AVG 9.0 File Server

Manual do Usuário

Revisão do documento 90.1 (5.10.2009)

Conteúdo

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG 9.0 File Server**.

Parabéns pela aquisição do AVG 9.0 File Server!

AVG 9.0 File Serveré um dos vários produtos premiados do AVG criados para fornecer a você paz de espírito e total segurança para o seu computador. Como ocorreu com todos os produtos AVG, o **AVG 9.0 File Server** 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 9.0 File Server** 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.

2. Requisitos para instalação

2.1. Sistemas operacionais com suporte

AVG 9.0 File Server destina-se à proteção de estações de trabalho com os seguintes sistemas operacionais:

- Windows 2000
- Windows XP e Windows XP Pro x64 Edition
- Windows Vista e Windows Vista x64 Edition
- Windows 2000 Server
- Windows 2003 Server e Windows 2003 Server x64 Edition
- Windows 2008 Server e Windows 2008 Server x64 Edition

(e possíveis service packs posteriores para sistemas operacionais específicos)

2.2. Requisitos de hardware

Os requisitos mínimos de hardware para **AVG 9.0 File Server:**

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

Requisitos de hardware recomendados para**AVG 9.0 File Server**:

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

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.avg.com).

Antes de começar a instalar o AVG, é altamente recomendável que você visite o site da AVG (http://www.avg.com) para verificar se há um novo arquivo de instalação. Dessa forma, você poderá garantir a instalação da versão mais recente do AVG 9.0 File Server disponível.

Recomendamos que você experimente a nossa nova ferramenta, o AVG Download Manager, que o ajudará a selecionar o arquivo de instalação apropriado!

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

AVG Download Manageré 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, **AVG Download Manager** o download 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 (SP2 e superior), Windows Vista (todas as edições).*

AVG Download Manager está disponível para download no site da AVG (http://www.avg.com). Veja a seguir uma descrição breve de cada etapa que você precisará seguir no **AVG Download Manager**:

4.1. Seleção de Idioma

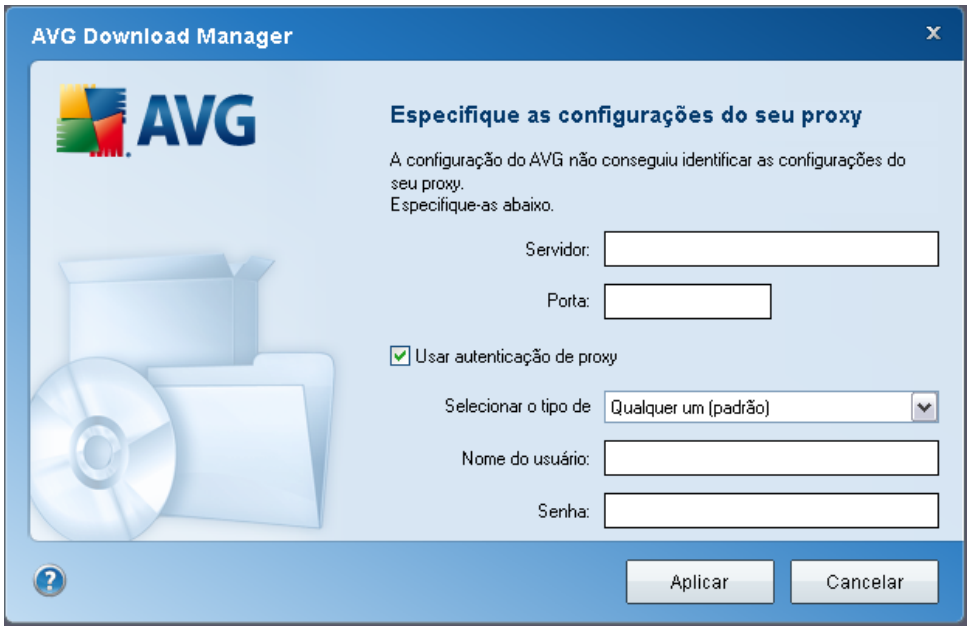
Nesta primeira etapa do **AVG Download Manager** , selecione o idioma da instalação no menu suspenso. Observe que a sua seleção de idioma se aplica somente ao processo de instalação; após a instalação, você poderá alterar o idioma diretamente das configurações do programa. Em seguida, pressione o botão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

4.2. Verificação de conectividade

Na próxima etapa, 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.

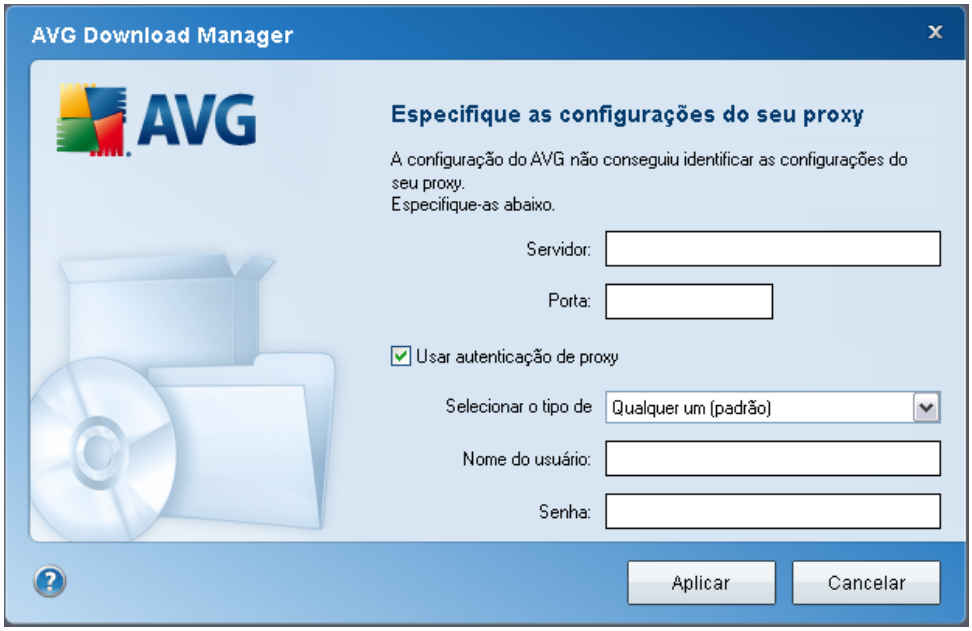
- Se o teste não mostrar conectividade, certifique-se de estar realmente conectado à Internet. Em seguida, clique no botão ***Repetir***.

- 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**.

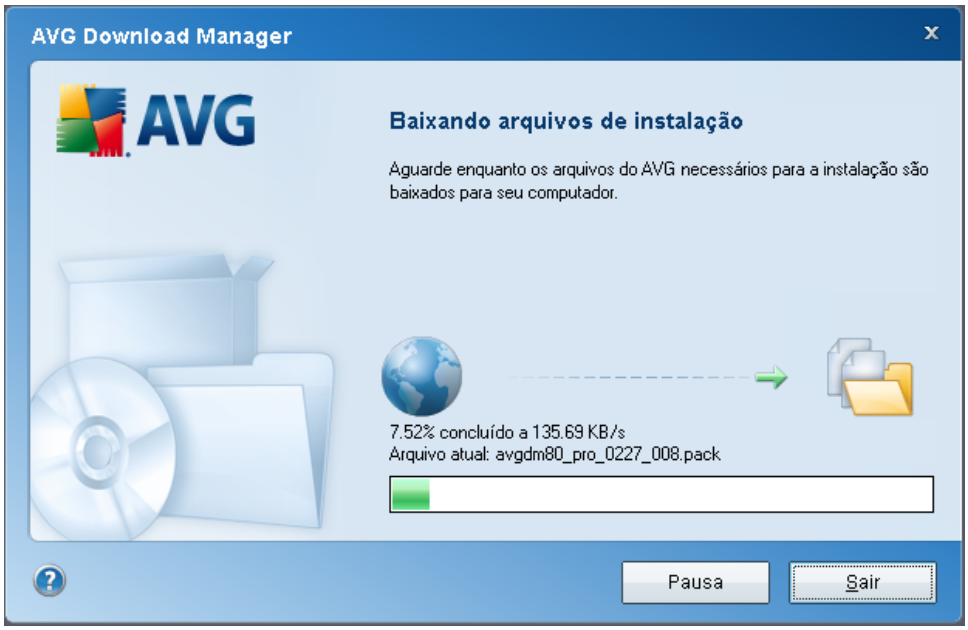
4.4. Selecione o tipo de licença

Durante esta etapa, você deve escolher o tipo de licença do produto que gostaria de

baixar. A descrição fornecida permitirá que você escolha aquela que melhor se adequar a você:

- ***Versão completa*** - isto é, ***AVG Anti-Virus***, ***AVG Anti-Virus e Firewall*** ou ***AVG Internet SecurityAVG File Server***
- ***Versão de avaliação*** - oferece a oportunidade de usar todos os recursos do produto AVG completo por um período limitado de 30 dias
- ***Versão gratuita*** - oferece proteção a usuários domésticos gratuitamente. Entretanto, as funções do aplicativo são limitadas! Além disso, a versão gratuita inclui alguns dos recursos disponíveis no produto pago.

4.5. Arquivos de download para instalação



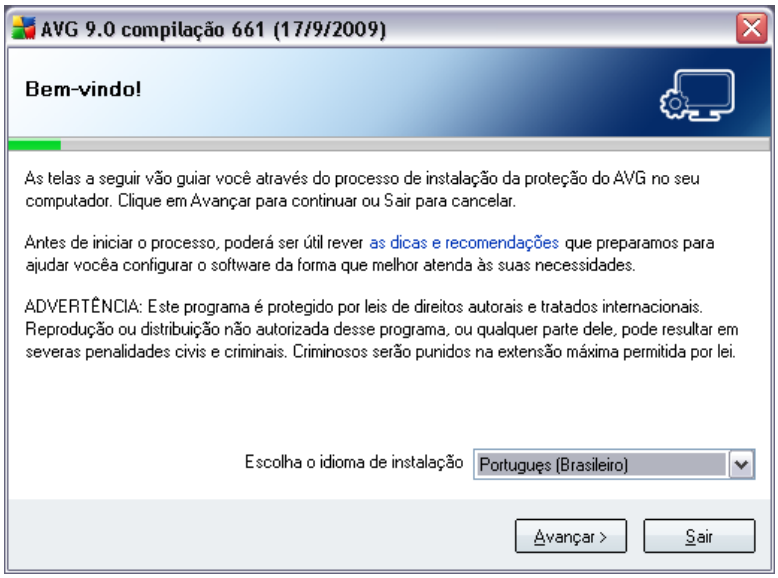
Agora, você forneceu todas as informações necessárias para o **AVG Download Manager** iniciar o download do pacote de instalação e lançar o processo de instalação. Você avançará para o Processo de Instalação do AVG.

5. Processo de instalação do AVG

Para instalar o**AVG 9.0 File Server no computador, é necessário 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.avg.com), seção ***Downloads***. 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:

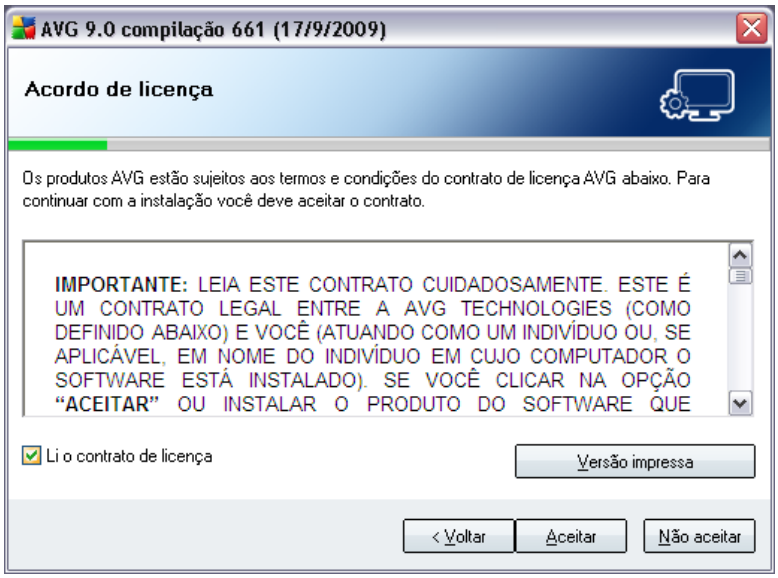
5.1. Início da instalação



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.*

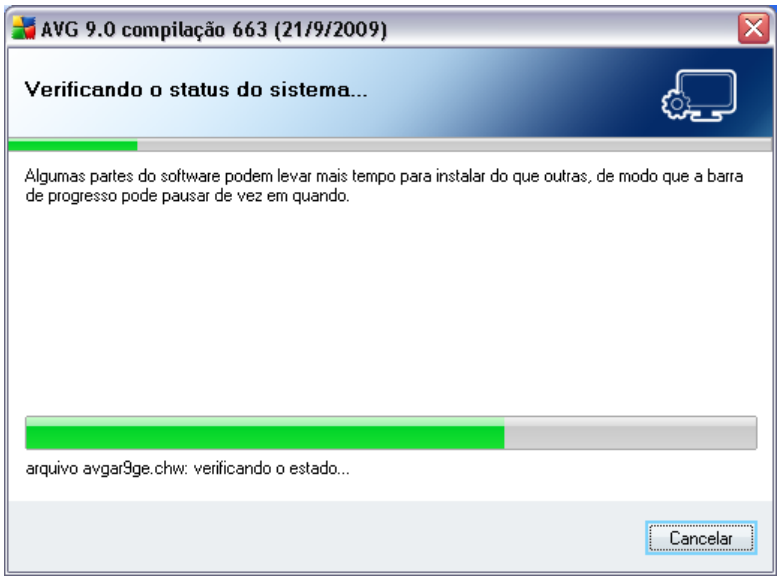
5.2. Contrato de licença



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***.

