9 Anti-Virus plus Firewall**.

Botões de controle

- ***Registre-se*** - estabelece uma conexão com a página de registro do site da AVG (http://www.avgbrasil.com.br). Informe os dados de registro; somente os clientes que registrarem seus produtos AVG poderão receber suporte técnico gratuito.
- ***Reativar*** - abre a caixa de diálogo ***Ativar AVG*** com os dados inseridos na caixa de diálogo ***Personalizar AVG*** do processo de instalação. Nessa caixa de diálogo é possível inserir o número da licença para substituir o número de vendas (*o número com o qual você instalou o AVG*) ou para substituir o número antigo da licença (*por exemplo, durante a atualização de um novo produto AVG*).

Observação: Se estiver utilizando a versão do *AVG 9 Anti-Virus plus Firewall*, **os botões aparecem como** *Comprar agora* **e** *Ativar, permitindo que você compre a versão completa do programa imediatamente. Para* **AVG 9 Anti-Virus plus Firewall** *instalado com um número de vendas, os botões são exibidos como* ***Registrar*** *e* ***Ativar****.*

- ***Voltar*** - pressione esse botão para voltar para a interface do usuário do AVG padrão (visão geral dos componentes).

8.7. Link Scanner

8.7.1. Princípios do Link Scanner

O componente ***LinkScanner*** oferece proteção contra sites, que são designados para instalar malware em seu computador através de plugins ou do navegador da Web. A tecnologia do ***LinkScanner*** consiste em dois recursos, o ***AVG Search-Shield*** e o ***AVG Active Surf-Shield***:

- ***O AVG Search Shield***contém uma lista de sites (*endereços de URL*) que são conhecidos por serem perigosos. Ao pesquisar no Google, Yahoo!, Bing, Altavista, Yandex ou Baidu, todos os resultados da pesquisa são verificadas de acordo com esta lista e é mostrado um ícone de veredicto (*para resultados de pesquisa do Yahoo! apenas ícones de veredictos "site explorado" são mostrados*). Além disso, se você inserir algum endereço diretamente no navegador, clique em um link em qualquer site ou, por exemplo, em seu e-mail e isso é verificado automaticamente e bloqueado, se necessário.

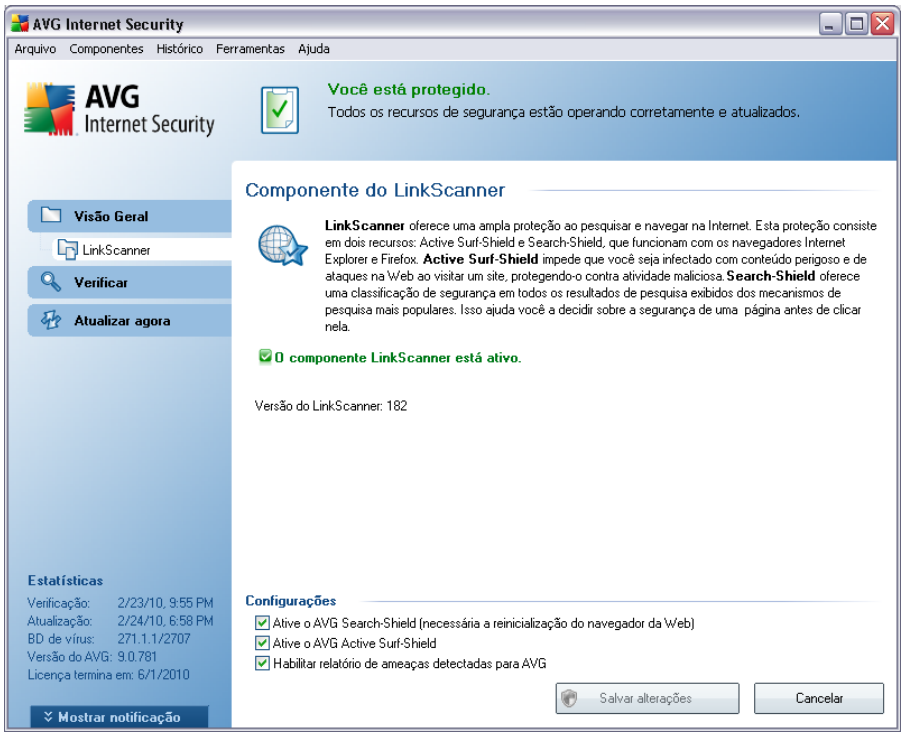
- ***O AVG Active Surf-Shield*** verifica o conteúdo dos sites que você estiver visitando, independente do endereço deles. Mesmo que algum site não seja detectado pelo ***AVG Search Shield*** (*por exemplo, quando um novo site mal-intencionado é criado ou quando um site limpo agora contém algum malware*), ele será detectado e bloqueado pelo ***AVG Active Surf-Shield*** quando você tentar visitá-lo.

***Observação: o** AVG Link Scanner não se destina a plataformas de servidores!*

8.7.2. Interface do Link Scanner

O componente ***LinkScanner*** é composto por duas partes que podem ser ativadas e desativadas na interface do ***componente LinkScanner***:

A interface do componente ***LinkScanner***fornece uma breve descrição da funcionalidade do componente, bem como informações sobre o seu status atual (*O componente LinkScanner está ativo.*). Além disso, você pode encontrar informações sobre o número de versão mais recente do banco de dados do ***LinkScanner*** (|*Versão do LinkScanner*).



Na parte inferior da caixa de diálogo, é possível editar várias opções:

- ***Ativar o AVG Search-Shield*** - (*ativado por padrão*): ícones de notificação de aviso em pesquisas realizadas no Google, Yahoo, Bing, Yandex, Altavista ou Baidu com verificação antecipada do conteúdo de sites retornado pelo mecanismo de pesquisa.

- ***Ativar AVG Active Surf-Shield*** - (*ativo por padrão*): proteção ativa (*em tempo real*) contra sites exploradores à medida que são acessados. As conexões conhecidas com sites maliciosos e seu conteúdo exploratório são bloqueadas à medida que são acessados por meio de um navegador da Web *ou outro aplicativo que utilize HTTP*).

- ***Ativar relatórios de ameaças detectadas para a AVG*** - marque esse item para permitir relatórios de explorações e sites mal-intencionados descobertos pelos usuários por meio do ***Safe Surf*** ou do ***Safe Search*** para alimentar o banco de dados que coleta informações sobre atividades mal-intencionadas na Web.

8.7.3. AVG Search-Shield

Ao pesquisar na Internet com o ***AVG Search-Shield*** ativado, todos os resultados retornados dos mecanismos de pesquisa mais conhecidos, como Yahoo!, Google, Bing, Altavista, Yandex etc. serão avaliados quanto a links perigosos ou suspeitos. Ao verificar esses links e marcar os perigosos, o ***AVG Link Scanner*** indicará o problema antes de você clicar em links suspeitos ou perigosos, portanto você poderá ter certeza de que acessará apenas sites seguros.

Quando um link estiver sendo avaliado na página de resultados da pesquisa, você verá um sinal gráfico próximo ao link informando que a verificação do link está em andamento. Quando a avaliação estiver terminada, o respectivo ícone informativo será exibido:

A página do link é segura (*com o mecanismo de pesquisa do Yahoo! no Barra de Ferramentas de Segurança do AVG, esse ícone não será exibido!*).

A página do link não contém ameaças, mas é suspeita (*de origem ou intenção duvidosa, portanto, não é recomendada para compras online etc.*).

A página de link pode ser segura, mas contém outros links para páginas definitivamente perigosas, ou de código suspeito, embora não esteja diretamente empregando uma ameaça no momento.

A página de link contém ameaças ativas! Para sua própria segurança, você não poderá visitar esta página.

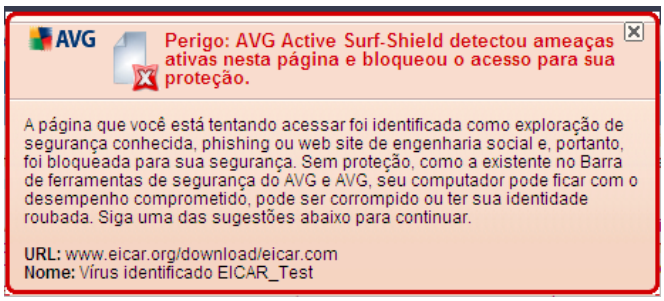
A página do link não está acessível e não pôde ser verificada.

Passar o mouse sobre um ícone de classificação individual exibirá detalhes sobre o link específico em questão. Informações incluem detalhes adicionais da ameaça (se houver), o endereço IP do link e quando a página foi verificada pelo AVG:

8.7.4. AVG Active Surf-Shield

Essa poderosa proteção bloqueará o conteúdo mal-intencionado de qualquer página da Web que você tente abrir e impedirá que seja baixada para o seu computador. Com esse recurso ativado, clicar em um link ou digitar uma URL para um site perigoso bloqueará automaticamente a abertura da página da Web, protegendo-o inadvertidamente contra infecção. É importante lembrar que as páginas da Web exploradas podem infectar seu computador simplesmente com uma visita ao site afetado; por isso, quando você solicitar uma página da Web perigosa contendo explorações ou outras ameaças sérias, o ***AVG Link Scanner*** não permitirá que seu navegador a exiba.

Se você encontrar um site malicioso em seu navegador da Web, o ***AVG LinkScanner*** emitirá um aviso com uma tela semelhante a esta:



A inserção de um site da Web como este é altamente de risco e, portanto, não é recomendada!

8.8. Proteção On-line

8.8.1. Princípios da Proteção On-line

A Proteção Onlineé um tipo de proteção residente em tempo real. Ela verifica o conteúdo de paginas da Web visitadas (e possíveis arquivos incluídos nelas) mesmo antes destas serem exibidas no navegador da Web ou baixadas no computador.

A Proteção Online detecta que a página que você está prestes a visitar inclui um javascript perigoso e impede a exibição da pagina. Além disso, ela reconhece malware contido em uma página e interrompe seu download imediatamente, para que nunca entre no seu computador.

Observação: o *Proteção Online AVG não se destina a plataformas de servidores!*

8.8.2. Interface da Proteção On-line

A interface do componente Proteção Online descreve o comportamento desse tipo de proteção. Você pode encontrar mais informações no status atual do componente (o *Proteção Online está ativa e funcionando perfeitamente.*). Na parte inferior da caixa de diálogo, você encontrará as opções de edição básicas da funcionalidade desse componente.

Configuração básica do componente

Em primeiro lugar, você tem a opção de ativar/desativar a Proteção Online marcando o item ***Habilitar a Proteção Online***. Esta opção fica ativada por padrão e o componente ***Proteção Online*** fica ativo. Entretanto, se você não tiver um bom motivo para alterar essas configurações, é recomendável manter o componente ativo. Se o item estiver marcado e a ***Proteção Online*** estiver em execução, mais opções de configuração estarão disponíveis e poderão ser editadas em duas guias:

- ***Web*** - você pode editar a configuração do componente referente à verificação do conteúdo do site da Web. A interface de edição permite configurar as seguintes opções elementares:

- ***Proteção Web*** - esta opção confirma que a ***Proteção Online*** deve realizar a verificação do conteúdo das páginas www. Desde que essa opção esteja ativada (*por padrão*), você pode ativar/desativar estes itens:

  - ***Verificar arquivos*** - verifique o conteúdo dos arquivos possivelmente incluídos na página www a ser exibida

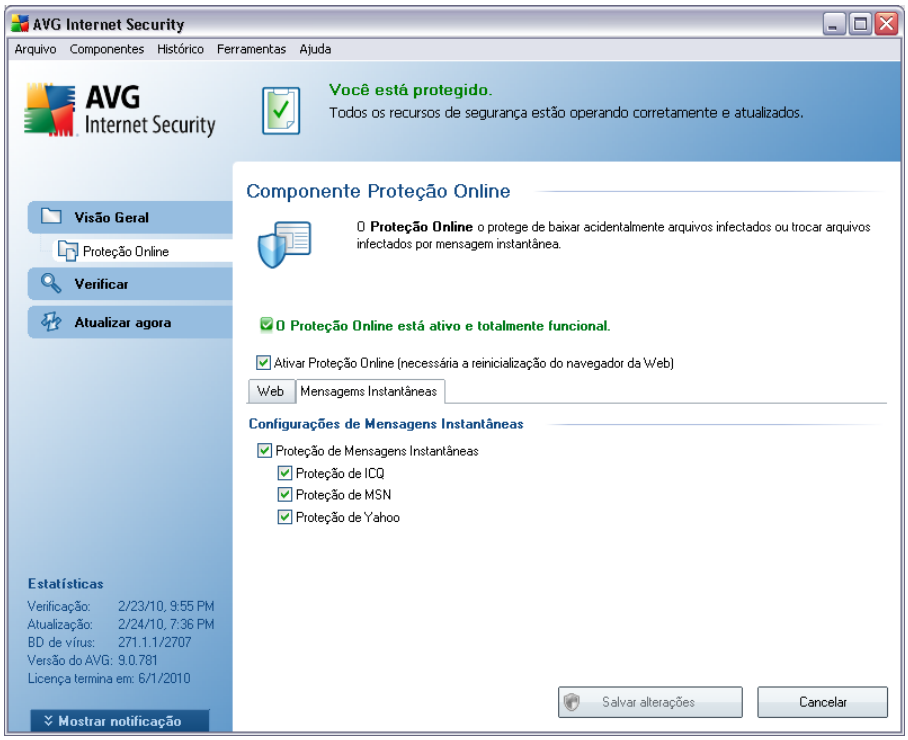
  - ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador

  - ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

  - ***Usar análise heurística*** - verifique o conteúdo da página a ser exibida usando o método de análise heurística (emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual. Dessa forma, pode detectar até mesmo códigos mal-intencionados ainda não descritos no banco de dados de vírus). (consulte os Princípios do Anti-Vírus***

  - ***Tamanho máximo do arquivo verificado*** - se os arquivos incluídos estiverem presentes na página exibida, você poderá verificar também seu conteúdo, mesmo antes de eles serem baixados no computador. Entretanto, a verificação de arquivos grandes pode levar tempo e o download da página da Web pode ficar significativamente mais lento. Use a barra deslizante para especificar o tamanho máximo de um arquivo que ainda será verificado com a ***Proteção Online***. Mesmo que o arquivo baixado seja maior que o especificado e, desse modo, não seja verificado com a ***Proteção Online***, ainda assim você estará protegido; caso o arquivo esteja infectado, a ***Proteção Residente*** detectará isso imediatamente.

- ***Mensagem Instantânea*** - permite editar as configurações de componente referentes à verificação de mensagens instantâneas (*por exemplo, ICQ, MSN Messenger, Yahoo ...*).



  - Proteção de Mensagens Instantâneas - marque este item se quiser que a Proteção Online verifique se a comunicação on-line está livre de vírus. Desde que esta opção esteja ativa, será possível especificar melhor qual aplicativo de mensagens instantâneas você deseja controlar - atualmente, **AVG 9 Anti-Virus plus Firewall** é compatível com os aplicativos ICQ, MSN e Yahoo.

Nota: o *fornecedor do software configurou todos os componentes do AVG para propiciar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema****Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

Botões de controle

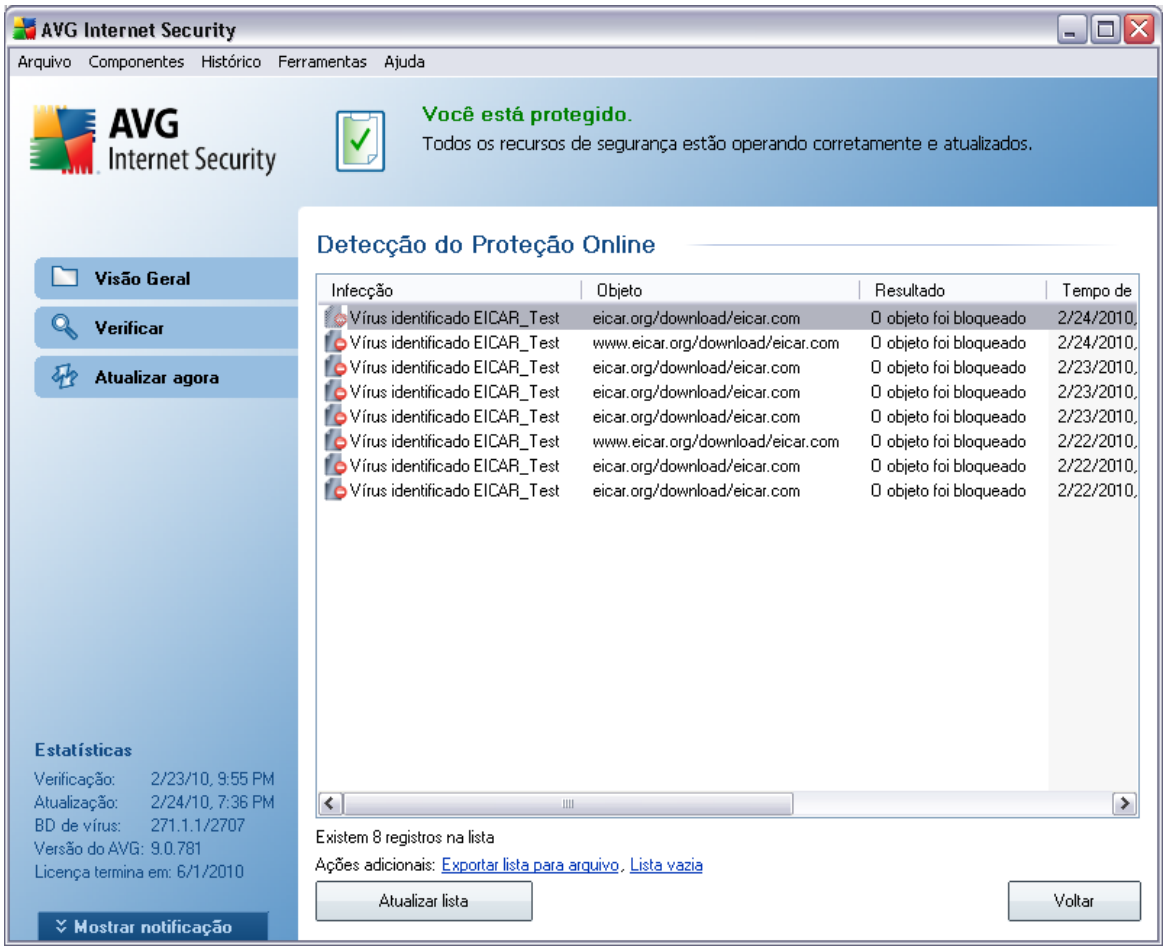
Estes são os botões de controle disponíveis na interface da ***Proteção Online***:

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione este botão para retornar à interface do usuário do AVG padrão (*visão geral dos componentes*)

8.8.3. Detecção da Proteção On-line

A Proteção Online verifica o conteúdo de páginas da Web visitadas e possíveis arquivos incluídos nelas mesmo antes de elas serem exibidas no navegador da Web ou baixadas para o seu computador. Se uma ameaça for detectada, você será alertado imediatamente pela seguinte caixa de diálogo:

A página da Web suspeita não será aberta, e a detecção da ameaça será registrada na lista de ***Detecções da Proteção Online*** - essa visão geral de ameaças detectadas está acessível no menu do sistema ***Histórico/detecções da Proteção Online***.



Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção***- descrição (*possivelmente até o nome*) do objeto detectado
- ***Objeto*** - origem do objeto (*página da Web*)
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que a ameaça foi detectada e bloqueada
- ***Tipo de Objeto*** - tipo de objeto detectado
- ***Processo*** - qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir todas as entradas de objetos detectados (***Lista vazia***). O botão ***Atualizar lista*** atualizará a lista de detecções feitas pela ***Proteção Online***. O botão ***Voltar*** leva você de volta à ***interface do usuário do AVG padrão*** (visão geral dos componentes).

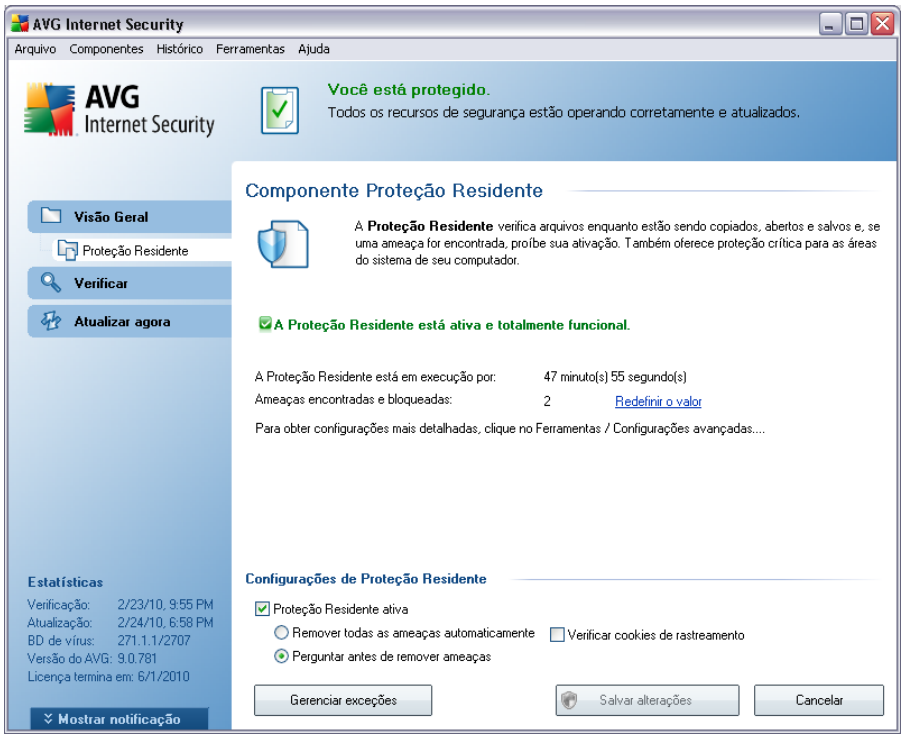
8.9. Proteção Residente

8.9.1. Princípios da Proteção Residente

O componente ***Proteção Residente*** oferece proteção contínua a seu computador.Ele verifica todos os arquivos que estão sendo abertos, salvos ou copiados e protege as áreas de sistema do computador. Quando a ***Proteção Residente*** descobre um vírus em um arquivo acessado, ela pára as operações em execução no momento e não permite que o vírus seja ativado. Normalmente, você sequer nota o processo, pois ele acontece "em segundo plano", e você só é notificado quando são encontradas ameaças; ao mesmo tempo, a ***Proteção Residente*** evita que as ameaças sejam ativadas e as remove. A ***Proteção Residente*** está sendo carregada na memória do computador durante a inicialização.

Aviso: a Proteção Residente é carregada na memória do computador durante a inicialização e é vital que você a mantenha ativada todo o tempo!

8.9.2. Interface da Proteção Residente



Além de uma visão geral dos dados estatísticos mais importantes e informações sobre o status atual do componente (a *Proteção Residente está ativa e funcionando perfeitamente*), a interface da ***Proteção Residente*** oferece também algumas opções de configurações de componente básicas. Estas são as estatísticas:

- ***A Proteção Residente esteve ativa em*** - fornece a hora desde a última inicialização do componente
- ***Ameaças detectadas e bloqueadas*** - número de infecções detectadas e impedidas de serem executadas/abertas ((*se necessário, este valor pode ser redefinido, por exemplo, para fins estatísticos - Redefinir valor*)

Configuração básica do componente

Na parte inferior da caixa de diálogo, você encontrará a seção chamada ***Configurações da Proteção Residente***, na qual é possível editar algumas configurações básicas da funcionalidade do componente *a configuração detalhada, como nos demais componentes, está disponível por meio do item Ferramentas/*

Configurações Avançadas do menu do sistema).

A opção ***Proteção Residente está ativa*** permite ativar/desativar facilmente a proteção residente. Por padrão, a função está ativa. Com a proteção residente ativa, é possível decidir como as infecções possivelmente detectadas devem ser tratadas (removidas):

- automaticamente (***Remover todas as ameaças automaticamente***)
- ou somente após a aprovação do usuário (***Perguntar antes de remover ameaças***)

Esta opção não afeta o nível de segurança e se reflete apenas em suas preferências.

Nos dois casos, você ainda pode selecionar se deseja ***Verificar cookies de rastreamento***. Em casos específicos, você pode ativar esta opção para obter níveis de segurança máximos, mas ela fica desativada por padrão. (*cookies = parcelas de texto enviadas por um servidor a um navegador da Web e em seguida enviadas de volta inalteradas pelo navegador sempre que ele acessa esse servidor. Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas*).

Nota: o *fornecedor do software configurou todos os componentes do AVG para propiciar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema****Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

Botões de controle

Estes são os botões de controle disponíveis na interface da ***Proteção Residente***:

- ***Gerenciar exceções*** abre a caixa de diálogo ***Proteção Residente - Exclusões de Diretórios*** em que é possível definir as pastas que devem ser excluídas da verificação do ***Proteção Residente***
- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione esse botão para voltar para a ***interface do usuário do AVG*** padrão (visão geral dos componentes).

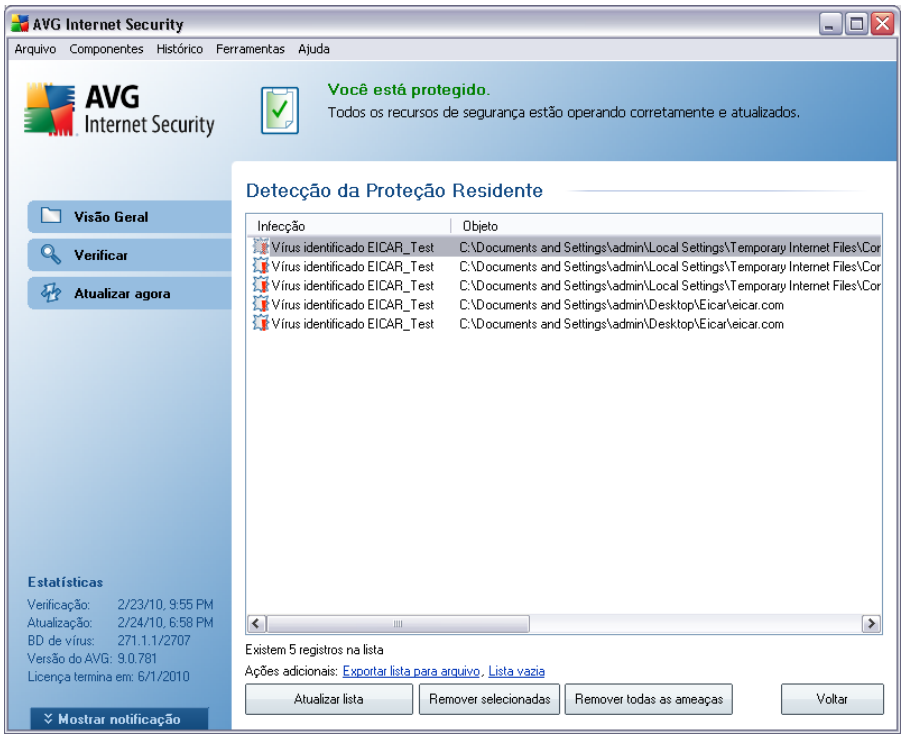
8.9.3. Detecção da Proteção Residente

A Proteção Residente verifica os arquivos à medida que são copiados, abertos ou salvos. Quando um vírus ou qualquer tipo de ameaça é detectado, você será alertado imediatamente por meio da seguinte caixa de diálogo:

A caixa de diálogo fornece informações sobre a ameaça detectada e pede que você decida que ação deverá ser tomada:

- ***Recuperar*** - se uma solução estiver disponível, o AVG irá curar o arquivo infectado automaticamente; esta é a ação recomendada
- ***Mover para Quarentena*** - o vírus será movido para a ***Quarentena de Vírus do AVG***
- ***Ir para o arquivo*** - essa opção redireciona o usuário ao local exato do objeto suspeito (*abre a nova janela do Windows Explorer*)
- ***Ignorar*** - NÃO recomendamos o uso desta opção, a não ser que exista um bom motivo!

A visão geral completa de todas as ameaças detectadas pela ***Proteção Residente*** está disponível na caixa de diálogo ***Detecção da Proteção Residente***, acessível por meio da opção de menu do sistema ***Histórico/descobertas da Proteção Residente***:



A ***detecção da Proteção Residente*** oferece uma visão geral dos objetos detectados pela ***Proteção Residente***, avaliados como perigosos e recuperados ou movidos para a ***Quarentena de Vírus***. Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção*** - descrição (possivelmente até o nome) do objeto detectado
- ***Objeto*** - localização do objeto
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que o objeto foi detectado
- ***Tipo de Objeto*** - tipo de objeto detectado
- ***Processo*** - qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir

todas as entradas de objetos detectados (***Lista vazia***). O botão ***Atualizar lista*** atualizará a lista de detecções feitas pela ***Proteção Residente***. O botão ***Voltar*** leva você de volta à ***interface do usuário do AVG padrão*** (visão geral dos componentes).

8.10. Gerenciador de Atualizações

8.10.1. Princípios do Gerenciador de Atualizações

Nenhum software de segurança pode garantir proteção real de vários tipos de ameaças se não for regularmente atualizado! Os criadores de vírus estão sempre em busca de novas brechas que possam explorar em softwares e sistemas operacionais. Novos vírus, novos malwares, novos ataques de hackers surgem diariamente. Por esse motivo, os fornecedores de software estão continuamente emitindo atualizações e patches de segurança para corrigir qualquer brecha de segurança que seja descoberta.

É fundamental atualizar o AVG regularmente!

O ***Gerenciador de Atualizações*** o ajuda a controlar a atualização regularmente. Nesse componente você pode programar downloads automáticos de arquivos de atualização da Internet ou da rede local. As atualizações das definições de vírus essenciais devem ser feitas diariamente, se possível. Atualizações de programas menos urgentes podem ser feitas semanalmente.

Nota: *consulte o capítulo Atualizações do AVG para obter mais informações sobre os tipos e níveis de atualização.*

8.10.2. Interface do Gerenciador de Atualizações

A interface do ***Gerenciador de Atualizações*** exibe informações sobre a funcionalidade do componente e seu status atual (*Gerenciador de atualização está ativo.*) e fornece os dados estatísticos relevantes:

- ***Atualização mais recente*** - especifica quando e a que horas o banco de dados foi atualizado
- ***Versão do banco de dados de vírus*** - define o número da versão mais recente do banco de dados. Esse número aumenta a cada atualização da base de vírus
- ***Próxima atualização programada*** - especifica quando e em que horário o banco de dados está programado para uma nova atualização

Configuração básica do componente

Na parte inferior da caixa de diálogo, você encontrará a seção ***Configurações do Gerenciador de Atualizações*** , onde é possível realizar algumas alterações nas regras

de inicialização do processo de atualização. Você pode definir se deseja que os arquivos de atualização sejam baixados automaticamente (***Iniciar atualizações automáticas***) ou apenas sob demanda. Por padrão, a opção ***Iniciar atualizações automáticas*** é ativada e recomendamos mantê-la dessa forma. O download regular dos arquivos de atualização mais recentes é crucial para a funcionalidade adequada de um sotware de segurança.

Além disso, você pode definir quando a atualização será iniciada:

- ***Periodicamente*** - define o intervalo de tempo
- ***Em uma data específica*** - define o dia e a hora exatos

Por padrão, a atualização é definida para a cada 4 horas. É altamente recomendável manter essa configuração, a menos que você tenha um motivo real para alterá-la.

Nota: *o fornecedor do software configurou todos os componentes do AVG para propiciar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema* ***Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

Botões de controle

Os botões de controle disponíveis na interface do ***Gerenciador de Atualizações*** são os seguintes:

- ***Atualizar agora*** - inicializa uma atualização imediata sob demanda.
- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione esse botão para voltar para a ***interface do usuário do AVG*** padrão (visão geral dos componentes).

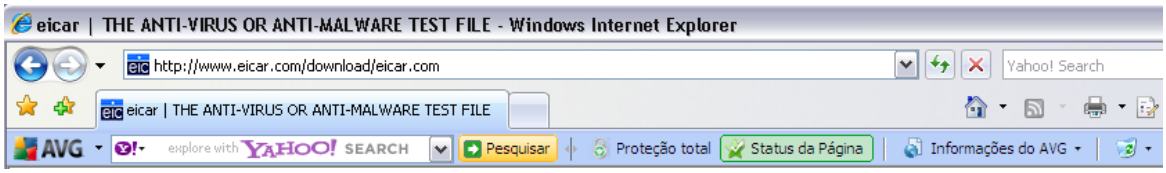
9. Barra de Ferramentas de Segurança do AVG

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

Se você optar por instalar a barra de ferramentas durante a instalação do **AVG 9 Anti-Virus plus Firewall, ela será adicionada ao navegador da Web automaticamente.** Se você estiver usando um navegador da Internet alternativo (por exemplo, o Avant Browser), poderá perceber um comportamento inesperado.

9.1. Barra de Ferramentas de Segurança do AVG Interface

A ***Barra de Ferramentas de Segurança do AVG*** foi desenvolvida para funcionar com o ***MS Internet Explorer*** (*versão 6.0 ou posterior*) e o ***Mozilla Firefox*** (*versão 2.0 ou posterior*). Quando você decidir que deseja instalar a ***Barra de Ferramentas de Segurança do AVG*** *(durante o processo de instalação do AVG, será necessário decidir se deseja ou não instalar o componente*), o componente estará localizado no navegador da Web, abaixo da barra de endereços:



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

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

- ***Logotipo AVG*** - oferece acesso a itens gerais da barra de ferramentas. Clique no botão do logotipo para ser redirecionado ao site do AVG (http://www.avgbrasil.com.br). Clicar no ponteiro ao lado do ícone do AVG abrirá o seguinte:
    - ***Informações da barra de ferramentas*** - link para a página inicial do ***Barra de Ferramentas de Segurança do AVG que contém informações detalhadas sobre a proteção da barra de ferramentas***
    - ***Iniciar AVG 9 Anti-Virus plus Firewall*** - abre a interface de usuário do **AVG 9 Anti-Virus plus Firewall**

- ***Opções*** - abre uma caixa de diálogo de configuração na qual você pode ajustar as configurações do ***AVG Security Toolbar*** para que elas atendam às suas necessidades - consulte o capítulo ***Opções da Barra de Ferramentas de Segurança AVG***

- ***Excluir histórico*** - permite *Excluir o histórico completo* da Barra de Ferramentas de Segurança AVG ou *Excluir o histórico de pesquisa, Excluir o histórico do navegador, Excluir o histórico baixado*e *Excluir cookies*.

- ***Atualizar*** - verifica se há novas atualizações para a ***Barra de Ferramentas de Segurança do AVG***

- ***Ajuda*** - oferece opções para abrir o arquivo de ajuda, enviar feedback do produto, ou exibir detalhes da versão atual da barra de ferramentas

- ***Caixa de pesquisa*** - Insira uma palavra ou frase na caixa de pesquisa. Pressione ***Pesquisar*** para iniciar a pesquisa usando o mecanismo de pesquisa especificado (*você pode especificar o mecanismo de pesquisa desejado a ser usado nas Opções avançadas da Barra de Ferramentas de Segurança do AVG, e pode escolher entre Yahoo!, Wikipedia, Baidu, WebHledani ou Yandex*sem importar qual página é exibida no momento. A caixa de pesquisa também lista o histórico de pesquisa. As pesquisas feitas com a caixa de pesquisa são analisadas usando a proteção ***AVG Search-Shield***.

- ***Proteção total*** - este botão aparece de modo opcional como ***Proteção total*** / ***Proteção limitada*** / ***Sem proteção*** dependendo da **AVG 9 Anti-Virus plus Firewall**configuração

- ***Status da Página*** - diretamente na barra de ferramentas, este botão exibe a avaliação da página da Web carregada no momento, com base nos critérios do componente ***AVG Search-Shield*** ((*A página é segura / suspeita / positivamente perigosa / contém ameaças / não pode ser verificada* Clique no botão para abrir um painel de informações com dados detalhados na página da Web especificada.

- ***AVG Info*** - oferece links para importantes informações de segurança localizadas no site do AVG (http://www.avgbrasil.com.br).

    - ***Informações da barra de ferramentas*** - link para a página inicial da ***Barra de Ferramentas de Segurança do AVG que contém informações detalhadas sobre a proteção da barra de ferramentas***

    - ***Sobre ameaças***- abre a página da Web do AVG fornecendo informações sobre ameaças e vírus atuais na Internet

- ***Notícias do AVG*** - abre a página da Web que fornece as publicações mais recentes relacionadas ao AVG
- ***Nível atual de ameaças*** - abre a página da Web do AVG Virus Lab, com uma exibição gráfica do nível atual de ameaças na Web
- ***Enciclopédia de vírus*** - abre a página da Enciclopédia de vírus, onde é possível pesquisar vírus específicos por nome e obter informações detalhadas sobre cada um

9.2. Opções da Barra de Ferramentas de Segurança do AVG

Todos os parâmetros de configuração da ***Barra de Ferramentas de Segurança AVG*** podem ser acessados diretamente do painel ***Barra de Ferramentas de Segurança AVG***. A interface de edição é aberta por meio do item de menu da barra de ferramentas *AVG / Opções* em uma nova caixa de diálogo denominada ***Opções da barra de ferramentas***, dividida em quatro seções:

9.2.1. Guia Geral

Nesta guia você pode especificar botões que devem ser exibidos/ocultos no painel ***Barra de Ferramentas de Segurança do AVG.*** Marque qualquer opção no caso de você querer que o respectivo botão seja exibido. A outra busca descreve a funcionalidade de cada um dos botões da barra de ferramentas:

- ***Botão Notícias do AVG*** - o botão abre a página da Web que fornece as publicações mais recentes relacionadas ao AVG
- ***Botão Notícias*** - o botão fornece uma visão geral estruturada das notícias atuais através da imprensa diária
- ***Botão AVG Info*** - o botão oferece informações na barra de ferramentas do AVG, sobre as ameaças atuais e o nível de ameaça na internet, abre a enciclopédia de vírus e fornece mais notícias relacionadas aos produtos do AVG
- ***Botão Excluir histórico*** - esse botão permite Excluir o histórico inteiro ou Excluir o histórico de pesquisas, Excluir o histórico do navegador, Excluir o histórico de downloads ou Excluir cookies diretamente do painel AVG Security Toolbar.

9.2.2. Guia Botões úteis

A guia***Botões úteis*** permite selecionar aplicativos a partir de uma lista e ter seus ícones exibidos na interface da barra de ferramentas. Um ícone serve como um link rápido que permite ativar o respectivo aplicativo imediatamente.

9.2.3. Guia Segurança

A guia ***Segurança*** está dividida em duas seções, ***AVG Browser Security*** e ***Classificações***, onde é possível marcar caixas de seleção específicas para atribuir a funcionalidade da ***Barra de Ferramentas de Segurança AVG*** que você deseja usar:

- ***AVG Browser Security*** - marque esse item para ativar ou desativar os serviços ***AVG Search-Shield*** e/ou ***AVG Active Surf-Shield***
- ***Classificações*** - selecione símbolos gráficos usados para classificações de resultados de pesquisa por parte do componente ***AVG Search-Shield*** que você deseja usar:
  - a página é segura
  - a página é um tanto suspeita
  - a página contém links para páginas positivamente perigosas
  - a página contém ameaças ativas
  - a página não está acessível e, portanto, não pôde ser verificada

Marque a respectiva opção para confirmar que você deseja ser informado sobre esse nível de ameaça específico. No entanto, a exibição da marca vermelha atribuída a páginas que contêm ameaças ativas e perigosas não pode ser desativada. ***Mais uma vez, recomenda-se manter a configuração padrão definida pelo fornecedor do programa, a não ser que você tenha um motivo concreto para alterá-la.***

9.2.4. Guia Opções avançadas

Na guia ***Opções avançadas*** selecione primeiro qual o mecanismo de pesquisa você deseja usar como padrão. Você tem que escolher entre *Yahoo!, Baidu, WebHledani*, e *Yandex*. Tendo alterado o mecanismo de busca padrão, reinicie o seu navegador de internet para que as alterações tenham efeito.

Posteriormente, você pode ativar ou desativar outras configurações da ***Barra de Ferramentas de Segurança do AVG***:

- ***Definir e manter o Yahoo! como provedor de pesquisa para a barra de Endereço*** - (*ativada por padrão*) - se essa opção for marcada, você poderá digitar diretamente uma palavra-chave de pesquisa na barra de endereço do seu navegador da Internet, e o serviço Yahoo! será usado automaticamente para procurar sites relevantes.

- ***Deixar que o AVG faça sugestões no caso de erros de navegação do***

navegador (404/DNS) - (*ativada por padrão*) - ao pesquisar na Web, se acabar acessando uma página inexistente, ou uma página que não pode ser exibida (erro 404), você será redirecionado automaticamente a uma página da Web que permite selecionar a partir de uma visão geral de páginas alternativas relacionadas ao tópico.

- ***Definir e manter o Yahoo! como provedor de pesquisa para o navegador*** - (*desativada por padrão*) - o Yahoo! é o mecanismo de pesquisa na Web padrão no AVG Security Toolbar e, ao ativar essa opção, ele também poderá se tornar o mecanismo de pesquisa padrão do seu navegador.

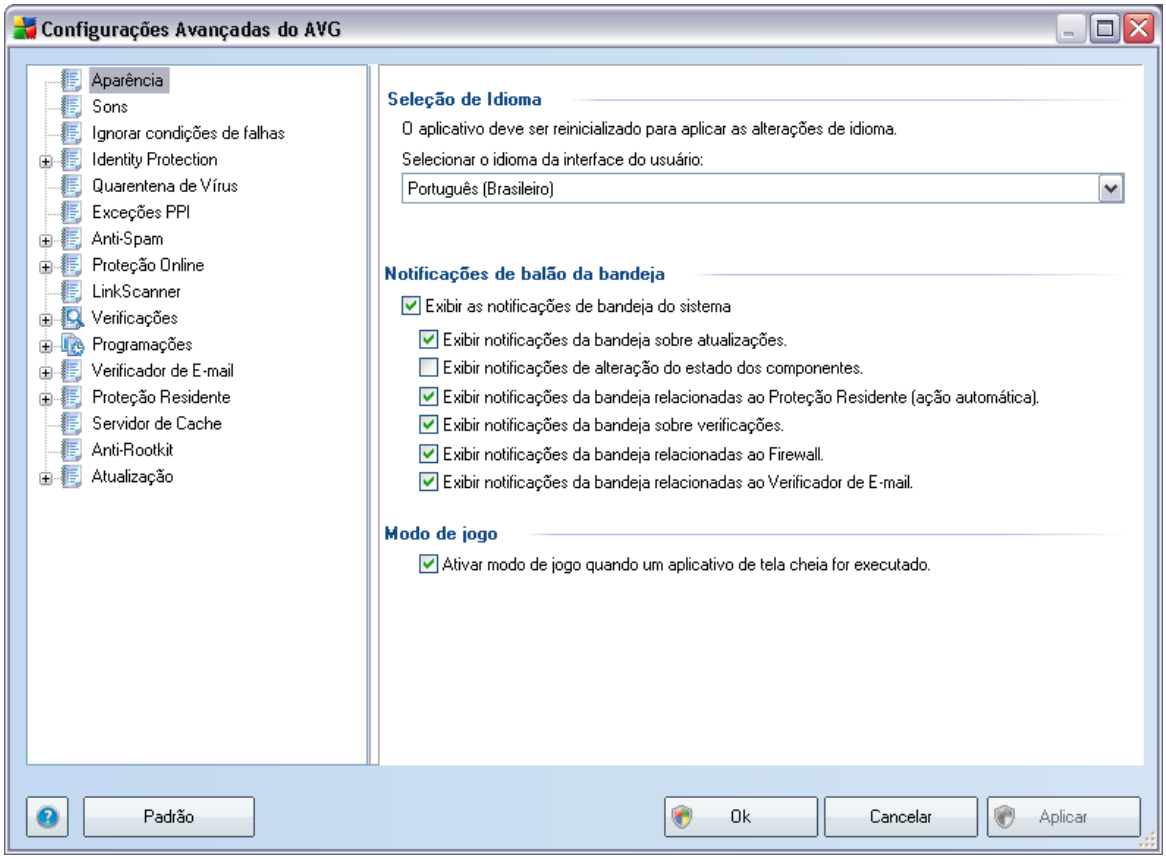
- ***Exibir novamente a Barra de Ferramentas de Segurança AVG quando oculta (semanalmente)*** - (*ativada por padrão*) - essa opção permanece ativada por padrão e, quando o ***Barra de Ferramentas de Segurança AVG*** ficar oculta acidentalmente, ela será exibida novamente em até uma semana.

10. Configurações Avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG 9 Anti-Virus plus Firewall** é aberta em uma nova janela denominada ***Configurações Avançadas do AVG***. A janela é dividida em duas seções: a parte da esquerda oferece uma navegação organizada em árvore para as opções de configuração do programa. Selecione o componente do qual deseja alterar a configuração do (*ou sua parte específica*) para abrir a caixa de edição na seção à direita da janela.

10.1. Aparência

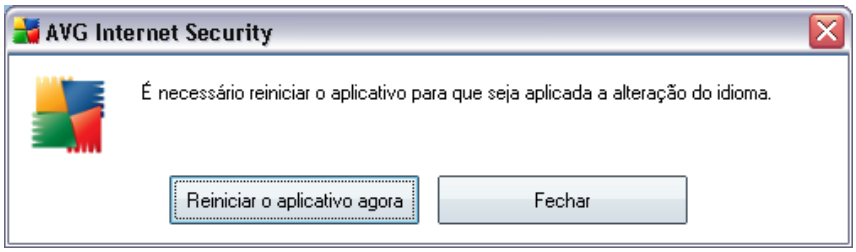
O primeiro item na árvore de navegação, ***Aparência***, refere-se às configurações gerais dainterface de usuário do AVG e algumas opções elementares do comportamento do aplicativo:



Seleção de Idioma

Na seção ***Seleção de Idioma*** você pode escolher o idioma desejado no menu suspenso; o idioma será usado em toda a interface de usuário do AVG. O menu suspenso só oferece os idiomas selecionados anteriormente para serem usados durante o processo de instalação (consulte o capítulo Instalação Personalizada - Seleção do Componente). Entretanto, para concluir a alteração do aplicativo para outro idioma, é necessário reiniciar a interface do usuário. Siga estas etapas:

- Selecione o idioma desejado para o aplicativo e confirme a seleção pressionando o botão ***Aplicar*** (canto inferior direito)
- Pressione o botão ***OK*** para confirmar
- É exibida uma nova janela de diálogo pop-up informando que a alteração de idioma da interface do usuário do AVG exige a reinicialização do aplicativo:



Notificações de balão da bandeja

Nesta seção, você poderá suprimir a exibição das notificações do balão da bandeja no status do aplicativo. Por padrão, as notificações do balão podem ser exibidas e é recomendável manter essa configuração. As notificações do balão geralmente informam sobre alguma alteração de status do componente do AVG e você deve ter atenção a elas.

Entretanto, se por alguma razão você decidir que não deseja que essas notificações sejam exibidas ou se desejar a exibição de apenas algumas notificações (relacionadas a um componente do AVG específico), poderá definir e especificar suas preferências selecionando/cancelando a seleção das seguintes opções:

- ***Exibir notificações da bandeja do sistema*** - por padrão, este item é selecionado (*como ativado*) e as notificações são exibidas. Desmarque esse item para desativar completamente a exibição de todas as notificações do balão. Quanto ativado, é possível selecionar quais notificações específicas devem ser exibidas:
    - ***Exibir notificações na bandeja sobre atualizações*** - decida se as

informações relativas ao início, andamento ou finalização do processo do de atualização do AVG devem ser exibidas;

- ***Exibir notificações de mudança de estado de componentes*** - decidir se informações relativas à atividade/inatividade de componentes ou seu possível problema devem ser exibidas. Ao relatar o status de falha de um componente, esta opção se iguala à função informativa do ícone da bandeja do sistema (mudança de cor) relatando um problema em quaisquer componentes da AVG;

- ***Exibir ***notificações referentes a Proteção Residente*** - decida se as informações relativas a salvar, copiar e abrir processos devem ser exibidas ou omitidas*esta configuração apenas demonstra se a opção Tratamento automáticoProteção Residenteestá ativada*

- ***Exibir notificações sobre verificação*** - decida se as informações sobre início automático da verificação agendada, seu andamento e resultados devem ser exibidos;

- ***Exibir notificações na bandeja relativas ao Firewall*** - decidir se as informações relativas ao status e processo do Firewall, como avisos de ativação/desativação do componente, possível bloqueio de tráfego etc. devem ser exibidas

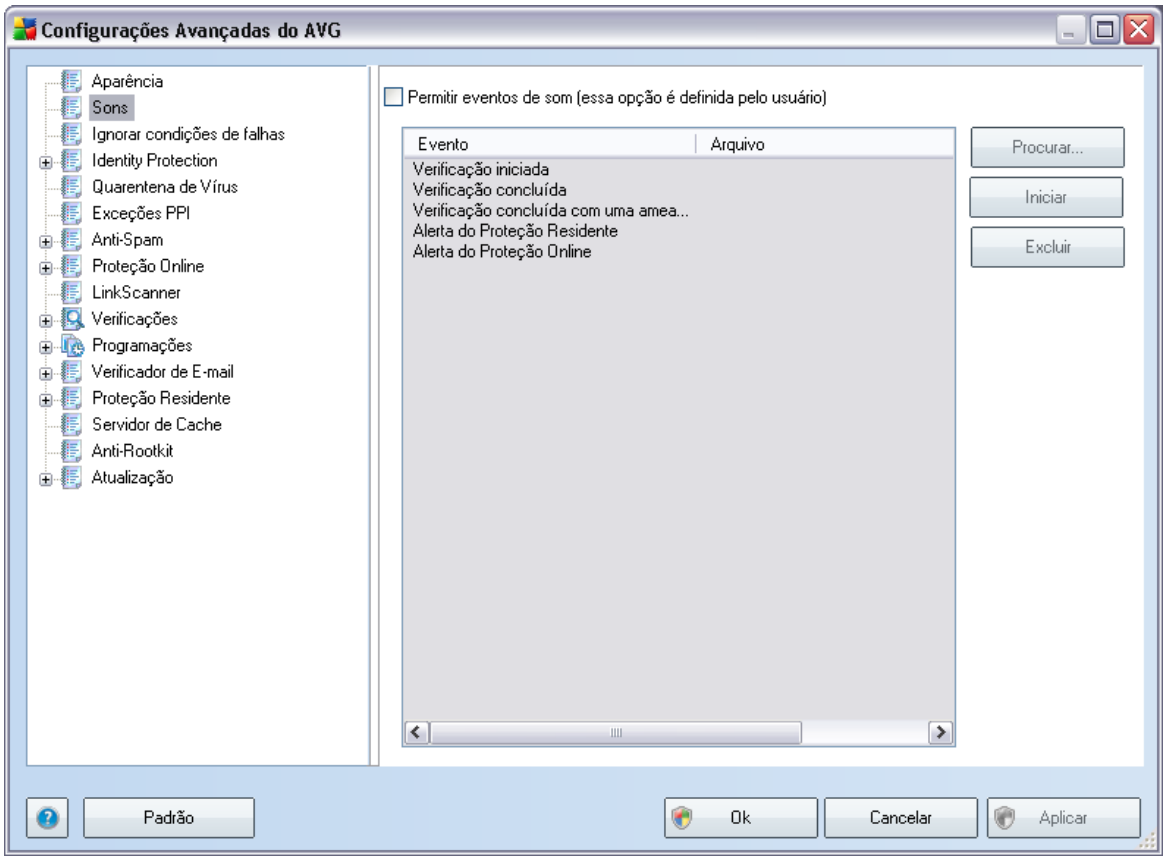
- ***Exibir notificações da bandeja relacionadas ao Verificador de E-mail*** - decida se as informações sobre a verificação de todas as mensagens de e-mail de entrada e saída serão exibidas..

Modo de jogo

Esta função do AVG foi desenvolvida para aplicativos de tela inteira em que possíveis balões de informação do AVG (exibidos por exemplo, quando uma verificação programada é iniciada)seriam perturbadores (podem minimizar o aplicativo ou corromper seus gráficos). Para evitar essa situação, mantenha marcada a caixa de diálogo referente à opção para ***Ativar modo de jogo quando um aplicativo de tela inteira for executado*** (*configuração padrão*).

10.2. Sons

Na caixa de diálogo ***Sons***, você pode especificar se deseja receber informações sobre ações especificas do AVG via notificação sonora. Em caso positivo, marque a opção ***Ativar eventos sonoros*** (*desativada por padrão*) para ativar a lista de ações do AVG:

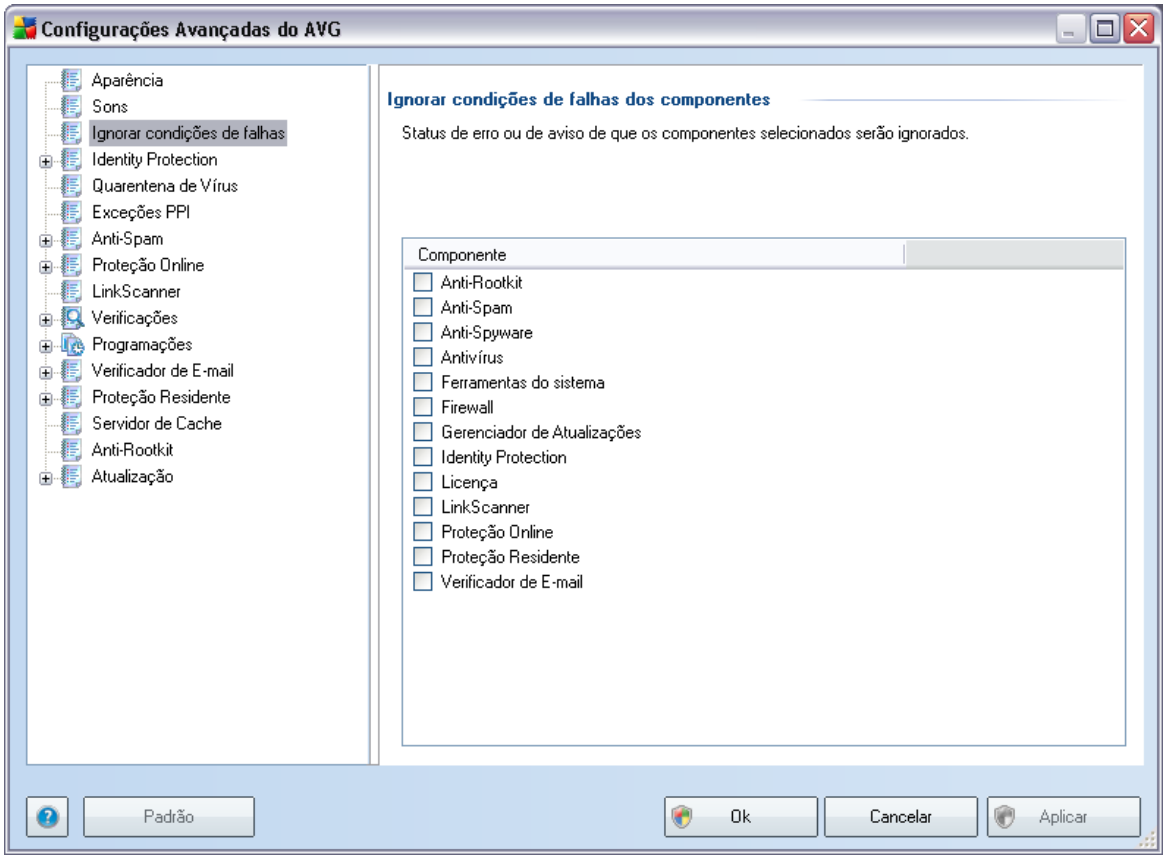


Em seguida, selecione o respectivo evento na lista e procure (usando a opção ***Procurar***) um som apropriado no disco rígido que deseja atribuir a esse evento. Para ouvir o som selecionado, realce o evento na lista e pressione o botão ***Reproduzir***. Use o botão ***Excluir*** para remover o som atribuído a um evento específico.

Observação: *apenas sons *.wav podem ser usados!*

10.3. Ignorar condições de falhas

Na caixa de diálogo ***Ignorar condições de falhas dos componentes*** você pode marcar aqueles componentes sobre os quais não deseja obter informações:



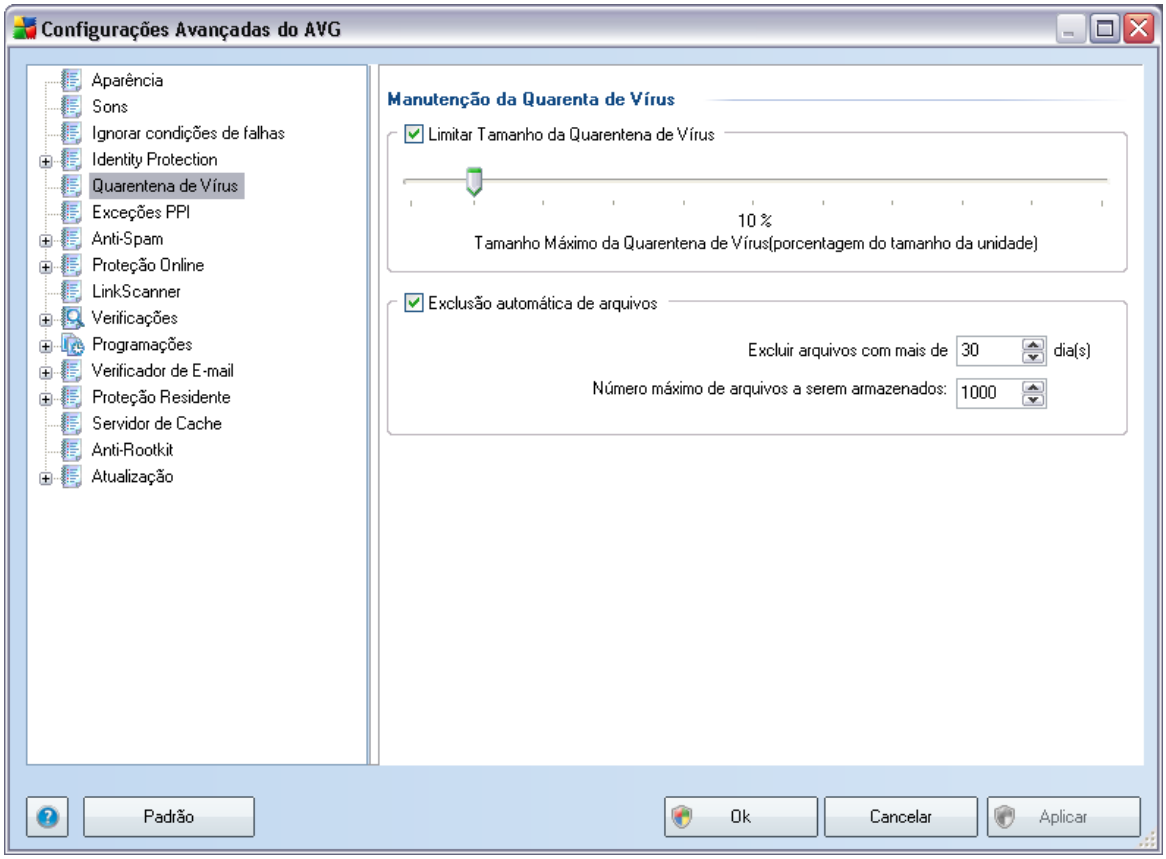
Por padrão não há componentes selecionados nesta lista. Isto significa que, caso qualquer componente receba um status de erro, você será informado sobre isso imediatamente via:

- ***ícone da bandeja do sistema*** - enquanto todos os componentes do AVG estão funcionando adequadamente, o ícone é exibido em quatro cores; entretanto, se ocorrer um erro, os ícones aparecem com um ponto de exclamação amarelo,
- descrição textual do problema na seção ***Informações sobre Status de Segurança*** na janela principal do AVG

Pode acontecer que, por alguma razão, você precise desligar um componente por certo tempo (*não é recomendável, você deve tentar manter todos os componentes sempre ligados e em sua configuração padrão, mas pode acontecer*). Neste caso, o ícone da bandeja do sistema relata automaticamente o status de erro do componente. Entretanto, neste caso em particular, não se pode falar de um erro, pois você deliberadamente o induziu, e está ciente do provável risco. Ao mesmo tempo, assim que é exibido em cinza, o ícone não pode relatar qualquer outro erro que possa aparecer.

Neste caso, na caixa de diálogo acima você pode selecionar componentes que podem estar com status de erro (*ou desligados*) e sobre os quais você não deseja receber informações. A mesma opção ***Ignorando o estado do componente*** também está disponível para componentes específicos diretamente da visão geral dos componentes na janela principal do AVG.

10.4. Quarentena de vírus



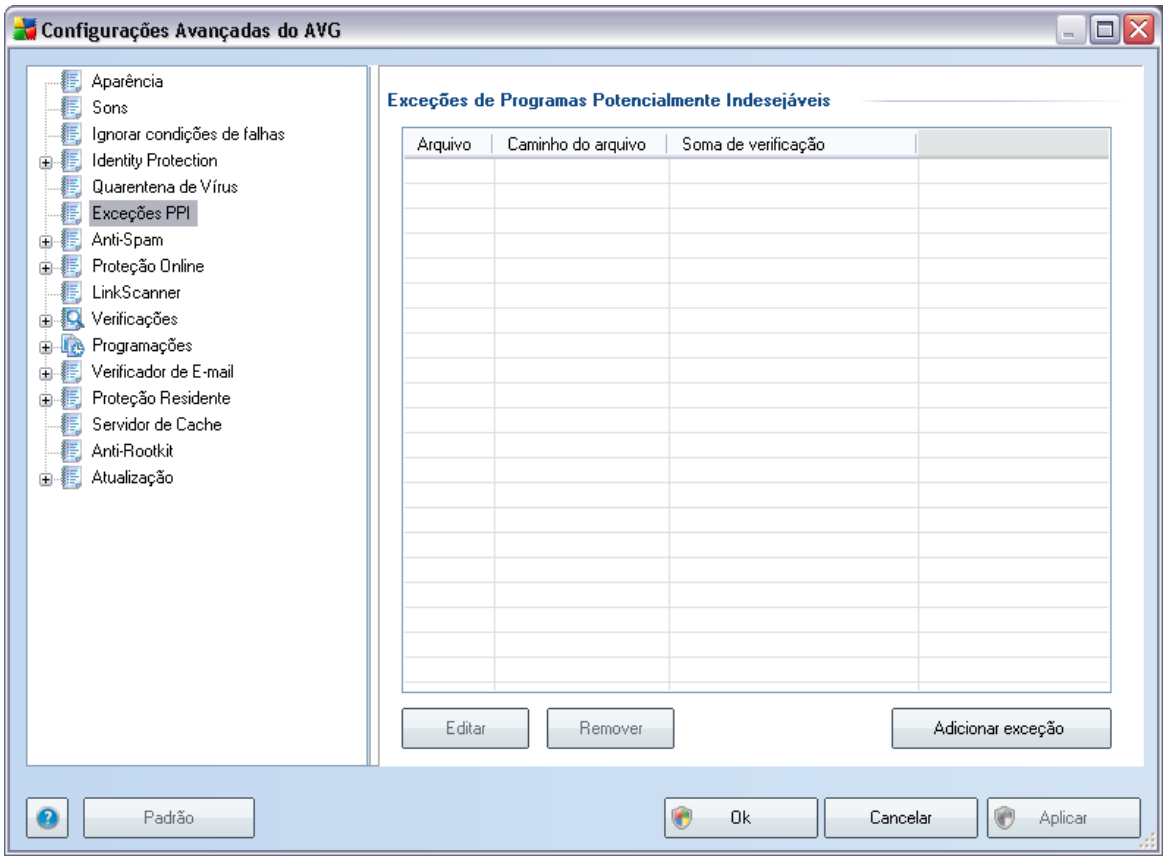
A caixa de diálogo ***Manutenção da quarentena*** permite definir vários parâmetros relativos à administração de objetos armazenados na ***Quarentena***:

- ***Limitar tamanho da Quarentena de vírus*** - use o controle deslizante para definir o tamanho máximo da ***Quarentena de vírus***. O tamanho é especificado proporcionalmente ao tamanho do seu disco rígido local.

- ***Exclusão automática de arquivo*** - nessa seção, defina a duração máxima de armazenamento dos objetos na ***Quarentena*** (***Excluir arquivos mais antigos que...***) e o número máximo de arquivos a serem armazenados na ***Quarentena*** (***Número máximo de arquivos a serem armazenados***).

10.5. Exceções PPI

O AVG 9 Anti-Virus plus Firewall é capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL que possam ser potencialmente indesejáveis no sistema. Pode ser que o usuário deseje manter, em alguns casos, determinados programas indesejáveis no computador (*programas instalados propositalmente*). Alguns programas, especialmente os gratuitos, incluem adware. Esse adware pode ser detectado e reportado pelo AVG como um ***programa potencialmente indesejável***. Se desejar manter esse programa no computador, você poderá defini-lo como uma exceção de programa potencialmente indesejável:



A caixa de diálogo ***Exceções de Programa Potencialmente Indesejável*** exibe uma lista das exceções definidas e válidas atualmente dos programas não desejados. É possível editar a lista, excluir itens existentes ou adicionar novas exceções. As informações a seguir podem ser encontradas na lista para cada exceção:

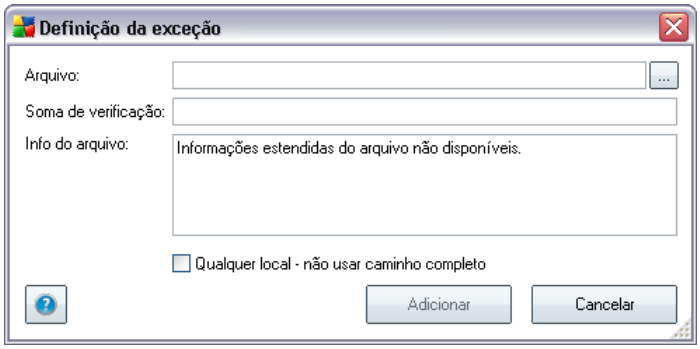
- ***Arquivo*** - fornece o nome do respectivo aplicativo
- ***Caminho do arquivo*** - mostra a localização do aplicativo
- ***Soma de Verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de Verificação é uma seqüência de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo escolhido dos outros arquivos. A Soma de Verificação é gerada e exibida após a adição bem-sucedida do arquivo.

Botões de controle

- ***Editar*** - abre uma caixa de diálogo de edição (*idêntica à da definição de exceção; veja abaixo*) de uma exceção já definida, na qual é possível alterar os parâmetros de exceção

- ***Remover*** - exclui o item selecionado da lista de exceções

- ***Adicionar exceção*** - abre uma caixa de diálogo de exceção na qual é possível definir os parâmetros da nova exceção a ser criada:



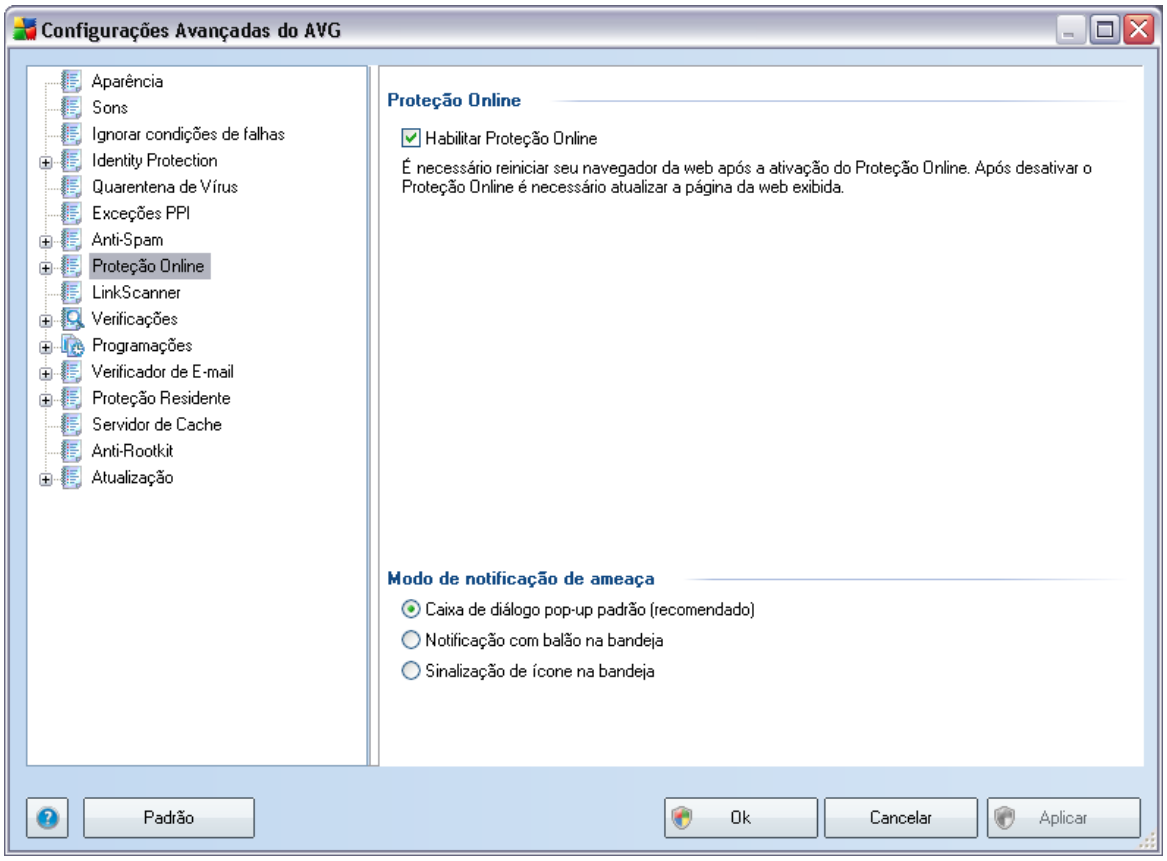
  - ***Arquivo*** - digite o caminho completo para o arquivo que deseja marcar como uma exceção

  - ***Soma de Verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de Verificação é uma seqüência de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo escolhido dos outros arquivos. A Soma de Verificação é gerada e exibida após a adição bem-sucedida do arquivo.

  - ***Informações do Arquivo*** - exibe outras informações disponíveis sobre o arquivo (*informações de licença/versão etc.*)

  - ***Qualquer local - não use caminhos completos*** - se quiser definir o arquivo como uma exceção apenas no local específico, deixe a caixa de seleção desmarcada

10.6. Proteção On-line



A caixa de diálogo ***Proteção da Web*** permite ativar/desativar totalmente o componente ***Proteção Online*** por meio da opção ***Ativar On-line Shield*** (*ativada por padrão*). Para obter configurações mais avançadas sobre esse componente, continue nas caixas de diálogo seguintes, conforme relacionado na árvore de navegação:

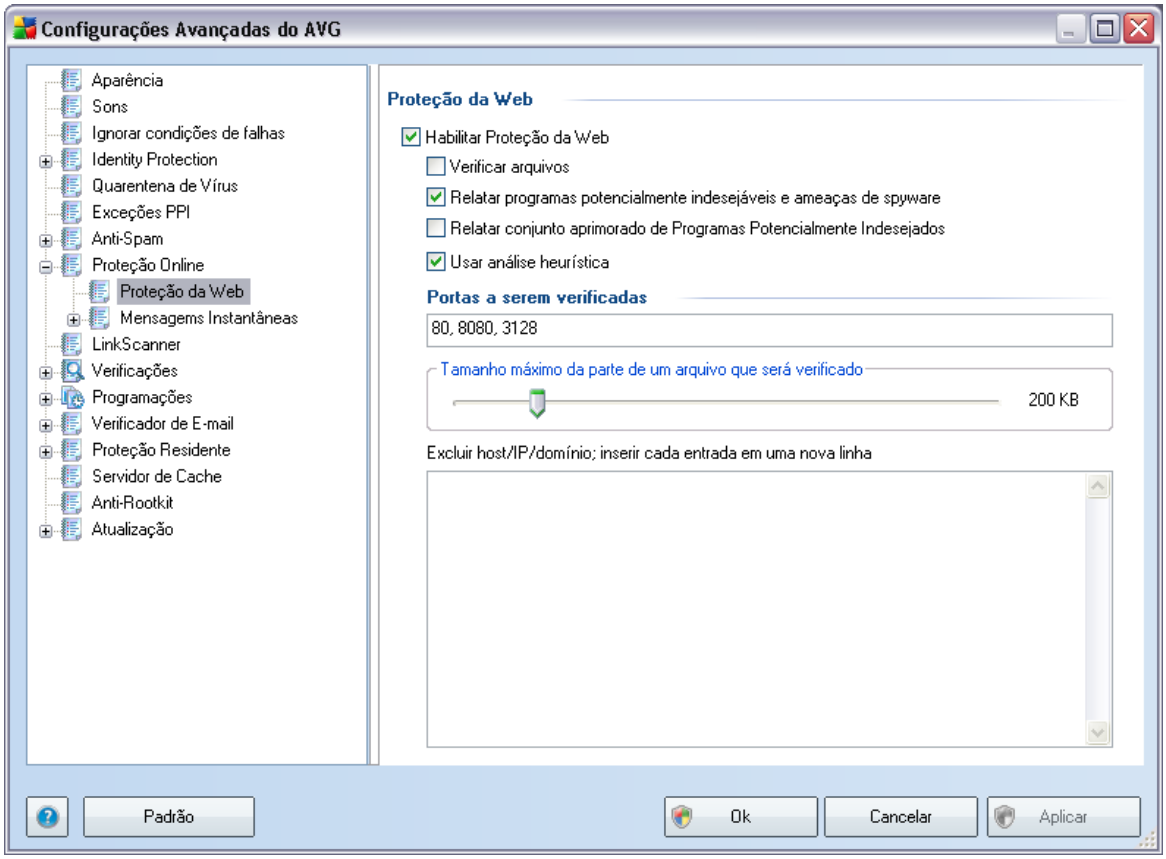
- ***Proteção da Web***
- ***Mensagens Instantâneas***

Modo de notificação de ameaças

Na parte inferior da caixa de diálogo, selecione de que maneira você gostaria de ser informado sobre possíveis ameaças detectadas: por meio de uma caixa de diálogo pop-

up, notificação de balão na bandeja ou nas informações de ícone na bandeja.

10.6.1. Proteção da Web



Na caixa de diálogo ***Proteção da Web***, você pode editar a configuração do componente com relação à verificação do conteúdo do site da Web. A interface de edição permite configurar as seguintes opções elementares:

- ***Ativar Proteção da Web*** - essa opção confirma que o ***Proteção Online*** deve realizar a verificação do conteúdo das páginas www. Desde que essa opção esteja ativada (*por padrão*), você pode ativar/desativar estes itens:
    - ***Verificar arquivos*** - verifique o conteúdo dos arquivos possivelmente incluídos na página www a ser exibida.
    - ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar***

spyware, bem como vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

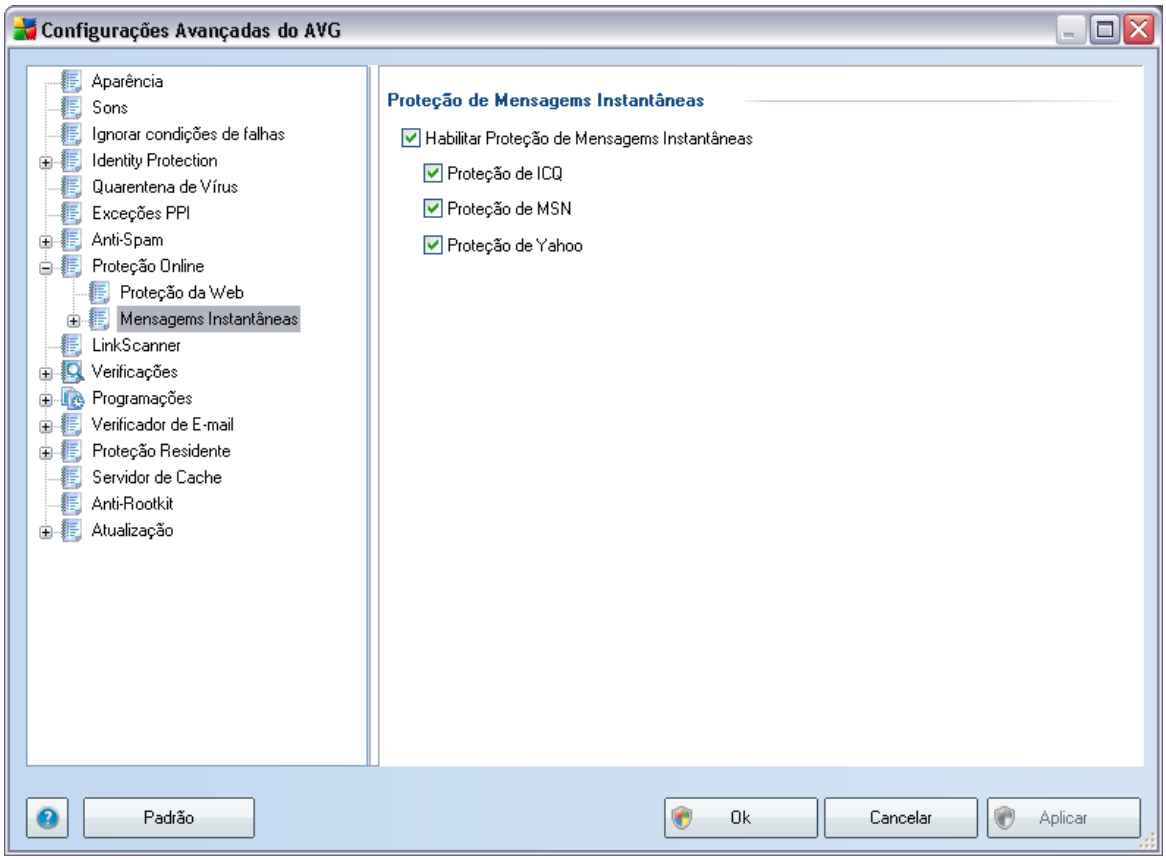
- ***Usar análise heurística*** - verifique o conteúdo da página a ser exibida usando o método de análise heurística(*emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual*).

- ***Portas a serem verificadas*** - este campo lista os números de porta de comunicação http padrão. Se a configuração do computador for diferente, mude o número da porta conforme necessário.

- ***Tamanho máximo de um arquivo a ser verificado*** - se os arquivos incluídos estiverem presentes na página exibida, você também poderá verificar o conteúdo deles, mesmo antes que serem baixados para seu computador. Entretanto, a verificação de arquivos grandes pode levar tempo e o download da página da Web pode ficar significativamente mais lento. Use a barra deslizante para especificar o tamanho máximo de um arquivo que ainda será verificado pela ***Proteção Online***. Mesmo se o arquivo baixado for maior que o especificado, deixando de ser verificado pela Proteção Online, você ainda estará protegido. Se o arquivo estiver infectado, a ***Proteção Residente*** o detectará imediatamente.

- ***Excluir host/IP/domínio*** - no campo de texto você pode digitar o nome exato de um servidor (*host, endereço IP, endereço IP com máscara ou URL*) ou um domínio que não deve ser verificado pela ***Proteção Online***. Portanto, exclua apenas o host que você tenha certeza de que nunca permitirá conteúdo web perigoso.