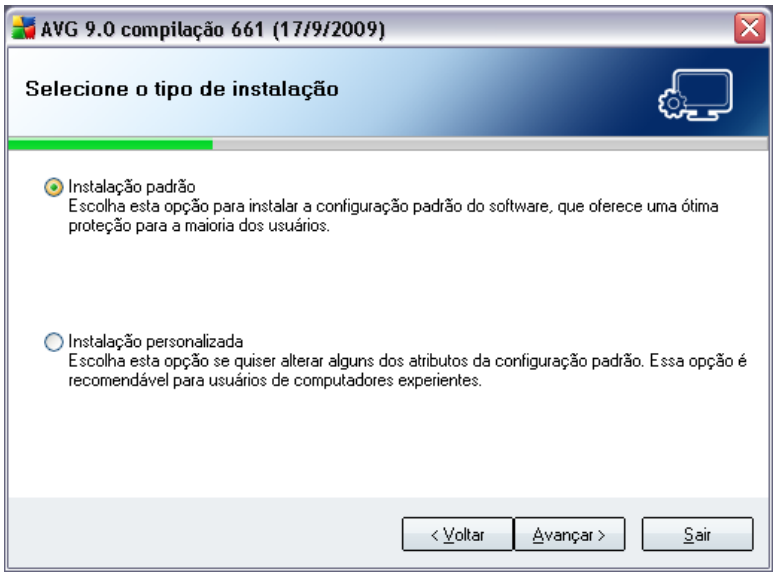
Se você não concordar com o contrato de licença, pressione o botão ***Não aceito*** e o processo de instalação será encerrado imediatamente.

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.

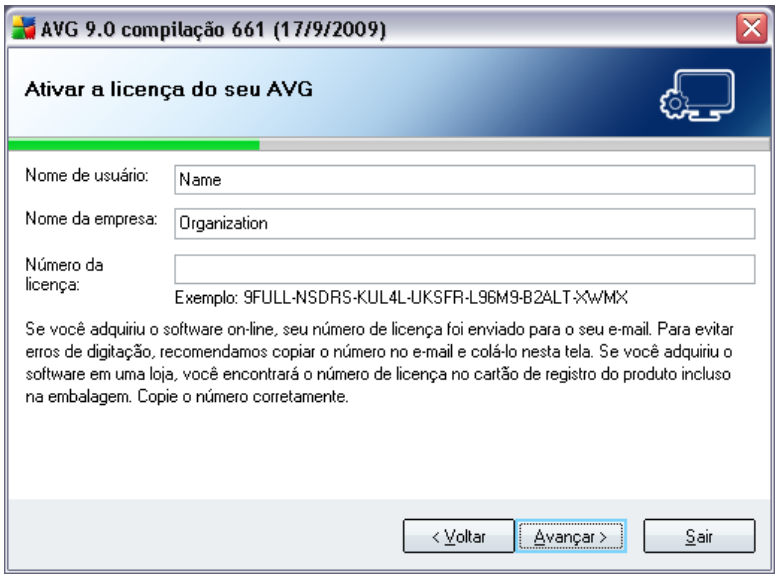
A instalação personalizada só deve ser usada por usuários experientes que tenham um motivo válido para instalar o AVG com configurações diferentes das padrão, ou seja, para se ajustar aos requisitos específicos do sistema.

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 9.0 File Server**. O número da licença está no e-mail de confirmação recebido

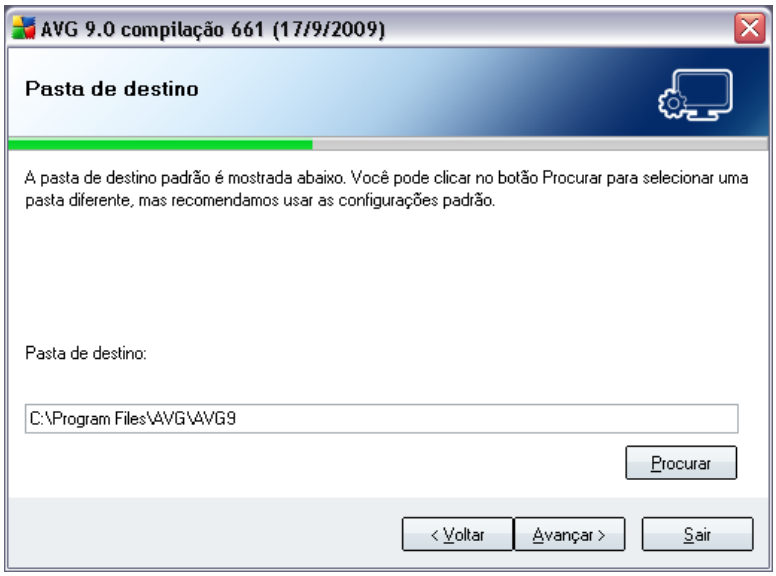
depois da aquisição do **AVG 9.0 File Server** on-line. Digite o número exatamente como mostrado. Se o formulário digital do número de licença estiver disponível (*no e-mail*), é recomendável usar o método de copiar e colar para inseri-lo.



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 ***Instalação do AVG*** **.** Se a instalação personalizada tiver sido selecionada, você continuará na caixa de diálogo ***Pasta de Destino***.

5.6. Instalação personalizada - Pasta de destino

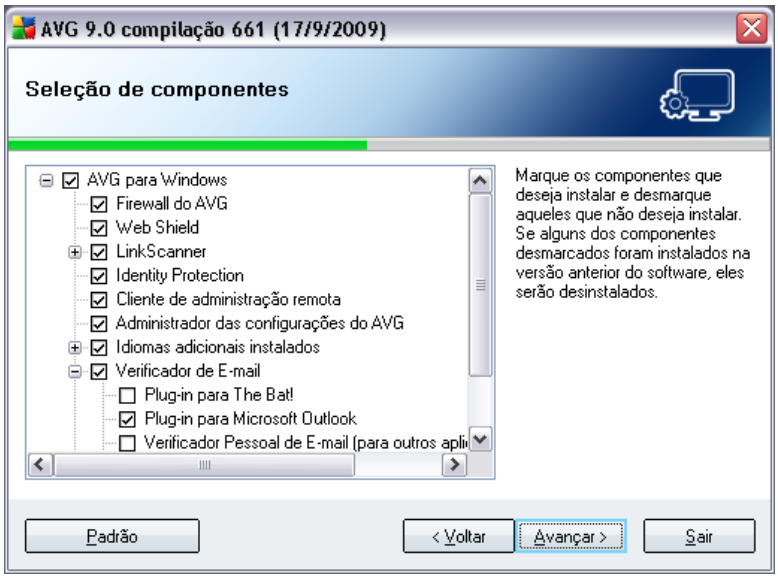


A caixa de diálogo ***Pasta de destino*** permite especificar o local de instalação do **AVG 9.0 File Server**. Por padrão, o AVG será instalado na pasta Arquivos de Programas da unidade C:. Se a pasta ainda não existir, uma nova caixa de diálogo solicitará que você confirme se deseja que o AVG a crie 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 os componentes do que podem ser instalados.**AVG 9.0 File Server** 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.

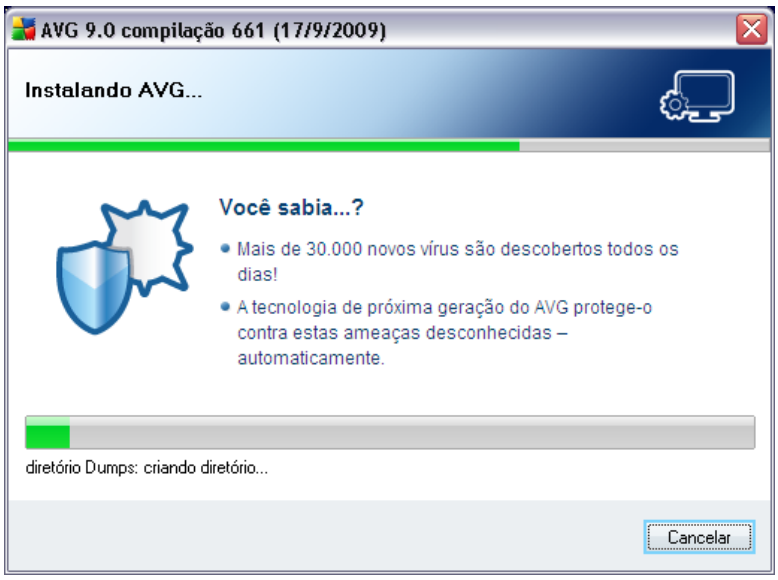
- ***Administração Remota***

  Se você planeja conectar o computador posteriormente à Administração remota do AVG, marque o respectivo item para que ele também seja instalado.

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

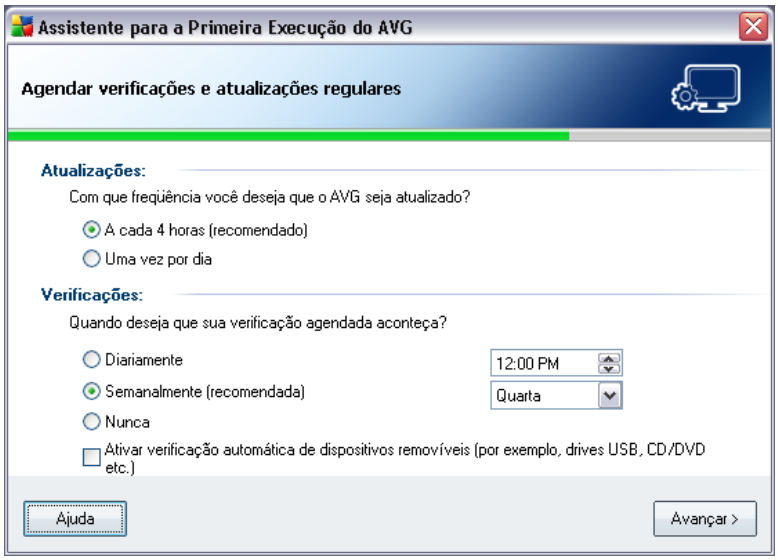
5.8. Instalando o AVG

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



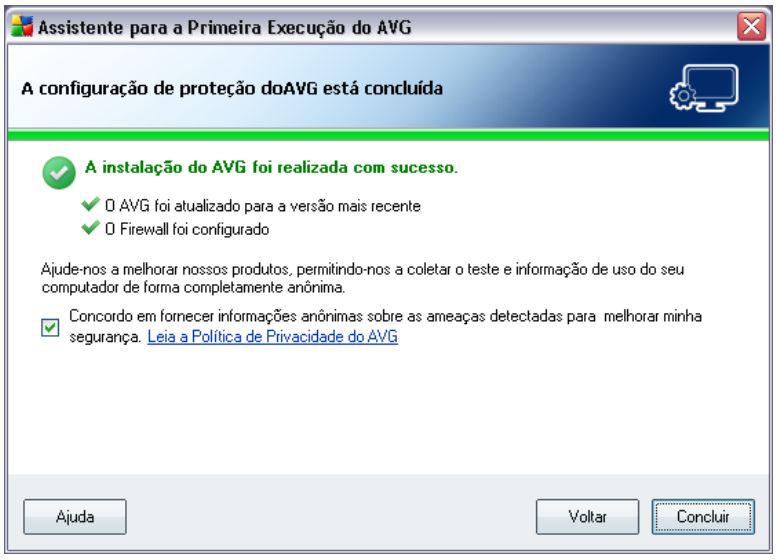
Após a conclusão do processo de instalação, você será redirecionado à próxima caixa de diálogo automaticamente.