10.6.2. Mensagens Instantâneas

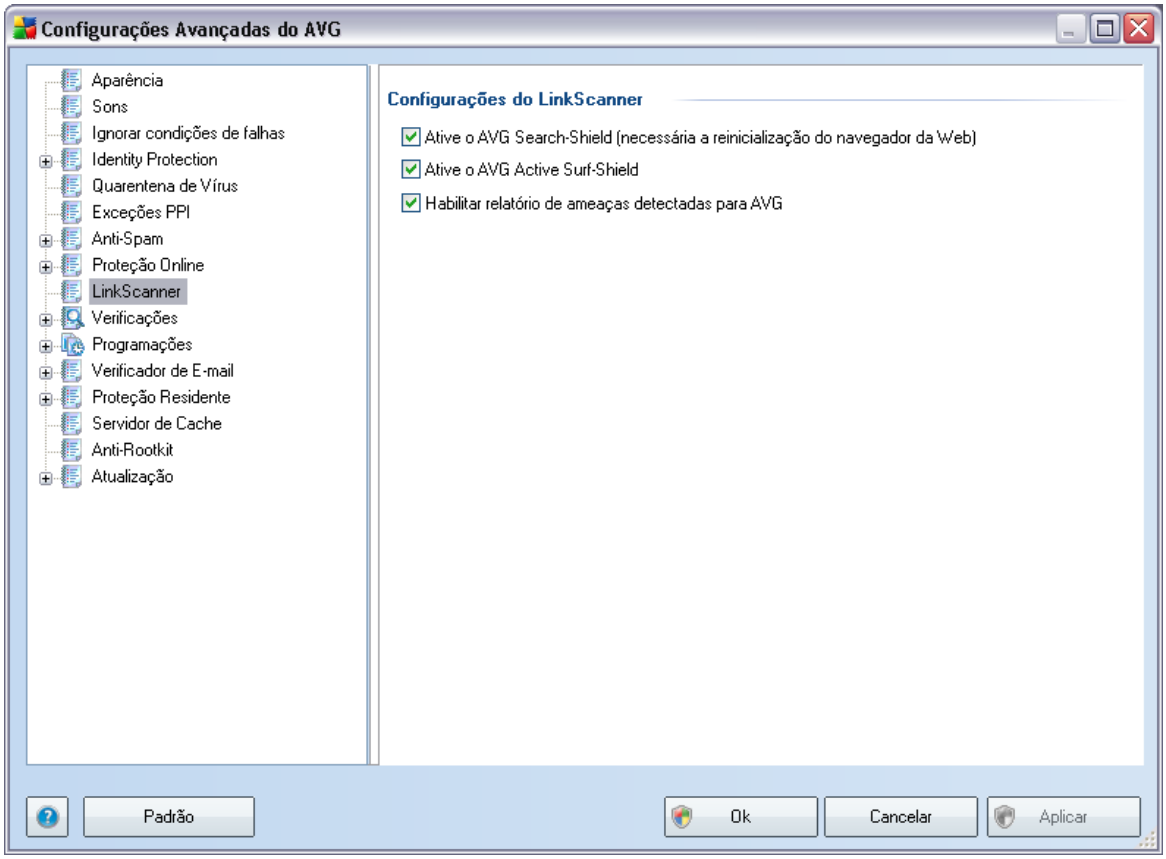


Na caixa de diálogo ***Proteção de Mensagens Instantâneas***, é possível editar as configurações dos componentes da ***Proteção Online*** referentes à verificação de mensagens instantâneas. No momento, os três programas de mensagens instantâneas têm suporte: ***ICQ***, ***MSN*** e ***Yahoo*** - marque o item apropriado para cada um deles, se quiser que a ***Proteção Online*** verifique se a comunicação on-line está livre de vírus.

Para obter outras especificações sobre usuários permitidos/bloqueados, você pode ver e editar a respectiva caixa de diálogo (***ICQ Avançado***, ***MSN Avançado, Yahoo Avançado***) e especificar a ***Lista de exceções*** (*lista de usuários com permissão para se comunicar com você*) e a ***Lista negra*** (*usuários que devem ser bloqueados*).

10.7. Link Scanner

A caixa de diálogo ***Configurações do LinkScanner*** permite ativar ou desativar os recursos básicos do ***LinkScanner***:



- ***Ativar o AVG Search-Shield*** - (*por padrão*): ícones de notificação de aviso em pesquisas realizadas no Google, Yahoo, Bing, Yandex, Altavista ou Baidu com verificação antecipada do conteúdo de sites retornado pelo mecanismo de pesquisa.

- ***Ativar AVG Active Surf-Shield*** - (*ativo por padrão*): proteção ativa (*em tempo real*) contra sites exploradores à medida que são acessados. As conexões conhecidas com sites maliciosos e seu conteúdo exploratório são bloqueadas à medida que são acessados por meio de um navegador da Web *ou outro aplicativo que utilize HTTP*).

- ***Ativar relatórios de ameaças detectadas para a AVG*** - (*ativada por padrão*

): marque esse item para permitir relatórios de explorações e sites mal-intencionados descobertos pelos usuários por meio do ***AVG Active Surf-Shield*** ou do ***AVG Search-Shield*** para alimentar o banco de dados que coleta informações sobre atividades mal-intencionadas na Web.

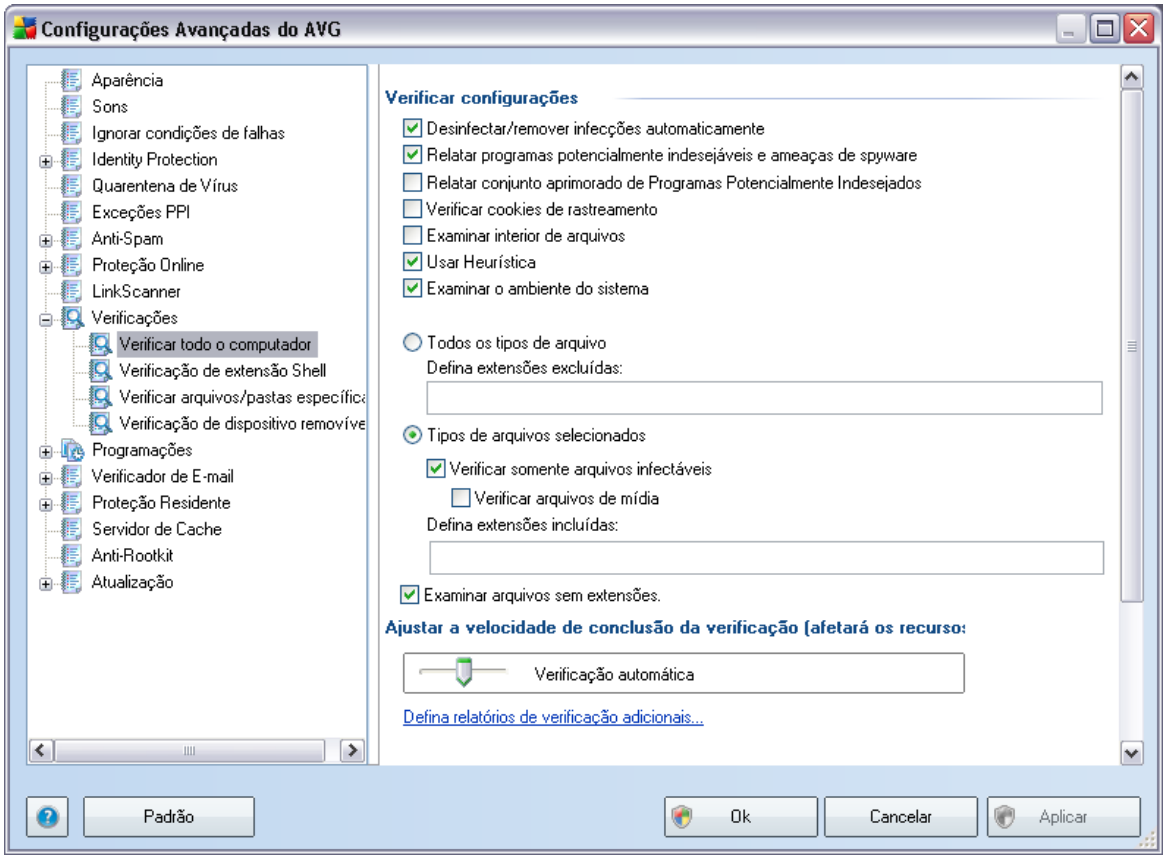
10.8. Verificações

As configurações de verificação avançada estão divididas em três categorias referentes a tipos específicos de verificação, conforme definido pelo fornecedor do software:

- ***Verificar Todo o Computador*** - verificação padrão predefinida de todo o computador
- ***Verificação de Extensão Shell*** - verificação específica de um objeto selecionado diretamente do ambiente do Windows Explorer
- ***Verificar Arquivos ou Pastas Específicas*** - verificação padrão predefinida de áreas selecionadas do computador
- ***Verificação de Dispositivos Removíveis*** - verificação específica de dispositivos removíveis conectados ao seu computador

10.8.1. Verificar todo o computador

A opção ***Verificar todo o computador*** permite editar parâmetros de uma das verificações predefinidas pelo fornecedor do software, ***Verificar todo o computador***.



Configurações da verificação

Na guia ***Configurações da verificação*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados.

- ***Reparar ou remover vírus automaticamente*** - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a ***Quarentena de Vírus***.
- ***Informar programas potencialmente indesejáveis e ameaças de***

spyware – marque para ativar o mecanismo ***Anti-Spyware e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** - esse parâmetro do componente Anti-Spyware define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências ou conteúdo de suas compras eletrônicas*)

- ***Verificar dentro dos arquivos*** - esse parâmetro define que a verificação deve ocorrer em todos os arquivos, incluindo os armazenados dentro de arquivos como ZIP ou RAR.

- ***Usar Heurística*** - a análise heurística (emulação dinâmica das instruções do objeto verificado, *em um ambiente de computador virtual) será um dos métodos usados para detecção de vírus durante a verificação;*

- ***Verificar ambiente do sistema*** - a verificação ocorrerá nas áreas de sistema do computador.

Além disso, você deve decidir se deseja verificar

- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas) que não devem ser verificadas;

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é

possível especificar por extensões, quais são os arquivos que sempre devem ser verificados.

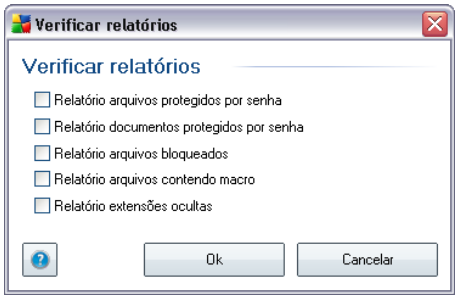
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Prioridade do processo de verificação

Na seção ***Verificar prioridade do processo*** , você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível médio de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos do sistema será bem maior durante sua execução e as outras atividades do PC terão o desempenho reduzido (*essa opção pode ser usada quando o computador está ligado, mas ninguém está trabalhando nele*). Por outro lado, você pode diminuir a utilização dos recursos do sistema ampliando a duração da verificação.

Defina relatórios de verificação adicionais...

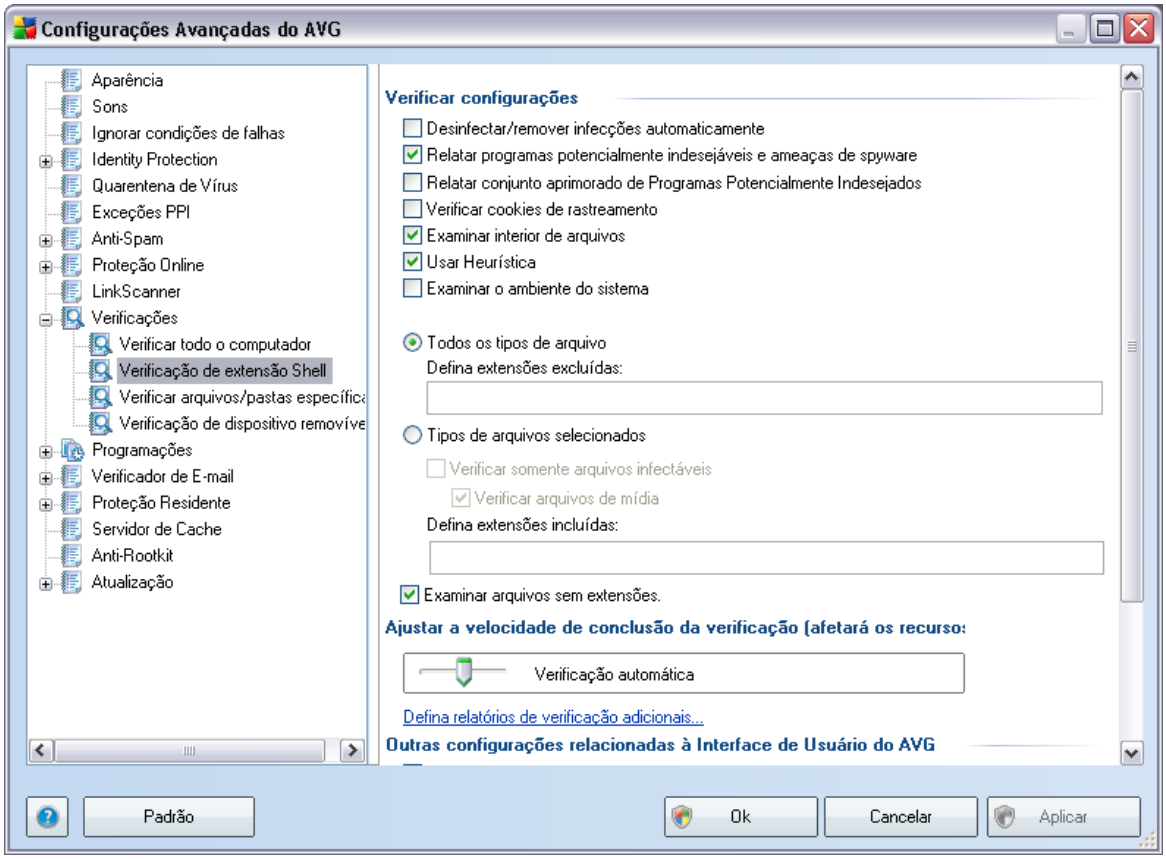
Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



10.8.2. Verificação de extensão Shell

Da mesma forma que o item anterior, ***Verificar todo o computador*****, este item denominado** Verificação da extensão shell ***oferece várias opções para editar a verificação predefinida pelo fornecedor do software***. Dessa vez a configuração é relacionada à verificação de objetos específicos inicializados diretamente no ambiente do Windows Explorer (*extensão shell*). Consulte o capítulo ***Verificação do Windows***

Explorer:



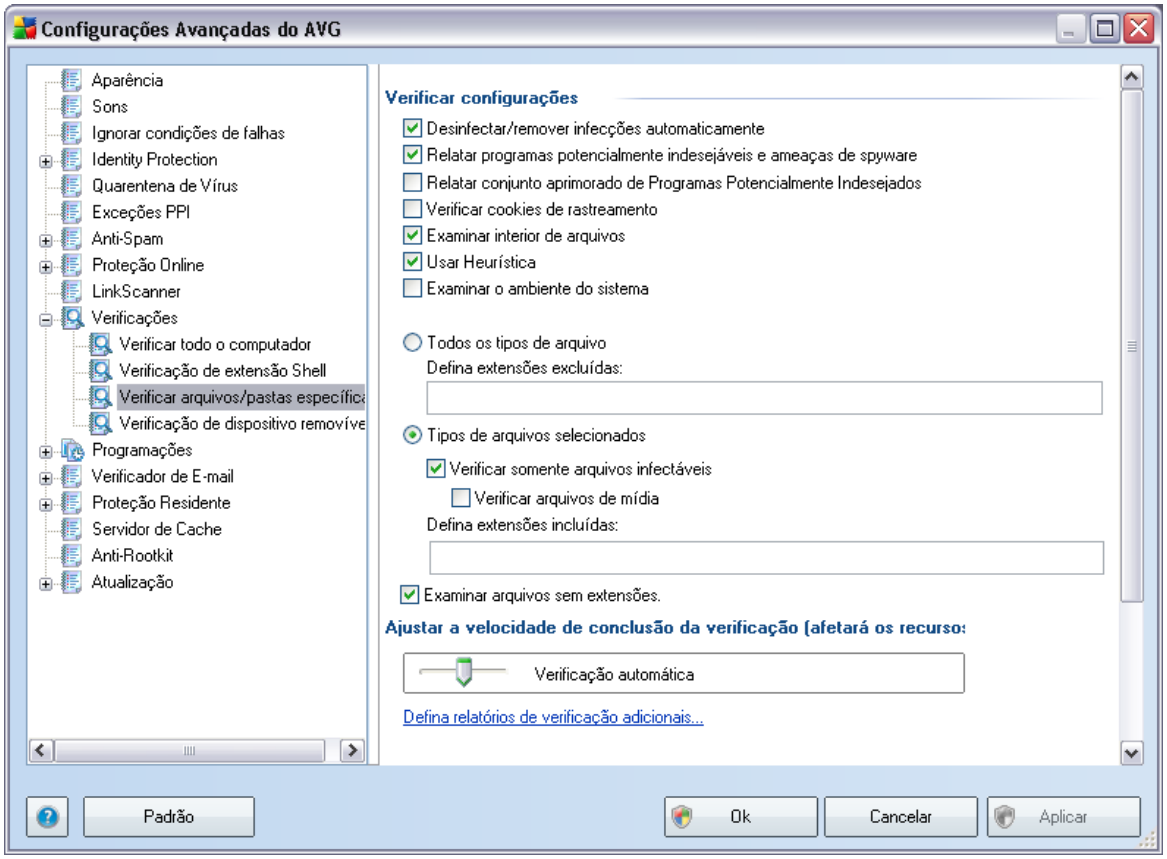
A lista de parâmetros é idêntica à disponível para ***Verificar todo o computador***. Entretanto, as configurações padrão são diferentes: com ***Verificar todo o computador***, a maioria dos parâmetros era selecionada, enquanto para ***Verificação da extensão shell*** (***Verificação do Windows Explorer***), somente os parâmetros relevantes são ativados.

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo* ***Configurações Avançadas do AVG / Verificações / Verificar Todo o Computador****.*

10.8.3. Verificar arquivos ou pastas específicas

A interface de edição de ***Verificar arquivos ou pastas específicos*** é idêntica à caixa de edição ***Verificar Todo o Computador***. Todas as opções de configuração são as mesmas, porém as configurações padrão são mais rigorosas em ***Verificar todo o***

computador .

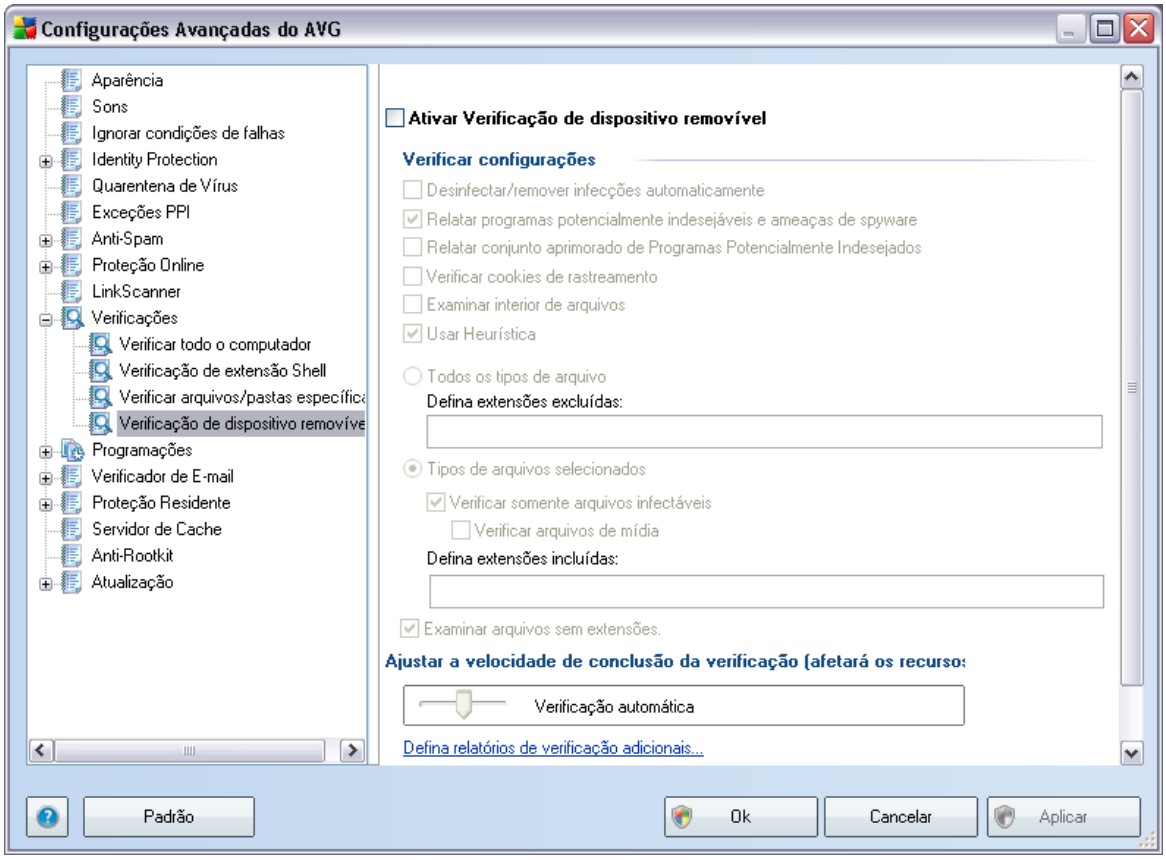


Todo os parâmetros definidos nesta caixa de diálogo de configuração são válidos somente para as áreas selecionadas para verificação com a ***Verificação de arquivos ou pastas específicos***!

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo* ***Configurações Avançadas do AVG / Verificações / Verificar Todo o Computador****.*

10.8.4. Verificação de dispositivo removível

A interface de edição de ***Verificação de dispositivo removível*** também é muito semelhante à caixa de diálogo de edição ***Verificar todo o computador***:



A ***Verificação de dispositivo removível*** é ativada automaticamente quando você conecta um dispositivo removível ao computador. Por padrão, essa verificação está desativada. No entanto, é essencial verificar dispositivos removíveis em busca de ameaças potenciais, pois são uma das fontes principais de infecção. Para que a verificação esteja pronta e seja iniciada quando necessário, marque a opção ***Ativar verificação de dispositivo removível*** .

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo* ***Configurações Avançadas do AVG / Verificações / Verificar Todo o Computador****.*

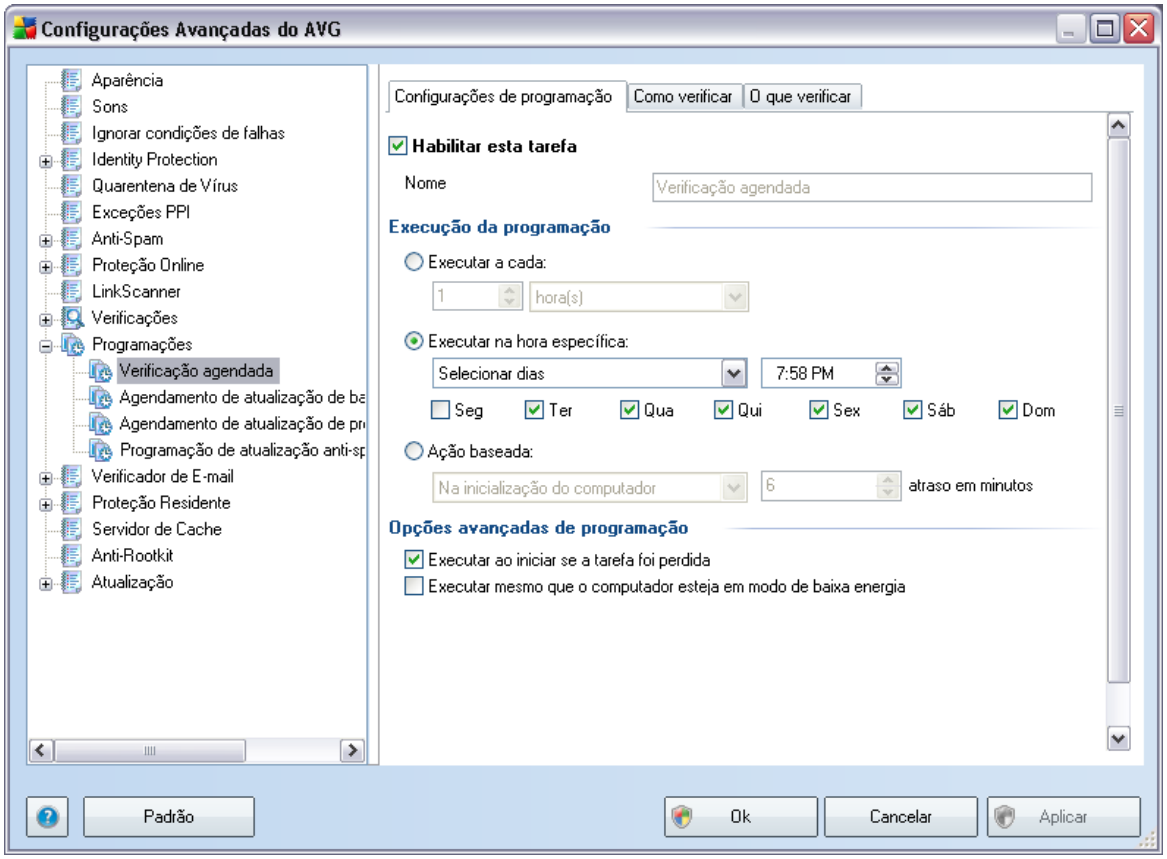
10.9. Programações

Na seção ***Agendamentos***, é possível editar as configurações padrão de:

- Agendamento de verificação de todo o computador
- Agendamento de atualização de banco de dados de vírus
- Agendamento de atualização de programa

10.9.1. Verificação agendada

Os parâmetros da verificação agendada podem ser editados(*ou uma nova configuração de agenda*) em três guias:



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente o teste programado e ativá-lo novamente conforme necessário.

Em seguida, no campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa. Para programações recém-adicionadas (*é possível adicionar uma nova programação clicando com o botão direito no item* ***Verificação programada*** *na área de navegação esquerda*), você pode especificar o seu próprio nome e, nesse caso, o campo de texto ficará aberto para edição. Tente sempre usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

Exemplo: *não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc. Além disso, não é necessário especificar no nome da verificação se ela é uma verificação de todo o computador ou somente uma verificação de pastas ou arquivos selecionados. Suas verificações serão sempre uma versão específica da verificação de arquivos ou pastas selecionados.*

Nessa caixa de diálogo você ainda poderá definir os seguintes parâmetros de verificação:

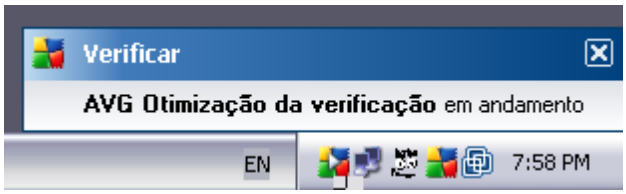
Execução da programação

Aqui, você pode especificar intervalos de tempo para a ativação da verificação recém-programada. O tempo pode ser definido pela repetição da ativação da verificação depois de um determinado período (***Executar a cada ...***), pela definição de uma data e hora exatas (***Executar em uma hora específica...***) ou possivelmente pela definição de um evento ao qual a ativação da verificação deve ser associada (***Ação baseada na inicialização do computador***).

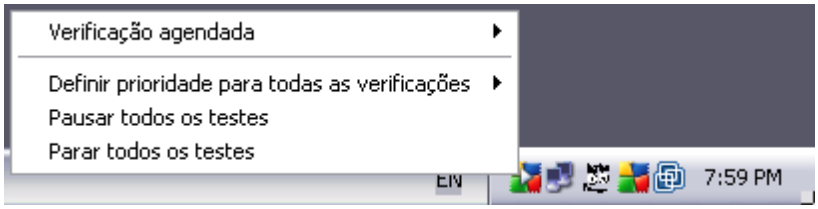
Opções avançadas de programação

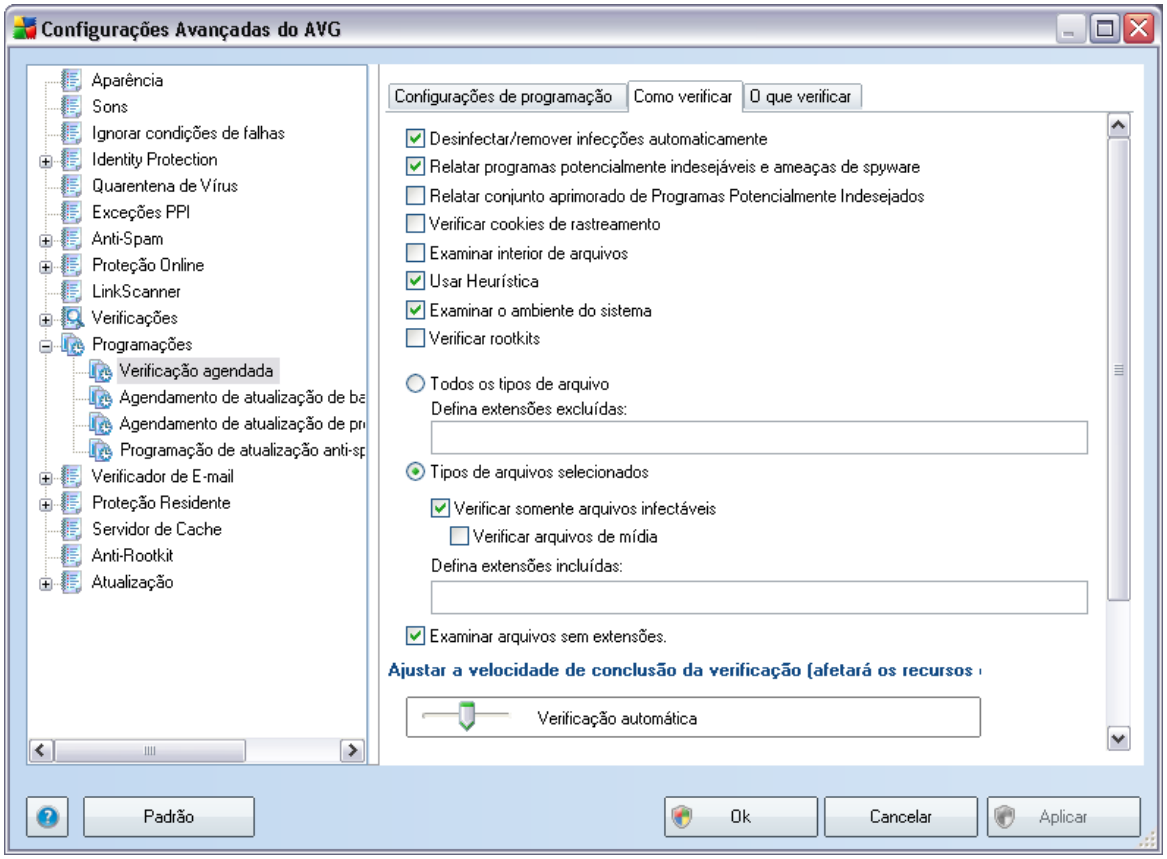
Essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

Uma vez que a verificação agendada é iniciada no horário que você especificou, você será informado deste fato por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema:



Um novo ícone AVG na bandeja do sistema aparece (*em sua cor normal e com uma seta branca - veja a imagem acima*) informando que uma verificação agendada está em execução. Clique com o botão direito no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação:





Na guia ***Como verificar*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros é ativada e a funcionalidade será aplicada durante a verificação. A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida:

- ***Reparar ou remover vírus automaticamente*** - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a ***Quarentena de Vírus***.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter

esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** - (*ativado por padrão*): esse parâmetro do componente ***Anti-Spyware*** define que os cookies devem ser detectados durante a verificação (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de suas compras eletrônicas*);

- ***Verificar interior dos arquivos*** - (*ativado por padrão*): esse parâmetro define que a verificação deve atuar em todos os arquivos, mesmo se eles estiverem compactados em algum tipo de arquivo, como ZIP, RAR etc.

- ***Usar Heurística*** - (*ativado por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado,em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***Verificar ambiente do sistema*** - (*ativado por padrão*): a verificação também atuará nas áreas do sistema do seu computador.

- ***Verificar rootkits*** - marque este item se desejar incluir a detecção de rootkit na verificação de todo o computador. A detecção de rootkit também está disponível por meio do componente ***Anti-Rootkit***;

Além disso, você deve decidir se deseja verificar

- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas)

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes,*

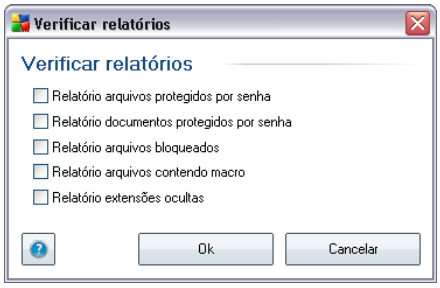
e é muito improvável que eles sejam infectados por vírus). Mais uma vez, é possível especificar por extensões, quais são os arquivos que sempre devem ser verificados.

- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

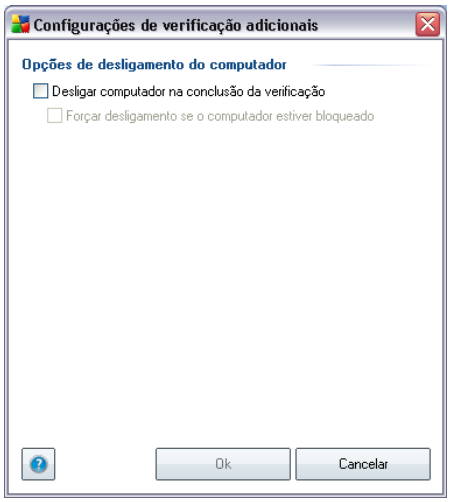
Prioridade do processo de verificação

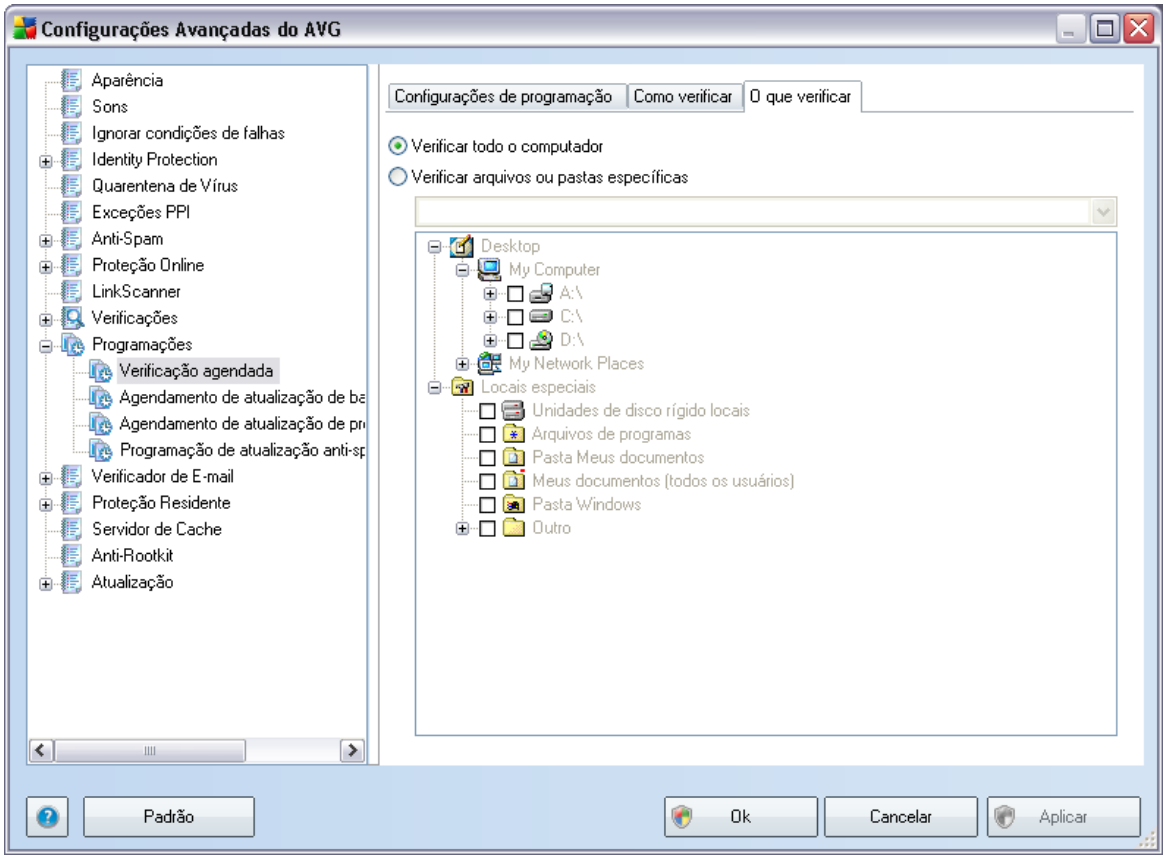
Na seção ***Verificar prioridade do processo*** , você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível médio de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos do sistema será bem maior durante sua execução e as outras atividades do PC terão o desempenho reduzido (*essa opção pode ser usada quando o computador está ligado, mas ninguém está trabalhando nele*). Por outro lado, você pode diminuir a utilização dos recursos do sistema ampliando a duração da verificação.

Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



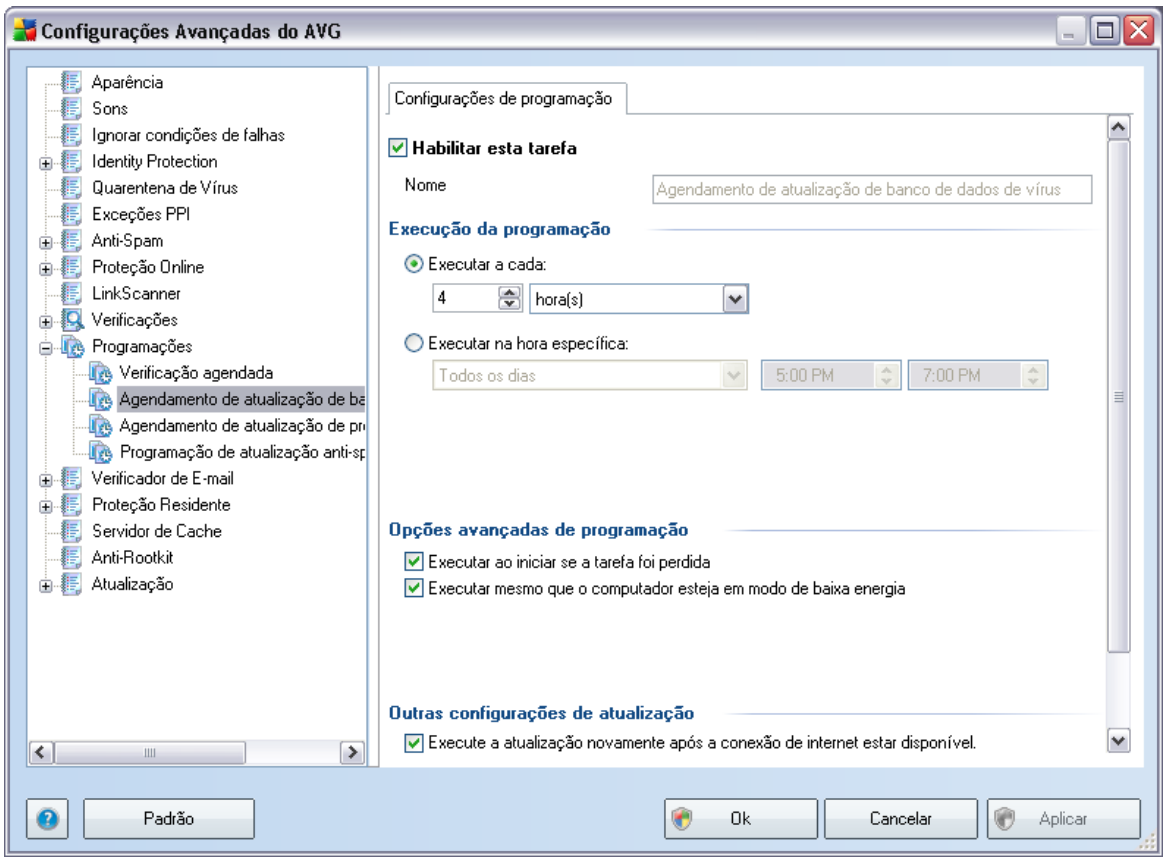
Clique em ***Configurações de verificação adicionais ...*** para abrir uma nova caixa de diálogo ***Opções de desligamento do computador*** que permite decidir se o computador deve ser desligado automaticamente assim que o processo de verificação estiver terminado. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).


Configurações de verificação adicionais
Opções de desligamento do computador
Desligar computador na conclusão da verificação
Forçar desligamento se o computador estiver bloqueado
Ok
Cancelar


Configurações Avançadas do AVG
Aparência
Sons
Ignorar condições de falhas
Identity Protection
Quarentena de Vírus
Exceções PPI
Anti-Spam
Proteção Online
LinkScanner
Verificações
Programações
Verificação agendada
Agendamento de atualização de ba
Agendamento de atualização de pr
Programação de atualização anti-sp
Verificador de E-mail
Proteção Residente
Servidor de Cache
Anti-Rootkit
Atualização
Configurações de programação
Como verificar
O que verificar
Verificar todo o computador
Verificar arquivos ou pastas específicas
Desktop
My Computer
A:\
C:\
D:\
My Network Places
Locais especiais
Unidades de disco rígido locais
Arquivos de programas
Pasta Meus documentos
Meus documentos (todos os usuários)
Pasta Windows
Outro
Padrão
Ok
Cancelar
Aplicar

Na guia ***O que verificar***, você pode definir se deseja programar a verificação de todo o computador ou a verificação de arquivos ou pastas específicas***. Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação.

10.9.2. Agendamento de atualização de banco de dados de vírus



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente a atualização do banco de dados de vírus agendada e ativá-la novamente conforme necessário. O banco de dados básico de vírus é coberto no componente ***Gerenciador de Atualização***. Nessa caixa de diálogo, você pode configurar parâmetros detalhados de agendamento de atualização do banco de dados de vírus. No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Nessa seção, especifique os intervalos de tempo para a inicialização da atualização do banco de dados de vírus recém-agendada. O prazo pode ser definido pelo início repetido de atualização após certo período de tempo (***Executar a cada...***) ou definindo um data e hora exatos (***Executar na hora específica...***).

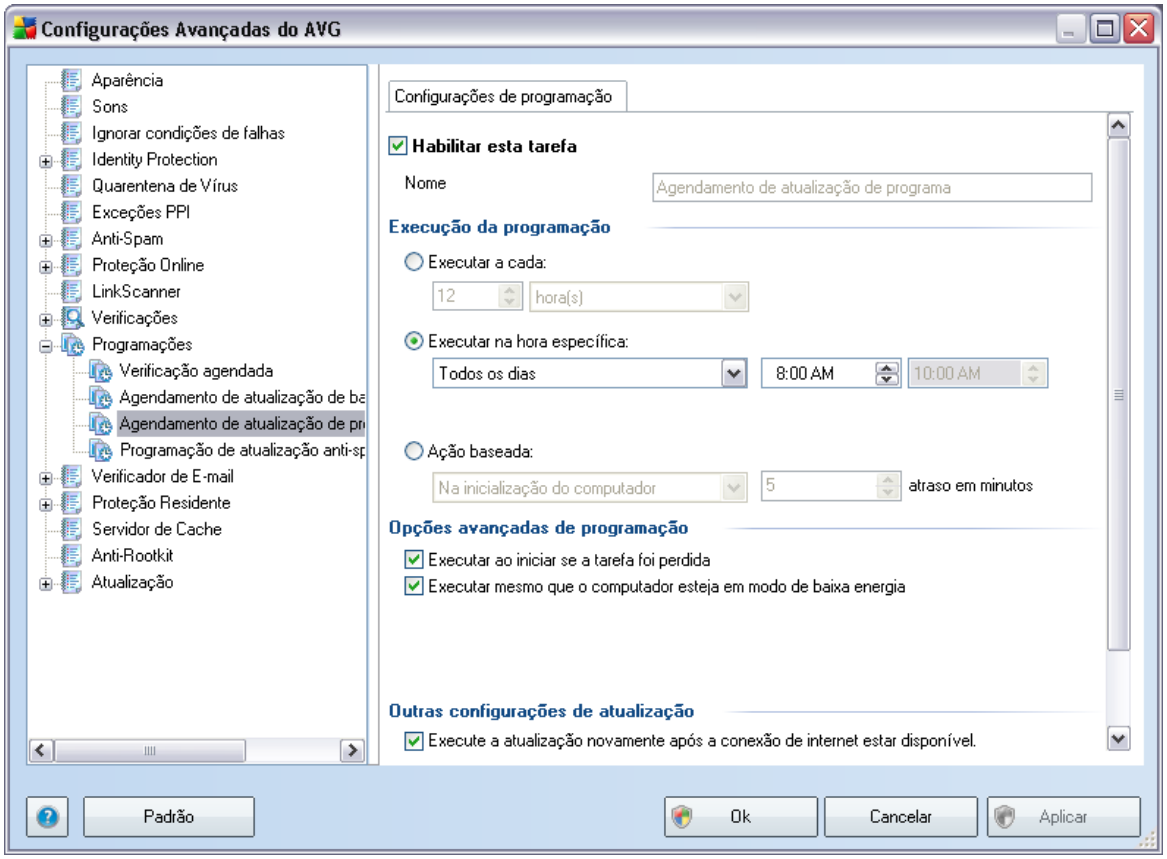
Opções avançadas de programação

Essa seção permite definir sob quais condições a atualização do banco de dados de vírus deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

Outras configurações de atualização

Por fim, marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

Assim que a atualização programada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo* ***Configurações avançadas/Aparência***).



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente a atualização do programa agendada e ativá-la novamente conforme necessário. No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Aqui, especifique os intervalos de tempo para iniciar a atualização do programa recém-programada. O tempo pode ser definido pela repetição da inicialização da atualização depois de um determinado período (***Executar a cada...***), pela definição de uma data e hora exatas (***Executar em uma hora específica...***) ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (***Ação baseada na inicialização do computador***).

Opções avançadas de programação

Essa seção permite definir sob quais condições a atualização do programa deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

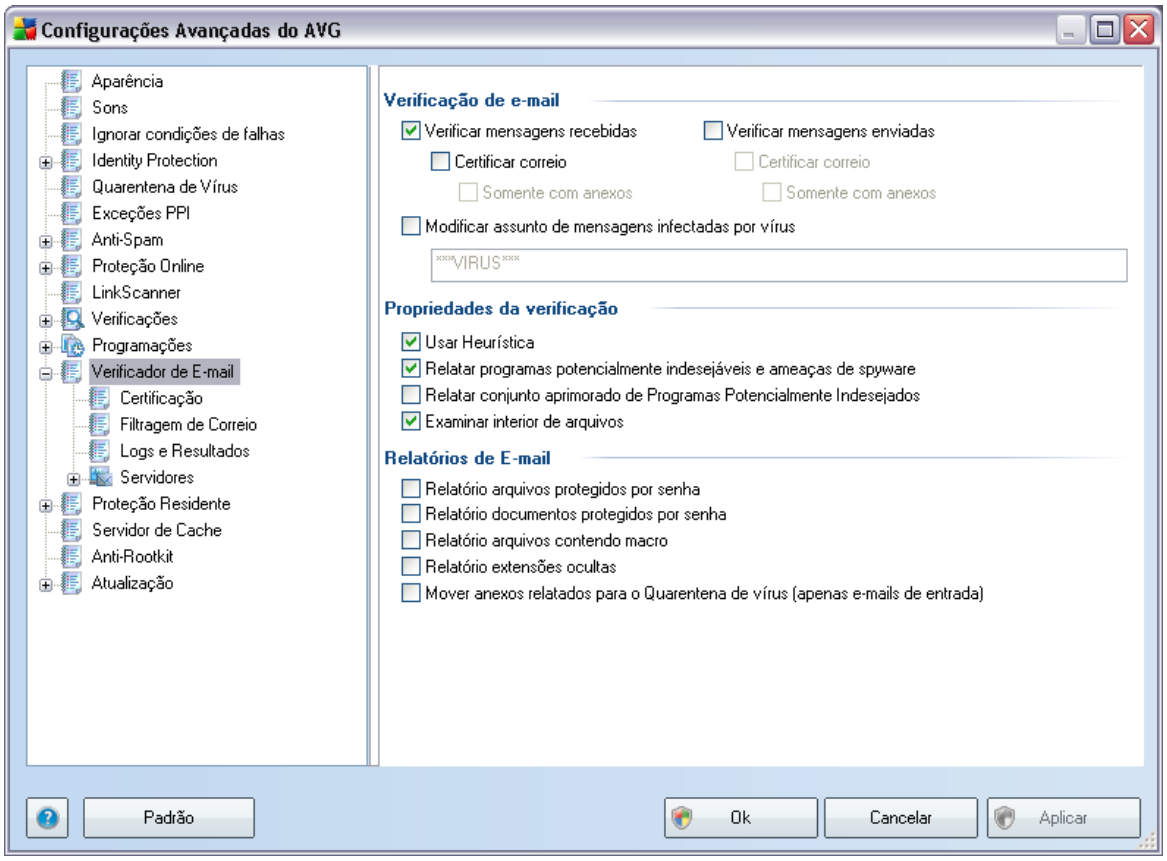
Outras configurações de atualização

Marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

Assim que a atualização programada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo* ***Configurações avançadas/Aparência***).

Observação: *se ocorrer uma coincidência de tempo de uma atualização de programa agendada e uma verificação agendada, o processo de atualização terá maior prioridade, e a verificação será interrompida.*

10.10. Verificador de e-mail



A caixa de diálogo ***Verificador de E-mail*** é dividida em três seções:

- ***Verificação de e-mail*** - nesta seção, você pode definir as funções básicas a seguir para mensagens de e-mail recebidas e/ou enviadas:
    - Se as mensagens de e-mail devem ser verificadas em busca de vírus.
    - Se o texto de certificação deve ser adicionado ao final de cada mensagem para confirmar que ela não contém vírus. O texto pode ser ajustado na caixa de diálogo Certificação.
    - Se o texto de certificação deve ser adicionado somente a mensagens com anexos.

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

caixa e digite o valor desejado no campo de texto. Ele será então adicionado ao campo de assunto de toda mensagem de e-mail infectada para facilitar a identificação e filtragem. O valor padrão recomendável é ***VÍRUS***.

- ***Propriedades de verificação*** - nesta seção, você pode especificar como as mensagens de e-mail serão verificadas:

    - ***Usar análise heurística*** – marque para usar o método de detecção de análise heurística ao verificar mensagens de e-mail.*** Quando essa opção está ativada, você pode filtrar anexos de e-mail não apenas por extensão, mas também o conteúdo real do anexo será considerado. A filtragem pode ser definida na caixa de diálogo Filtragem de e-mail.

    - ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

    - ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

    - ***Verificar dentro de arquivos*** – marque para verificar os conteúdos de arquivos anexados às mensagens de e-mail.

- ***Relatório de anexos de e-mail*** - nesta seção, você pode definir relatórios adicionais sobre arquivos potencialmente perigosos ou suspeitos. Observe que nenhuma caixa de diálogo de advertência será exibida, apenas um texto de certificação será adicionado ao final da mensagem de e-mail e todos esses relatórios serão listados na caixa de diálogo Detecção do Verificador de e-mail:

    - ***Reportar arquivos protegidos por senha –*** arquivos (ZIP, RAR, etc.) protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa para reportá-los como potencialmente perigosos.

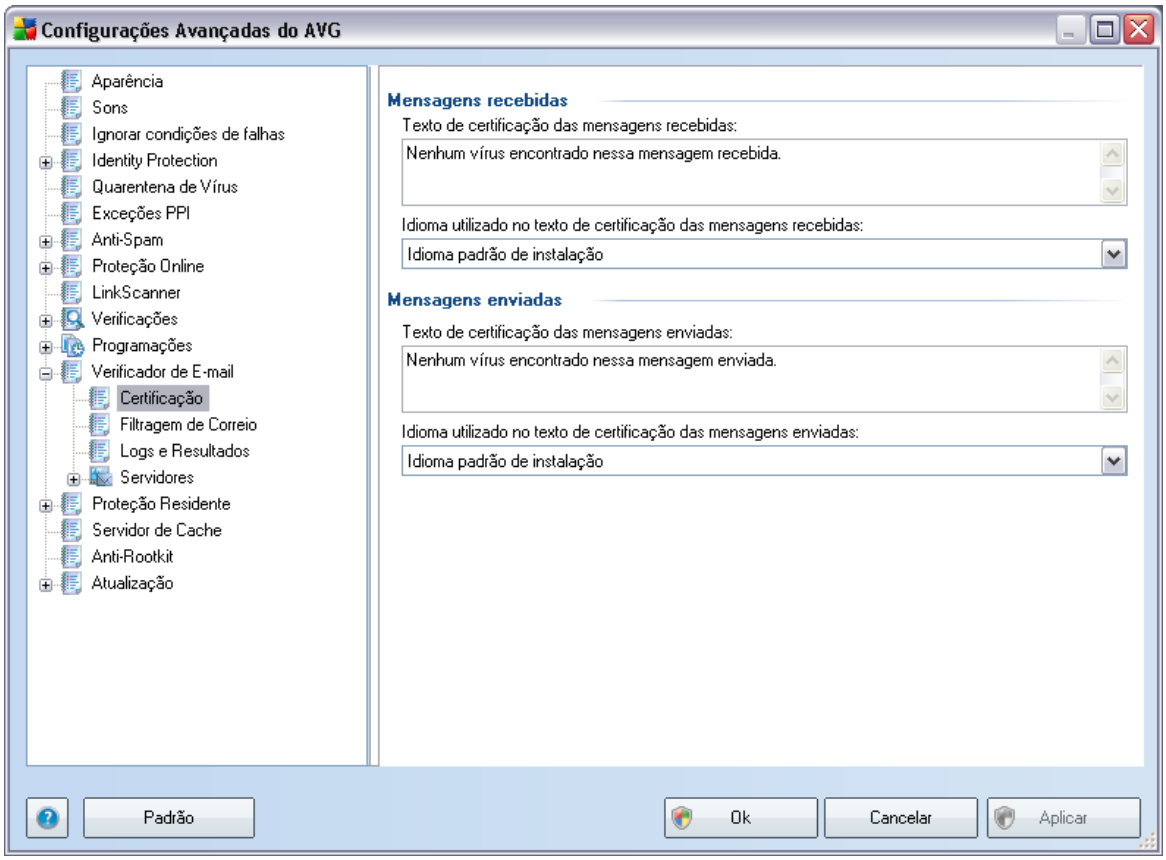
- ***Reporte documentos protegidos por senha*** – documentos protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa para reportá-los como potencialmente perigosos.

- ***Reporte arquivos contendo macros*** – uma macro é uma seqüência predefinida de etapas com o objetivo de executar certas tarefas mais fáceis para um usuário (macros do MS Word são amplamente conhecidas). Como tal, uma macro pode conter instruções potencialmente perigosas e convém você marcar a caixa para garantir que os arquivos com macros sejam reportados como suspeitos.

- ***Reporte extensões ocultas –*** extensões ocultas podem fazer um arquivo executável suspeito, "alguma coisa.txt.exe", por exemplo, parecer-se com um arquivo de texto comum inofensivo "alguma coisa. txt". Marque a caixa para reportá-los como potencialmente perigosos.

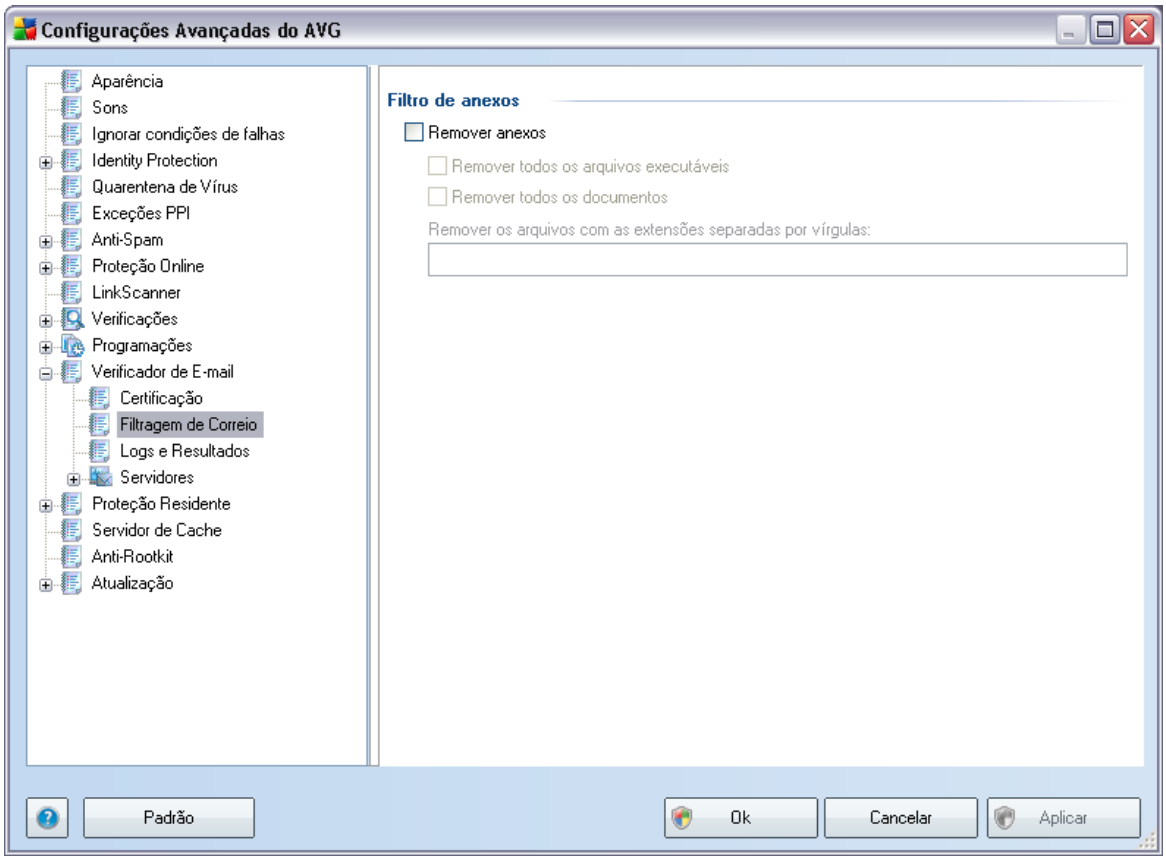
- ***Mover anexos de e-mail informados para a área de Quarentena*** - especifique se você deseja ser notificado por e-mail sobre arquivos protegidos por senha, documentos protegidos por senha, arquivos contendo macros e/ou arquivos com extensão oculta detectados como um anexo de uma mensagem de e-mail verificada. Se uma mensagem desse tipo for identificada durante a verificação, defina se o objeto infectado detectado deve ser movido para a ***Quarentena***.

10.10.1. Certificação



Na caixa de diálogo ***Certificação*** é possível especificar o texto que a nota de certificação deve conter e em que idioma. Essa especificação deve ser separada para as ***Mensagens recebidas*** e ***Mensagens enviadas***.

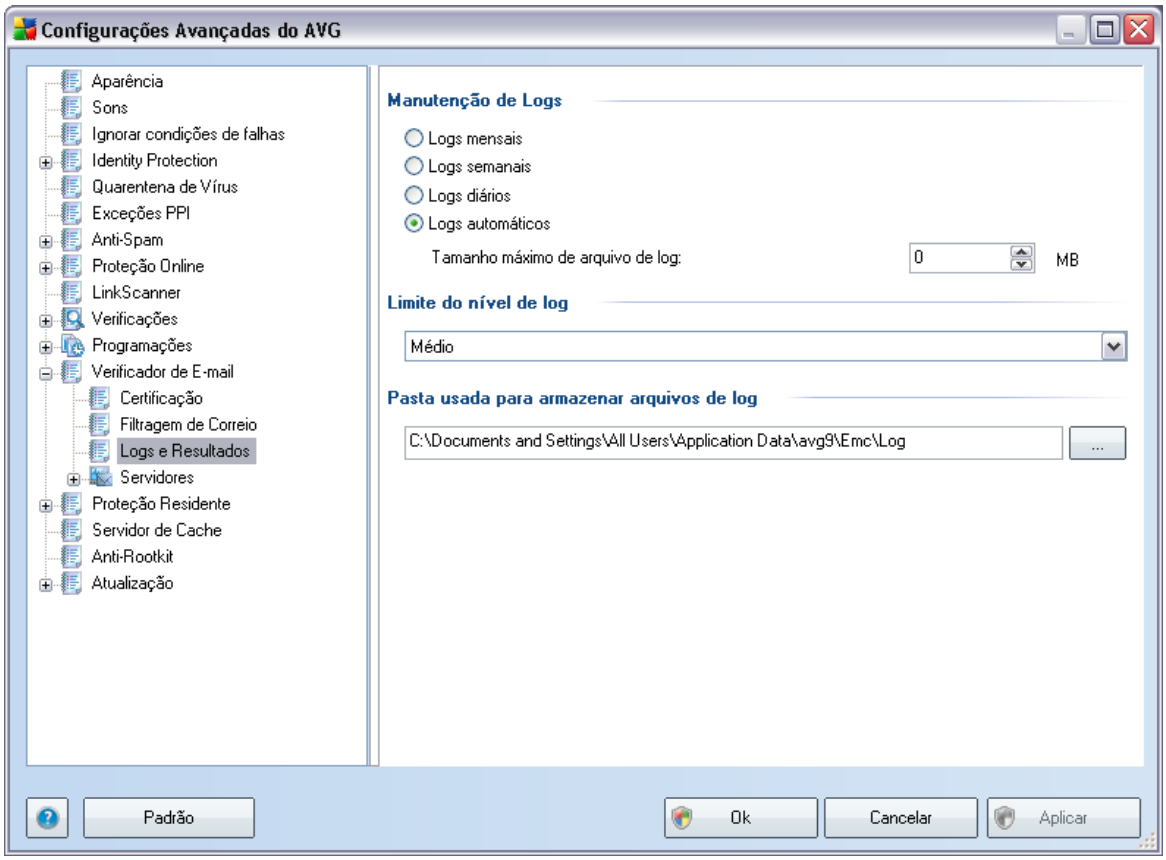
10.10.2. Filtragem de correio



A caixa de diálogo ***Filtro de anexo*** permite configurar parâmetros para a verificação de anexos de mensagens de e-mail. Por padrão, a opção ***Remover anexos*** é desativada. Se você desejar ativá-la, todos anexos de mensagens de e-mail detectados como infectados ou potencialmente perigosos serão removidos automaticamente. Se você desejar especificar os tipos de anexo que devem ser removidos, selecione a opção apropriada:

- ***Remover todos os arquivos executáveis*** - todos os arquivos *.exe serão excluídos.
- ***Remover todos os documentos*** - todos os arquivos *.doc, *.docx, *.xls, *.xlsx serão excluídos.
- ***Remover arquivos com extensões separadas por vírgulas*** - removerá todos os arquivos com as extensões definidas.

10.10.3. Logs e resultados

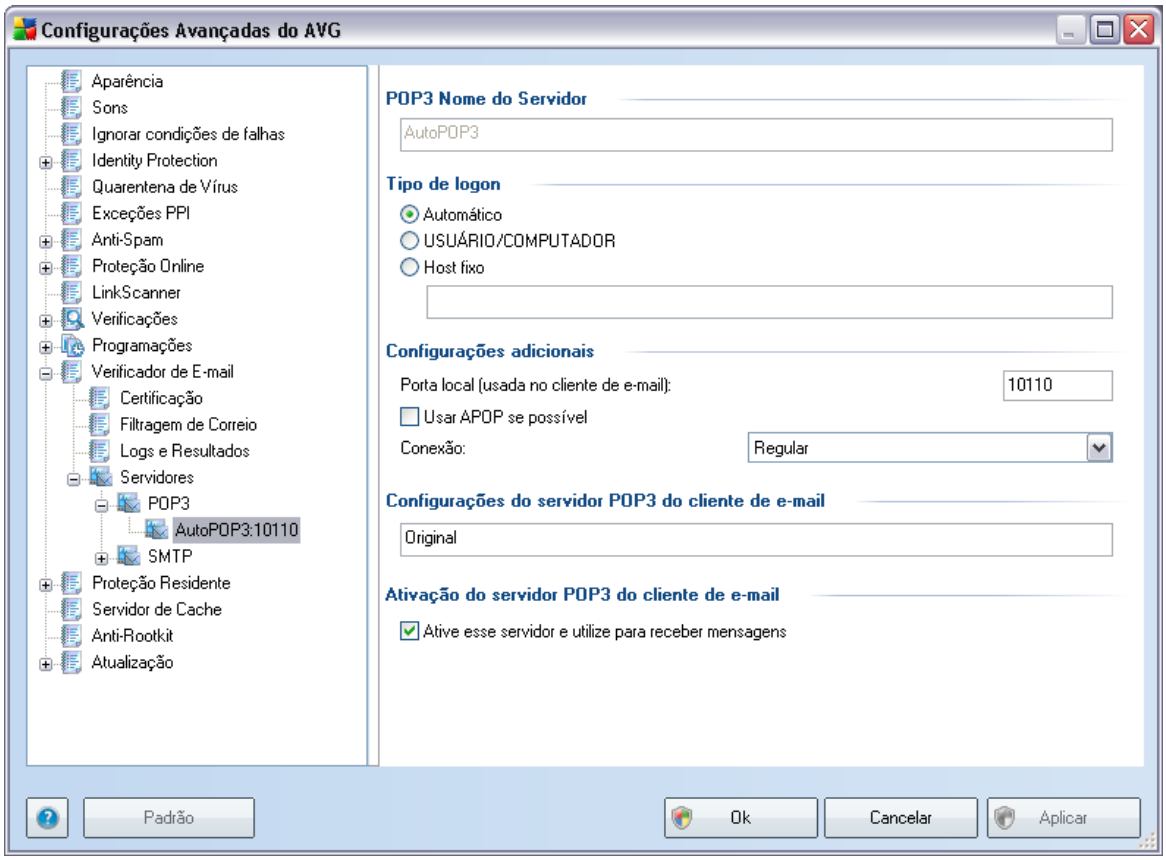


A caixa de diálogo aberta pelo item de navegação ***Logs e Resultados*** permite especificar os parâmetros para a manutenção dos resultados da verificação de e-mail. A janela de diálogo divide-se em várias seções:

- ***Manutenção dos Logs*** - defina se você deseja registrar as informações de verificação de e-mail diariamente, semanalmente, mensalmente etc e especifique o tamanho máximo do arquivo de log (*em MB*)
- ***Limite do nível de log*** - o nível médio é definido por padrão. Você pode definir um nível mais baixo (*registrando informações de conexão elementares*) ou o mais alto (*registrando todo o tráfego*)
- ***Pasta usada para armazenar arquivos de log*** - define onde o arquivo de log deve ser localizado

10.10.4. Servidores

Na seção ***Servidores*** , você pode editar os parâmetros de servidores do componente ***Verificador de E-mail*** ou configurar um novo servidor usando o botão ***Adicionar novo servidor***.



Nessa caixa de diálogo (aberta via ***Servidores/POP3***), você pode configurar um novo servidor do ***Verificador de E-mail*** usando o protocolo POP3 para e-mails recebidos.

- ***Nome do Servidor POP3*** - digite o nome do servidor ou mantenha o nome padrão AutoPOP3
- ***Tipo de login*** - define o método para determinar o servidor de e-mail usado para e-mails recebidos:
    - ***Automático*** - o login será feito automaticamente, de acordo com as

configurações do cliente de e-mail.

- ***USUÁRIO/COMPUTADOR*** - o método mais simples e mais freqüentemente usado para determinar o servidor de e-mail de destino é o método de proxy. Para usá-lo, especifique o nome ou o endereço (ou também a porta) como parte do nome do usuário de login para o servidor de e-mail especificado, separando-os com o caractere /. Por exemplo, para a conta usuário1 no servidor pop.acme.com e a porta 8200, use usuário1/pop.acme.com:8200 como nome de login.

- ***Host fixo*** - nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mail. O nome de login permanecerá inalterado. Para um nome, você pode usar um nome de domínio (por exemplo, pop.acme.com), assim como um endereço IP (por exemplo, 123.45.67.89). Se o servidor de e-mail usar uma porta não padrão, você poderá especificar essa porta depois do nome do servidor usando um ponto-e-vírgula como delimitador (por exemplo, pop.acme:8200). A porta padrão para a comunicação POP3 é 110.

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

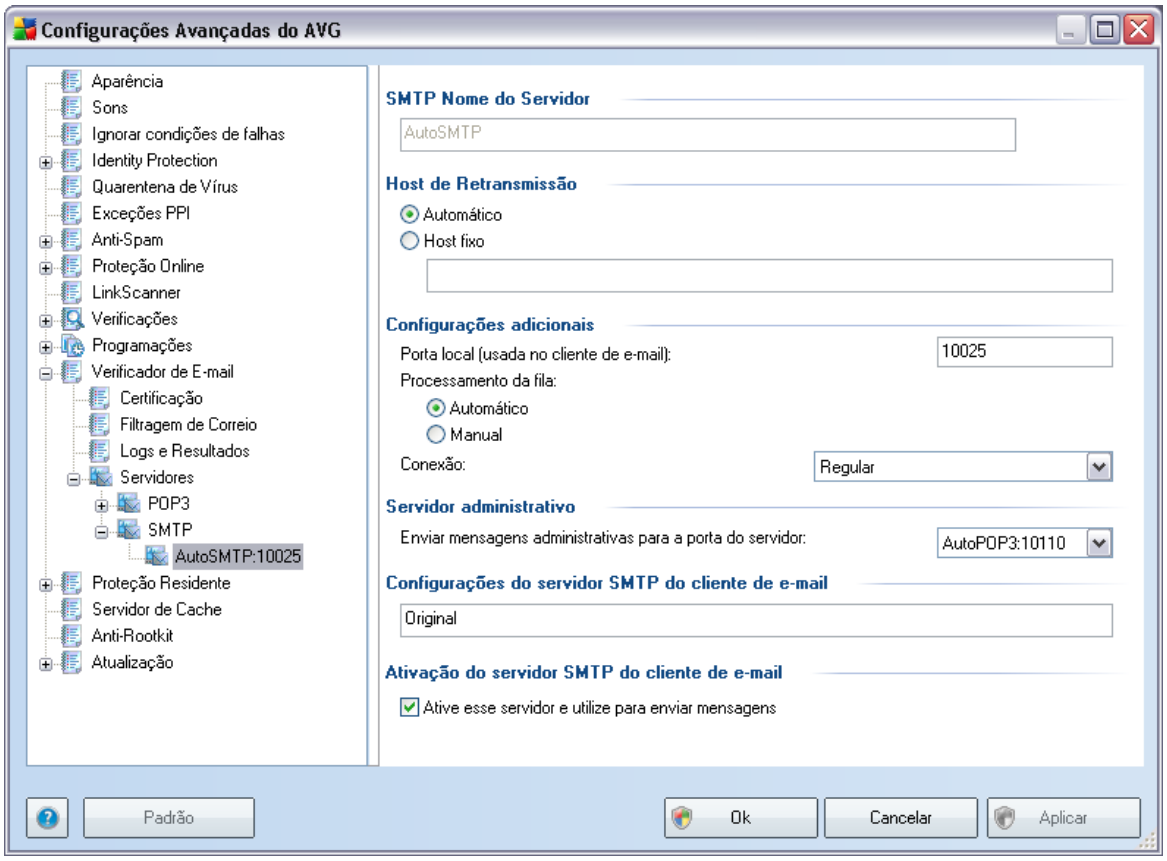
  - ***Porta local*** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação POP3.

  - ***Usar APOP quando disponível*** - essa opção fornece login de servidor de e-mail mais seguro Isso garante que o ***Verificador de E-mail*** usará um método alternativo para encaminhar a senha da conta de usuário para login, enviando a senha para o servidor em um formato criptografado, e não aberto, por meio de uma cadeia variável recebida do servidor. Naturalmente, esse recurso estará disponível somente quando houver suporte no servidor de e-mail de destino.

  - ***Conexão*** - no menu suspenso, é possível especificar o tipo de conexão que será usada (regular/SSL/SSL padrão). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso estará disponível somente quando houver suporte no servidor de e-mail de destino.

- ***Configurações do servidor POP3 do cliente de e-mail*** - fornece informações resumidas sobre as configurações necessárias para configurar corretamente o cliente de e-mail (de forma que o ***Verificador de E-mail*** verifique todos os e-mails recebidos). Esse é um resumo baseado nos parâmetros correspondentes especificados nesta caixa de diálogo e em outras caixas de diálogo relacionadas.

- ***Ativação do servidor POP3 do cliente de e-mail*** - marque/desmarque esse item para ativar ou desativar o servidor POP3 especificado



Nessa caixa de diálogo (aberta via ***Servidores/SMTP***), você pode configurar um novo servidor do ***Verificador de E-mail*** usando o protocolo SMTP para mensagens enviadas:

- ***Nome do Servidor SMTP -*** digite o nome do servidor ou mantenha o nome padrão AutoSMTP
- ***Host de Retransmissão -*** define o método para determinar o servidor de e-mail usado para o e-mail de saída:
    - ***Automático*** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail

- **_Host fixo_** - nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mails. Você pode usar um nome de domínio (por exemplo, smtp.acme.com), assim como um endereço IP (por exemplo, 123.45.67.89) para um nome. Se o servidor de e-mail usar uma porta não padrão, você poderá digitar essa porta depois do nome do servidor usando dois pontos como delimitador (por exemplo, smtp.acme:8200). A porta padrão para a comunicação SMTP 25 é.

- **_Configurações adicionais_** - especifica parâmetros mais detalhados:

  - **_Porta local_** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação SMTP.

  - **_Processamento da fila_** - determina o comportamento do **_Verificador de e-mail_** ao processar os requisitos para envio de mensagens de e-mail:

    - Automático – os e-mails de saída são imediatamente enviados ao servidor de e-mail de destino

    - Manual - a mensagem é inserida na fila de saída de mensagens e enviada depois

  - **_Conexão_** - no menu suspenso, é possível especificar o tipo de conexão que será usada (regular/SSL/SSL padrão). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso está disponível somente quando houver suporte no servidor de e-mail de destino.

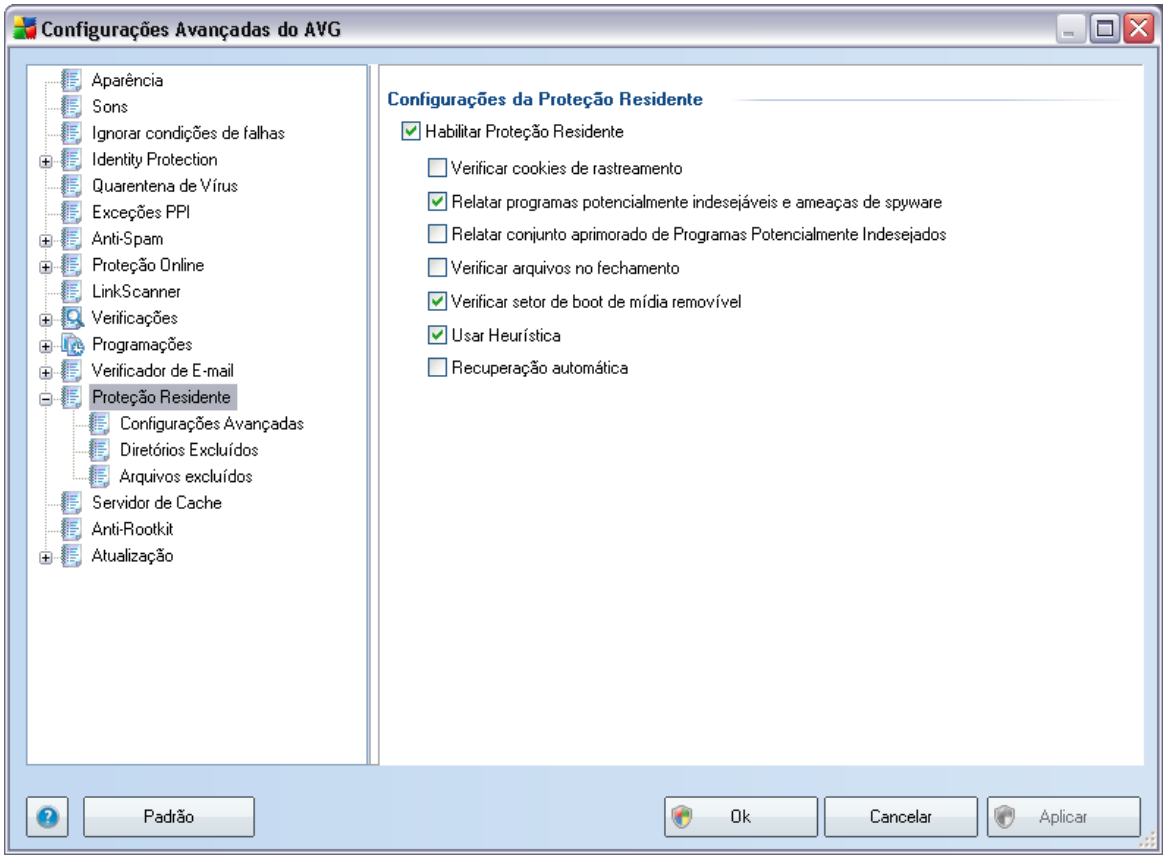
- **_Servidor administrativo_** - mostra o número de porta do servidor que será usada para a entrega reversa dos relatórios de administração. Essas mensagens são geradas, por exemplo, quando o servidor de e-mail de destino rejeita a mensagem enviada ou quando esse servidor de e-mail não está disponível.

- **_A seção Configurações do servidor SMTP do cliente de e-mail_** - apresenta informações sobre como configurar o aplicativo de e-mail cliente de forma que as mensagens de e-mail enviadas sejam verificadas com o uso do servidor atualmente modificado para exame dos e-mails enviados. Esse é um resumo baseado nos parâmetros correspondentes especificados nesta caixa de diálogo e em outras caixas de diálogo relacionadas.

- **_Ativação do servidor SMTP do cliente de e-mail_** - marque/desmarque esse item para ativar ou desativar o servidor SMTP especificado

10.11. Proteção Residente

O componente ***Proteção Residente*** realiza a proteção em tempo real contra vírus, spywares e outros malwares em arquivos e pastas.



Na caixa de diálogo ***Configurações da Proteção Residente*** , é possível ativar ou desativar a ***Proteção Residente*** completamente marcando/desmarcando o item ***Habilitar Proteção Residente*** (*essa opção é ativada por padrão*). Além disso, você pode selecionar quais recursos da ***Proteção Residente*** devem ser ativados:

- ***Verificar cookies de rastreamento*** - esse parâmetro define que os cookies devem ser detectados durante a verificação. (*Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas*)
- ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar***

spyware, bem como vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar arquivos no fechamento*** - a verificação durante o fechamento garante que o AVG verifique objetos ativos (por exemplo, aplicativos, documentos etc.) quando eles estiverem sendo abertos e também quando estiverem sendo fechados. Esse recurso ajuda a proteger o computador contra alguns tipos de vírus sofisticados.

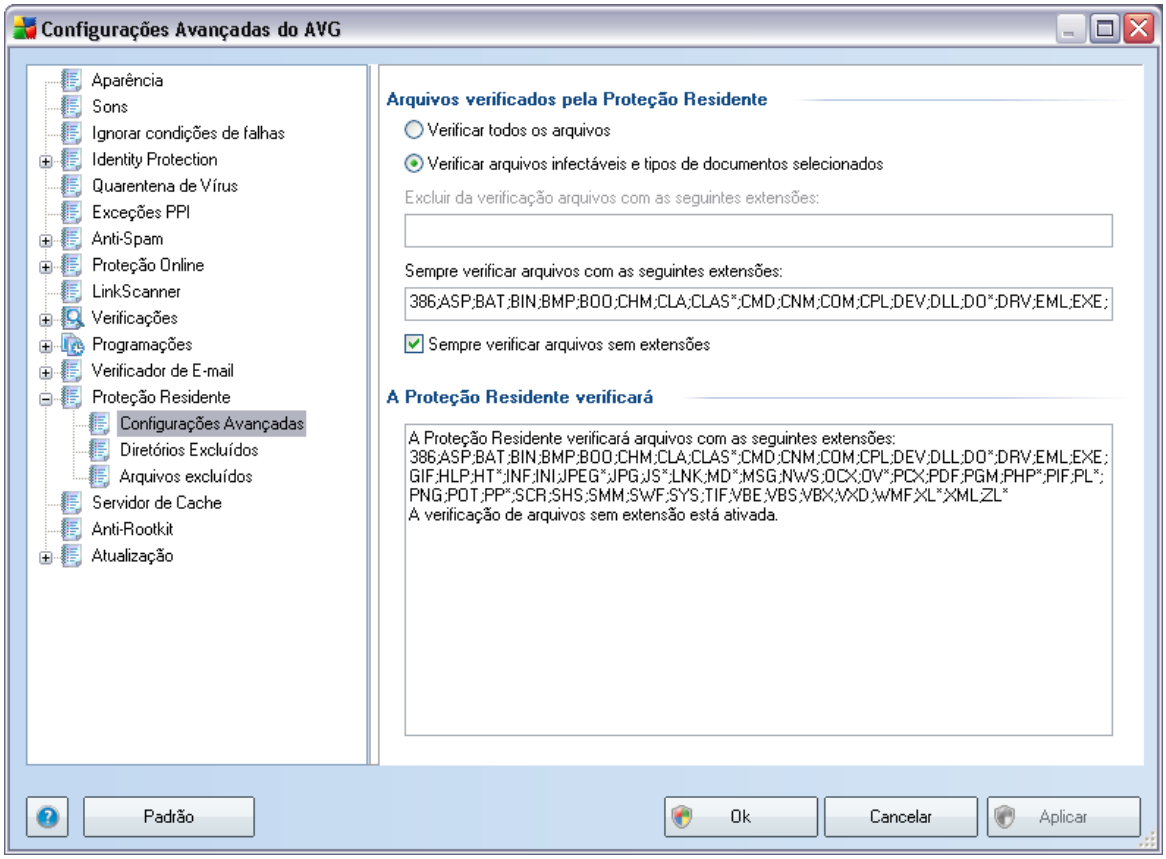
- ***Verificar setor de inicialização de mídia removível*** - (*ativado por padrão*)

- ***Usar Heurística*** - (*ativado por padrão*) a análise heurística será usada para detecção (*emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual*).