5.9. 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.

5.10. A configuração da proteção do AVG está concluída



Agora, o **AVG 9.0 File Server** está 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. Registro do produto

Ao concluir a instalação do **AVG 9.0 File Server**, registre o produto online no site do AVG (http://www.avg.com), 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.

6.2. 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
- no menu ***Iniciar/Programas/AVG 9.0/Interface do Usuário do AVG***

6.3. 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 9.0 File Server** . 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***.

6.4. Teste Eicar

Para confirmar se o **AVG 9.0 File Server** foi instalado corretamente, realize um 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, a ***Proteção Residente*** ***reagirá a ele com um aviso.*** Esse aviso da ***Proteção Residente*** ***demonstra que o AVG está instalado corretamente em seu computador.***

Se o AVG falhar na identificação do teste EICAR como sendo um vírus, você deverá verificar novamente a configuração do programa.

6.5. Configuração padrão do AVG

A configuração padrão (*isto é, como o aplicativo é configurado logo após a instalação*) do **AVG 9.0 File Server**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

AVG 9.0 File Server abre 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. Ele se localiza horizontalmente, na parte superior da janela principal do **AVG 9.0 File Server**. 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 9.0 File Server**. 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***

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

- ***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***

- ***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 9.0 File Server** .

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 9.0 File Server**

- ***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 9.0 File**

Server. Em geral, é recomendável manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.

7.1.5. Ajuda

- ***Conteúdo*** - abre os arquivos de ajuda do AVG
- ***Obter ajuda on-line*** - abre o site da AVG (http://www.avg.com) na página de suporte técnico ao cliente
- ***Seu AVG Web*** - abre o site da AVG (http://www.avg.com)
- ***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.avg.com). Informe os dados de registro; somente os clientes que registrarem seus produtos AVG poderão receber suporte técnico gratuito.
- ***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 9.0 File Server**. 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 da 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 freqüência 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 ***Testes 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 (*imagem 2)*.

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

A seção **AVG 9.0 File Server*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 Anti-Rootkit*** detecta programas e tecnologias que tentam camuflar malware - detalhes>>
- ***A Licença*** fornece o texto completo do Contrato de licença do AVG - 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 pela cor cinza do 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 8.0.xx, onde 8.0 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

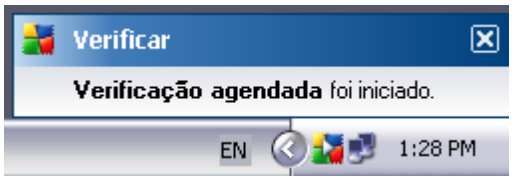
O Ícone da Bandeja do Sistema (*na barra de tarefas do Windows*) indica o status atual do **AVG 9.0 File Server.** Ele fica visível sempre na bandeja do sistema, independentemente de a janela principal do AVG estar aberta ou fechada.

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 cinza 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, 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. Anti-Vírus

8.1.1. Princípios do Anti-Vírus

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.

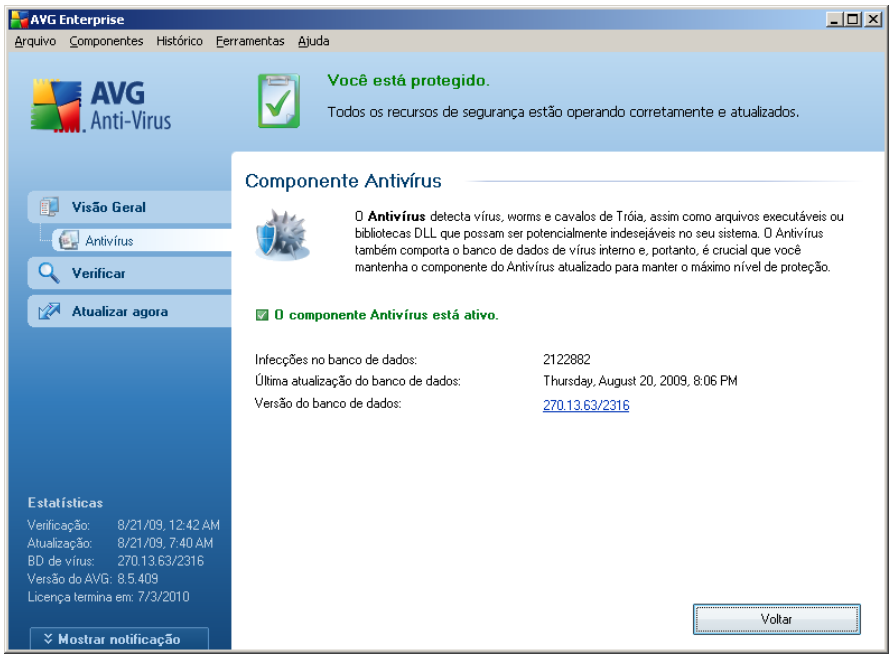
O recurso importante da proteção antivírus é que nenhum vírus conhecido pode ser executado no computador!

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 nova caixa de diálogo Configurações Avançadas do AVG.*

8.2. Anti-Spyware

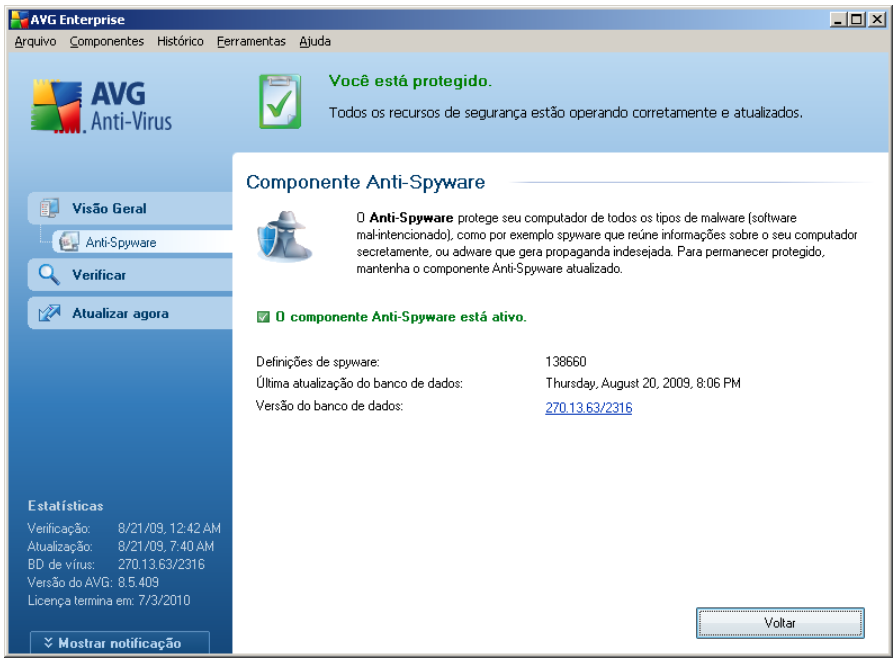
8.2.1. Princípios do Anti-Spyware

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 últimas atualizações de banco de dados e **AVG 9.0 File Server**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***:

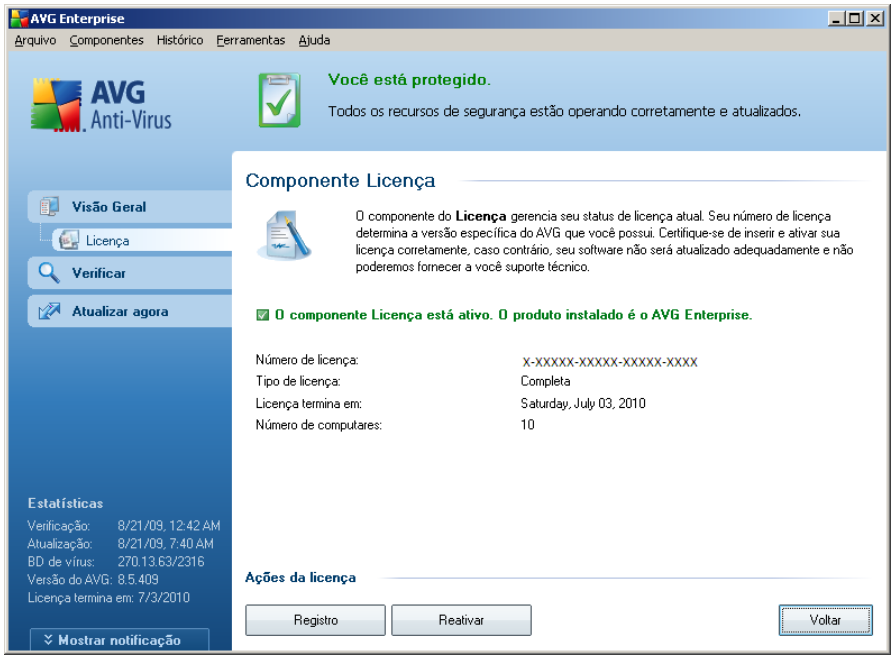
- ***Definições de spyware*** - o número fornece a contagem de amostras de spyware definidas na versão do banco de dados de spyware mais recente.
- ***Atualização mais recente do banco de dados*** - especifica quando e a que horas o banco de dados do spyware foi atualizado
- ***Versão do banco de dados*** - 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 nova caixa de diálogo* [*Configurações Avançadas do AVG*](#)*.*

8.3. 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 9.0 File Server** 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 9.0 File Server**.

Botões de controle

- ***Registre-se*** - estabelece uma conexão com a página de registro do site da AVG (http://www.avg.com). 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*).

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

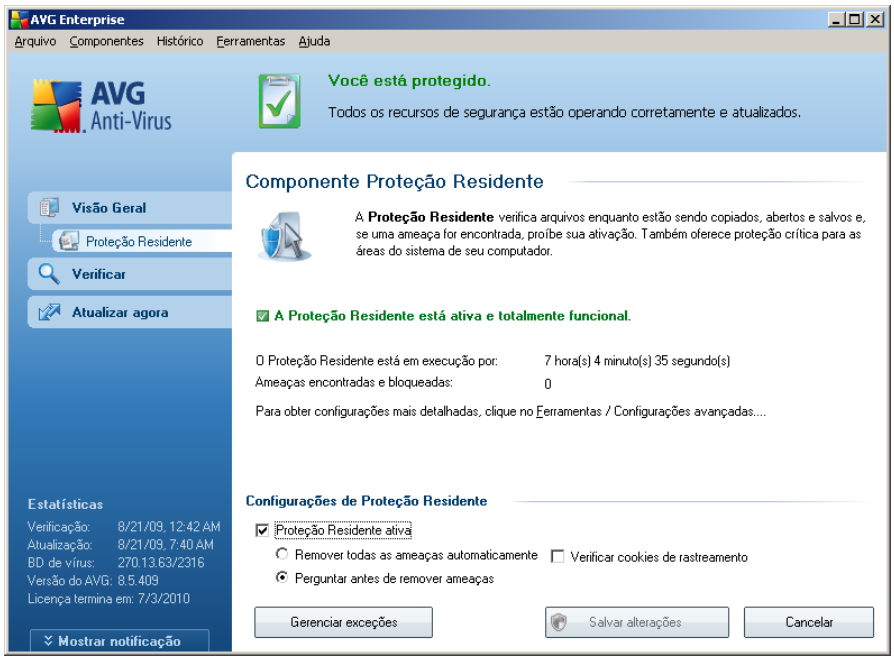
8.4. Proteção Residente

8.4.1. 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!

8.4.2. 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 ***Remover os cookies automaticamente.*** 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 nova caixa de diálogo Configurações Avançadas do AVG.*

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).