- ***Reparo automático*** - todas as infecções detectadas serão reparadas automaticamente, se houver solução disponível

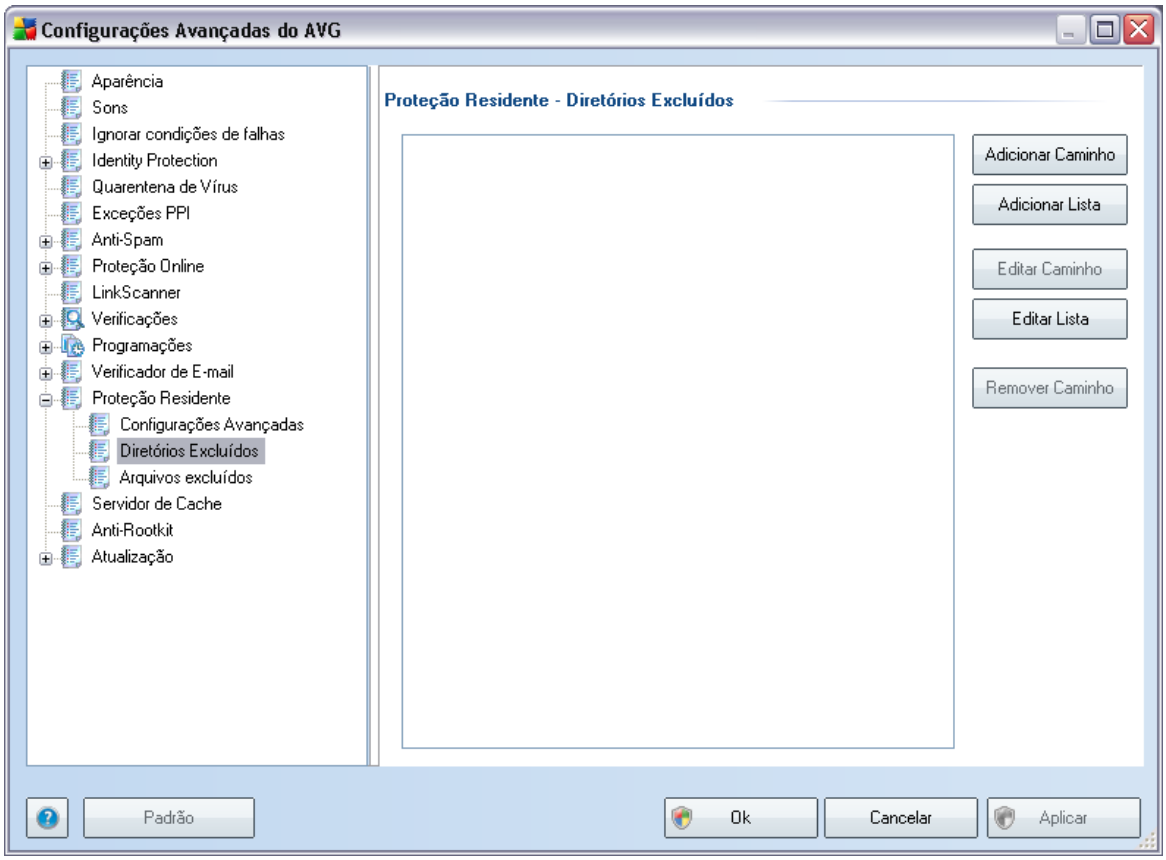
10.11.1. Configurações Avançadas

Na caixa de diálogo ***Arquivos verificados pela Proteção Residente***, é possível configurar os arquivos que serão verificados (*por extensão específica*):



Decida se deseja que todos os arquivos sejam verificados ou apenas os infectáveis. Nesse caso, você poderá especificar uma lista de extensões definindo arquivos que devem ser excluídos da verificação, assim como uma lista de extensões de arquivo que definam arquivos que devam ser verificados em todas as circunstâncias.

10.11.2. Exclusões de diretórios



A caixa de diálogo ***Proteção Residente - Exclusões de Diretório*** oferece a possibilidade de definir as pastas que devem ser excluídas da verificação da ***Proteção Residente***.

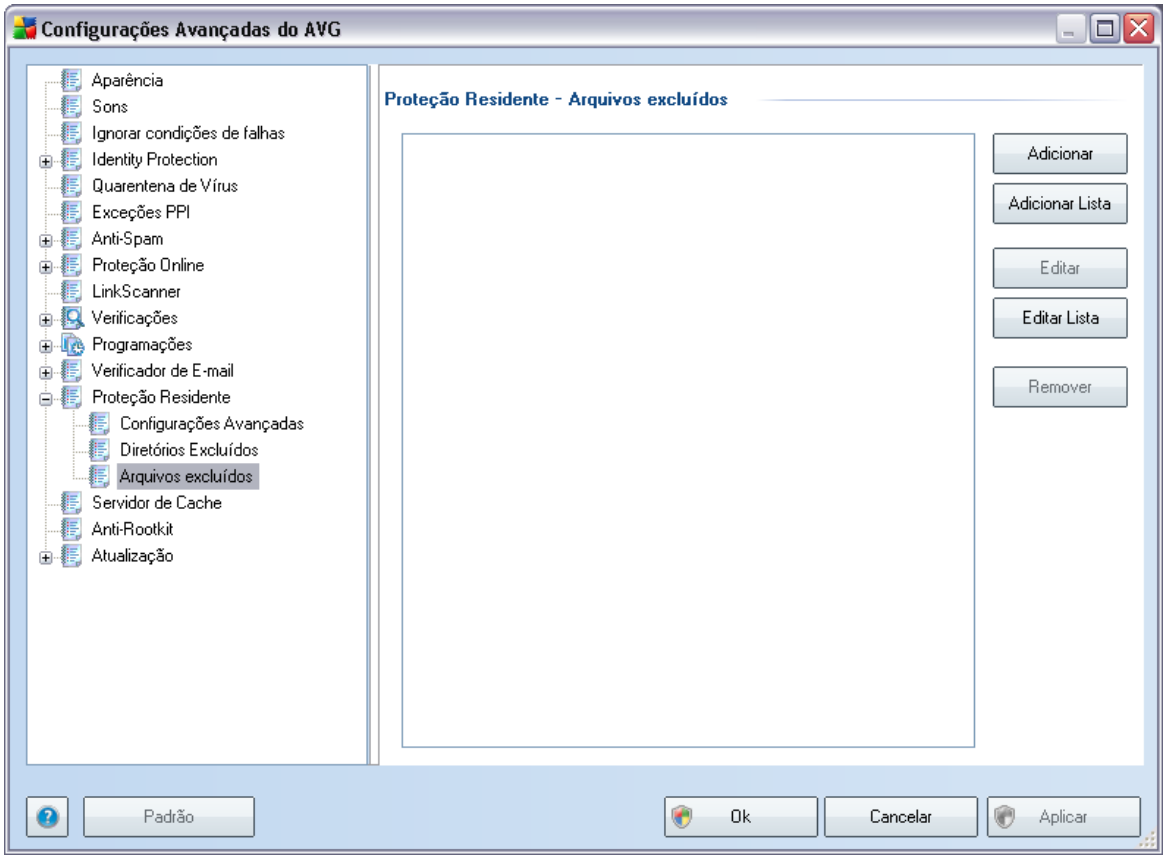
Se isto não for necessário, é altamente recomendável não excluir nenhum diretório.

Essa caixa de diálogo fornece os seguintes botões de controle:

- ***Adicionar caminho*** - permite especificar os diretórios a serem excluídos da verificação, selecionando-os um a um, na árvore de navegação do disco local.
- ***Adicionar Lista*** - permite digitar a lista inteira de diretórios a serem excluídos da verificação da ***Proteção Residente***.

- ***Editar Caminho*** - permite editar o caminho especificado para uma pasta selecionada.
- ***Editar Lista*** - permite editar a lista de pastas
- ***Remover caminho*** - permite excluir o caminho para uma pasta selecionada da lista

10.11.3. Arquivos excluídos



A caixa de diálogo ***Proteção Residente - Arquivos excluídos*** tem um comportamento idêntico ao da caixa de diálogo ***Proteção Residente - Exclusões de diretórios*** previamente descrita. Porém, em vez de pastas, você pode agora definir arquivos específicos que devem ser excluídos da verificação da ***Proteção Residente.***

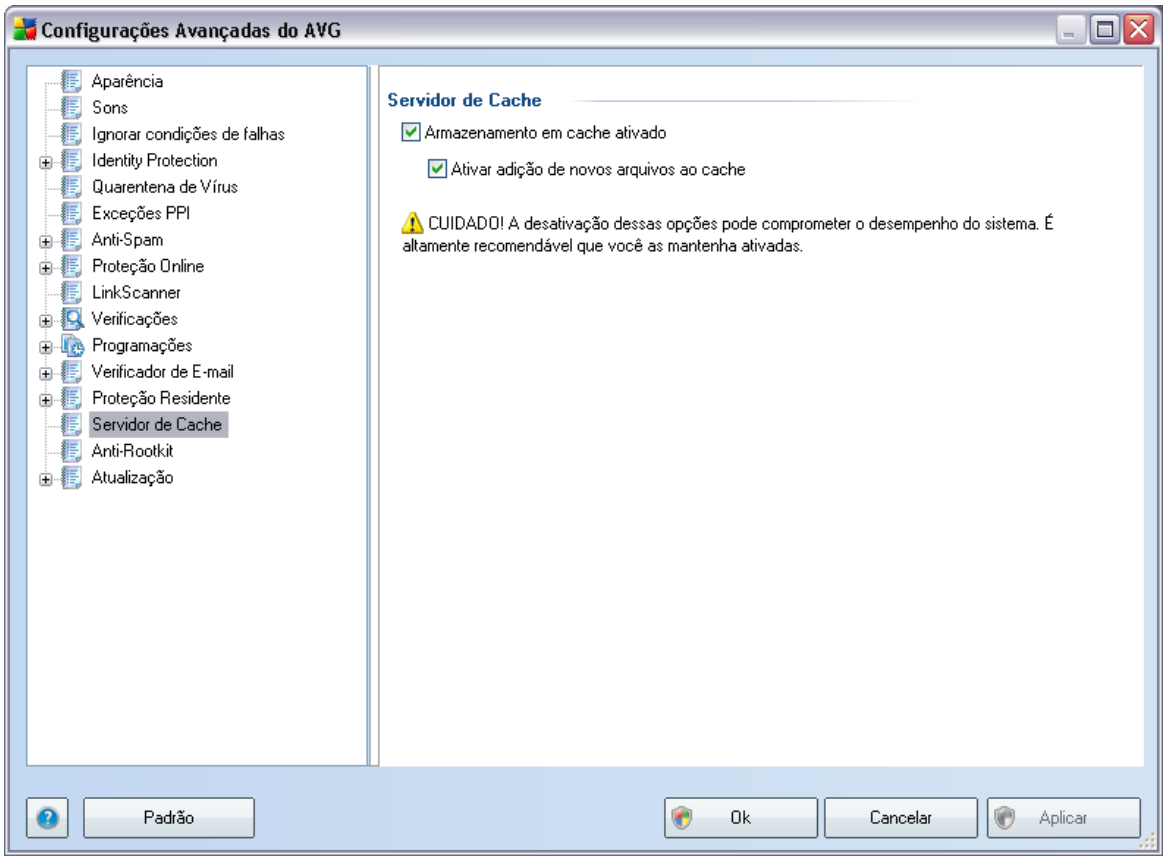
Se isso não for necessário, é altamente recomendável não excluir nenhum arquivo.

Essa caixa de diálogo fornece os seguintes botões de controle:

- ***Adicionar*** - especifique arquivos a serem excluídos da verificação, selecionando-os um a um na árvore de navegação do disco local
- ***Adicionar Lista*** - permite digitar a lista inteira de arquivos a serem excluídos da verificação da ***Proteção Residente***.
- ***Editar*** - permite editar o caminho especificado para um arquivo selecionado
- ***Editar Lista*** - permite editar a lista de arquivos
- ***Remover*** - permite excluir o caminho para um arquivo selecionado da lista

10.12. Servidor de Cache

O ***Servidor de cache*** é um processo designado para acelerar qualquer verificação (*verificação sobre demanda, verificação programada total do computador, verificação da Proteção Residente*. Coleta e mantém informações de arquivos confiáveis (*arquivos de sistema com assinatura digital, etc.*): Esses arquivos são ignorados pelo mecanismo de verificação.



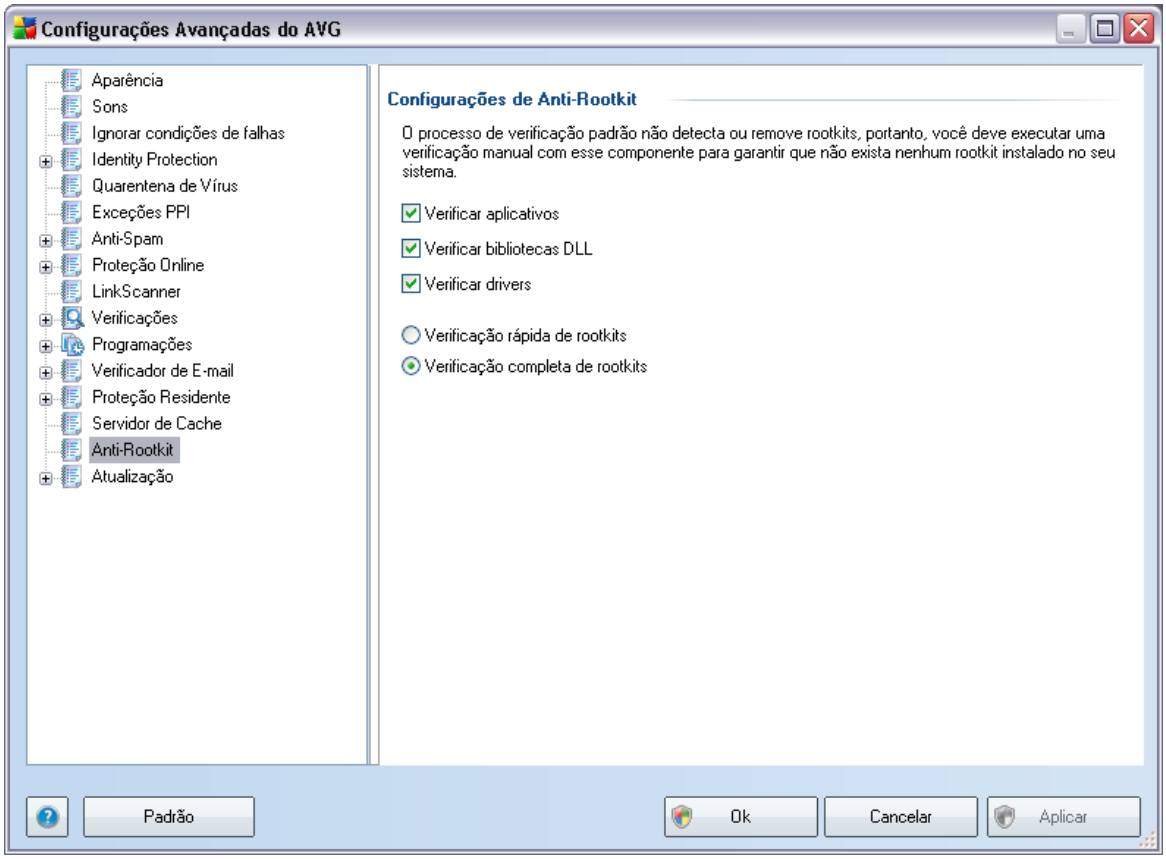
A caixa de diálogo configurações oferece duas opções:

- ***Caching ativado*** (*ativado por padrão*) - desmarque a caixa para desativar o ***Servidor de Cache*** e esvaziar a memória de cache. Observe que a verificação pode desacelerar, e o desempenho global de computador diminuir, conforme é feita a verificação de todos os arquivos únicos em uso procurando primeiro pela existência de vírus e spyware.

- ***Ativar inclusão de novos arquivos em cache*** (*ativado por padrão*) - desmarque a caixa para parar de adicionar mais arquivos na memória cache. Todos os arquivos já armazenados em cache serão mantidos e utilizados até que o cache seja desativado completamente, ou até a próxima atualização do banco de dados de vírus.

10.13. Anti-Rootkit

Nesta caixa de diálogo você pode editar a configuração do componente ***Anti-Rootkit***:



A edição de todas as funções do componente ***Anti-Rootkit***conforme oferecido nesta caixa de diálogo também está acessível diretamente na ***interface do componente Anti-Rootkit***.

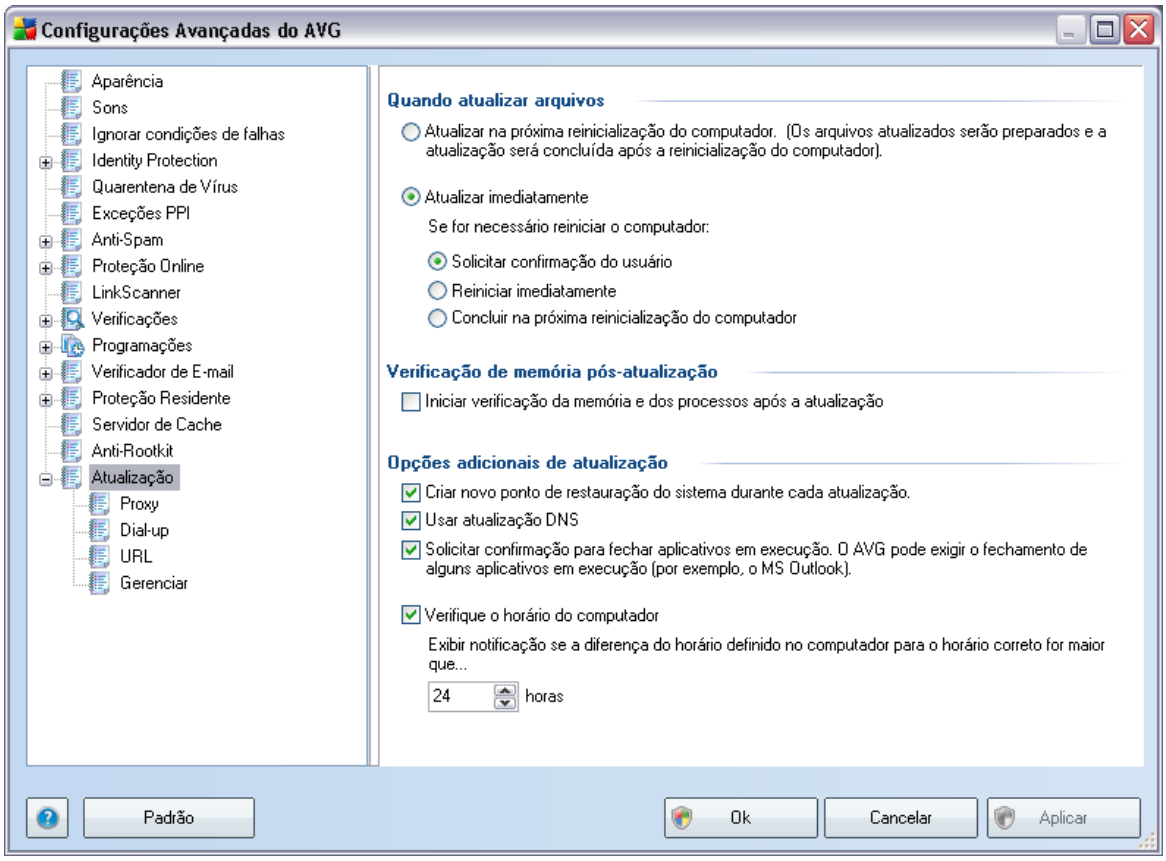
Marque as respectivas caixas de seleção para especificar objetos que devem ser verificados:

- ***Verificar aplicativos***
- ***Verificar bibliotecas DLL***
- ***Verificar drivers***

Em seguida, você pode selecionar o modo de verificação do rootkit:

- ***Verificação rápida do rootkit*** - verifica todos os processos em execução, unidades carregadas e pasta do sistema (*tipicamente c:\Windows*)
- ***Verificação completa do rootkit*** - verifica todos os processos em execução, unidades carregadas, a pasta do sistema (*tipicamente c:\Windows*além de todos os discos locais (*incluindo o disco flash, mas excluindo as unidades de CD/disquete*)

10.14. Atualizar



O item de navegação ***Atualizar*** abre uma nova caixa de diálogo, onde é possível especificar parâmetros gerais relativos à atualização do AVG:

Quando atualizar arquivos

Nessa seção você pode selecionar duas alternativas: a atualização pode ser programada para a próxima reinicialização do PC ou você pode iniciar a atualização imediatamente. Por padrão, a opção de atualização imediata é selecionada, pois dessa forma o AVG pode proteger com o nível de segurança máximo. A programação de uma atualização para a próxima reinicialização do PC só pode ser recomendada se você estiver certo de que o computador é reiniciado regularmente, pelo menos diariamente.

Se você decidir manter a configuração padrão e inicializar o processo de atualização imediatamente, poderá especificar as circunstâncias sob as quais uma possível reinicialização necessária será realizada:

- ***Requer confirmação do usuário*** - você será solicitado a aprovar a reinicialização do PC necessária para finalizar o processo de atualização.
- ***Reiniciar imediatamente*** - o computador será reiniciado automaticamente após a conclusão do processo de atualização e sua aprovação não será necessária.
- ***Concluir na próxima reinicialização do computador*** - a finalização do processo de atualização será adiada até a próxima reinicialização do computador. Novamente, tenha em mente que essa opção só é recomendada se você tiver certeza que o computador será reiniciado regularmente, pelo menos diariamente

Verificação de memória pós-atualização

Marque essa caixa de seleção para definir que deseja iniciar uma nova verificação de memória depois de cada atualização concluída com êxito. A atualização mais atual baixada pode conter novas definições de vírus, e estas devem ser aplicadas à verificação imediatamente.

Opções adicionais de atualização

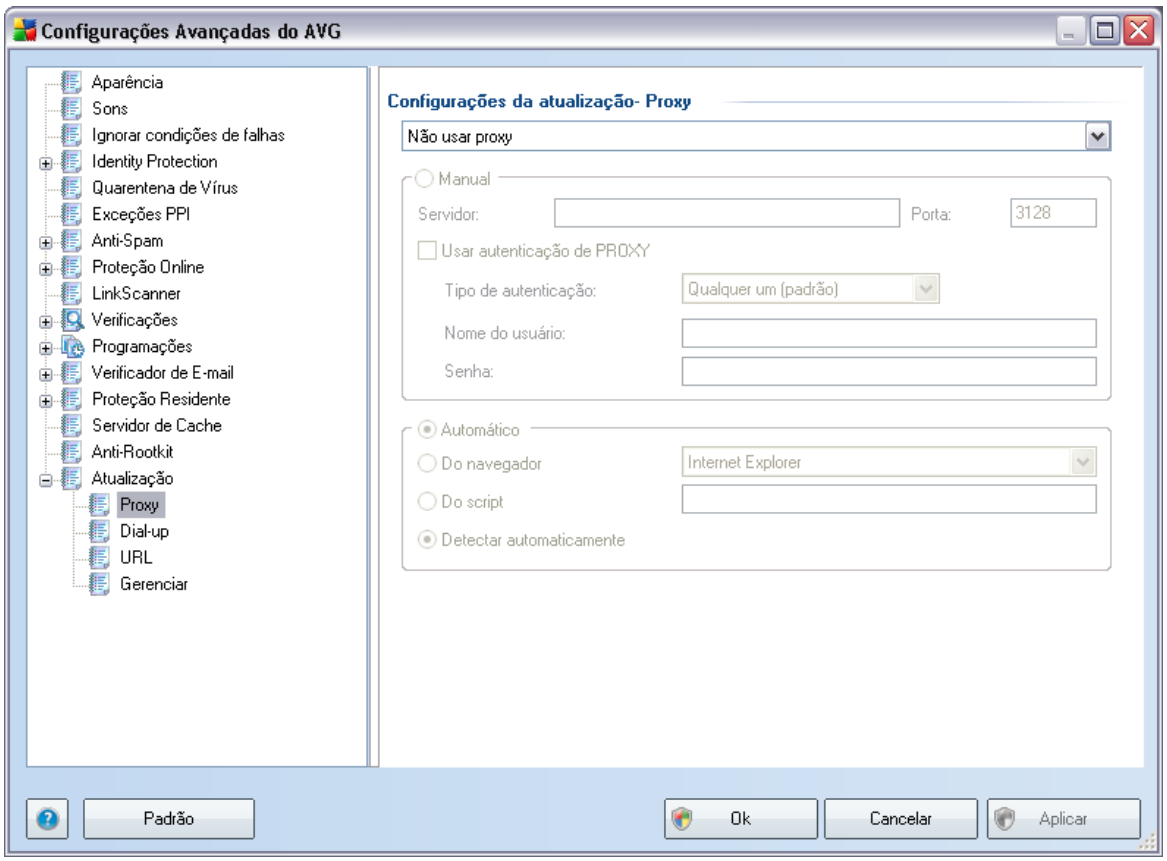
- ***Criar novo ponto de restauração do sistema após cada atualização do programa*** - após cada ativação da atualização do programa AVG, um ponto de restauração do sistema é criado. No caso de falha no processo de atualização e seu sistema operacional, você pode restaurar o seu SO para a configuração original deste ponto. Esta opção está disponível em Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauração do Sistema, mas quaisquer alterações podem ser recomendadas apenas para usuários experientes! Mantenha esta caixa de seleção marcada se quiser usar o recurso.

- ***Usar atualização DNS*** - marque esta caixa de seleção para confirmar que você deseja usar o método de detecção de arquivos de atualização que elimina a quantidade de dados transferidos entre o servidor de atualização e o cliente AVG;

- ***O Requer confirmação para fechar aplicativos em execução*** (*ativado por padrão*) ajudará você a se certificar de que nenhum aplicativo em execução no momento será fechado sem a sua permissão - se necessário para a conclusão do processo de atualização;

- ***Marcar o horário definido do computador*** - marque esta opção para declarar que você deseja que seja exibida uma notificação caso o horário do computador seja diferente do horário correto em um número de horas maior que o especificado.

10.14.1. Proxy



O servidor proxy é um servidor autônomo ou um serviço executado em um PC que

garante conexão segura à Internet. De acordo com as regras de rede especificadas, você poderá acessar a Internet diretamente ou por meio do servidor proxy; as duas possibilidades também podem ser permitidas ao mesmo tempo. Em seguida, no primeiro item da caixa de diálogo ***Configurações da Atualização - Proxy*** , você deverá selecionar o menu da caixa de combinação, se desejar:

- ***Usar proxy***
- ***Não usar servidor proxy***- configurações padrão
- ***Tentar conectar usando proxy e, se falhar, conectar diretamente***

Se você selecionar uma opção usando o servidor proxy, terá que especificar alguns outros dados. As configurações do servidor podem ser definidas manualmente ou automaticamente.

Configuração manual

Se você selecionar a configuração manual (selecione a opção *Manual* ***para ativar a seção apropriada da caixa de diálogo****)*, terá que especificar os seguintes itens:

- ***Servidor***– especifique o endereço IP do servidor ou o nome do servidor.
- ***Porta*** - especifique o número da porta que permite o acesso à Internet (por padrão, esse número está definido como 3128, mas pode ser definido de forma diferente - *se não tiver certeza, entre em contato com o administrador da rede*).

O servidor proxy também pode ter configurado regras especificas para cada usuário. Se o servidor proxy estiver configurado dessa forma, selecione a opção ***Usar autenticação PROXY*** para verificar se o nome de usuário e a senha são válidos para conexão à Internet por meio do servidor proxy.

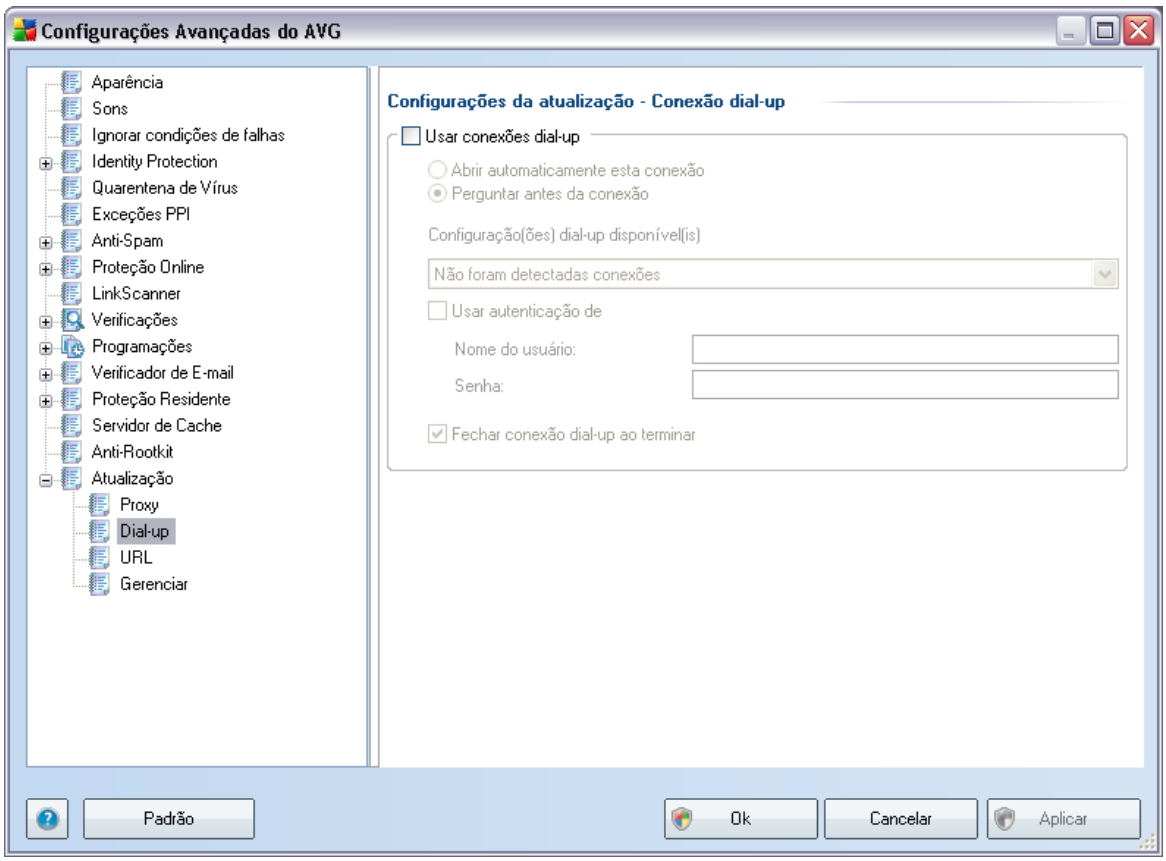
Configuração automática

Se você selecionar configuração automática (*marque a opção Automática* ***para ativar a seção da caixa de diálogo apropriada****)*, selecione de onde a configuração do proxy deve ser realizada:

- ***A partir do navegador*** - a configuração será lida a partir do navegador da Internet padrão

- ***Do script*** - a configuração será lida de um script de download com a função retornando o endereço proxy
- ***Detecção automática*** - a configuração será detectada de forma automática e direta do servidor proxy

10.14.2. Dial-up

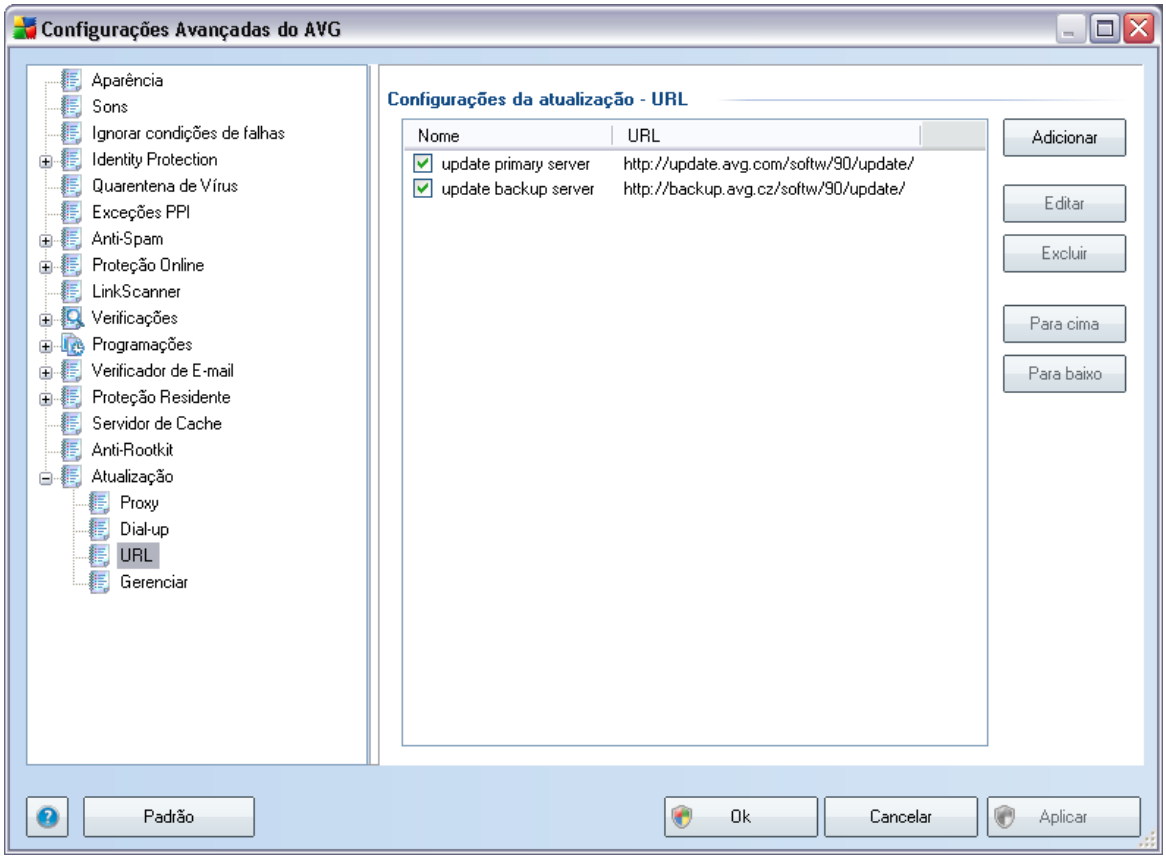


Todos os parâmetros definidos opcionalmente na caixa de diálogo ***Atualizar configurações - Conexão dial-Up*** referem-se à conexão discada à Internet. Os campos da guia estarão inativos até que a opção ***Usar conexões dial-up***, que ativará os campos, esteja marcada.

Especifique se você deseja se conectar à Internet automaticamente (***Abrir esta conexão automaticamente***) ou se deseja confirmar a conexão manualmente, todas as vezes (***Perguntar antes da conexão***). Para conexão automática, você poderá decidir se a conexão deve ser fechada após o término da atualização (***Fechar***

conexão dial-up ao terminar).

10.14.3. URL



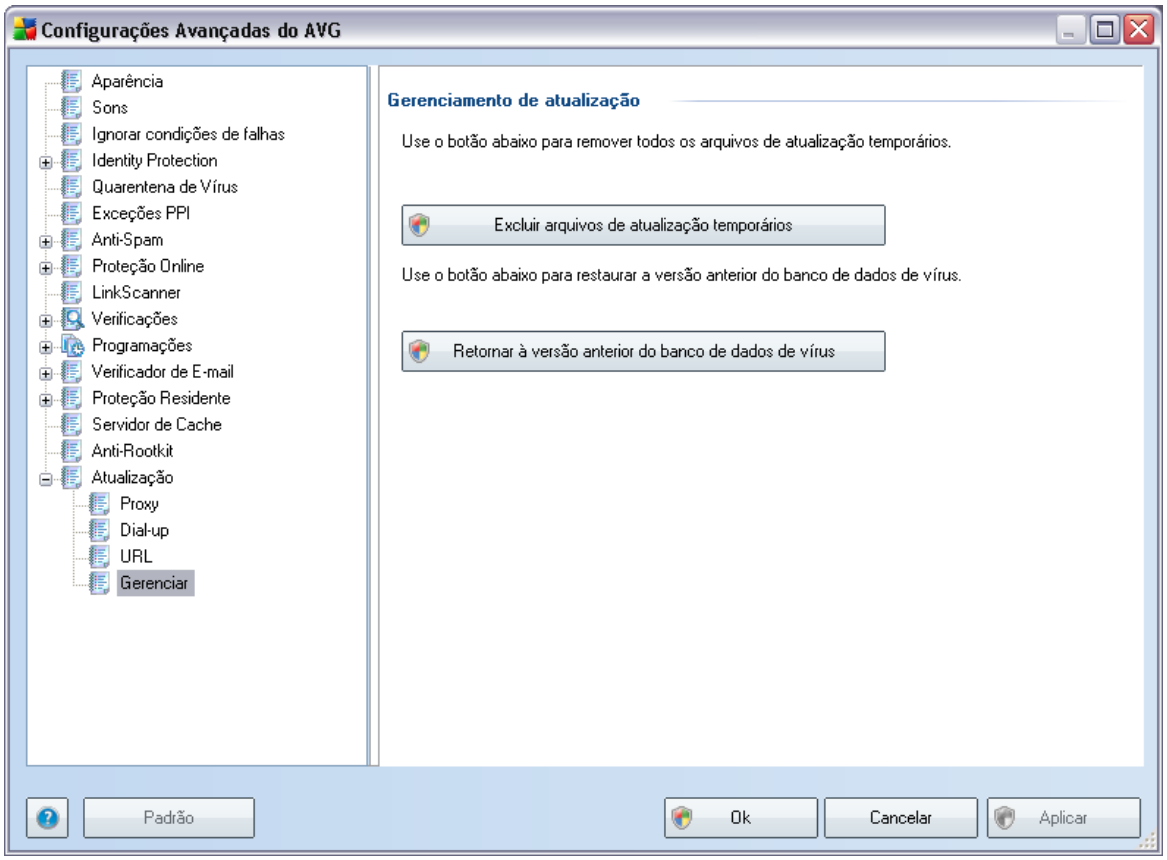
A caixa de diálogo ***URL*** oferece uma lista de endereços da Internet, de onde você poderá baixar os arquivos de atualização. A lista e os itens podem ser modificados por meio dos seguintes botões de controle:

- ***Adicionar***- abre uma janela de diálogo onde você especificará a nova URL a ser adicionada à lista
- ***Editar*** – abre uma janela de diálogo, onde você poderá editar os parâmetros da URL selecionada
- ***Excluir*** - exclui a URL selecionada da lista
- ***Mover para Cima*** -move a URL selecionada uma posição acima na lista

- ***Mover para Baixo*** – move a URL selecionada uma posição abaixo na lista.