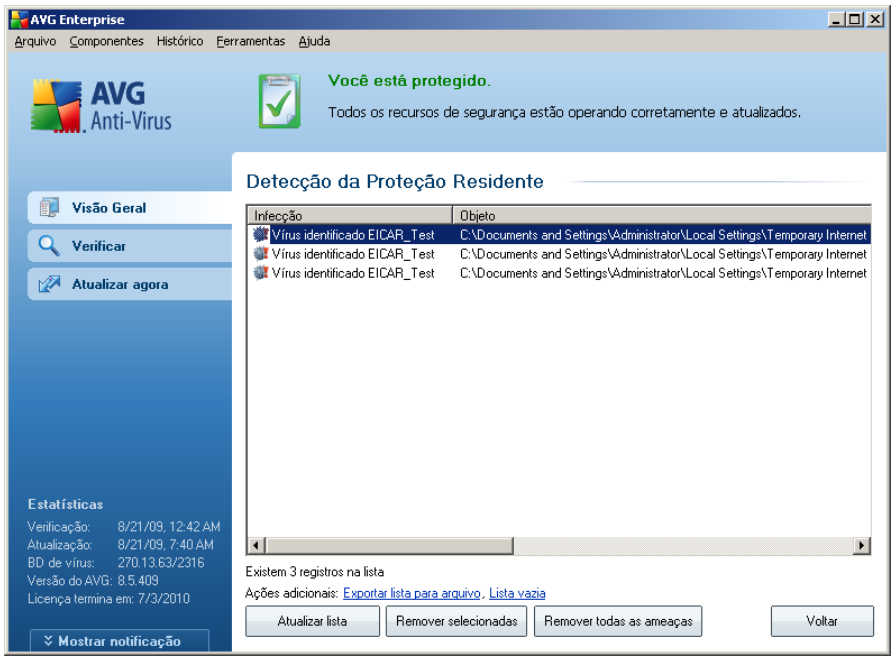
8.4.3. Detecção da Proteção Residente

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).

8.5. Gerenciador de Atualizações

8.5.1. Princípios do Gerenciador de Atualizações

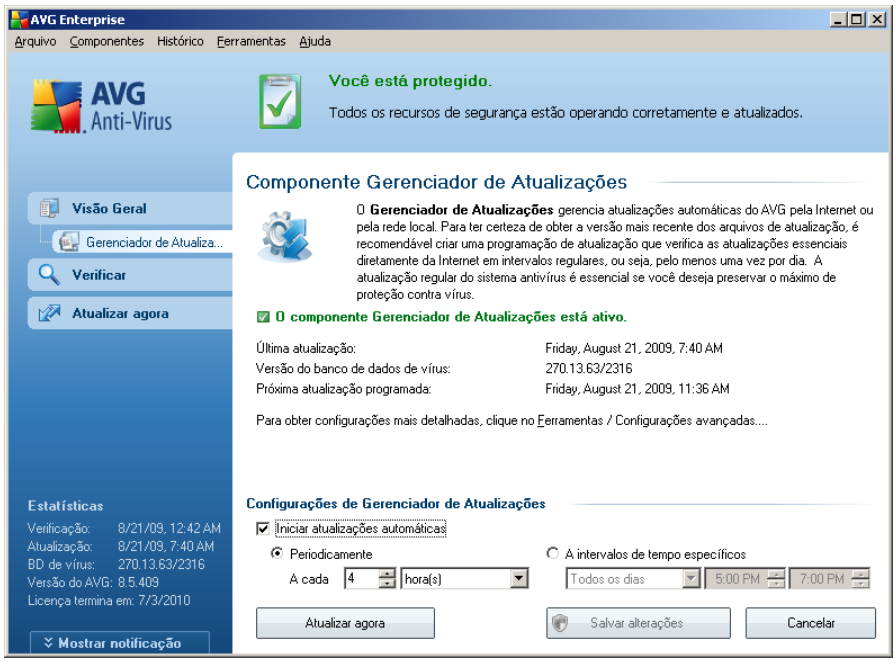
Nenhum software de segurança pode garantir proteção real de vários tipos de ameaças se não for regularmente atualizado! Os criadores de vírus estão sempre em busca de novas brechas que possam explorar em softwares e sistemas operacionais. Novos vírus, novos malwares, novos ataques de hackers surgem diariamente. 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.*

8.5.2. 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 software 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 nova caixa de diálogo Configurações Avançadas do AVG.*

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).

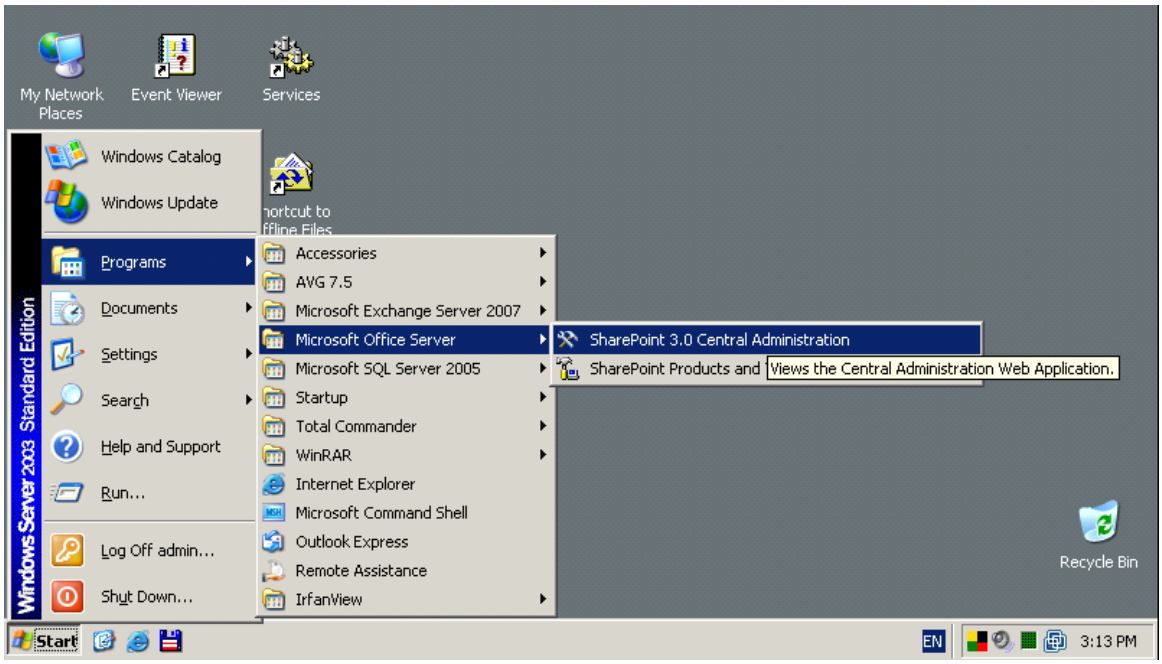
9. AVG para SharePoint Portal Server

Este capítulo trata da manutenção do AVG no ***MS SharePoint Portal Server***, que pode ser considerado um tipo especial de servidor de arquivos.

9.1. Manutenção do Programa

AVG para SharePoint Portal Serverusa a interface de verificação de vírus Microsoft SP VSAPI 1.4 para proteger o servidor contra a possível infecção de vírus. Os objetos no servidor são testados em relação à presença de malware quando baixados e/ou enviados do servidor ou no servidor por seus usuários. A configuração da proteção antivírus pode ser definida usando a interface da ***Administração Central*** do seu SharePoint Portal Sever. Na ***Administração Central*** você também pode exibir e gerenciar o **AVG para SharePoint Portal Server** arquivo de log.

Você pode iniciar a ***Administração Central do SharePoint Portal Server*** quando conectado ao computador em que seu servidor estiver sendo executado. A interface do administrador está baseada na Web (*bem como a interface do usuário do SharePoint Portal Server*), e você pode abri-la usando a opção ***Administração Central do SharePoint (3.0)*** na pasta ***Programas/Servidor Microsoft Office*** (***ou SharePoint Portal Server***) do menu Iniciar do ***Windows*** :



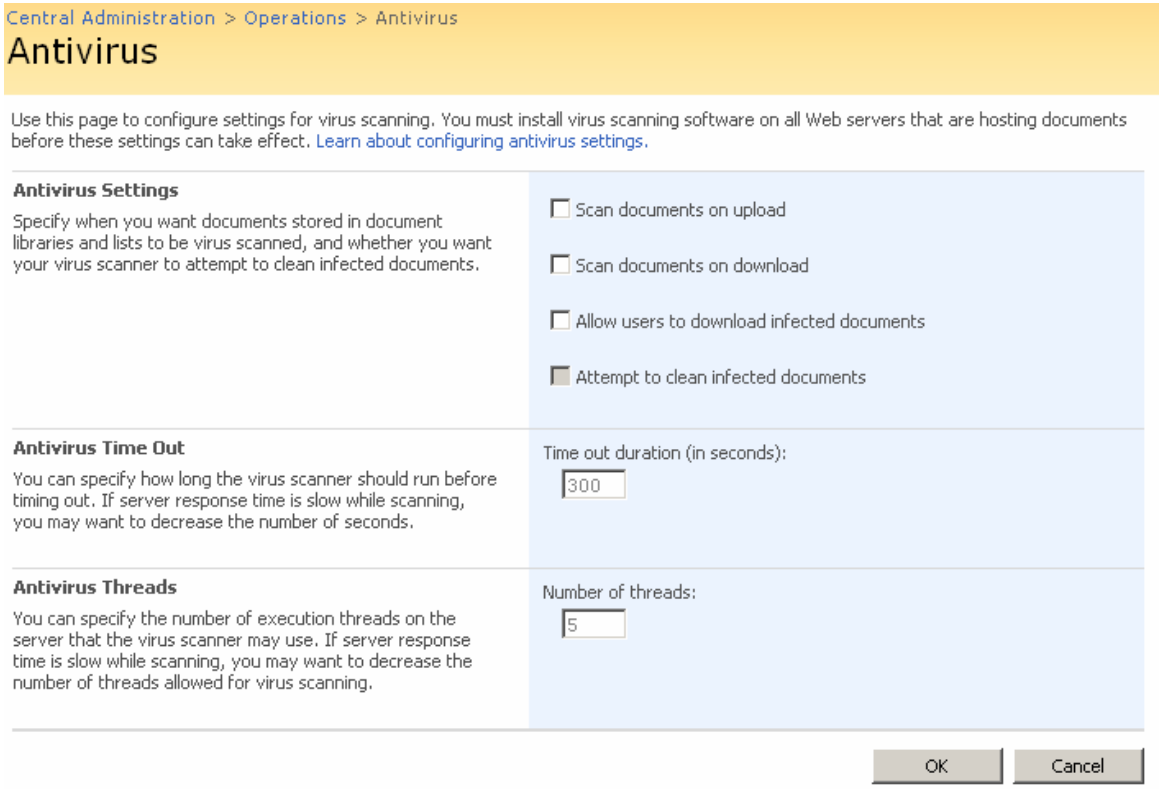
Você também pode digitar remotamente a página da Web da ***Administração Central***

do SharePoint Portal Server usando os direitos de acesso e URL apropriados.

9.2. AVG para Configuração SPPS - SharePoint 2007

Na interface da ***Administração Central do SharePoint 3.0*** você pode configurar com facilidade parâmetros de desempenho e ações do **AVG para SharePoint Portal Server** verificador. Selecione a opção ***Operações*** na seção***Administração Central***. Uma nova caixa de diálogo será exibida. Selecione o item ***Anti-vírus***na parte ***Configuração de segurança***.