10.14.4. Gerenciar

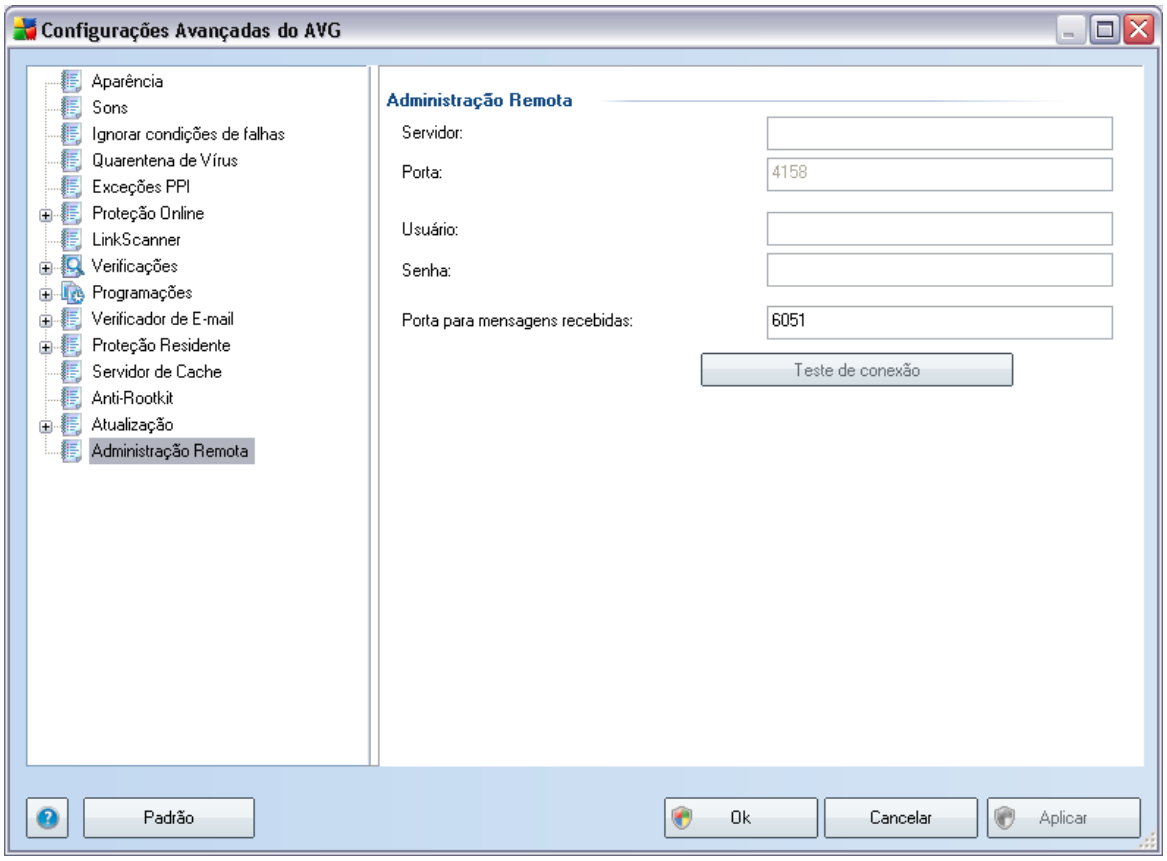
A caixa de diálogo ***Gerenciar*** oferece duas opções acessíveis via dois botões:



- ***Excluir arquivos de atualização temporários*** - pressione este botão para excluir todos os arquivos de atualização redundantes do seu disco rígido (*por padrão, eles são armazenados por 30 dias*)

- ***Retornar banco de dados de vírus para a versão anterior*** –pressione este botão para excluir a versão mais recente da base de vírus do seu disco rígido e retornar à versão salva anteriormente (*a nova versão da base de vírus fará parte da próxima atualização*)

10.15. Administração Remota



A configuração ***Administração Remota*** se refere à conexão da estação do cliente AVG ao sistema de administração remota. Se você planeja conectar a estação apropriada à administração remota, especifique os seguintes parâmetros:

- ***Servidor*** - nome do servidor (ou endereço IP do servidor) em que o AVG Admin Server está instalado
- ***Porta*** - fornece o número da porta em que o cliente do AVG se comunica com o AVG Admin Server (*o número da porta 4158 é considerado padrão. Se você usá-lo, não terá que especificá-lo explicitamente*)
- ***Login*** - se a comunicação entre o cliente AVG e o AVG Admin Server for definida como segura, forneça o nome de usuário ...
- ***Senha*** - ... e a senha

- ***Porta para mensagens recebidas*** - número da porta em que o cliente AVG aceita mensagens recebidas do AVG Admin Server

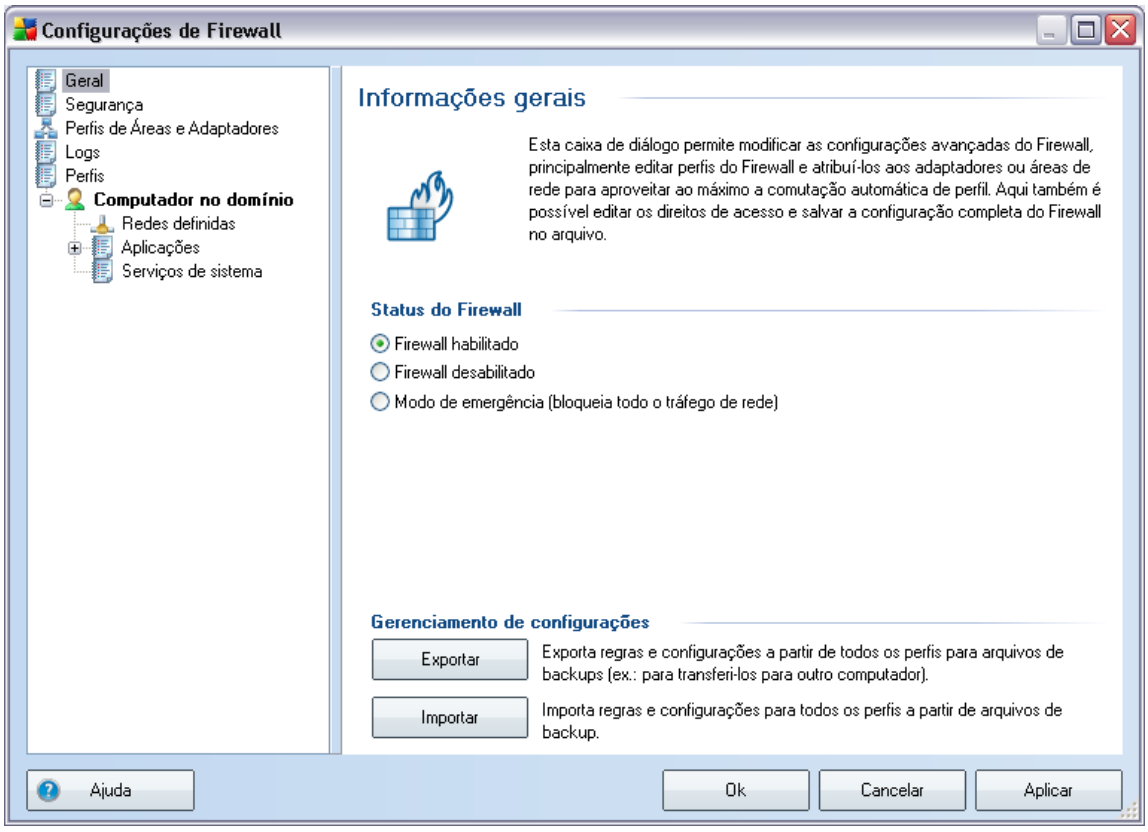
O botão ***Testar conexão*** ajuda você a verificar que todos os dados mencionados acima são válidos e podem ser usados para conectar com sucesso ao DataCenter.

Nota: *para obter uma descrição detalhada sobre a administração remota, consulte a documentação do AVG Network Edition.*

11. Configurações de Firewall

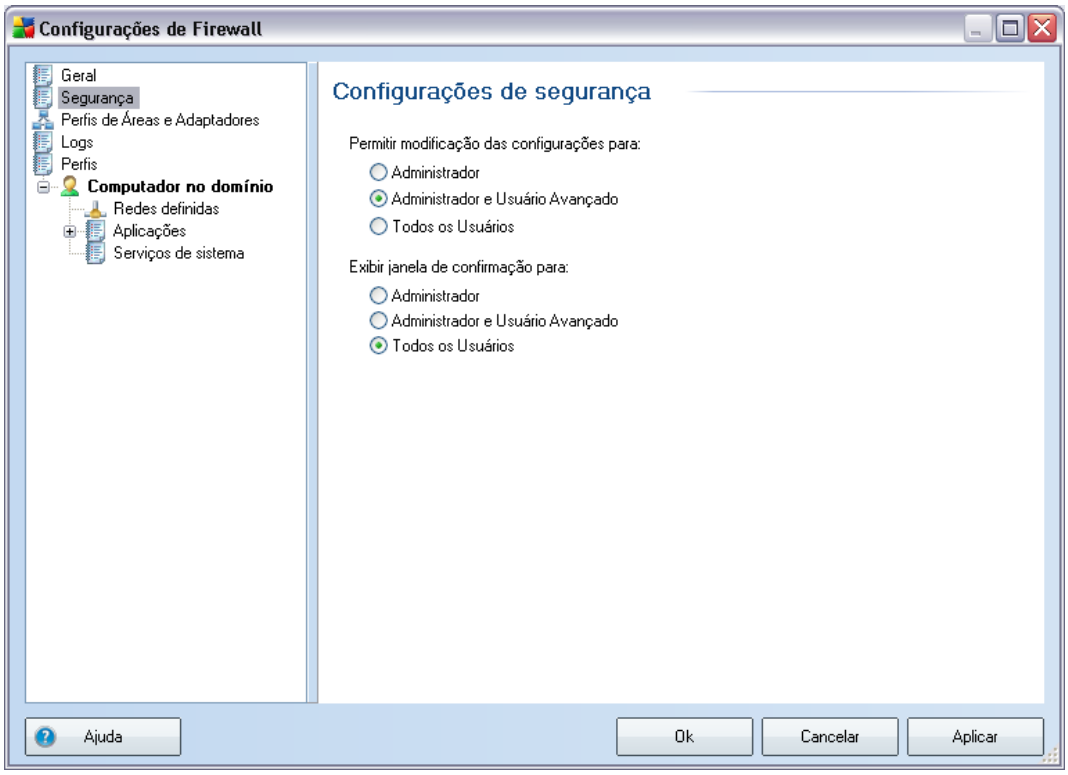
A configuração do ***Firewall*** é aberta em uma nova janela com várias caixas de diálogo para configuração de parâmetros avançados do componente. ***Entretanto, a edição da configuração avançada destina-se apenas a usuários especialistas e experientes.***

11.1. Geral



Em ***Informações gerais***, você pode ***Exportar***/***Importar*** a configuração do ***Firewall***; ou seja, exportar as regras e as configurações de ***Firewall*** definidas para arquivos de back-up ou, por outro lado, importar o arquivo de back-up inteiro.

11.2. Segurança



Na caixa de diálogo ***Configurações de segurança***, é possível definir regras gerais de comportamento do ***Firewall*** independentemente do perfil selecionado:

- ***Permitir modificação de configurações*** - especifique quem tem permissão para alterar a configuração do ***Firewall***
- ***Mostrar a caixa de diálogo de confirmação*** - especifique para quem as caixas de diálogo de confirmação (*caixas de diálogo que solicitam uma decisão em situações não cobertas por uma regra definida do* ***Firewall***) devem ser exibidas

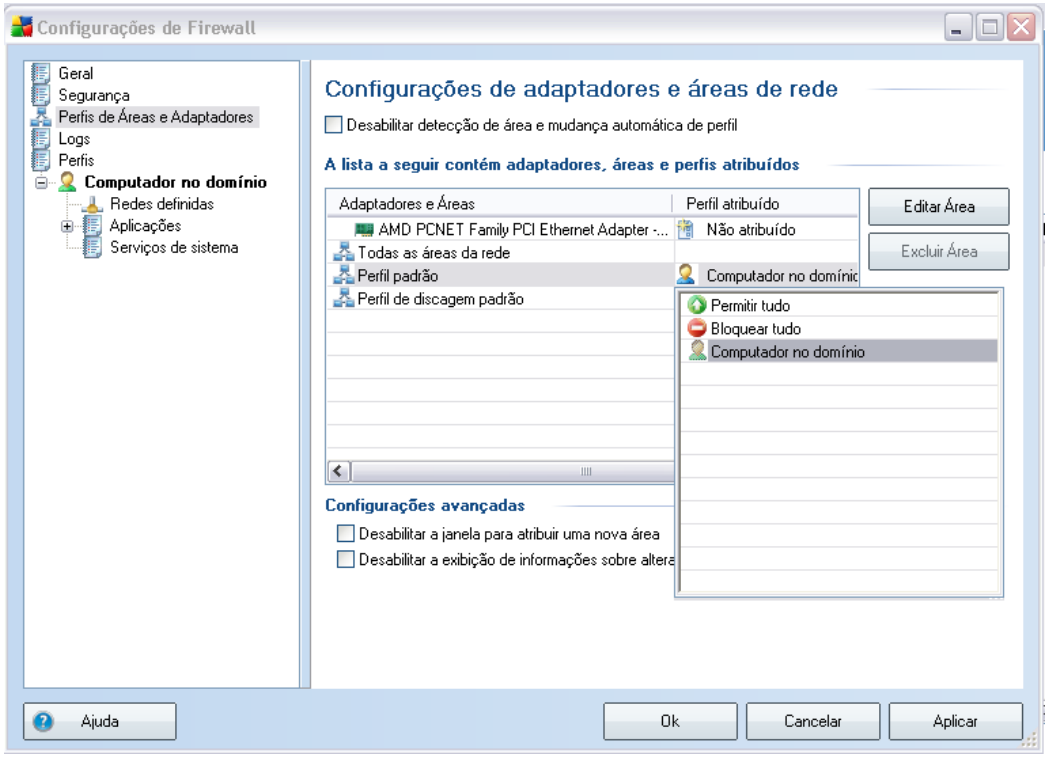
Nos dois casos, é possível atribuir o direito específico a um dos seguintes grupos de usuários:

- ***Administrador*** - controla totalmente o computador e tem o direito de atribuir cada usuário a grupos com permissões definidas especificamente

- ***Administradores e Usuários Avançados*** - o administrador pode atribuir qualquer usuário a um grupo especifico (*Usuários Avançados*) e definir permissões dos membros do grupo.

- ***Todos os Usuários*** - outros usuários não atribuídos a nenhum grupo específico.

11.3. Perfis de áreas e adaptadores



Nas caixas de diálogo ***Configurações de áreas de rede e adaptadores*** , é possível editar as configurações relacionadas à atribuição de perfis definidos a adaptadores específicos e respectivas redes:

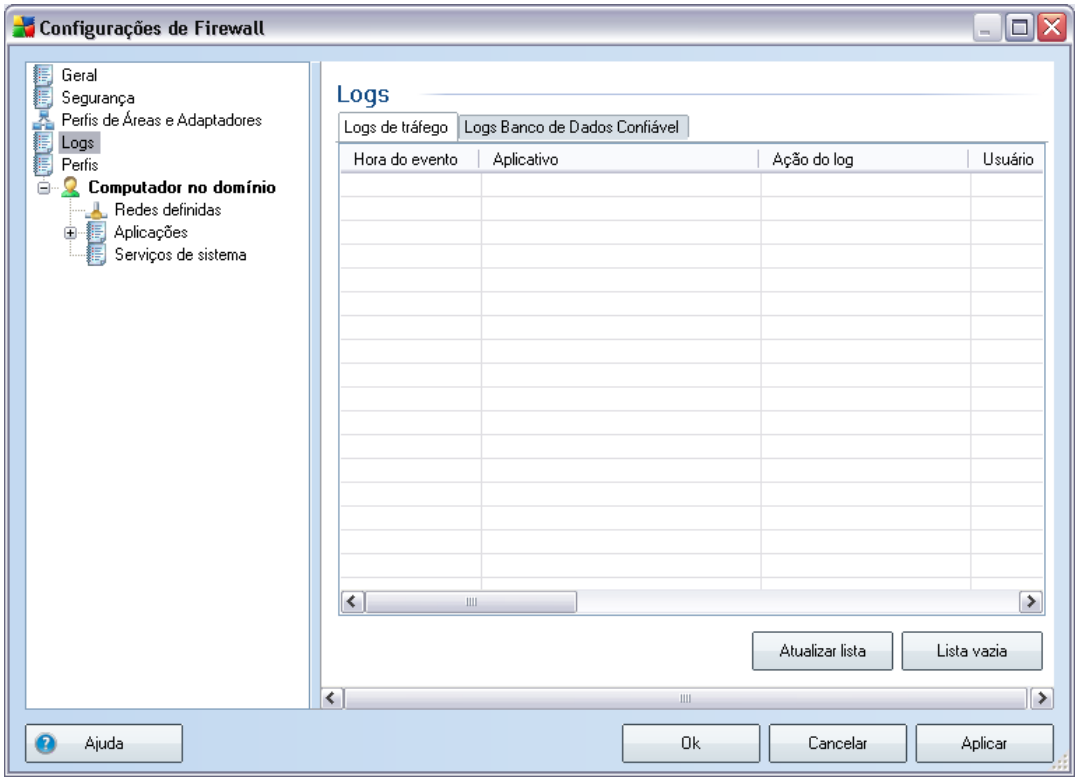
- ***Desativar detecção de área e troca automática de perfil*** - um dos perfis definidos pode ser atribuído a cada tipo de interface de rede, a cada área respectivamente. Se não quiser definir perfis específicos, será usado um perfil comum definido com base na sua seleção para uso do computador e design de rede do computador durante o ***Processo de instalação***. Entretanto, se você optar por especificar perfis e atribuí-los a determinados adaptadores e áreas e posteriormente, por algum motivo, quiser trocar esse esquema

temporariamente, marque a opção ***Desativar detecção de área e perfil automático***.

- ***Lista de adaptadores, áreas e perfis atribuídos*** - nesta lista, é possível encontrar uma visão geral de áreas e adaptadores detectados. Para cada um deles, é possível atribuir um perfil específico para o menu de perfis definidos. Para abrir esse menu, clique no respectivo item na lista de adaptadores e selecione o perfil.

- ***Configurações avançadas*** - marque a respectiva opção para desativar o recurso de exibição de mensagens de informação.

11.4. Logs



A caixa de diálogo ***Logs*** permite revisar a lista de todas as ações e eventos registrados do ***Firewall***, com uma descrição detalhada dos parâmetros relevantes (*horário do evento, nome do aplicativo, ação respectiva, nome do usuário, PID, direção do tráfego, tipo de protocolo, números das portas remotas e locais, etc.*) em duas guias:

- ***Logs de tráfego*** - oferece informações sobre atividades de todos os aplicativos que tentaram se conectar à rede.

- ***Logs do banco de dado confiável*** - *O banco de dado confiável* é um banco de dados interno do AVG que coleta informações sobre aplicativos certificados e confiáveis que sempre têm permissão para se comunicarem on-line. Da primeira vez que um novo aplicativo tentar se conectar à rede (*ou seja, quando ainda não houver uma regra de firewall especificada para esse aplicativo*), será necessário descobrir se a comunicação de rede deve ser permitida para o respectivo aplicativo. Em primeiro lugar, o AVG pesquisa o *Banco de dado confiável* e, se o aplicativo estiver listado, ele receberá acesso automático à rede. Somente depois disso, desde que não haja informações sobre o aplicativo disponíveis no banco de dados, você será solicitado a especificar em uma caixa de diálogo à parte se deseja permitir que esse aplicativo acesse a rede.

Botões de controle

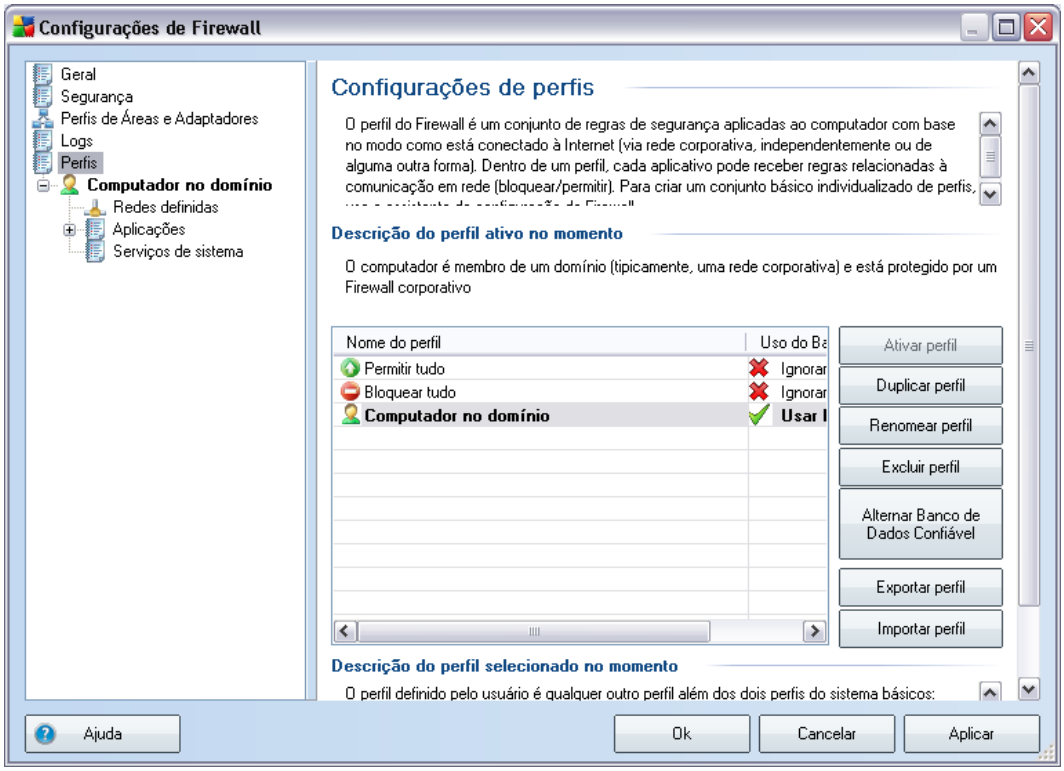
- ***Ajuda*** - abre a caixa de diálogo relacionada aos arquivos de ajuda.

- ***Atualizar lista***- todos os parâmetros registrados podem ser organizados de acordo com o atributo selecionado: cronologicamente (*datas*) ou alfabeticamente (*outras colunas*) - basta clicar no respectivo cabeçalho de coluna. Use o botão ***Atualizar lista*** para atualizar as informações exibidas no momento.

- ***Esvaziar lista*** - excluir todas as entradas na tabela.

11.5. Perfis

Na caixa de diálogo ***Configurações do perfil***, é possível encontrar uma lista de todos os perfis disponíveis.



Todos os demais perfis que não sejam de sistema podem ser editados nesta caixa de diálogo usando os seguintes botões de controle:

- ***Ativar perfil*** - este botão define o perfil selecionado como ativo, o que significa que a configuração do perfil selecionado será usada pelo ***Firewall*** para controlar o tráfego da rede
- ***Perfil duplicado*** - cria uma cópia idêntica do perfil selecionado; posteriormente, você poderá editar e renomear a cópia para criar um novo perfil baseado na cópia original duplicada
- ***Renomear perfil*** - permite definir um novo nome para um perfil selecionado
- ***Excluir perfil*** - exclui o perfil selecionado da lista

- ***Alternar banco de dados confiável*** - para o perfil selecionado, você pode optar por usar as informações do *Banco de dados confiável* (*o banco de dados confiável é um banco de dados interno do AVG que coleta dados sobre aplicativos confiáveis e certificados que sempre têm permissão de comunicação on-line.*)

- ***Exportar perfil*** - registra a configuração do perfil selecionado em um arquivo que será salvo para possível uso futuro

- ***Importar perfil*** - define as configurações do perfil selecionado com base nos dados exportados do arquivo de configuração de backup

- ***Ajuda*** - abre a caixa de diálogo relacionada ao arquivo de ajuda

Na seção inferior da caixa de diálogo, localize a descrição de um perfil atualmente selecionado na lista acima.

Com base no número de perfis definidos mencionados na lista da caixa de diálogo ***Perfil*** , a estrutura do menu de navegação à esquerda também muda. Cada perfil definido cria uma ramificação específica no item ***Perfil***. Os perfis específicos podem ser editados nas seguintes caixas de diálogo *, que são idênticas para todos os perfis*):

11.5.1. Informações do perfil

A caixa de diálogo ***Informações do perfil*** é a primeira caixa de diálogo de uma seção na qual é possível editar a configuração de cada perfil em caixas de diálogo separadas referentes a parâmetros específicos do perfil.

- ***Usar banco de dados confiável para este perfil*** - (*ativada por padrão*) marque a opção para ativar o *Banco de dados confiável* (*, ou seja, um banco de dados interno do AVG que coleta informações sobre aplicativos confiáveis e certificados que se comunicam on-line. Se ainda não houver uma regra especificada para o respectivo aplicativo, será necessário descobrir se esse aplicativo pode receber acesso à rede. O AVG pesquisa primeiro o Banco de dados confiável e, se o aplicativo estiver listado, ele será considerado seguro e terá permissão para se comunicar através da rede. Caso contrário, será solicitado que você decida se esse aplicativo deve receber permissão de comunicação na rede*) para o respectivo perfil

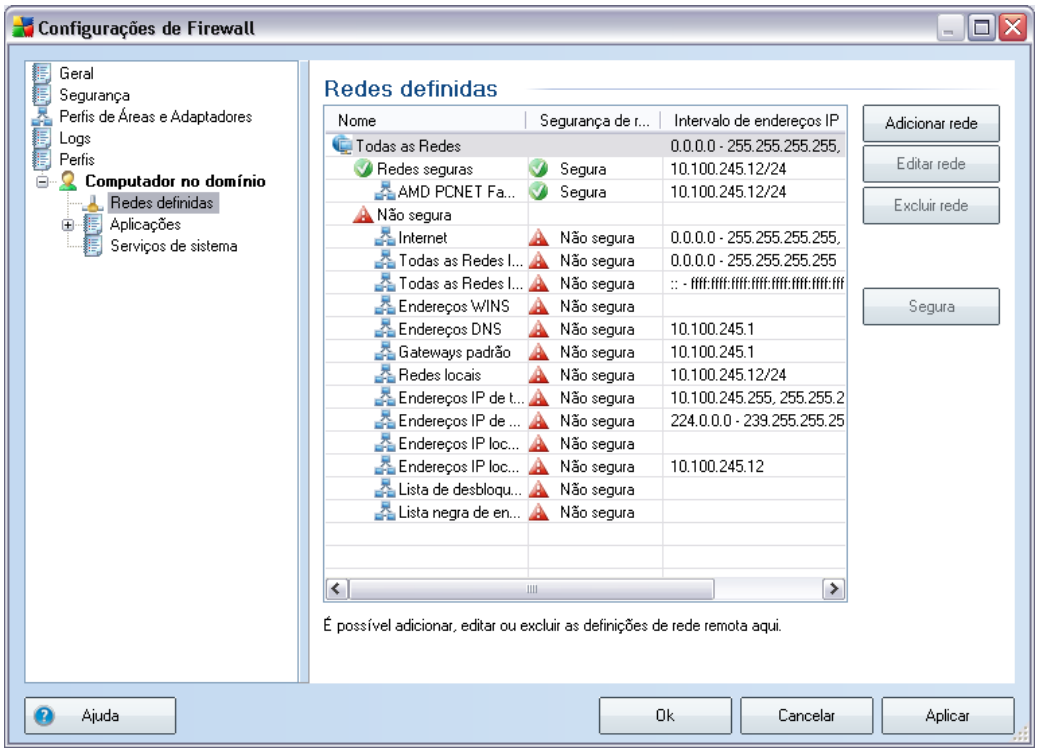
- ***Ativar rede de máquinas virtuais transpostas*** - (*desativada por padrão*) marque esse item para permitir que as máquinas virtuais no WMware se conectem diretamente à rede

Configurações de modo para jogos

Na seção ***Configurações de modo para jogos***, você pode decidir e confirmar marcando o respectivo item caso deseje exibir as mensagens de informação do ***Firewall*** durante a execução de um aplicativo em tela cheia no computador (*em geral, são jogos, mas podem ser utilizados em qualquer aplicativo de tela cheia, como apresentações em PPT*). Como as mensagens de informações podem ser um tanto quanto inconvenientes,

se você marcar o item ***Desativar notificações do Firewall durante a execução de jogos***, no menu suspenso, e depois selecionar que ação deve ser executada no caso de um aplicativo sem regras especificadas tentar se comunicar pela rede (*aplicativos que normalmente podem gerar uma caixa de diálogo de solicitação*), todos esses aplicativos poderão ser permitidos ou bloqueados.

11.5.2. Redes definidas



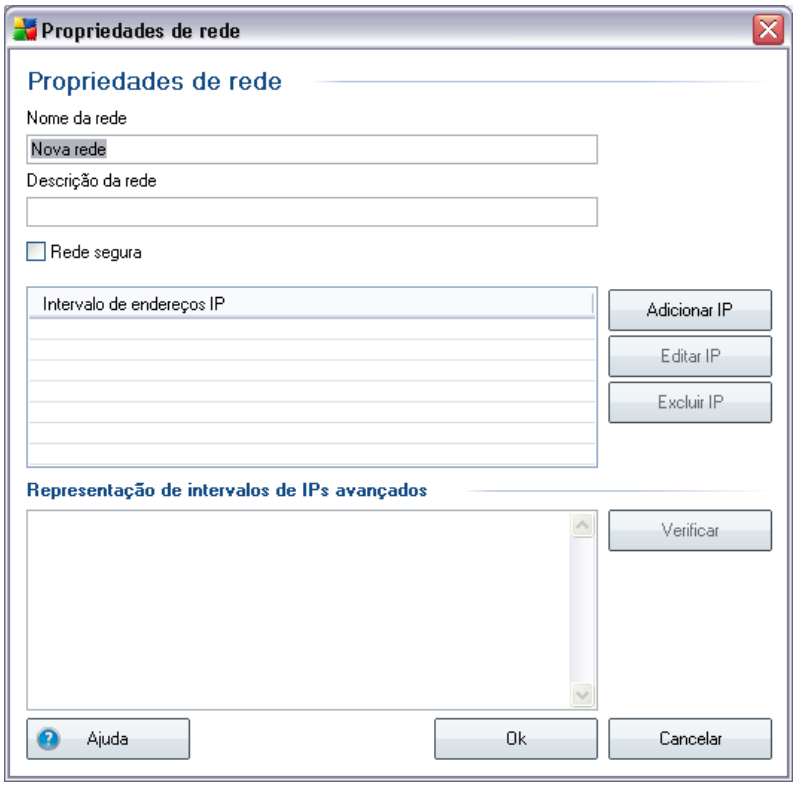
A caixa de diálogo ***Redes definidas*** oferece uma lista de todas as redes às quais seu computador está conectado. São fornecidas as informações a seguir em cada rede

detectada:

- ***Redes*** - lista de nomes de todas as redes às quais o computador está conectado
- ***Segurança de rede*** - por padrão, todas as redes são consideradas desprotegidas e somente se tiver certeza de que a respectiva rede é segura você poderá atribuí-la (*clique no item da lista referente à respectiva rede e selecione Seguro no menu de contexto*) - todas as redes seguras serão incluídas no grupo que pode se comunicar com o conjunto de regras do aplicativo para Permitir segurança
- ***Intervalo de endereços IP*** - cada rede será detectada automaticamente e especificada na forma de intervalo de endereços IP

Botões de controle

- ***Adicionar rede*** - abre a caixa de diálogo ***Propriedades de rede*** , na qual é possível editar parâmetros da nova rede definida:



Nessa caixa de diálogo, você pode especificar o ***Nome da rede***, fornecer a ***Descrição da rede*** e possivelmente atribuir a rede como segura. A nova rede pode ser definida manualmente em uma caixa de diálogo independente por meio do botão ***Adicionar IP*** (opcionalmente ***Editar IP*** / ***Excluir IP***); nessa caixa de diálogo você pode especificar a rede fornecendo o intervalo IP ou máscara.

Em um grande número de redes a serem definidas como parte da nova rede criada, é possível usar a opção ***Representação avançada do intervalo IP*** : digite a lista de todas as redes no respectivo campo de texto (*qualquer formato padrão é suportado*) e pressione o botão ***Verificar*** para ter certeza de que o formato pode ser reconhecido. Em seguida, pressione ***OK*** para confirmar e salvar os dados.

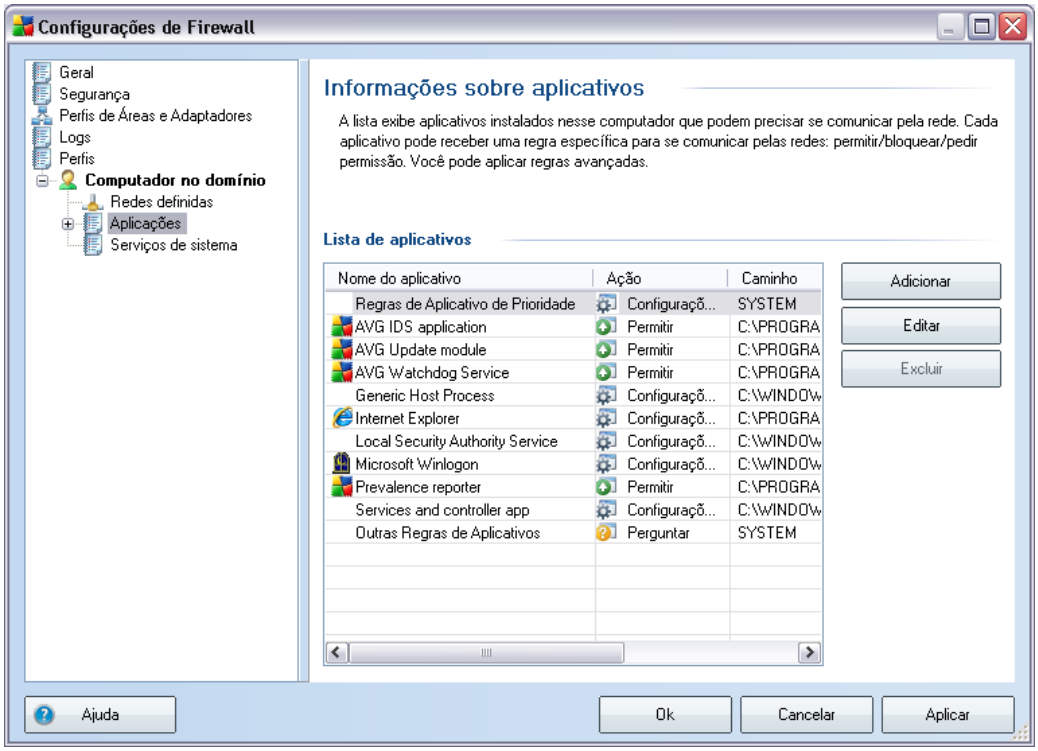
- ***Editar rede*** - abre a caixa de diálogo ***Propriedades da rede*** (*consulte acima*), na qual é possível editar parâmetros de uma rede já definida (*a caixa de diálogo é idêntica à caixa de diálogo de inclusão de nova rede; consulte a descrição no parágrafo anterior*)

- ***Excluir rede*** - remove a nota de uma rede selecionada da lista de redes

- ***Marcar como seguro -*** *por padrão, todas as redes são consideradas desprotegidas e somente se tiver certeza de que a respectiva rede é segura você poderá usar este botão para atribuí-la (e vice-versa, uma vez que a rede esteja atribuída como segura, o texto do botão muda para "Marcar como inseguro).*

- ***Ajuda*** - abre a caixa de diálogo relacionada ao arquivo de ajuda

11.5.3. Aplicativos



A caixa de diálogo Informações dos aplicativos ***lista todos os aplicativos que possam precisar se comunicar através da rede e ícones para a ação atribuída:***

- Permitir comunicação para todas as redes
- Permitir comunicação somente para redes definidas como Seguras
- Bloquear comunicação
- *Exibir caixa de diálogo de solicitação (o usuário poderá decidir no momento*

se deseja permitir ou bloquear a comunicação)

- Configurações avançadas definidas

Os aplicativos da lista foram detectados em seu computador (e a eles foram atribuídas as respectivas ações), durante a pesquisa do ***Assistente de configuração do Firewall*** ou, em caso de um aplicativo desconhecido ou instalado recentemente, posteriormente.

Nota: observe que somente um aplicativo já instalado pode ser detectado. Portanto, se você instalar um novo aplicativo posteriormente, será preciso definir regras de Firewall para esse. Por padrão, quando um novo aplicativo tenta se conectar através da rede pela primeira vez, o Firewall cria uma regra para esse automaticamente, de acordo com o Banco de dados confiável, ou pergunta se deseja permitir ou bloquear a comunicação. Neste último caso, você será capaz de salvar sua resposta como uma regra permanente (que será listada nesta caixa de diálogo).

É claro, você pode definir regras para o novo aplicativo imediatamente – nessa caixa de diálogo, pressione ***Adicionar*** e preencha os detalhes do aplicativo.

Além dos aplicativos, a lista também contém dois itens especiais:

- ***Regras prioritárias do aplicativo*** *(na parte superior da lista) são preferenciais e são aplicadas sempre antes das regras de qualquer aplicativo individual.*
- ***Outras regras de aplicativos*** *(na parte inferior da lista) são usadas como uma "última instância", quando não é aplicada nenhuma regra específica; por exemplo, para um aplicativo desconhecido e não definido.*

Esses itens têm diferentes opções de configuração em relação aos aplicativos comuns e são destinados somente a usuários experientes. Recomendamos fortemente que você não modifique as configurações

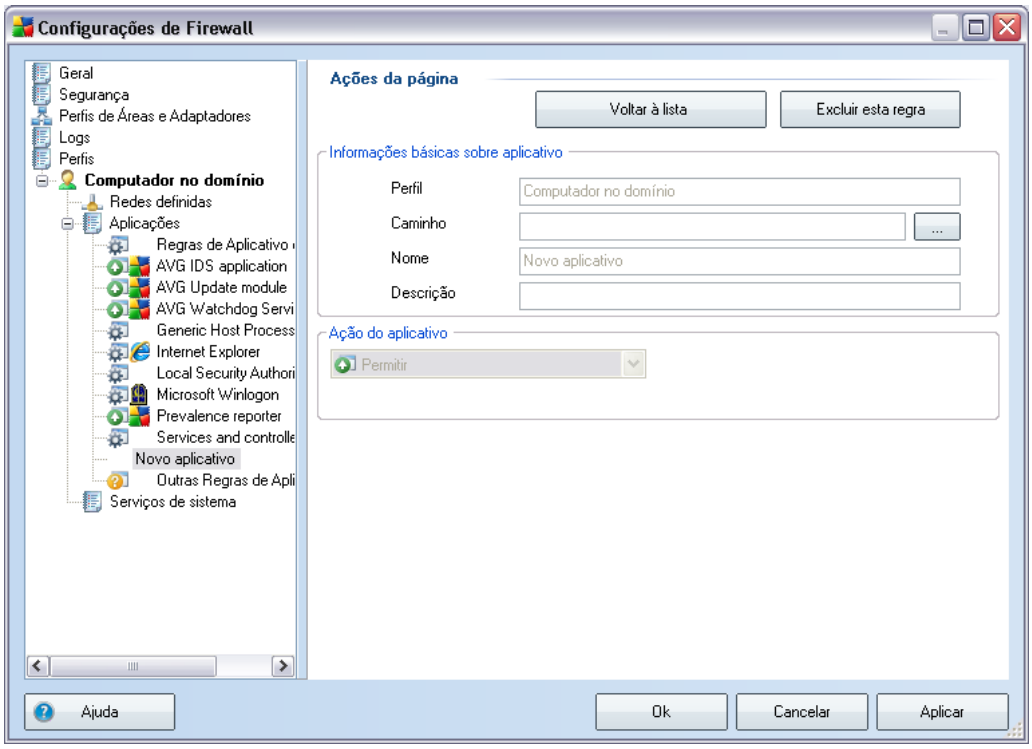
Botões de controle

É possível editar a lista usando os seguintes botões de controle:

- ***Adicionar*** - abre uma caixa de diálogo ***Ações da página*** para definir novas regras do aplicativo
- ***Editar*** - abre a mesma caixa de diálogo Ações da página para edição de um

conjunto de regras de um aplicativo existente***

- ***Excluir*** - remove o aplicativo selecionado da lista
- ***Ajuda*** - abre a caixa de diálogo relacionada ao arquivo de ajuda



Nessa caixa de diálogo, você pode definir as configurações para o respectivo aplicativo em detalhes.

Ações da página

- O bot©o***Voltar à lista*** exibirá a visão geral de todas as regras dos aplicativos definidos.
- O bot©o ***Excluir esta regra*** apagará a regra do aplicativo exibido. Observe que esta ação não pode ser revertida!

Informações básicas sobre aplicativo

Nesta seção, preencha o ***Nome*** do aplicativo e, opcionalmente, uma ***Descrição*** *(um breve comentário para sua informação*). No campo ***Caminho***, insira todo o caminho para o aplicativo (o arquivo executável) no disco; como alternativa, você pode localizar o aplicativo na estrutura em árvore de maneira conveniente após pressionar o botão "...".