Em seguida, esta janela será exibida:



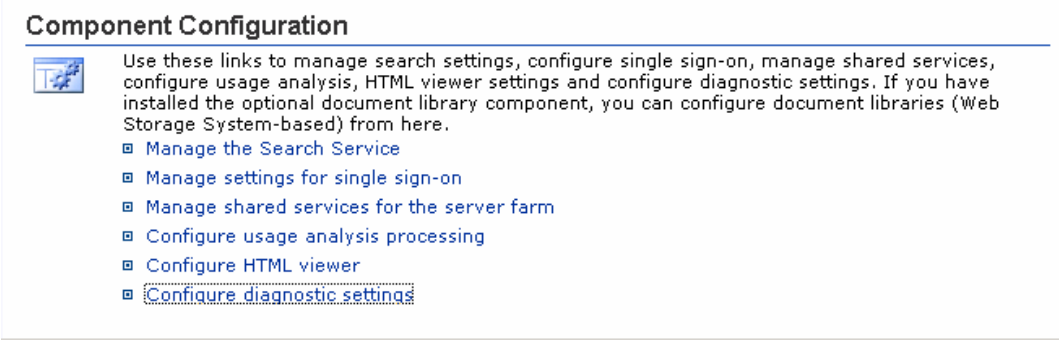
Você pode configurar várias **AVG para SharePoint Portal Server** ações de verificação e recursos de desempenho do antivírus aqui:

- ***Verificar documentos no envio*** – ativa/desativa a verificação de documentos que estão sendo enviados
- ***Verificar documentos no download*** – ativa/desativa a verificação dos documentos que estão sendo baixados
- ***Permitir que usuários façam download de documentos infectados*** – permite/não permite que usuários façam download de documentos infectados
- ***Limpar documentos infectados*** – ativa/desativa a eliminação automática de documentos infectados
- ***Duração de tempo limite*** (*em segundos*) - o número máximo de segundos durante o qual o processo de verificação de vírus será executado após a inicialização simples (diminuir o valor quando a resposta do servidor parecer lenta durante a verificação de documentos)

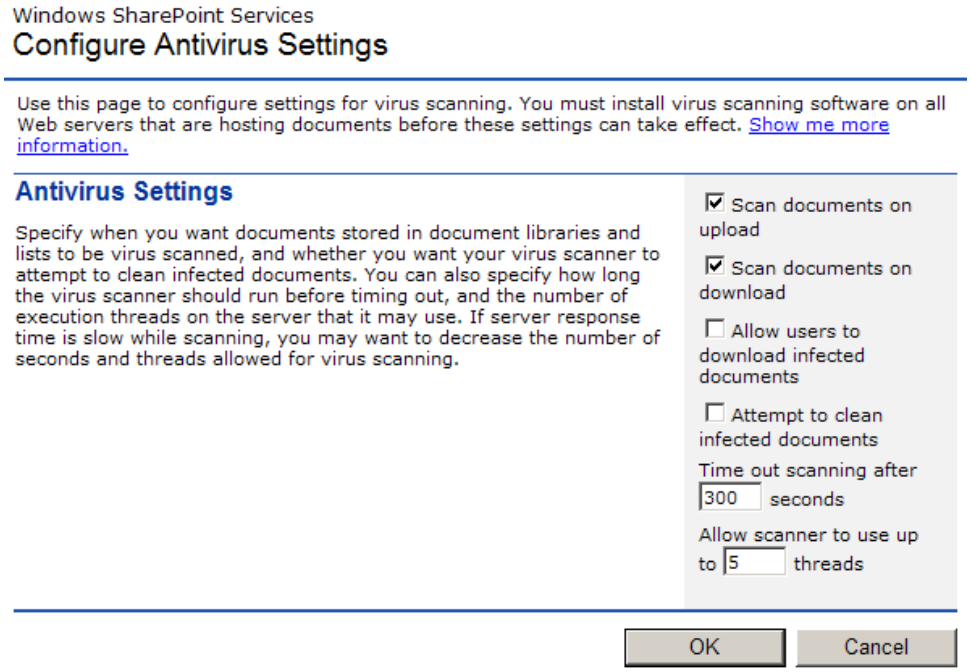
- ***Número de processos*** - você pode especificar o número de processos de verificação de vírus que podem ser executados simultaneamente; aumentar o número pode agilizar a velocidade da verificação devido ao nível de paralelismo mais alto; por outro lado, pode aumentar o tempo de resposta do servidor

9.3. AVG para Configuração SPPS - SharePoint 2003

Na interface da ***Administração Central do SharePoint Portal Server*** você pode configurar com facilidade os parâmetros de desempenho e as ações do **AVG para SharePoint Portal Server** verificador. Selecione a opção ***Configuração de ações do antivírus*** na seção ***Configuração de segurança***:



Em seguida, esta janela será exibida:



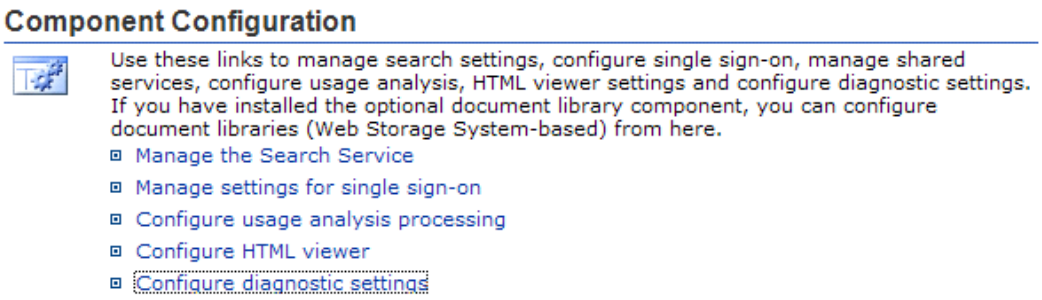
Você pode configurar várias **AVG para SharePoint Portal Server** ações de verificação e recursos de desempenho do antivírus aqui:

- ***Verificar documentos no envio*** – ativa/desativa a verificação de documentos que estão sendo enviados
- ***Verificar documentos no download*** – ativa/desativa a verificação dos documentos que estão sendo baixados
- ***Permitir que usuários façam download de documentos infectados*** – permite/não permite que usuários façam download de documentos infectados
- ***Limpar documentos infectados*** – ativa/desativa a eliminação automática de documentos infectados
- ***Tempo limite de verificação*** – o número máximo de segundos que o processo de verificação de vírus será executado após iniciliazação simples (*diminui o valor quando a resposta do servidor ' parecer lenta durante a verificação de documentos*)
- ***Máx. uso Subprocessos X durante a verificação de documentos*** – X especifica o número de processos de verificação de vírus que podem ser

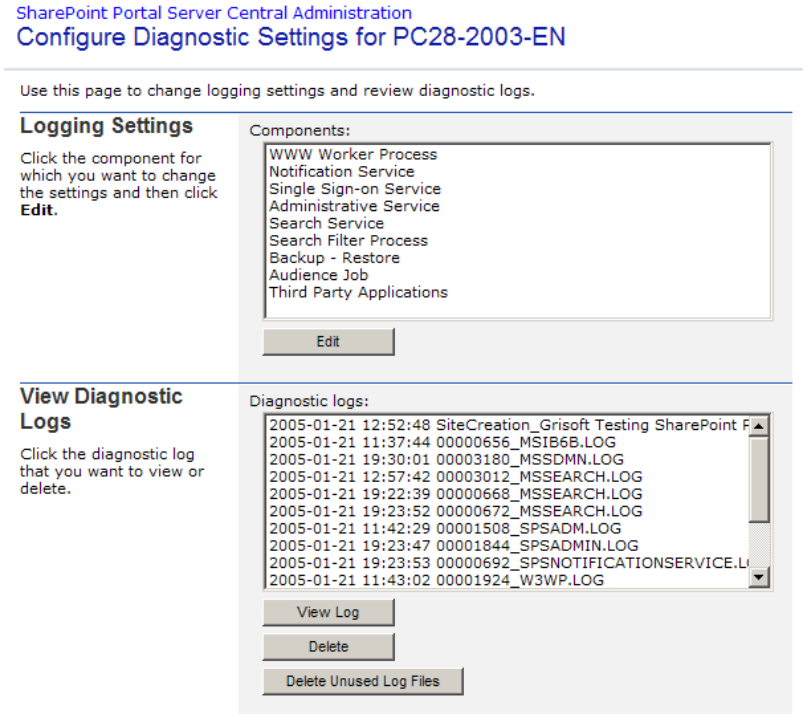
executados simultaneamente; aumentar o número pode agilizar a velocidade da verificação devido ao nível mais alto de paralelismo; por outro lado, pode aumentar o tempo de resposta do servidor

9.4. AVG para diagnóstico de edição SPPS

As mensagens de diagnóstico do **AVG para SharePoint Portal Server** podem ser exibidas após a seleção de ***Configuração de definições de diagnóstico*** na seção ***Configuração de componentes da Administração Central do SharePoint***:



Todas as informações de diagnóstico relacionadas ao desempenho do**AVG para SharePoint Portal Server** são armazenadas no arquivo *_AVG4SPS.LOG. O conteúdo deste arquivo pode ser exibido após selecionado na seção ***Exibir protocolos de diagnóstico*** da janela ***Configuração de definições de diagnóstico*** :



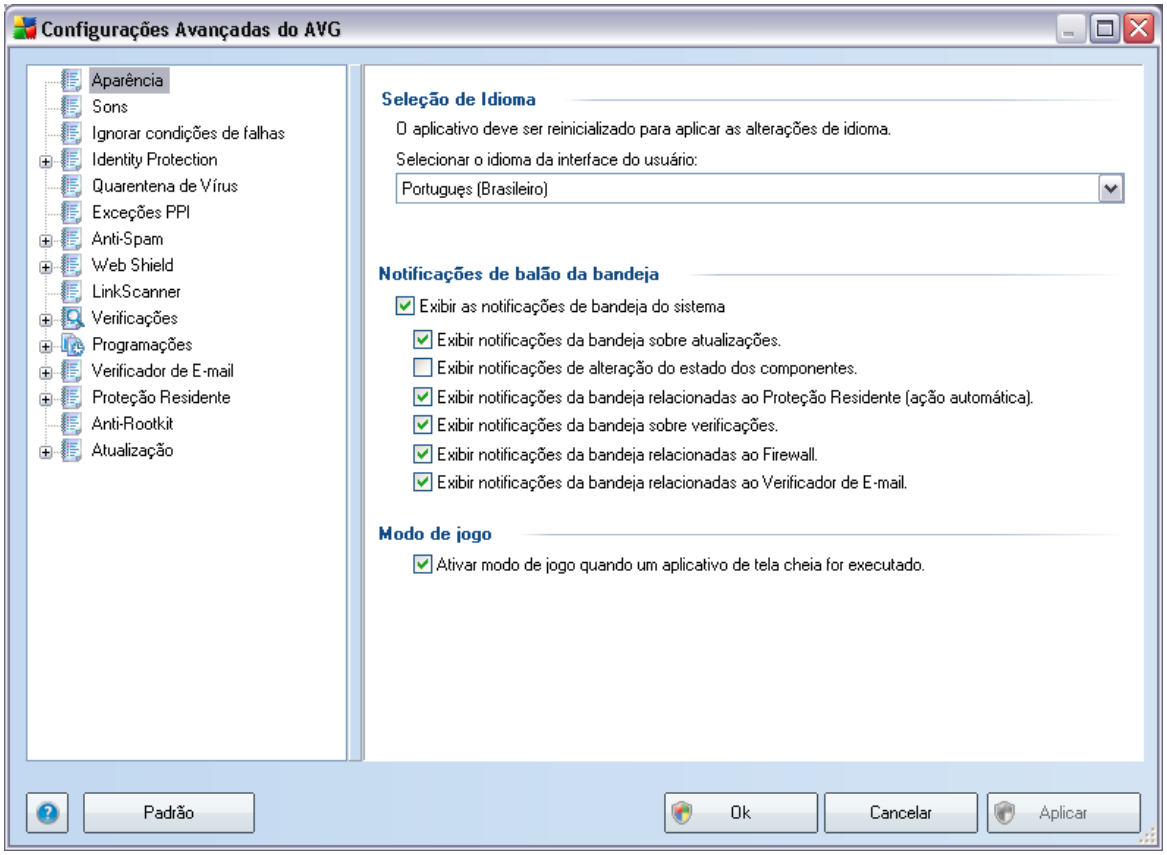
Pressione o botão ***Exibir log*** para exibir o arquivo de log do **AVG para SharePoint Portal Server**.