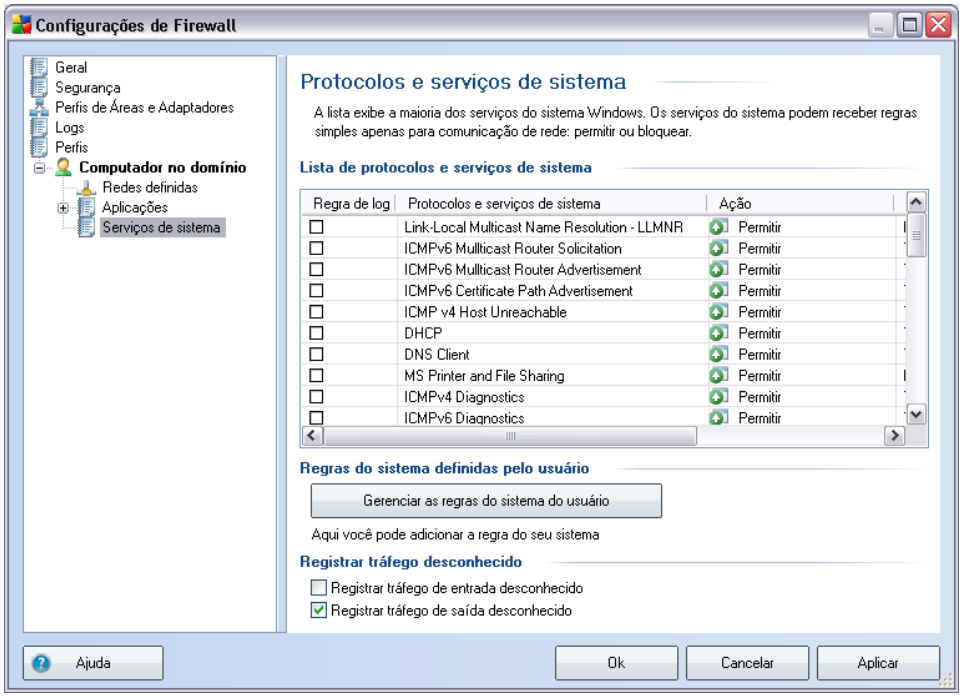
Ação do aplicativo

No menu suspenso, você pode selecionar a regra do Firewall para o aplicativo, ou seja, o que o Firewall deve fazer quando o aplicativo tentar se comunicar através da rede:

- ***Permitir para todos*** permitirá que o aplicativo se comunique em todas as redes e adaptadores definidos sem limitação.
- ***Permitir para segurança*** permitirá que o aplicativo se comunique em todas as redes definidas como Seguras (confiáveis).
- ***Bloquear*** impedirá a comunicação automaticamente; o aplicativo não terá permissão para se conectar a nenhuma rede.
- ***Solicitar*** exibirá uma caixa de diálogo permitindo que você decida permitir ou bloquear a tentativa de comunicação naquele momento.
- ***Configurações avançadas*** exibe opções de configuração ainda mais amplas e detalhadas na parte inferior da caixa diálogo na seção***Regras de detalhes do aplicativo***. Os detalhes serão aplicados de acordo com a ordem da lista, de modo que você poderá ***Promover*** ou ***Rebaixar*** as regras da lista conforme o necessário para estabelecer sua precedência. Após clicar em uma regra específica na lista, a visão geral dos detalhes da regra será exibida na parte inferior da caixa de diálogo. Qualquer valor em azul sem link pode ser alterado na caixa de diálogo clicando na respectiva configuração. Para excluir a regra destacada, simplesmente pressione***Remover***. Para definir uma nova regra, use o botão ***Incluir***para abrir a caixa de diálogo***Alterar detalhe de regra*** que lhe permite especificar todos os detalhes necessários.

11.5.4. Serviços do sistema

As edições na caixa de diálogo Serviços do sistema e protocolos SÓ devem ser feitas por usuários experientes!



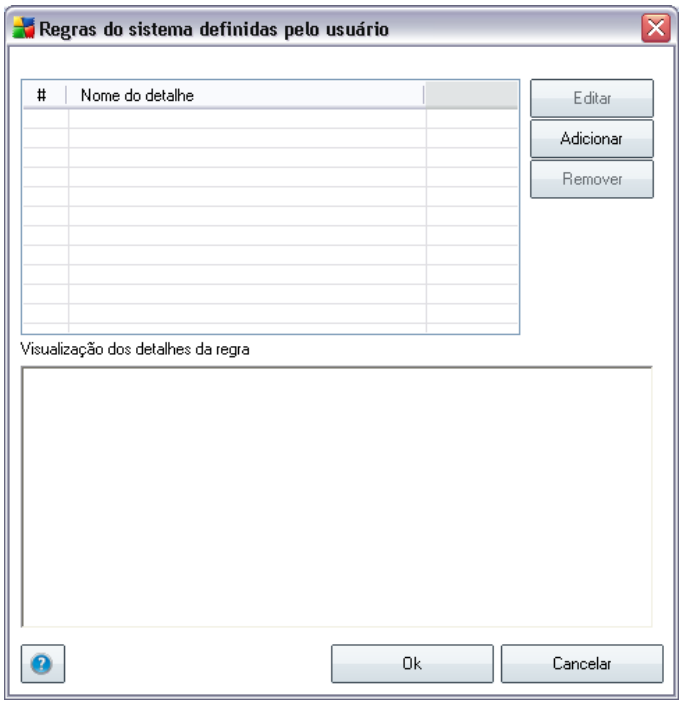
A caixa de diálogoProtocolos e serviços do sistema ***lista os protocolos e os serviços do sistema padrão do Windows que possam precisar se comunicar através da rede.*** O gráfico contém as seguintes colunas:

- ***Ação de regra de log*** - esta caixa permite que você ative o registro de cada aplicativo de regra nos Logs.
- ***Protocolos e serviços do sistema*** - esta coluna mostra um nome do respectivo serviço do sistema.
- ***Ação*** - esta coluna exibe um ícone para a ação atribuída:
  - Permitir comunicação para todas as redes
  - Permitir comunicação somente para redes definidas como Seguras
  - Bloquear comunicação

- ***Redes*** - esta coluna declara em que rede específica a regra do sistema se aplica.

A lista (*incluindo ações atribuídas*) pode ser editada usando os seguintes botões:

- Para editar as configurações de qualquer item na lista (incluindo as ações atribuídas), dê um clique com o botão direito no item e selecione ***Editar***.
- Para abrir uma nova caixa de diálogo para definir sua própria regra de serviço do sistema, veja a figura abaixo e pressione o botão ***Gerenciar as regras do sistema do usuário. A seção superior da caixa de diálogo Regras do sistema definidas pelo usuárioexibe a visão geral de todos os detalhes da regra do sistema editada no momento; a seção inferior exibe o detalhe selecionado.*** Os detalhes da regra definida pelo usuário podem ser editados, incluídos ou excluídos pelo botão correspondente; os detalhes da regra definida pelo fabricante podem ser somente editados:



Aviso:*Observe que as configurações de regra detalhada são avançadas, destinadas principalmente para administradores de rede que necessitam de controle total sobre a configuração de Firewall. Se você não estiver familiarizado com os tipos de*

protocolos de comunicação, números de porta de rede, definições de endereço IP etc, não modifique estas definições! Se você realmente precisa alterar a configuração, consulte os arquivos de ajuda da caixa de diálogo respectiva para detalhes específicos.

Registrar tráfego desconhecido

- ***Registrar tráfego de entrada desconhecido*** – marque a caixa para registrar nos Logs toda tentativa externa desconhecida de conexão com o seu computador.
- ***Registrar em log o tráfego de saída desconhecido*** – marque a caixa para registrar nos Logs toda tentativa desconhecida do seu computador para se conectar com um local externo.

12. Verificação do AVG

A verificação é uma parte crucial da funcionalidade **AVG 9 Anti-Virus plus Firewall**. Você pode executar testes sob demanda ou programá-los para serem executados periodicamente , em momentos de sua conveniência.

12.1. Interface da Verificação

A interface de verificação do AVG pode ser acessada pelo ***link rápido*** Verificador do Computador. Clique nesse link para passar para a caixa de diálogo ***Verificar ameaças*** . Nessa caixa de diálogo, você encontrará o seguinte:

- visão geral das verificações predefinidas - três tipos de verificação definidos pelo fornecedor do software estão prontos para uso imediato sob demanda ou de forma programada:
  - ***Verificar todo o computador***
  - ***Verificar arquivos ou pastas específicas***

- ***Verificação Anti-Rootkit***

- seção programação da verificação - onde é possível definir novos testes e criar novas programações, conforme necessário.

Botões de controle

Os botões de controle disponíveis na interface de teste são:

- ***Histórico da verificação*** - exibe a caixa de diálogo Visão geral dos resultados da verificação com todo o histórico da verificação

- ***Exibir Quarentena*** - abre uma nova janela com a Quarentena - um espaço em que as infecções detectadas são colocadas em quarentena

12.2. Verificações predefinidas

Um dos principais recursos do **AVG 9 Anti-Virus plus Firewall** é a verificação sob demanda. Testes sob demanda são desenvolvidos para verificar várias partes do seu computador, sempre que surgir a suspeita de uma possível infecção por vírus. De qualquer forma, é altamente recomendável realizar esses testes regularmente, ainda que você ache que nenhum vírus possa ser encontrado no seu computador.

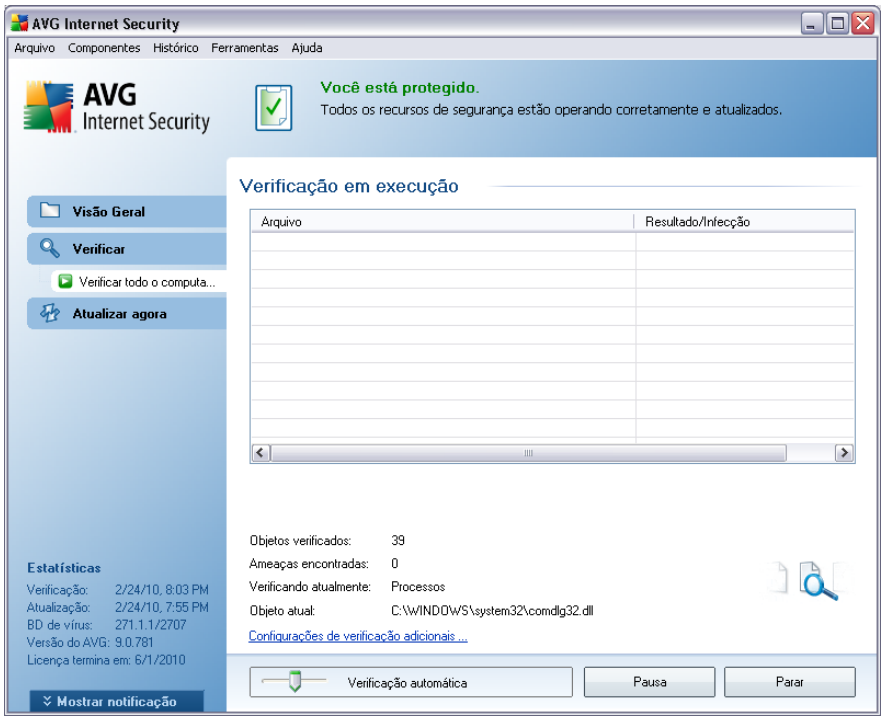
No **AVG 9 Anti-Virus plus Firewall**, você encontrará dois tipos de verificação predefinidas pelo fornecedor do software:

12.2.1. Verificar todo o computador

Verificar todo o computador - verifica todo o computador em busca de infecções e/ou programas potencialmente indesejados. Esse teste verificará todos os discos rígidos do computador, detectará e reparará qualquer vírus encontrado ou removerá a infecção para a ***Quarentena***. A Verificação de todo o computador deve ser programada em uma estação de trabalho pelo menos uma vez por semana.

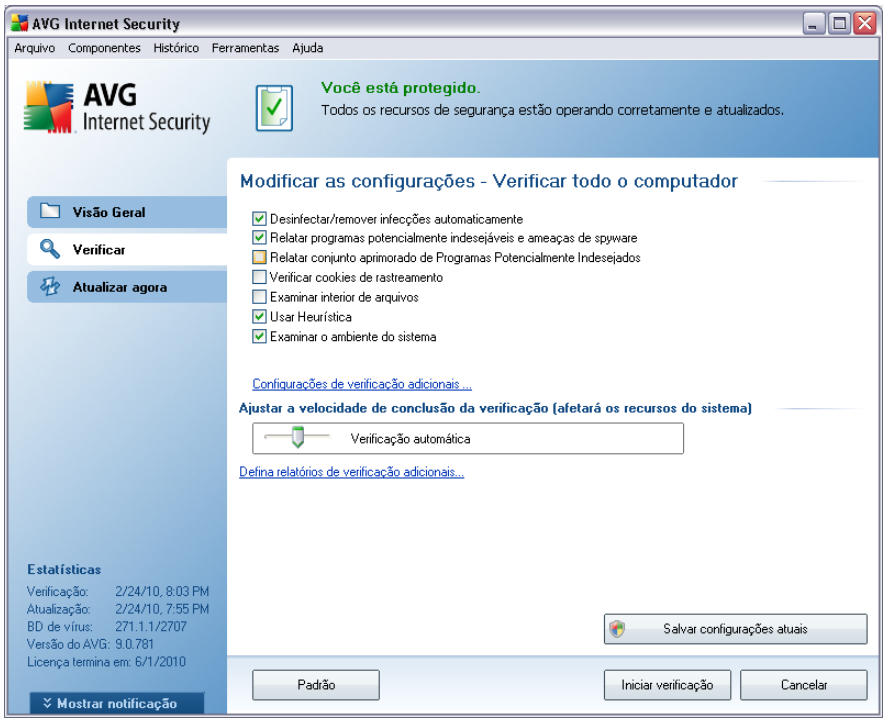
Iniciar verificação

A opção ***Verificar todo o computador*** pode ser iniciada diretamente na interface de verificação clicando no ícone de verificação. Se nenhuma outra configuração específica for configurada para esse tipo de verificação, ela será iniciada imediatamente dentro da caixa de diálogo de ***verificação em andamento*** *(veja a imagem)*. A verificação pode ser interrompida temporariamente (***Pausar***) ou cancelada (***Parar***) se necessário.



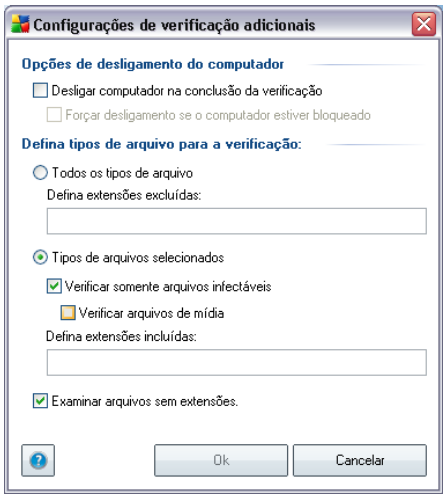
Verificar edições de configuração

Você tem a opção de editar as configurações padrão predefinidas de ***Verificar todo o computador***. Clique no link ***Alterar as configurações de verificação*** para abrir a caixa de diálogo ***Alterar configurações de verificação de Verificar todo o computador. É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.***



- ***Parâmetros de verificação*** - na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades. Por padrão, a maioria dos parâmetros é ativada e eles serão usados automaticamente durante a verificação.

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, onde é possível especificar os seguintes parâmetros:



- ***Opções de desligamento do computador*** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Definir tipos de arquivo para verificação*** - além disso, você deve decidir se deseja verificar os seguintes itens:

  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

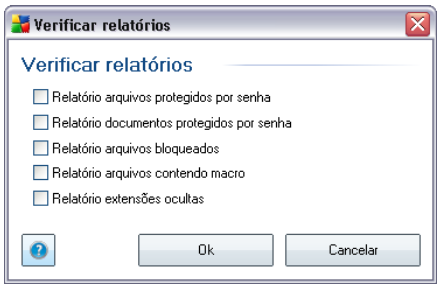
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões, quais são os arquivos que sempre devem ser verificados.

  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la

nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Prioridade do processo de verificação*** - você pode usar esse controle para alterar a prioridade do processo de verificação. Por padrão, a prioridade está definida para o nível médio (*Verificação automática*) que otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema sejam reduzidos (*procedimento útil quando quiser trabalhar no computador, sem se preocupar com o tempo que o sistema usará para fazer a verificação*) ou mais rápido, que aumenta os requisitos de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de descobertas devem ser relatados:



Aviso: *Essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo* ***Verificação do AVG / Programação da verificação / Como Verificar****. Se você decidir alterar as configurações padrão de* ***Verificar todo o computador****, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de todo o computador.*

12.2.2. Verificar arquivos ou pastas específicos

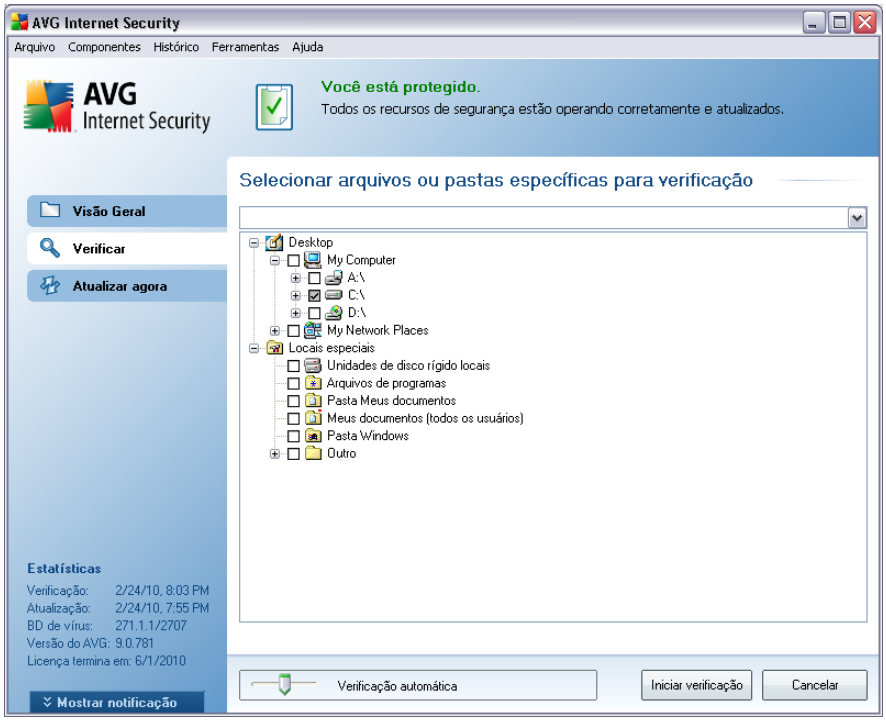
Verificar arquivos ou pastas específicas - verifica somente as áreas do computador que você tenha selecionado para verificação (*pastas selecionadas, disco rígido, unidades de disquete, CDs etc.*). O andamento da verificação em caso de detecção e tratamento de vírus é o mesmo da verificação de todo o computador: todos os vírus encontrados serão reparados ou removidos para a ***Quarentena de Vírus***. A verificação de arquivos ou pastas específicas pode ser usada para configurar seus próprios testes e sua programação com base nas suas necessidades.

Iniciar verificação

A opção ***Verificar arquivos ou pastas específicas*** pode ser iniciada diretamente na interface de verificação clicando no ícone de verificação. Uma nova caixa de diálogo chamada ***Selecionar arquivos ou pastas específicas para verificação*** será aberta. Na estrutura de árvores do computador, selecione as pastas que deseja verificar. O caminho para cada pasta selecionada será gerado automaticamente e exibido na caixa de texto na parte superior dessa caixa de diálogo.

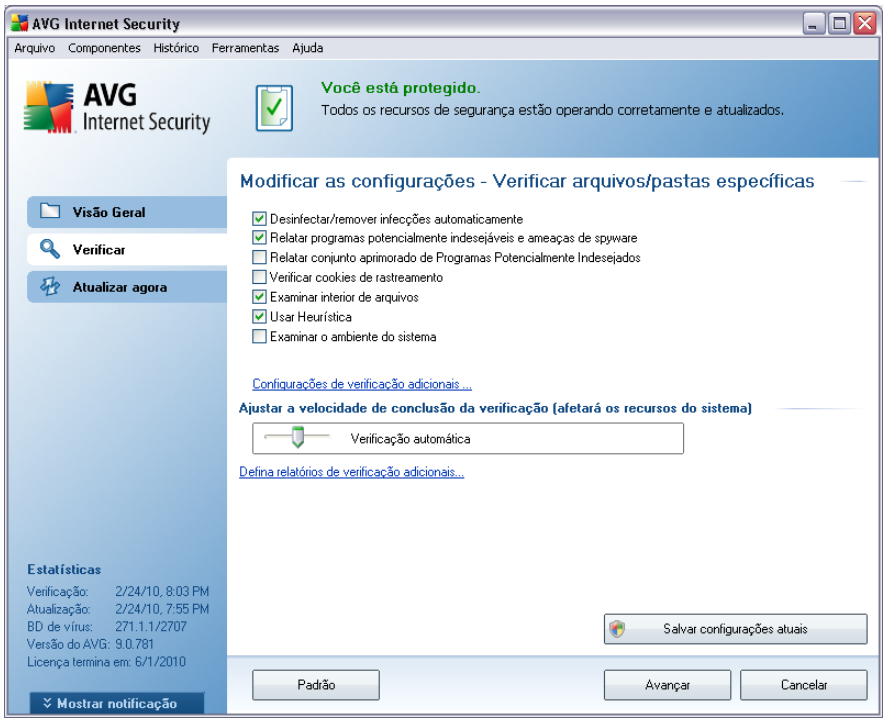
Também existe a possibilidade de fazer a verificação em uma determinada pasta enquanto suas subpastas são excluídas da verificação; para isso, insira um sinal de menos "**-**" na frente do caminho gerado automaticamente (*veja a imagem*). Para excluir da verificação a pasta inteira, use o parâmetro "!" .

Finalmente, para iniciar a verificação, pressione o botão ***Iniciar verificação***; o processo de verificação será basicamente idêntico à verificação de todo o conteúdo do computador.



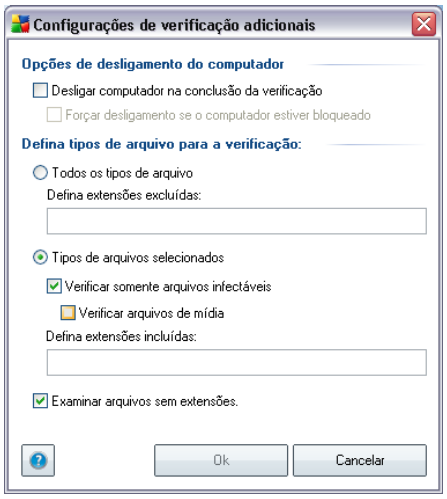
Verificar edições de configuração

Você tem a opção de editar as configurações padrão predefinidas de ***Verificar arquivos ou pastas específicas***. Acesse o link ***Alterar as configurações de verificação*** para abrir a caixa de diálogo ***Alterar configurações de verificação de Verificar arquivos ou pastas específicas***. ***É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.***



- ***Parâmetros de verificação*** - na lista dos parâmetros de verificação, você pode ativar/desativar parâmetros específicos conforme necessário (*para uma descrição detalhada dessa configuração, consulte o capítulo Configurações Avançadas do AVG / Verificações / Verificar Arquivos ou Pastas específicos*).

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo Configurações de verificação adicionais, onde é possível especificar os seguintes parâmetros:



- ***Opções de desligamento do computador*** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Definir tipos de arquivo para verificação*** - além disso, você deve decidir se deseja verificar os seguintes itens:

  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

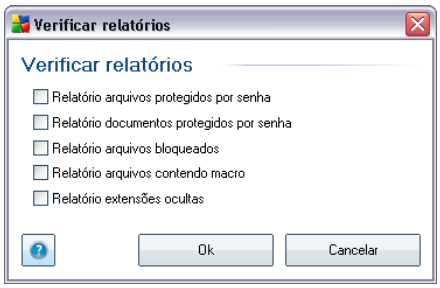
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões, quais são os arquivos que sempre devem ser verificados.

  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la

nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Prioridade do processo de verificação*** - você pode usar esse controle para alterar a prioridade do processo de verificação. Por padrão, a prioridade está definida para o nível médio (*Verificação automática*) que otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema sejam reduzidos (*procedimento útil quando quiser trabalhar no computador, sem se preocupar com o tempo que o sistema usará para fazer a verificação*) ou mais rápido, que aumenta os requisitos de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de localizações deve ser relatado:

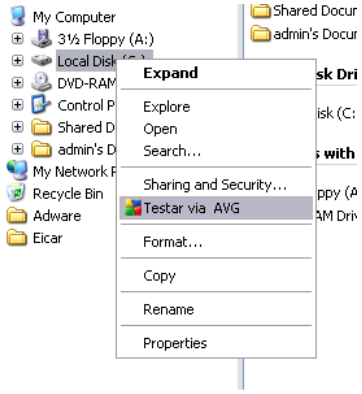


Aviso: *Essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo* ***Verificação do AVG / Programação da verificação / Como Verificar****. Se você decidir alterar as configurações padrão de* ***Verificar arquivos ou pastas específicas****, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de arquivos ou pastas específicas. Além disso, essa configuração será usada como modelo para todas as novas verificações programadas (* *todas as verificações personalizadas são baseadas na configuração atual de Verificação de arquivos ou pastas selecionados* *).*

12.3. Verificando o Windows Explorer

Além das verificações predefinidas inicializadas em todo o computador ou em áreas selecionadas, o **AVG 9 Anti-Virus plus Firewall ainda oferece a opção de uma verificação rápida de um objeto específico diretamente no ambiente do Windows Explorer.** Se você desejar abrir um arquivo desconhecido e não tiver

certeza sobre o seu conteúdo, poderá verificá-lo sob demanda. Siga estas etapas:



- No Windows Explorer, realce o arquivo (ou pasta) que deseja verificar
- Clique com o botão direito do mouse no objeto para abrir o menu de contexto
- Selecione a opção ***Verificar com AVG*** para que o arquivo seja verificado com o AVG

12.4. Verificação de linha de comando

No **AVG 9 Anti-Virus plus Firewall** há a opção de executar a verificação a partir da linha de comando. Você pode usar esta opção em servidores, ou ao criar um script em lote para ser iniciado automaticamente após a inicialização do computador. A partir da linha de comando, você pode iniciar a verificação com a maioria dos parâmetros como oferecido em uma interface gráfica de usuário AVG.

Para iniciar a verificação AVG da linha de comando, execute o seguinte comando dentro da pasta onde o AVG está instalado:

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

Sintaxe do comando

A seguir a sintaxe do comando:

- ***avgscanx /parâmetro*** ... por exemplo. ***avgscanx /comp*** para verificação de todo o computador

- ***avgscanx /parâmetro /parâmetro*** .. com vários parâmetros, estes devem estar alinhados em uma fila e separados por um espaço e um caracter de barra

- se o parâmetro exigir um valor específico a ser fornecido (por exemplo, o parâmetro ***/scan*** requer informações sobre quais são as áreas selecionadas do seu computador a serem verificadas, e você precisa informar o caminho exato da seção selecionada), os valores serão divididos por ponto e vírgula, como por exemplo: ***avgscanx /scan=C:\;D:***

Parâmetros de verificação

Para exibir uma visão completa dos parâmetros disponíveis, digite o respectivo comando junto com o parâmetro /? ou /HELP (por ex., ***avgscanx /?***). O único parâmetro obrigatório é /SCAN, que especifica que áreas do computador devem ser verificadas. Para obter explicações mais detalhadas das opções, consulte a visão geral dos parâmetros da linha de comando.

Para executar a verificação, pressione ***Enter***. Durante a verificação, você pode interromper o processo ao pressionar ***Ctrl+C*** ou ***Ctrl+Pause***.

Verificação CMD iniciada pela interface gráfica

Quando você executa seu computador no Modo de segurança do Windows, é também possível iniciar a verificação das linhas de comando pela interface gráfica do usuário. A verificação será iniciada pela linha de comando; a caixa de diálogo ***Composer da linha de comando*** apenas permite que você especifique a maioria dos parâmetros de verificação na interface gráfica amigável.

Como esta caixa de diálogo apenas está acessível pelo Modo de segurança do Windows, para obter uma descrição detalhada dela consulte o arquivo de ajuda acessível diretamente pela caixa de diálogo.

12.4.1. Parâmetros de verificação CMD

A seguir, veja uma lista de todos os parâmetros disponíveis para a verificação de linha de comando:

- ***/SCAN*** Verificar arquivos ou pastas específicos /SCAN=path;path (e.x. /SCAN=C:\;D:\)

- ***/COMP*** Verificar todo o computador

- ***/HEUR*** Usar análise heurística***
- ***/EXCLUDE*** Excluir caminho ou arquivo da verificação
- ***/@*** Arquivo de comando /nome de arquivo/
- ***/EXT*** Verificar essas extensões /por exemplo, EXT=EXE,DLL
- ***/NOEXT*** Não verificar essas extensões /por exemplo, NOEXT=JPG/
- ***/ARC*** Verificar arquivos
- ***/CLEAN*** Limpar automaticamente
- ***/TRASH*** Mover arquivos infectados para a Quarentena de Vírus***
- ***/QT*** Teste rápido
- ***/MACROW*** Relatar macros
- ***/PWDW*** Relatar arquivos protegidos por senha
- ***/IGNLOCKED*** Ignorar arquivos bloqueados
- ***/REPORT*** Relatar para arquivo / nome de arquivo/
- ***/REPAPPEND*** Acrescentar ao arquivo de relatório
- ***/REPOK*** Relatar arquivos não infectados como OK
- ***/NOBREAK*** Não permitir abortar com CTRL-BREAK
- ***/BOOT*** Ativar verificação de MBR/BOOT
- ***/PROC*** Verificar processos ativos
- ***/PUP*** Relatar "Programas potencialmente indesejáveis"
- ***/REG*** Verificar Registro
- ***/COO*** Verificar cookies
- ***/?*** Exibir ajuda neste tópico
- ***/HELP*** Exibir ajuda neste tópico

- ***/PRIORIDADE*** Definir prioridade de verificação /Baixa, Automática, Alta (veja Configurações avançadas / Verificações)
- ***/SHUTDOWN*** Desligar computador na conclusão da verificação
- ***/FORCESHUTDOWN*** Forçar computador a ser desligado na conclusão da verificação
- ***/ADS*** Verificar fluxos de dados alternativos (apenas NTFS)

12.5. Programação de verificação

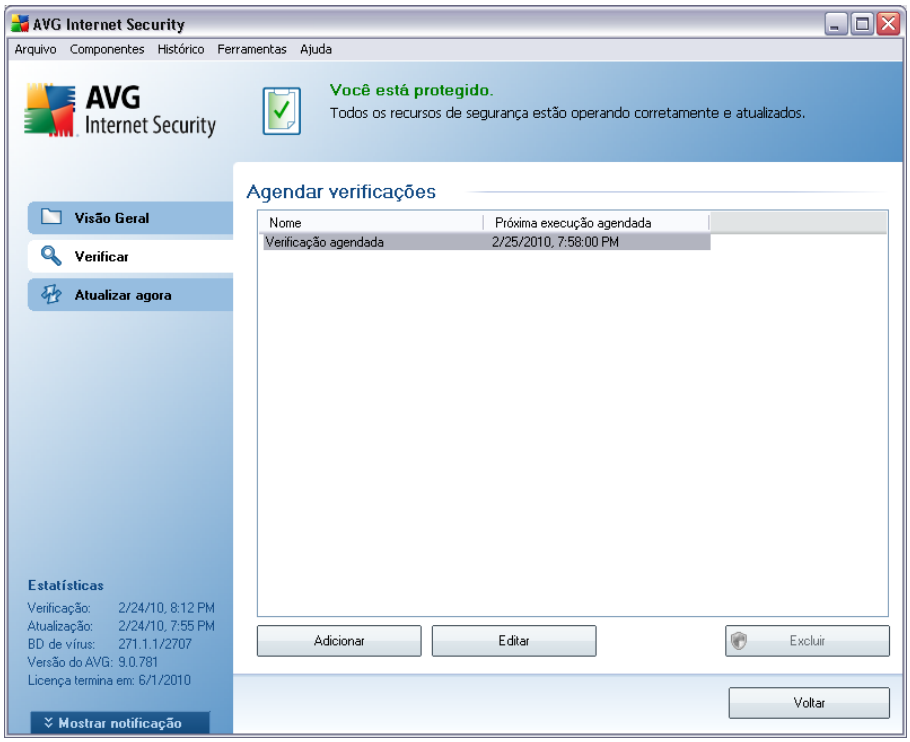
Com o **AVG 9 Anti-Virus plus Firewall**, é possível executar uma verificação sob demanda (por exemplo, quando você suspeitar de uma infecção no seu computador) ou com base em um plano programado. É altamente recomendável executar verificações com base em uma programação. Dessa forma, você pode assegurar que seu computador esteja protegido contra a possibilidade de infecção e não precisará se preocupar com a inicialização da verificação.

Inicialize a ***Verificação de todo o computador*** regularmente, pelo menos uma vez por semana. Se possível, inicialize a verificação de todo o computador diariamente, conforme definido na configuração padrão da programação da verificação.Se o computador estiver "sempre ligado", você poderá programar verificações fora dos horários de trabalho. Se o computador for desligado algumas vezes, programe verificações para a inicialização do computador, quando a tarefa tiver sido executada.

Para criar novas programações de verificação, consulte a interface de verificação do AVG e localize a seção ***Programar verificações*** , na parte inferior:

Agendar verificações

Clique no ícone gráfico na seção ***Programar verificações*** para abrir uma nova caixa de diálogo ***Programar verificações***, na qual você encontrará uma lista de todas as verificações atualmente programadas:



É possível editar/adicionar verificações usando os seguintes botões de controle:

- ***Adicionar programa de verificação*** - o botão abre a caixa de diálogo ***Configurações da verificação programada***, guia ***Configurações de programa***. Nessa caixa de diálogo, você pode especificar os parâmetros do teste definido recentemente.

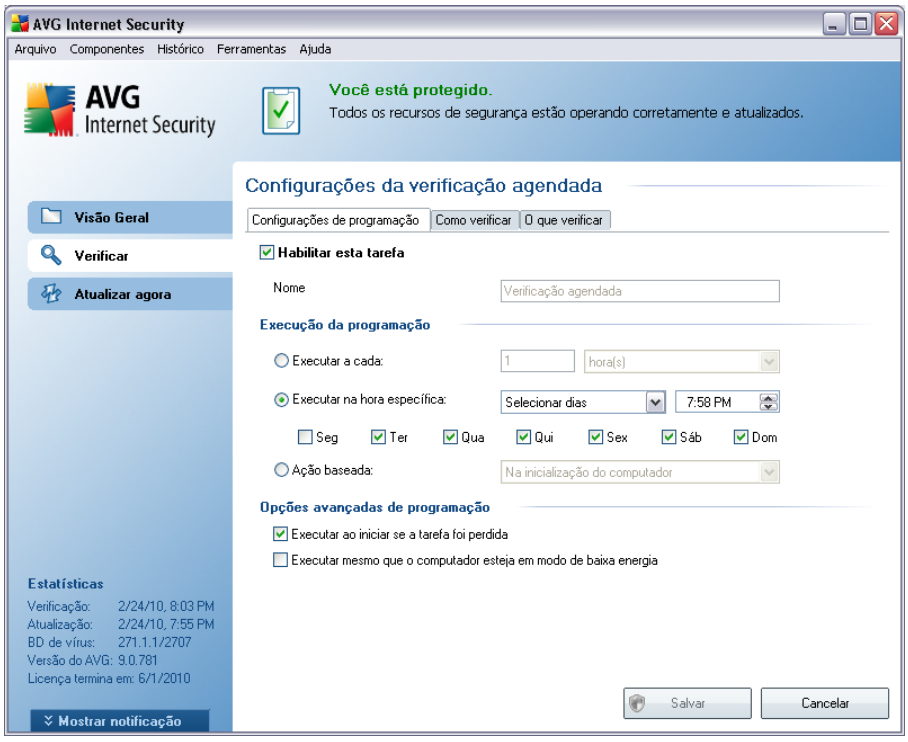
- ***Editar programa da verificação*** - esse botão só pode ser usado se você tiver selecionado um teste existente anteriormente na lista de testes programados. Nesse caso, o botão aparecerá ativo e você poderá clicar nele para passar para a caixa de diálogo ***Configurações da verificação programada*** , guia ***Configurações de programa***. Os parâmetros do teste selecionado já estão especificados e poderão ser editados aqui.

- ***Excluir programa da verificação*** - esse botão também ficará ativo se você tiver selecionado um teste existente anteriormente na lista de testes programados. Esse teste pode ser excluído da lista se você pressionar o botão de controle. Entretanto, você só poderá remover os próprios testes. O teste ***Programa de verificação de todo o computador*** predefinido com as configurações padrão nunca poderá ser excluído.

- ***Voltar*** - retornar à interface de verificação do AVG

12.5.1. Configurações de agendamento

Se quiser programar um novo teste e sua ativação regular, insira informações na caixa de diálogo ***Configurações para teste programado*** (*, clique no botão* ***Adicionar verificação programada*** *na caixa de diálogo* ***Programar verificações***). A caixa de diálogo é dividida em três guias:***Configurações de programa*** *- veja imagem abaixo (a guia padrão à qual você será automaticamente redirecionado),****Como verificar*** e ***O que verificar***.



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente o teste programado e ativá-lo novamente conforme necessário.

Em seguida, informe o nome da verificação que você está prestes a criar e agendar. Digite o nome no campo de texto, no item ***Nome***. Tente usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

Exemplo: *não é apropriado denominar a verificação como "Nova verificação" ou*

"Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc. Além disso, não é necessário especificar no nome da verificação se ela é uma verificação de todo o computador ou somente uma verificação de pastas ou arquivos selecionados. Suas verificações serão sempre uma versão específica da verificação de arquivos ou pastas selecionados.

Nessa caixa de diálogo você ainda poderá definir os seguintes parâmetros de verificação:

- ***Execução do programa*** - especifica os intervalos de tempo para a inicialização de novas verificações programadas. O tempo pode ser definido pela repetição da inicialização da verificação depois de um determinado período (***Executar a cada ...***) pela definição de uma data e hora exatas (***Executar em uma hora específica...***), ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (***Ação baseada na inicialização do computador***).

- ***Opções de programa avançadas*** - essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

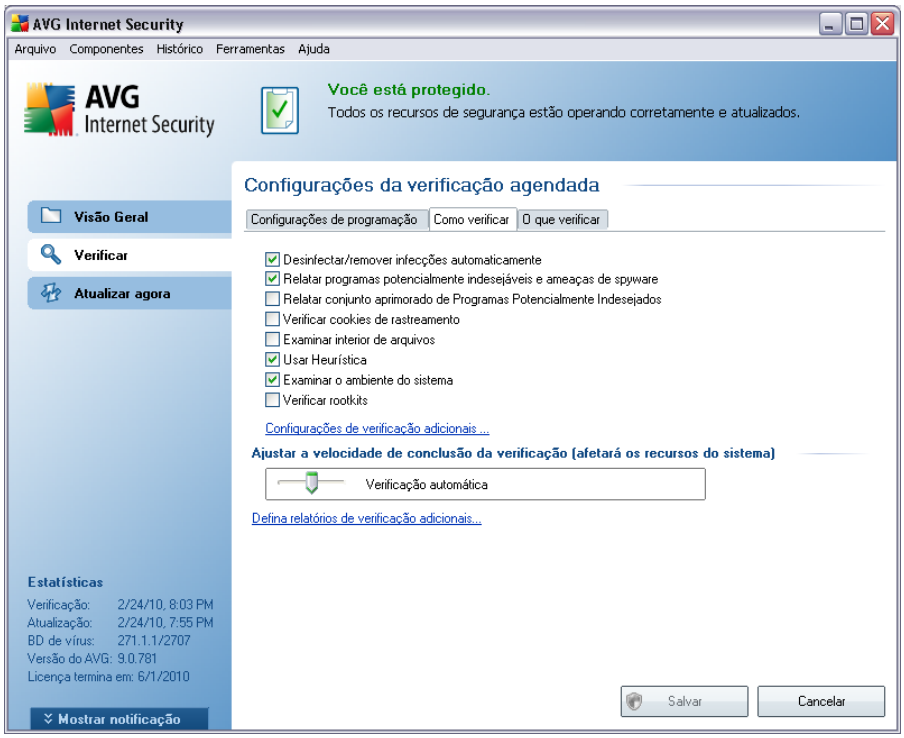
Botões de controle da caixa de diálogo Configurações para verificação programada

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações do programa***, ***Como verificar*** e ***O que verificar***), e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

12.5.2. Como verificar



Na guia ***Como verificar*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros é ativada e a funcionalidade será aplicada durante a verificação. A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida:

- ***Reparar ou remover vírus automaticamente*** - (*ativado por padrão*): se um vírus for identificado durante a verificação, pode ser reparado automaticamente, se houver solução disponível. Caso não seja possível reparar o arquivo infectado automaticamente ou se você decidir desativar essa opção, você será notificado das detecções de vírus e terá que decidir o que fazer com o vírus encontrado. A ação recomendada é remover o arquivo infectado para a ***Quarentena***.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter

esse recurso ativado, pois aumenta a segurança do computador

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – se a opção anterior estiver ativada, você também poderá marcar essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** - (*ativado por padrão*): esse parâmetro do componente ***Anti-Spyware*** define que os cookies devem ser detectados durante a verificação (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de suas compras eletrônicas*);

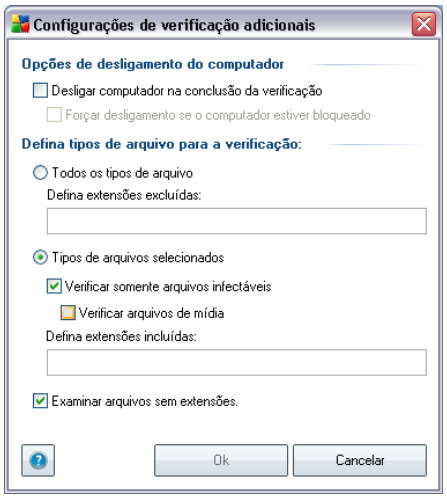
- ***Verificar interior dos arquivos*** - (*ativado por padrão*): esse parâmetro define que a verificação deve atuar em todos os arquivos, mesmo se eles estiverem compactados em algum tipo de arquivo, como ZIP, RAR etc.