10. Configurações Avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG 9.0 File Server** 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

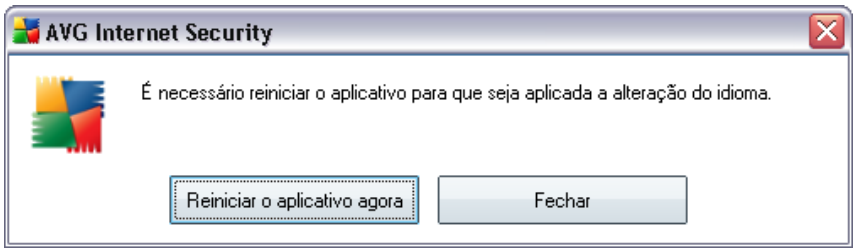
O primeiro item na árvore de navegação, ***Aparência***, refere-se às configurações gerais dainterface de usuário do AVG e algumas opções elementares do comportamento do aplicativo:



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;

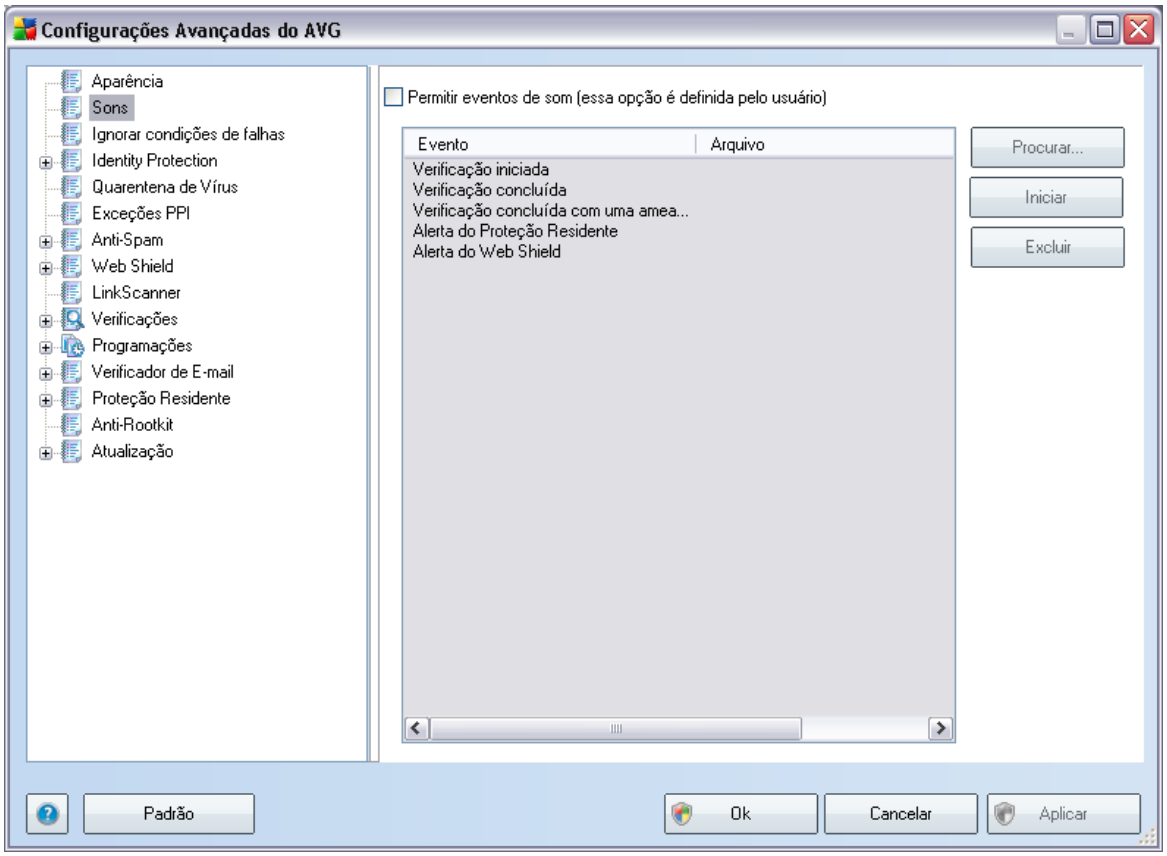
- ***Exibir notificações sobre verificação*** - decida se as informações sobre início automático da verificação agendada, seu andamento e resultados devem ser exibidos.

Modo de jogo

Essa função do AVG foi projetada para aplicativos de tela inteira que precisam se comunicar via Internet, e possíveis caixas de diálogo de solicitação do AVG poderiam afetar o aplicativo (*minimizá-lo 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:

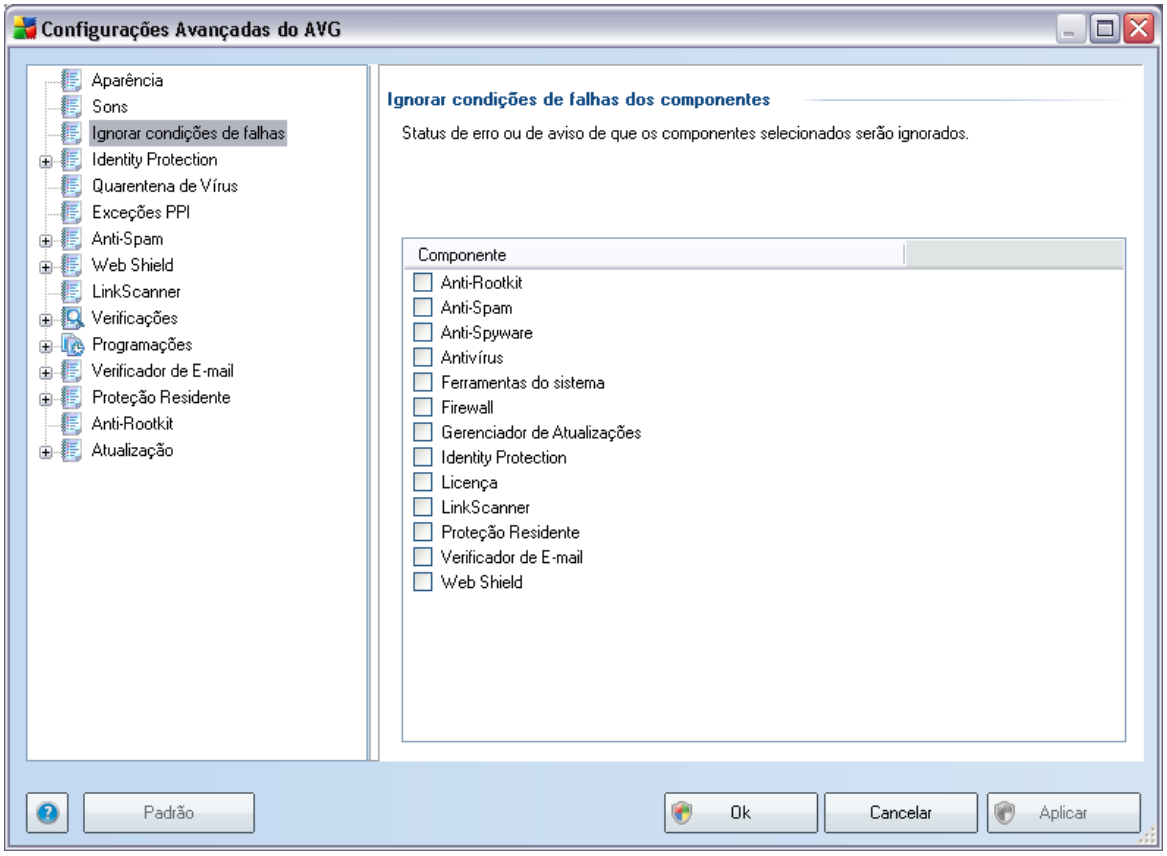


Em seguida, selecione o respectivo evento na lista e procure (usando a opção ***Procurar***) um som apropriado no disco rígido que deseja atribuir a esse evento. Para ouvir o som selecionado, realce o evento na lista e pressione o botão ***Reproduzir***. Use o botão ***Excluir*** para remover o som atribuído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



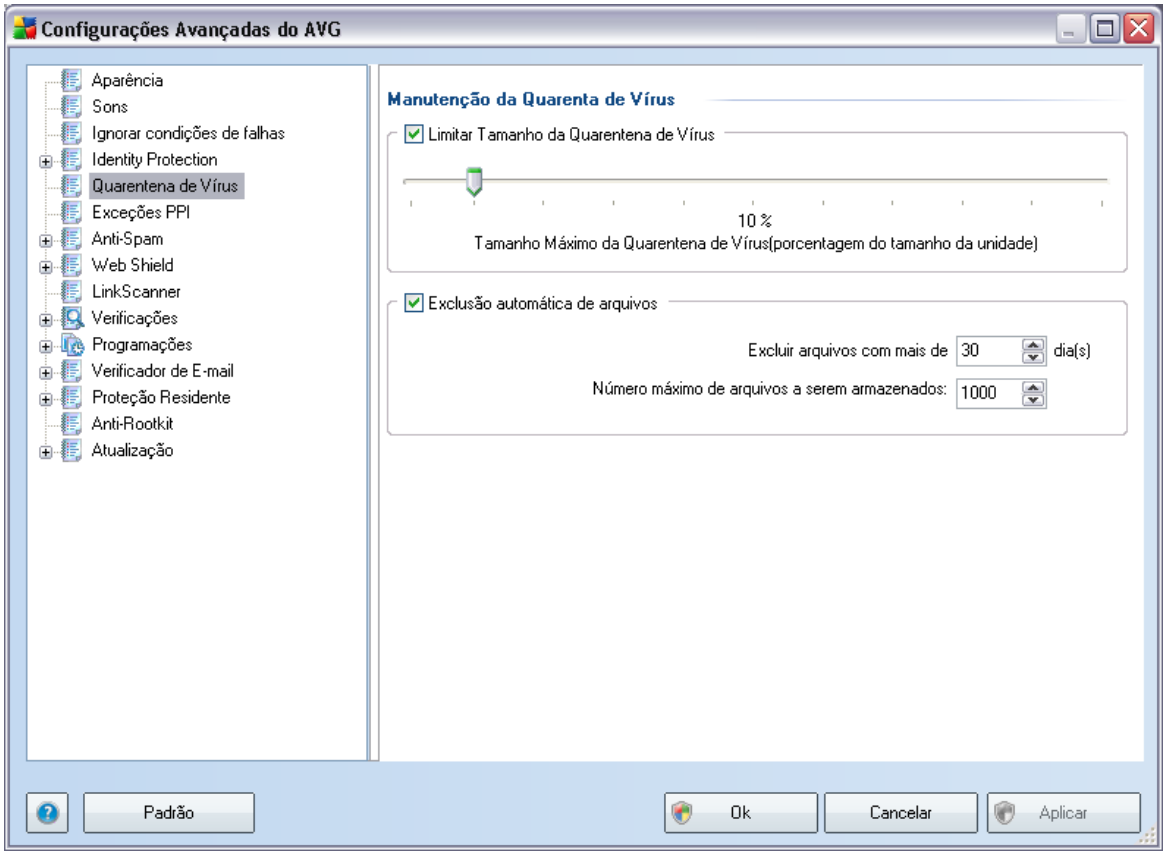
Por padrão não há componentes selecionados nesta lista. Isto significa que, caso qualquer componente receba um status de erro, você será informado sobre isso imediatamente via:

- ***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



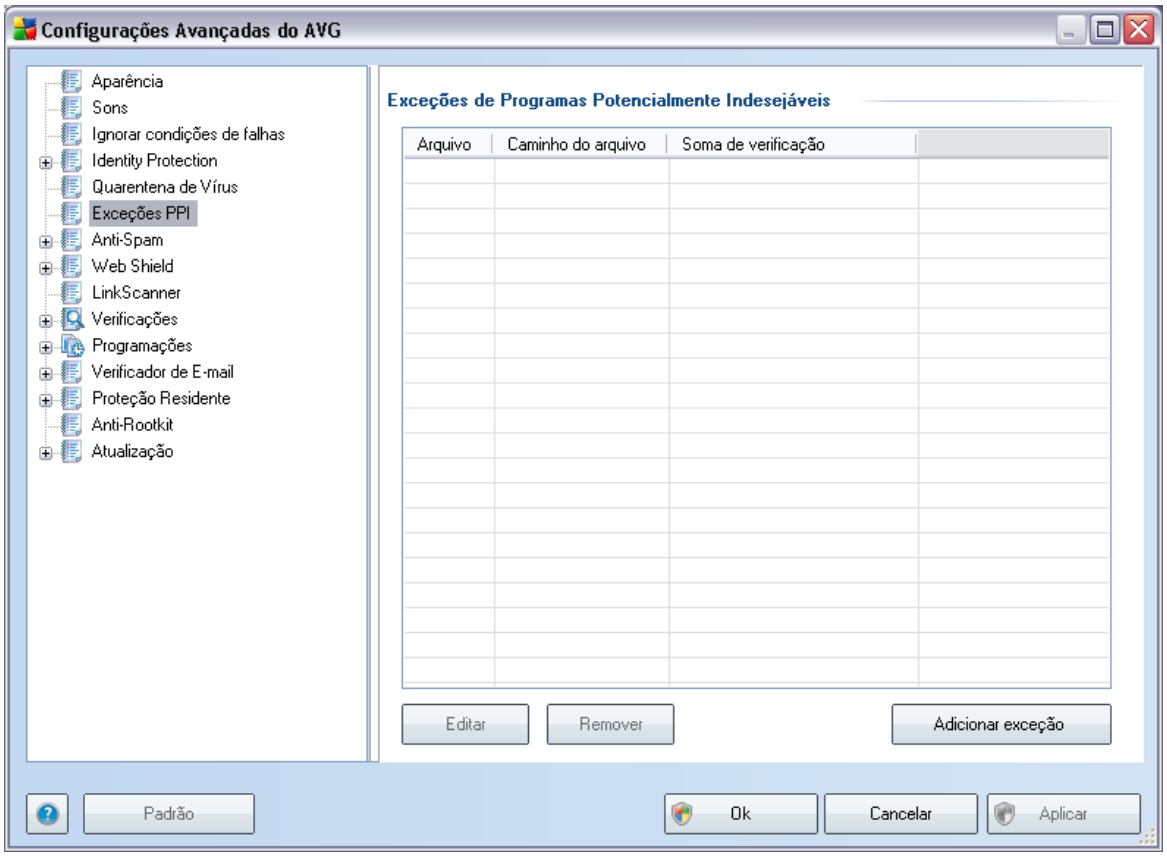
A caixa de diálogo ***Manutenção da quarentena*** permite definir vários parâmetros relativos à administração de objetos armazenados na ***Quarentena***:

- ***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

AVG 9.0 File Server O 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:

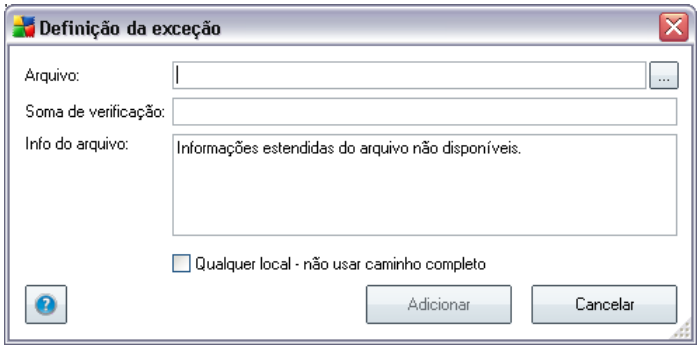
- ***Arquivo*** - fornece o nome do respectivo aplicativo
- ***Caminho do arquivo*** - mostra a localização do aplicativo
- ***Soma de Verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de Verificação é uma seqüência de caracteres gerados automaticamente, que permite ao 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. Verificações

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

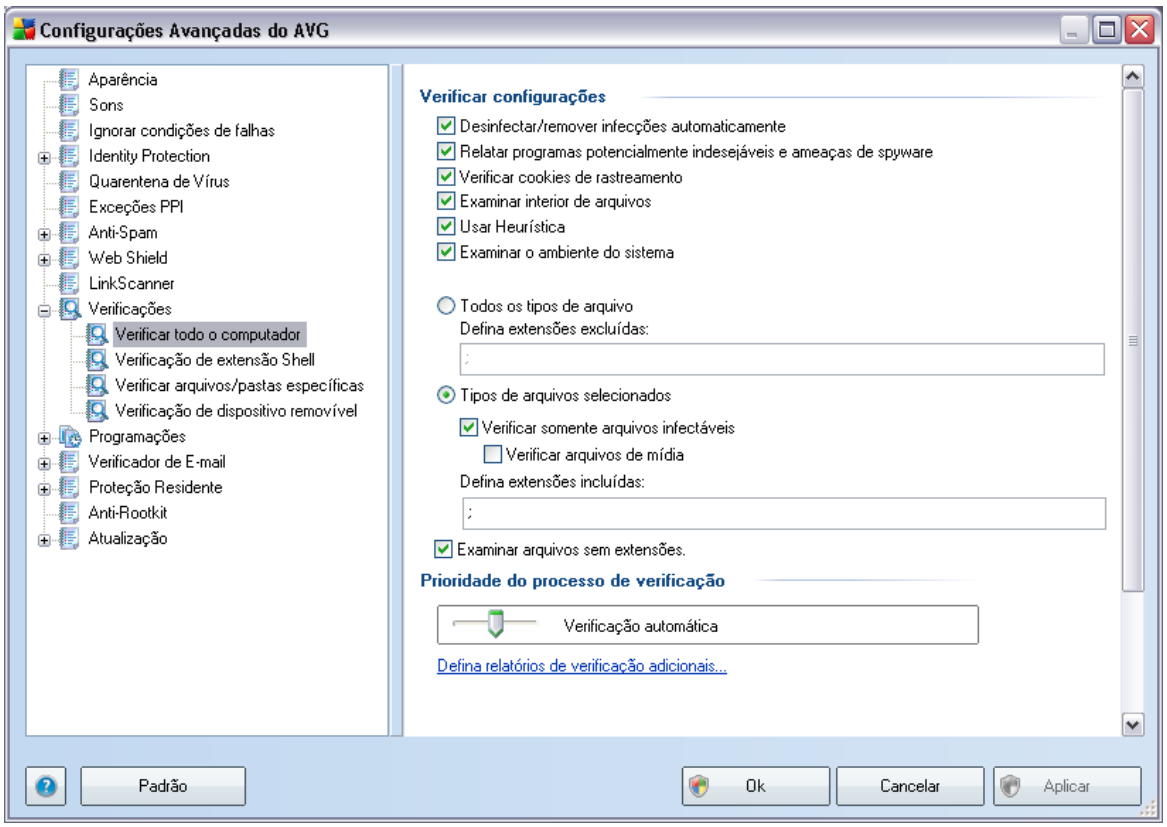
- ***Verificar Todo o Computador*** - verificação padrão predefinida de todo o

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

10.6.1. 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. 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. O método recomendado é remover o arquivo infectado para a Quarentena.

- ***Informar programas potencialmente indesejados e ameaças de spyware*** - esse parâmetro controla a funcionalidade ***Antivírus***, que permite detectar programas potencialmente indesejados (*arquivos executáveis que podem ser executados como spyware ou adware*), os quais poderão ser bloqueados ou removidos;

- ***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 que não devem ser verificadas; ou

- ***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.

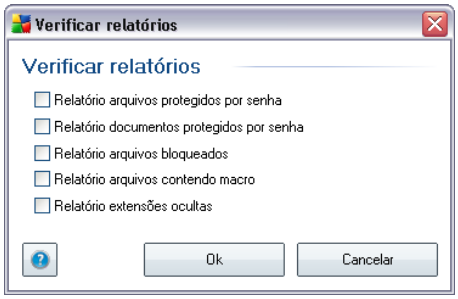
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

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.

Definir relatórios de verificação adicionais ...

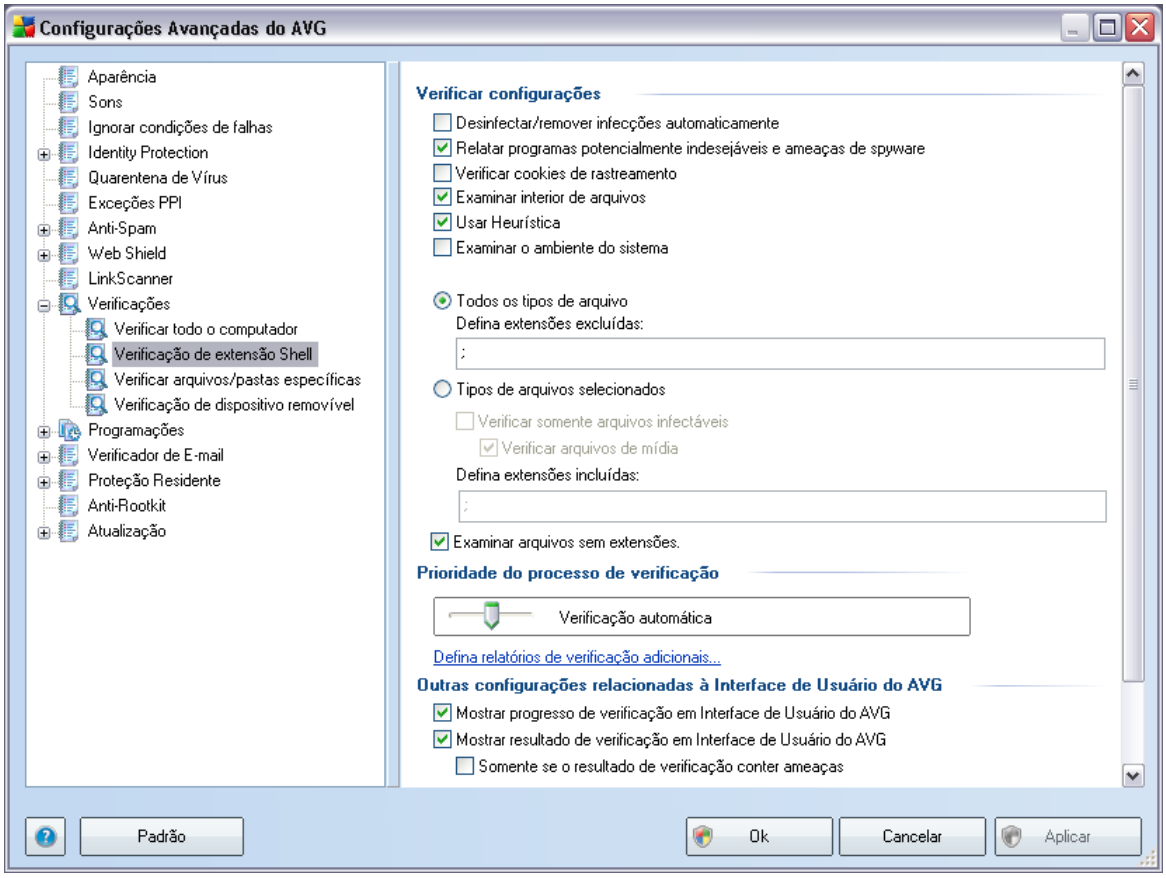
Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



10.6.2. 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:



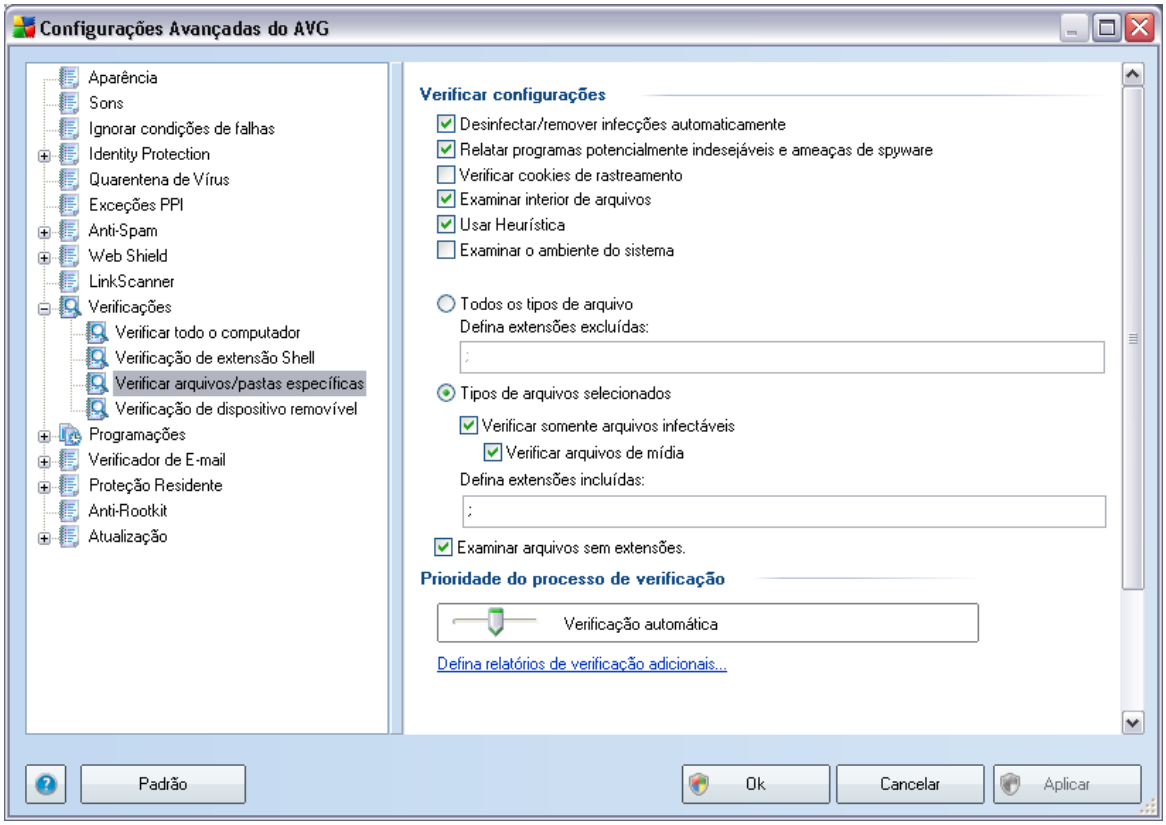
A lista de parâmetros é idêntica à disponível para ***Verificar todo o computador***. Entretanto, as configurações padrão são diferentes: com ***Verificar Todo o Computador***, a maioria dos parâmetros era selecionada, enquanto para ***Verificação da extensão shell*** (***Verificação do Windows Explorer***),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

10.6.3. 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 .