- ***Usar Heurística*** - (*ativado por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado,em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***Verificar ambiente do sistema*** - (*ativado por padrão*): a verificação também atuará nas áreas do sistema do seu computador.

Em seguida, é possível alterar a configuração de verificação da seguinte maneira:

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, onde é possível especificar os seguintes parâmetros:



- ***Opções de desligamento do computador*** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Definir tipos de arquivo para verificação*** - além disso, você deve decidir se deseja verificar os seguintes itens:

  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

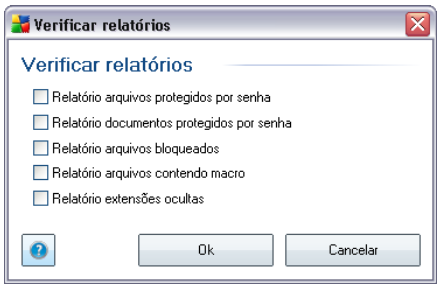
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões, quais são os arquivos que sempre devem ser verificados.

  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la

nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Prioridade do processo de verificação*** - você pode usar esse controle para alterar a prioridade do processo de verificação. Por padrão, a prioridade está definida para o nível médio (*Verificação automática*) que otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema sejam reduzidos (*procedimento útil quando quiser trabalhar no computador, sem se preocupar com o tempo que o sistema usará para fazer a verificação*) ou mais rápido, que aumenta os requisitos de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de descobertas devem ser relatados:



Observação: *por padrão, a configuração da verificação é definida para o desempenho ideal. A menos que você tenha um motivo válido para alterar essas configurações, é altamente recomendável manter a configuração predefinida. As alterações de configuração devem ser realizadas somente por usuários experientes. Para obter outras opções de configuração de verificação, consulte a caixa de diálogo* ***Configurações avançadas*** *por meio do item do menu de sistema* ***Arquivo/ Configurações avançadas****.*

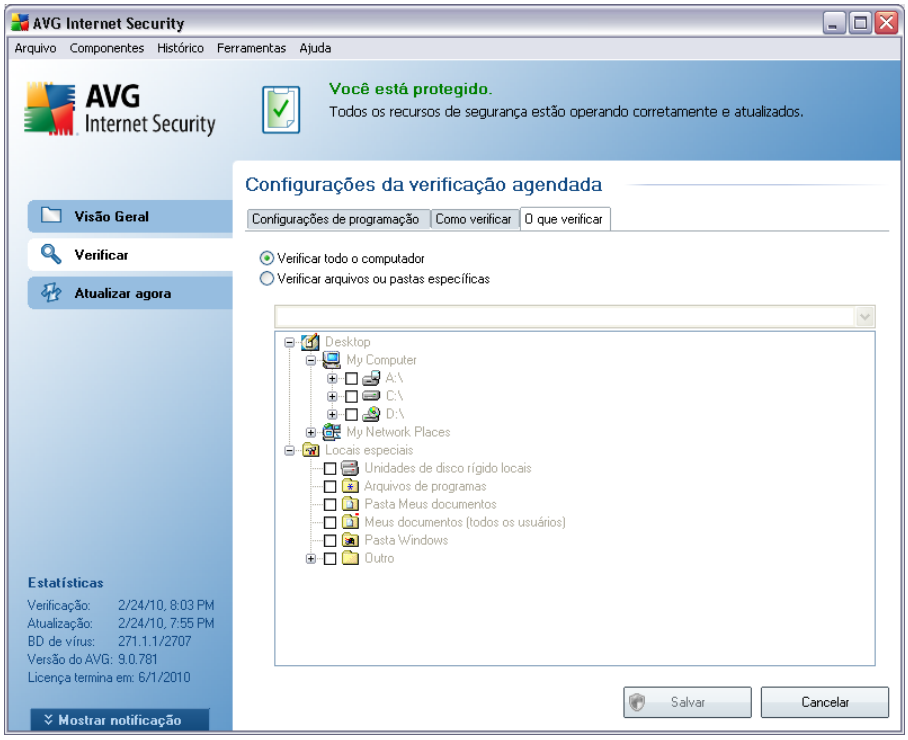
Botões de controle

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações de programa***, ***Como verificar e*** O que verificar***), e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no monento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

12.5.3. O que verificar



Na guia ***O que verificar***, você pode definir se deseja programar a verificação de todo o computador ou a verificação de arquivos ou pastas específicas***.

Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação (expanda os itens clicando no nó de mais até encontrar a pasta que deseja verificar). Você pode selecionar várias pastas marcando as respectivas caixas. As pastas selecionadas aparecerão no campo de texto na parte superior da caixa de diálogo e o menu suspenso manterá o histórico das verificações

selecionadas para um uso posterior. *Ou você pode inserir o caminho inteiro para a pasta desejada manualmente (se inserir vários caminhos, será necessário separar com pontos-e-vírgulas sem espaços extras*).

Na estrutura de árvore você também pode ver um ramo chamado ***Locais especiais***. A seguir encontre uma lista de locais que serão verificados uma vez que a respectiva caixa de seleção esteja marcada:

- ***Discos rígidos locais*** - todos os discos rígidos de seu computador
- ***Arquivos de programas*** - C:\Program Files\
- ***Pasta Meus Documentos*** - C:\Documents and Settings\User\My Documents\
- ***Documentos Compartilhados***- C:\Documents and Settings\All Users\Documents\
- ***Pasta do Windows*** - C:\Windows\
- ***Outro***
  - Drive de sistema – o disco rígido no qual o sistema operacional está instalado (normalmente C:)
  - Pasta do sistema – Windows/System32
  - Pasta de arquivos temporários – Documents and Settings/User/Local Settings/Temp
  - Arquivos temporários da Internet – Documents and Settings/User/Local Settings/Temporary Internet Files

Botões de controle da caixa de diálogo Configurações para verificação programada

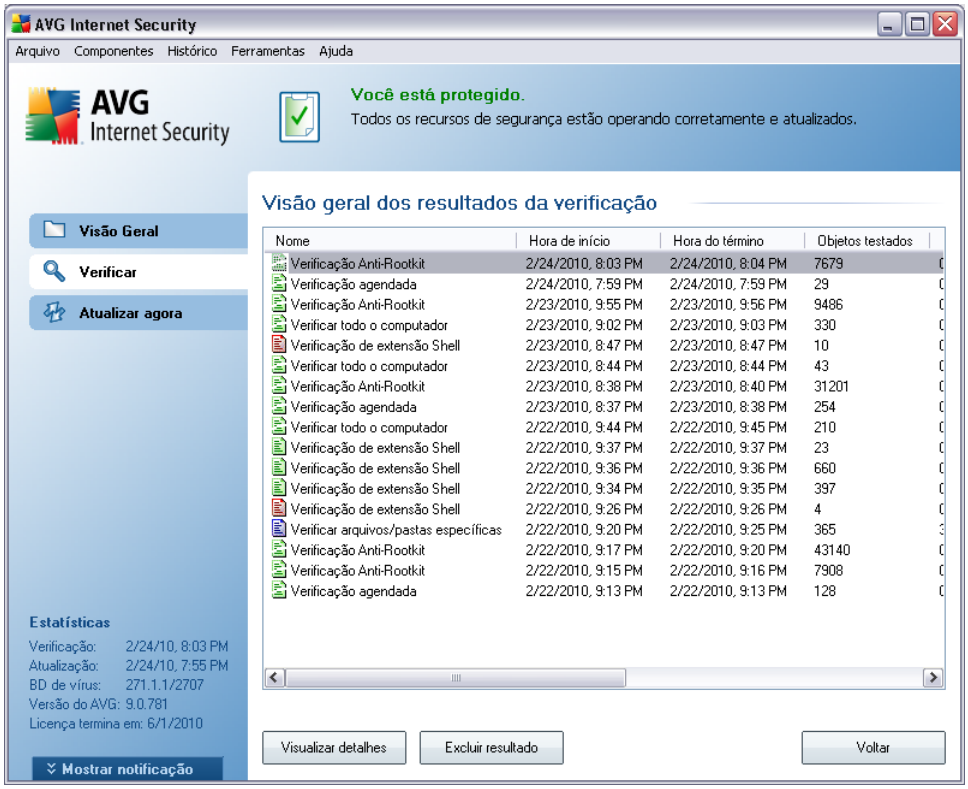
Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações do programa***, ***Como verificar***e ***O que verificar***), e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de

teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

12.6. Visão geral dos resultados da verificação



A caixa de diálogo ***Visão geral dos resultados de verificação*** pode ser acessada da interface de verificação do AVG, por meio do botão ***Histórico de verificação***. A caixa de diálogo fornece uma lista de todas as verificações inicializadas anteriormente e as informações sobre seus resultados:

- ***Nome*** - designação da verificação; pode ser o nome de uma das verificações predefinidas ou o nome que você tenha dado à verificação que programou. Todos os nomes incluem um ícone indicando o resultado da verificação:

  - o ícone verde informa que não foram detectadas infecções durante

a verificação

 - o ícone azul indica que uma infecção foi detectada durante a verificação, mas o objeto infectado foi removido automaticamente

 - o ícone vermelho avisa que uma infecção foi detectada durante a verificação e não foi possível removê-la!

Cada ícone pode ser sólido ou cortado ao meio. O ícone sólido indica uma verificação que foi concluída adequadamente. O ícone cortado ao meio indica que a verificação foi cancelada ou interrompida.

Nota: *para obter informações detalhadas sobre cada verificação, consulte a caixa de diálogo* ***Resultados da Verificação****, que pode ser acessada pelo botão* ***Exibir detalhes*** *(na parte inferior desta caixa de diálogo).*

- ***Horário de início*** - a data e a hora em que a verificação foi inicializada
- ***Horário de término*** - a data e a hora em que a verificação foi encerrada
- ***Objetos testados*** - número de objetos que foram verificados
- ***Infecções*** - número de infecções por vírus detectadas/removidas
- ***Spyware*** - número de spyware detectados/removidos

- ***Aviso*** - número de objetos suspeitos detectados ***
- ***Rootkits*** - número de rootkits detectados rootkits
  - ***Informações do log de verificação*** - informações relacionadas ao processo e o resultado da verificação (geralmente em sua finalização ou interrupção)

Botões de controle

Os botões de controle da caixa de diálogo ***Visão geral dos resultados da verificação*** são:

- ***Exibir detalhes***- pressione-o para ativar a caixa de diálogo***Resultados da verificação*** para exibir dados detalhados na verificação selecionada
- ***Excluir resultado*** - pressione-o para remover o item selecionado a partir da

visão geral dos resultados da verificação

- ***Voltar*** - volta para a caixa de diálogo padrão da interface de verificação do AVG

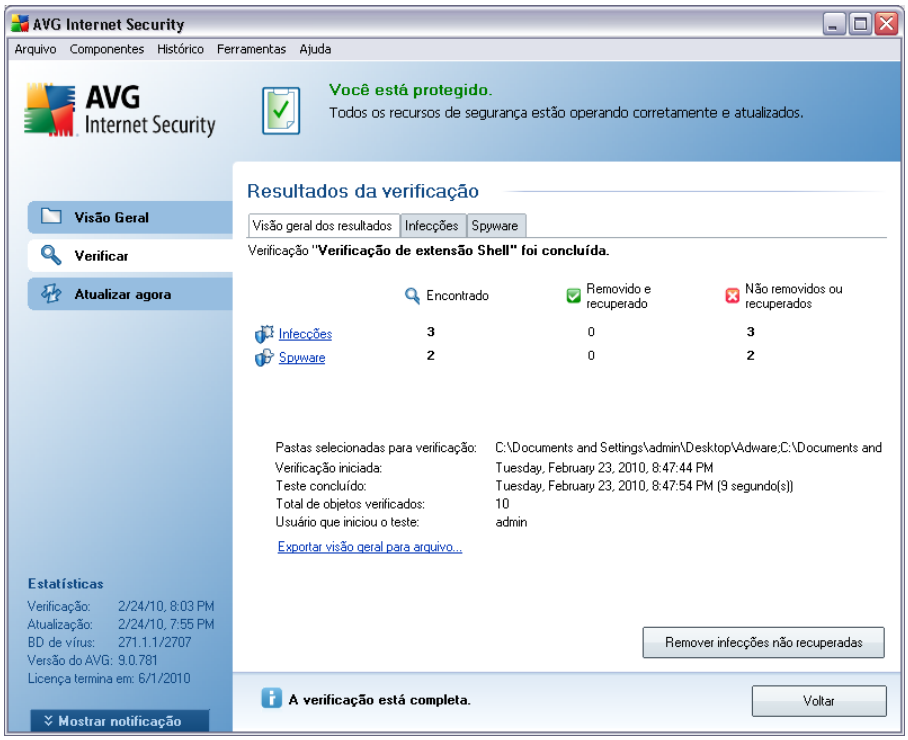
12.7. Detalhes dos resultados da verificação

Se na caixa de diálogo ***Visão Geral dos Resultados da Verificação*** uma verificação específica for selecionada, você poderá clicar no botão ***Exibir detalhes*** para passar para a caixa de diálogo ***Resultados da Verificação***, que fornece detalhes sobre o processo e o resultado da verificação selecionada.

A caixa de diálogo divide-se em várias guias:

- ***Visão Geral dos Resultados*** - essa guia é exibida sempre e fornece dados estatísticos descrevendo o processo de verificação.
- ***Infecções*** - essa guia é exibida somente se uma infecção por vírus tiver sido detectada durante a verificação
- ***Spyware*** - essa guia é exibida somente se um spyware tiver sido detectado durante a verificação
- ***Aviso*** - essa guia é exibida somente se cookies forem detectados durante a verificação
- ***Informações*** **-** essa guia é exibida somente se algumas ameaças potenciais tiverem sido detectadas, mas se não tiver sido possível classificá-las em nenhuma das categorias acima. A guia fornecerá uma mensagem de aviso sobre a descoberta. Além disso, você vai encontrar aqui informações sobre objetos que não podem ser verificados (por exemplo, arquivos protegidos por senha).

12.7.1. Guia Visão geral dos resultados



Na guia ***Verificar resultados***, é possível encontrar estatísticas detalhadas com informações sobre:

- infecções por vírus/spyware detectadas
- infecções por vírus/spyware removidas
- o número de infecções por vírus/spyware que não puderam ser removidas ou reparadas

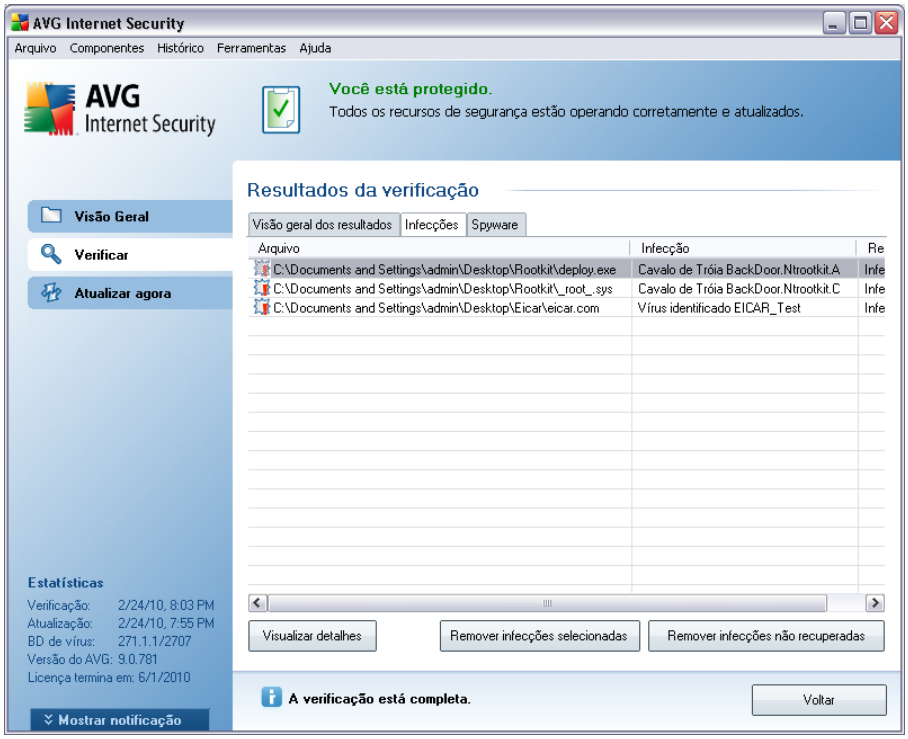
Além disso, você encontrará informações sobre a data e a hora exata da inicialização da verificação, o número total de objetos verificados, a duração da verificação e o número de erros ocorridos durante a verificação.

Botões de controle

Há somente um botão de controle disponível nessa caixa de diálogo. O botão ***Fechar resultados*** o leva de volta à caixa de diálogo ***Visão geral dos resultados da***

verificação.

12.7.2. Guia Infecções



A guia ***Infecções*** só é exibida na caixa de diálogo ***Verificar resultados*** se uma infecção de vírus for detectada durante uma verificação. A guia é dividida em três seções, que apresentam estas informações:

- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do vírus detectado (*para obter detalhes sobre o vírus específico, consulte a Enciclopédia de Vírus online*).
- ***Resultado*** - define o status atual do objeto infectado detectado durante a verificação.
    - ***Infectado*** - o objeto infectado foi detectado e mantido no local original (*por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica*).
    - ***Reparado*** - o objeto infectado foi reparado automaticamente e mantido

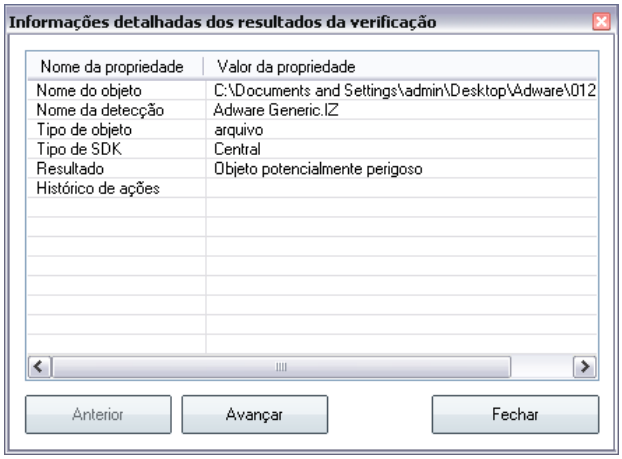
no local original

- **Movido para Quarentena de Vírus** - o objeto infectado foi movido para a **Quarentena de Vírus**.
- **Excluído** - o objeto infectado foi excluído.
- **Adicionado às excessões PPI**- a detecção foi avaliada como exceção e adicionada à lista de exceções PPI (*configurada na caixa de diálogo* **Excessões PPI** *das configurações avançadas*)
- **Arquivo bloqueado - não testado** - o objeto é bloqueado e o AVG não pode verificá-lo.
- **Objeto potecialmente perigoso** - o objeto foi detectado como potencialmente perigoso, mas não infectado (ele pode conter macros, por exemplo*).* As informações devem ser consideradas apenas um aviso.
- **Reinicialização necessária para concluir ação** - não é possível remover o objeto infectado. Para removê-lo completamente, é necessário reiniciar o computador.

Botões de controle

Há três botões de controle disponíveis nessa caixa de diálogo:

- **Exibir detalhes** - o botão abre uma nova janela de diálogo denominada **Detalhes do resultado da verificação**:



Nessa caixa de diálogo você pode encontrar informações sobre o local do objeto infectado detectado (***Nome da propriedade***). Usando os botões ***Voltar***/***Avançar***, você pode ver informações sobre descobertas específicas. Use o botão ***Fechar*** para fechar a caixa de diálogo.

- ***Remover infecções selecionadas*** - use o botão para mover a descoberta selecionada para a ***Quarentena.***
- ***Remover todas as infecções não reparadas*** - esse botão exclui todas as descobertas de vírus que não foram reparadas ou movidas para a ***Quarentena.***
- ***Fechar resultados*** - fecha a visão geral das informações e volta para a caixa de diálogo ***Visão geral dos resultados da verificação***.

12.7.3. Guia Spyware

A guia ***Spyware*** só é exibida na caixa de diálogo ***Verificar resultados*** se um spyware for detectado durante uma verificação. A guia é dividida em três seções, que apresentam estas informações:

- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do spyware detectado (*para obter detalhes sobre o vírus específico, consulte a* ***Enciclopédia de Vírus*** *on-line*).
- ***Resultado*** - define o status atual do objeto detectado durante a verificação.
  - ***Infectado*** - o objeto infectado foi detectado e mantido no local original (por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica).
  - ***Reparado*** - o objeto infectado foi reparado automaticamente e mantido no local original
  - ***Movido para Quarentena de Vírus*** - o objeto infectado foi movido para a ***Quarentena de Vírus*.**
  - ***Excluído*** - o objeto infectado foi excluído.
  - ***Adicionado a extensões PPI*** - a detecção foi avaliada como exceção e adicionada à lista de exceções PPI (*configurada na caixa de diálogo* ***Exceções PPI*** *das configurações avançadas*)
  - ***Arquivo bloqueado - não testado*** - o objeto é bloqueado e o AVG não

pode verificá-lo.

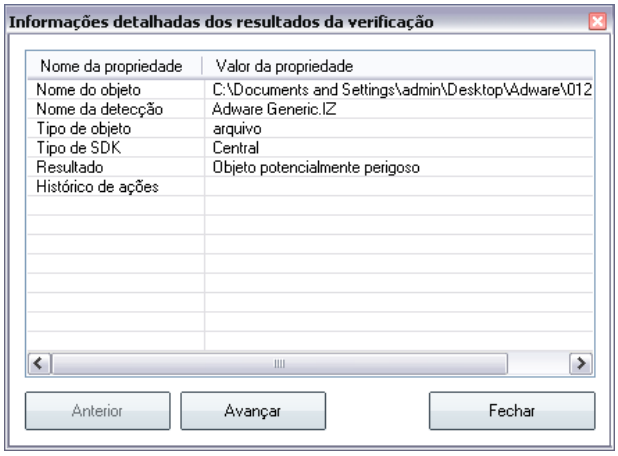
- **_Objeto potencialmente perigoso_** - o objeto foi detectado como potencialmente perigoso, mas não infectado (ele pode conter macros, por exemplo). As informações devem ser consideradas apenas um aviso.

- **_Reinicialização necessária para concluir ação_** - não é possível remover o objeto infectado. Para removê-lo completamente, é necessário reiniciar o computador.

Botões de controle

Há três botões de controle disponíveis nessa caixa de diálogo:

- **_Exibir detalhes_** - o botão abre uma nova janela de diálogo denominada Detalhes do resultado da verificação**:**



  Nessa caixa de diálogo você pode encontrar informações sobre o local do objeto infectado detectado (**_Nome da propriedade_**). Usando os botões **_Voltar_**/**_Avançar_**, você pode ver informações sobre descobertas específicas. Use o botão **_Fechar_** para sair da caixa de diálogo.

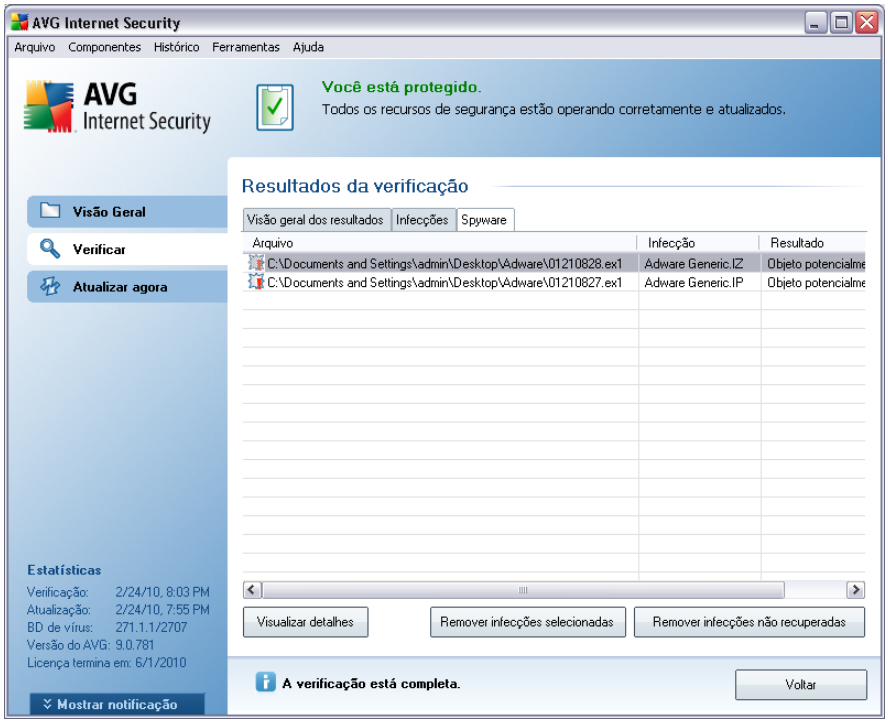
- **_Remover infecções selecionadas_** - use o botão para mover a descoberta selecionada para a ***Quarentena.***

- **_Remover todas as infecções não reparadas_** - esse botão exclui todas as descobertas de vírus que não foram reparadas ou movidas para a ***Quarentena.***

- ***Fechar resultados*** - fecha a visão geral das informações e volta para a caixa de diálogo ***Visão geral dos resultados da verificação***.

12.7.4. Guia Avisos

A guia ***Avisos*** exibe informações sobre objetos "suspeitos" (*normalmente arquivos*) detectados durante a verificação. Quando detectados pela ***Proteção Residente***, esses arquivos têm o acesso bloqueado. Exemplos típicos desse tipo de descoberta são: arquivos ocultos, cookies, chaves de Registro suspeitas, documentos ou arquivos protegidos por senha etc Tais arquivos não representam uma ameaça direta para o seu computador ou para a sua segurança. Informações sobre esses arquivos costumam ser úteis no caso de ser detectado um adware ou spyware no seu computador. Se o teste do AVG detectar apenas Avisos, nenhuma ação será necessária.



Esta é uma breve descrição dos exemplos mais comuns de tais objetos:

- ***Arquivos ocultos*** - por padrão, arquivos ocultos não são visíveis no Windows, e alguns vírus ou outras ameaças podem tentar evitar sua detecção armazenando seus arquivos com esse atributo. Se o AVG relatar um arquivo oculto que você suspeita ser mal-intencionado, será possível removê-lo para a ***Quarentena de vírus do AVG***.

- ***Cookies*** - cookies são arquivos de texto não-formatado usados em sites para armazenar informações específicas do usuário, usadas posteriormente para carregar o layout personalizado do site, preencher o nome do usuário etc.

- ***Chaves do registro suspeitas*** - certos tipos de malware armazenam suas informações no registro do Windows, para garantir o seu carregamento na inicialização ou ampliar seu efeito no sistema operacional.

12.7.5. Guia Rootkits

A guia ***Rootkits*** exibe informações sobre rootkits detectados durante a verificação; se você tiver ativado a ***Verificação anti-rootkit*** ou se tiver adicionado manualmente a opção de verificação anti-rootkit em ***Verificação do computador inteiro*** (*essa opção está desativada por padrão*).

Um rootkit é um programa criado para assumir o controle fundamental de um sistema de computador, sem autorização dos proprietários do sistema e gerentes legítimos.*** O acesso ao hardware é realmente necessário, pois um rootkit tem o objetivo de executar o controle do sistema operacional executado no hardware. Geralmente, os rootkits atuam para obscurecer sua presença no sistema por meio de subversão ou evasão de mecanismos de segurança padrão do sistema operacional. Freqüentemente, eles também são Cavalos de Tróia, levando os usuários a acreditarem que é confiável executá-los no sistema. As técnicas usadas para conseguir isso podem incluir ocultar processos em execução de programas de monitoramento ou ocultar arquivos ou dados do sistema operacional.

A estrutura dessa guia é basicamente a mesma que a da ***guia Infecções*** ou da ***guia Spyware***.

12.7.6. Guia Informações

A guia ***Informações*** contém dados como "descobertas" que não podem ser categorizadas como infecções, spyware etc. Elas também não podem ser rotuladas positivamente como perigosas, mas merecem a sua atenção. A verificação do AVG pode detectar arquivos que talvez não estejam infectados, mas que são suspeitos. Esses arquivos são indicados como ***Aviso*** ou como ***Informações***.

As ***Informações*** sobre severidade podem ser reportadas por um dos seguintes motivos:

- ***Compactado em tempo de execução*** - o arquivo foi compactado com um dos compactadores menos comuns, o que pode indicar uma tentativa de impedir a verificação desse arquivo. Entretanto, nem todos os relatórios de tal arquivo indica um vírus.

- ***Compactado em tempo de execução com recorrência*** - semelhante ao problema acima, mas menos freqüente entre os softwares comuns. Esses arquivos são suspeitos e convém considerar sua remoção ou envio para análise.

- ***Arquivamento ou documento protegido por senha*** - arquivos protegidos por senha não podem ser verificados pelo AVG (*ou em geral por qualquer outro programa anti-malware*).

- ***Documento com macros*** - o documento relatado contém macros, que podem ser mal-intencionadas.

- ***Extensão oculta*** - arquivos com extensão oculta podem parecer ser, por exemplo, imagens, quando na verdade são arquivos executáveis (*por exemplo, imagem.jpg.exe*). A segunda extensão não está visível no Windows por padrão, e o AVG relata esses arquivos para evitar a abertura acidental.

- ***Caminho de arquivo impróprio*** - se algum arquivo do sistema importante estiver em execução a partir de um caminho diferente do padrão (*por exemplo, winlogon.exe em execução a partir de um caminho diferente da pasta Windows*), o AVG irá relatar essa discrepância. Em alguns casos, vírus usam nomes de processos padrão do sistema para tornar sua presença menos aparente no sistema.

- ***Arquivo bloqueado*** - o arquivo relatado está bloqueado, e por isso não pode ser verificado pelo AVG. Isso normalmente significa que algum arquivo é&; constantemente utilizado pelo sistema (*por exemplo, arquivo swap*).

12.8. Quarentena de Vírus

A Quarentena de Vírus é um ambiente seguro para o gerenciamento de objetos suspeitos ou infectados detectados durante os testes do AVG. Depois que um objeto infectado for detectado durante a verificação e o AVG não puder repará-lo automaticamente, você será solicitado a decidir o que deve ser feito com o objeto suspeito. A solução recomendável é movê-lo para a ***Quarentena de Vírus*** para futuro tratamento. O principal objetivo da Quarentena de Vírus é conservar qualquer arquivo excluído por um certo período de tempo para que você tenha certeza de que não precisa mais dele em seu local original. Se você descobrir que a ausência de arquivos causa problemas, pode enviar o arquivo em questão para análise ou restaurá-lo para o local original.

A interface da ***Quarentena de Vírus*** é aberta em uma janela separada e oferece uma visão geral das informações de objetos infectados em quarentena:

- ***Severidade***informações sobre o tipo de infecção*com base em seu nível de infecção - todos os objetos listados podem estar positivamente ou potencialmente infectados.*
- ***Nome do vírus*** - especifica o nome da infecção detectada de acordo com a Enciclopédia de vírus (on-line)
- ***Caminho para o arquivo*** - caminho completo para o local original do arquivo infectado detectado
- ***Nome original do objeto*** - todos os objetos detectados listados na tabela foram rotulados com o nome padrão dado pelo AVG durante o processo de verificação. No caso de o objeto ter tido um nome original que é conhecido (*por ex., o nome de um anexo de e-mail que não corresponda ao conteúdo real do anexo*), ele será fornecido nesta coluna.
- ***Data do armazenamento*** - data e hora que o arquivo suspeito foi detectado e armazenado na ***Quarentena de Vírus***

Botões de controle

Os botões de controle a seguir podem ser acessados na interface da ***Quarentena de Vírus***:

- ***Restaurar*** - remove o arquivo infectado de volta ao local original do disco
- ***Restaurar Como*** - caso você decida mover o objeto infectado detectado da ***Quarentena de Vírus*** para uma pasta selecionada, use este botão. O objeto suspeito e detectado será salvo com o seu nome original. Caso o nome original não seja conhecido, será usado o nome padrão.
- ***Detalhes*** – esse botão aplica-se apenas às ameaças detectadas pelo ***Identity Protection***. Ao clicar, exibe uma visão geral sinótica dos detalhes da ameaça (quais arquivos/processos foram afetados, características do processo, etc.). Observe que para todos os outros itens que não sejam detectados pelo IDP, esse botão fica esmaecido e inativo!
- ***Excluir*** - remove de maneira completa e irreversível o arquivo infectado da ***Quarentena***

- ***Esvaziar a Quarentena*** - remove completamente todo o conteúdo da ***Quarentena de Vírus*** Removendo os arquivos da área de Quarentena de Vírus, estes arquivos serão removidos de modo irreversível do disco (não serão movidos para a Lixeira).

13. Atualizações do AVG

Manter o AVG atualizado é fundamental para garantir que todos os vírus recém-descobertos sejam detectados o mais rapidamente possível.

Durante o processo de instalação, você é solicitado a especificar com que freqüência deseja atualizar o AVG. *** ***As opções disponíveis são: A cada 4 horas ou Todo dia*** *** (consulte a caixa de diálogo Programar atualizações e verificações regulares. Como as atualizações do AVG não são lançadas de acordo com programações fixas, mas de acordo com o volume e a gravidade das novas ameaças, recomenda-se verificar as novas atualizações pelo menos uma vez ao dia. A verificação a cada 4 horas garantirá que o seu AVG 9 Anti-Virus plus Firewall se mantenha atualizado também durante o dia.

13.1. Níveis de Atualização

O AVG oferece dois níveis de atualização à sua escolha:

- ***A atualização de definições*** contém as alterações necessárias para a proteção antivírus confiável. Em geral, não inclui nenhuma alteração ao código e atualiza apenas o banco de dados de definições. Essa atualização deverá ser aplicada assim que estiver disponível.

- ***A atualização do programa*** contém várias alterações, correções e aperfeiçoamentos para o programa.

Ao programar uma atualização, é possível selecionar o nível de prioridade a ser baixado e aplicado.

Observação: *se ocorrer uma coincidência de tempo de uma atualização de programa agendada e uma verificação agendada, o processo de atualização terá maior prioridade, e a verificação será interrompida.*

13.2. Tipos de Atualizações

Você pode distinguir entre dois tipos de atualização:

- ***A atualização sob demanda*** é uma atualização imediata do AVG que pode ser executada a qualquer momento que surgir a necessidade.

- ***Atualização programada*** - no AVG, também é possível predefinir um plano de atualização. A atualização planejada, então, será executada periodicamente, de acordo com a definição da configuração. Sempre que forem apresentados novos arquivos de atualização no local especificado, eles serão baixados por download diretamente da Internet ou do diretório de rede. Quando nenhuma

atualização está disponível, nada acontece.

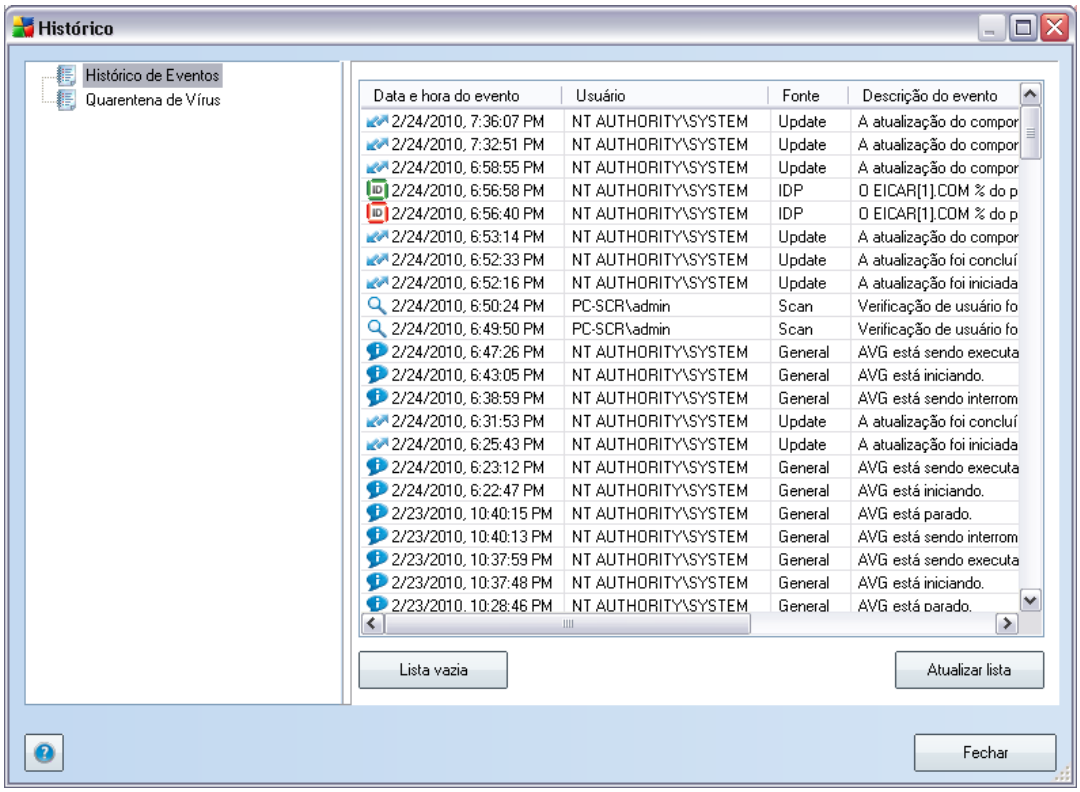
13.3. Processo de atualização

O processo de atualização pode ser inicializado imediatamente, conforme a necessidade surge, pelo link rápido ***Atualizar agora***. Esse link está disponível sempre em qualquer caixa de diálogo da Interface do usuário do AVG . Entretanto, é altamente recomendável realizar atualizações regularmente, conforme informado no programa de atualização editável com o componente Gerenciador de Atualizações.

Quando você inicia a atualização, o AVG primeiro verifica se há novos arquivos de atualização disponíveis. Se houver, o AVG inicia o download e inicializa o processo de atualização propriamente dito. Durante o processo de atualização, você será redirecionado para a interface ***Atualizar*** , onde poderá ver o andamento do processo em uma representação gráfica, bem como obter uma visão geral dos parâmetros estatísticos relevantes (*tamanho do arquivo de atualização, dados recebidos, velocidade de download, tempo decorrido etc.*).

***Nota**: Antes do início da atualização do programa AVG é criado um ponto de restauração. No caso de falha no processo de atualização e seu sistema operacional, você pode restaurar o seu SO para a configuração original deste ponto. Esta opção está disponível em Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauração do Sistema. Recomendável apenas para usuários experientes!*

14. Histórico de eventos



A caixa de diálogo ***Histórico de Eventos*** pode ser acessada no menu do sistema por meio do item ***Histórico/Log do Histórico de Eventos***. Nesta caixa de diálogo, você encontrará um resumo dos eventos importantes que ocorreram durante a operação do AVG 9 Anti-Virus plus Firewall**.** ***O Histórico de Eventos*** registra os seguintes tipos de eventos:

- Informações sobre atualizações do aplicativo AVG
- Início, fim ou interrupção de verificações (inclusive testes executados automaticamente)
- Eventos associados à detecção de vírus (pela proteção residente ou por verificação), incluindo o local de ocorrência
- Outros eventos importantes

Botões de controle

- ***Esvaziar lista*** - exclui todas as entradas da lista dos eventos
- ***Atualizar lista*** - atualiza todas as entradas da lista dos eventos

15. Perguntas Freqüentes e Suporte Técnico

Se você tiver algum problema com o seu AVG, seja comercial ou técnico, consulte a seção ***Perguntas freqüentes*** do site da AVG (http://www.avgbrasil.com.br).

Caso não consiga obter ajuda dessa forma, contate o departamento de suporte técnico por e-mail. Use o formulário de contato que pode ser acessado do menu do sistema via ***Ajuda/Obter ajuda online***.