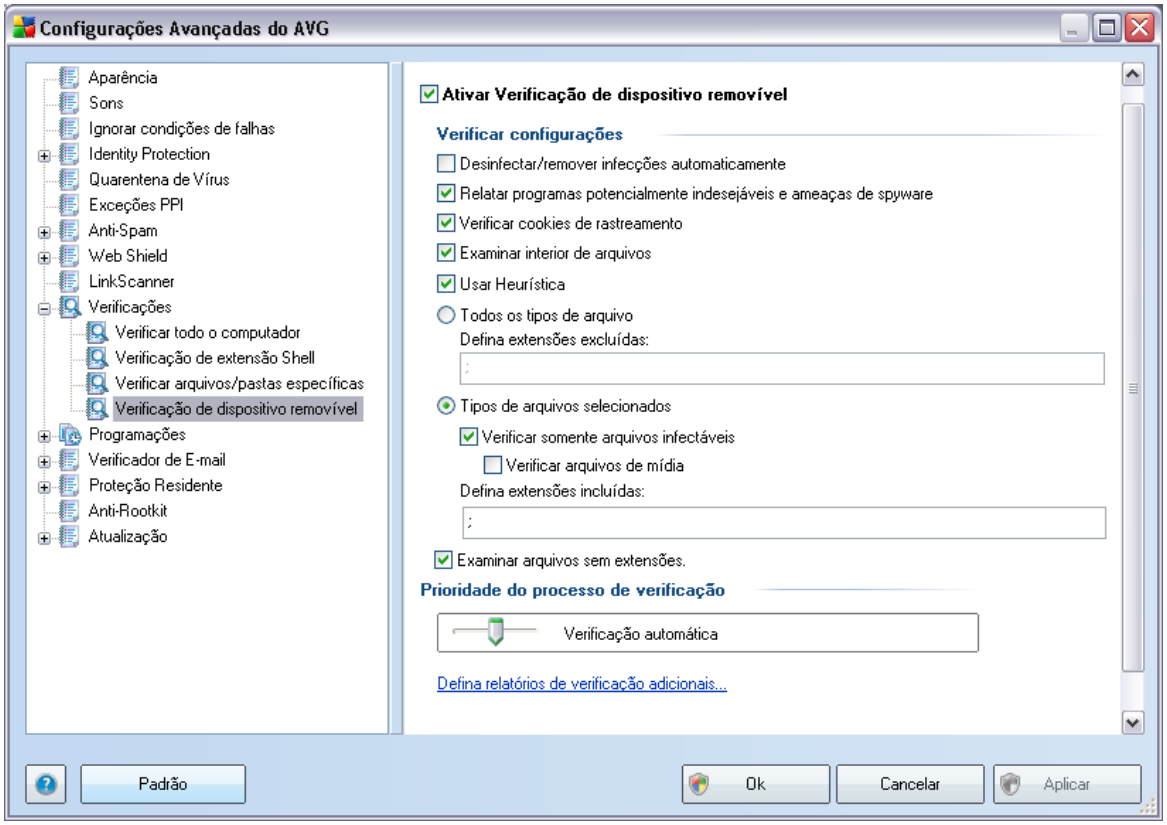


Todo os parâmetros definidos nesta caixa de diálogo de configuração são válidos somente para as áreas selecionadas para verificação com a ***Verificação de arquivos ou pastas específicos***! Se você marcar a opção ***Verificar rootkits*** nesta caixa de diálogo de configuração, somente um teste rápido de rootkit será executado, como a verificação de rootkit somente de áreas selecionadas.

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

10.6.4. 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****.*

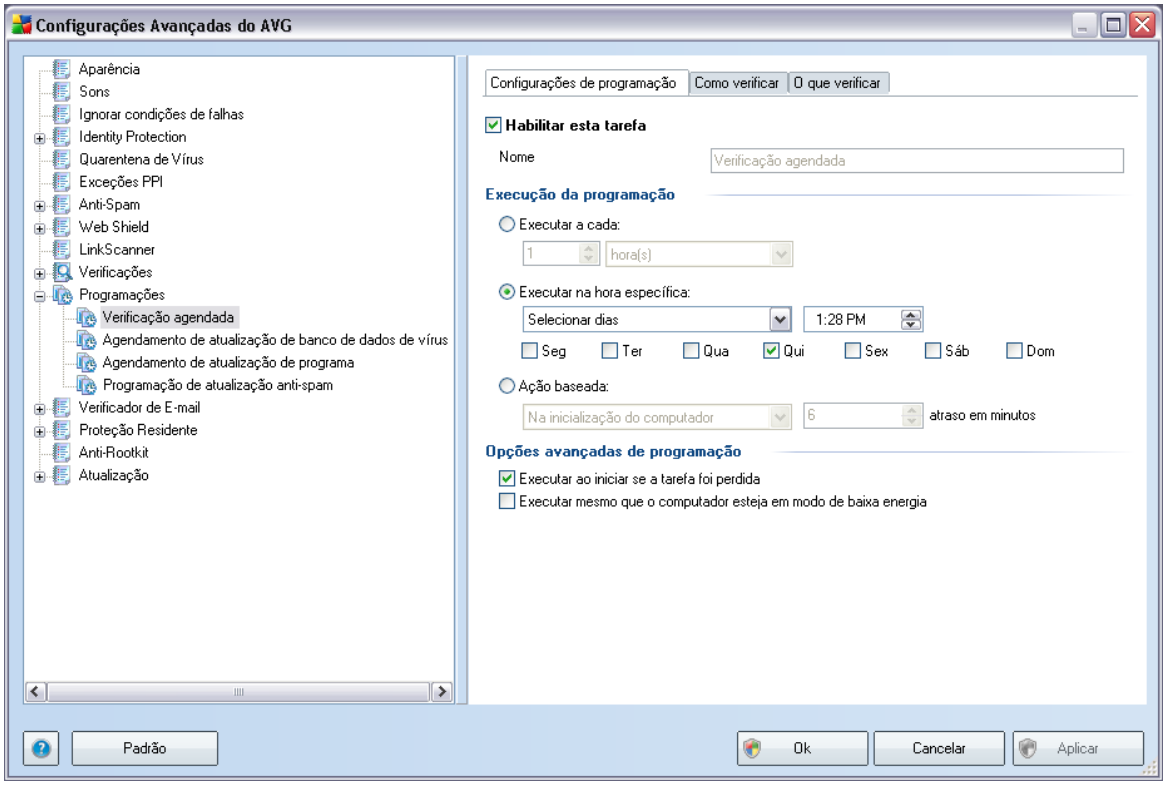
10.7. Programações

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

10.7.1. 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:

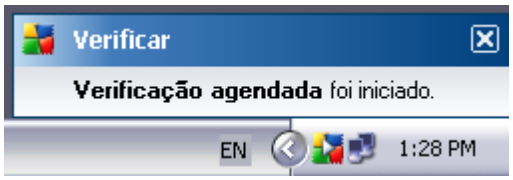
Execução da programação

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***).

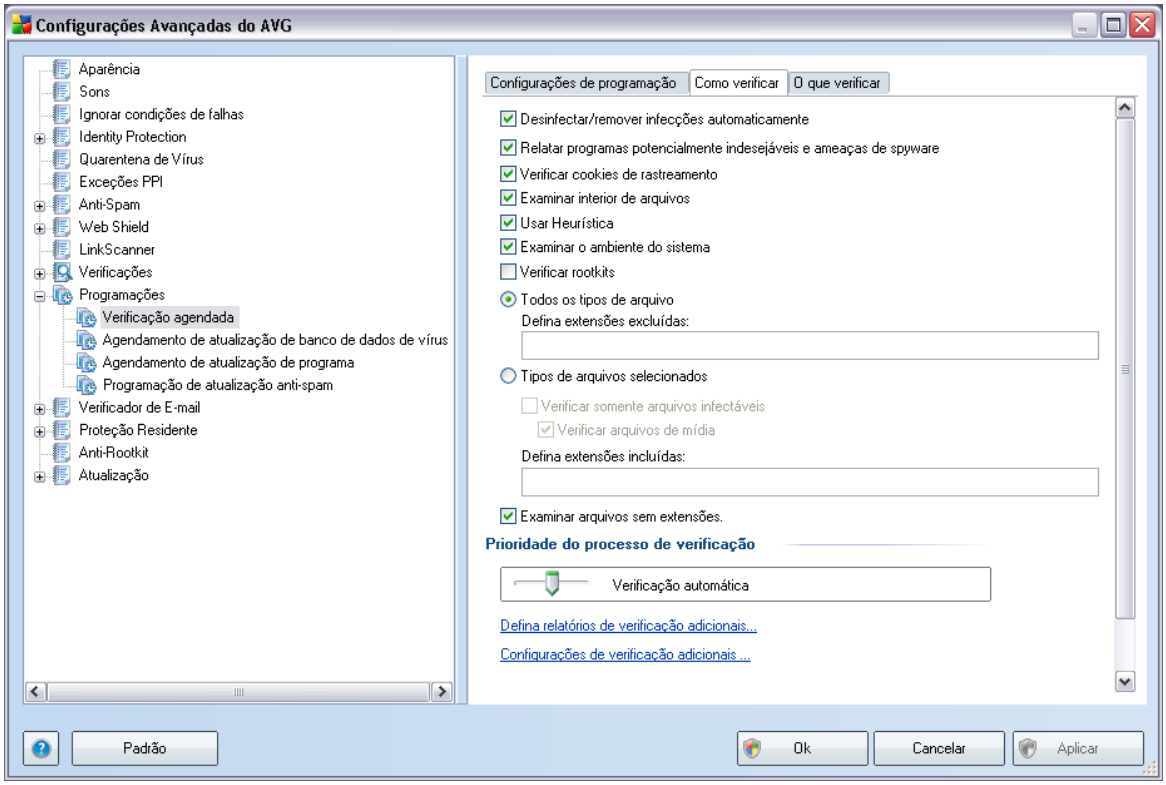
Opções avançadas de programação

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.



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 indesejados e ameaças de spyware*** - (*ativada por padrão*): esse parâmetro controla a funcionalidade Antivírus, que permite detectar programas potencialmente indesejados (*arquivos executáveis que podem ser executados como spyware ou adware*), os quais poderão ser bloqueados ou removidos;

- ***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 que não devem ser verificadas; ou

- ***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*

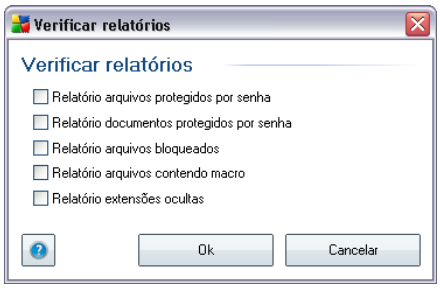
de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus). Mais uma vez, é possível especificar por extensões, quais são os arquivos que sempre devem ser verificados.

- 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.

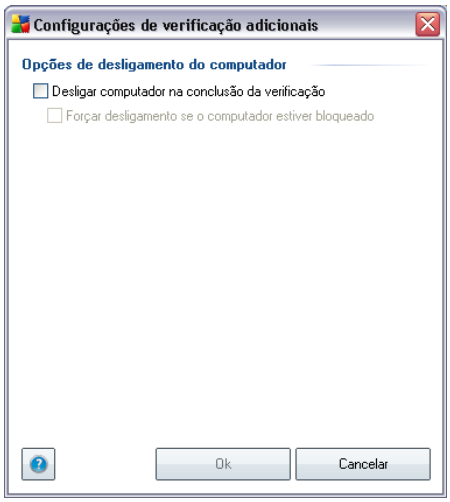
Prioridade do processo de verificação

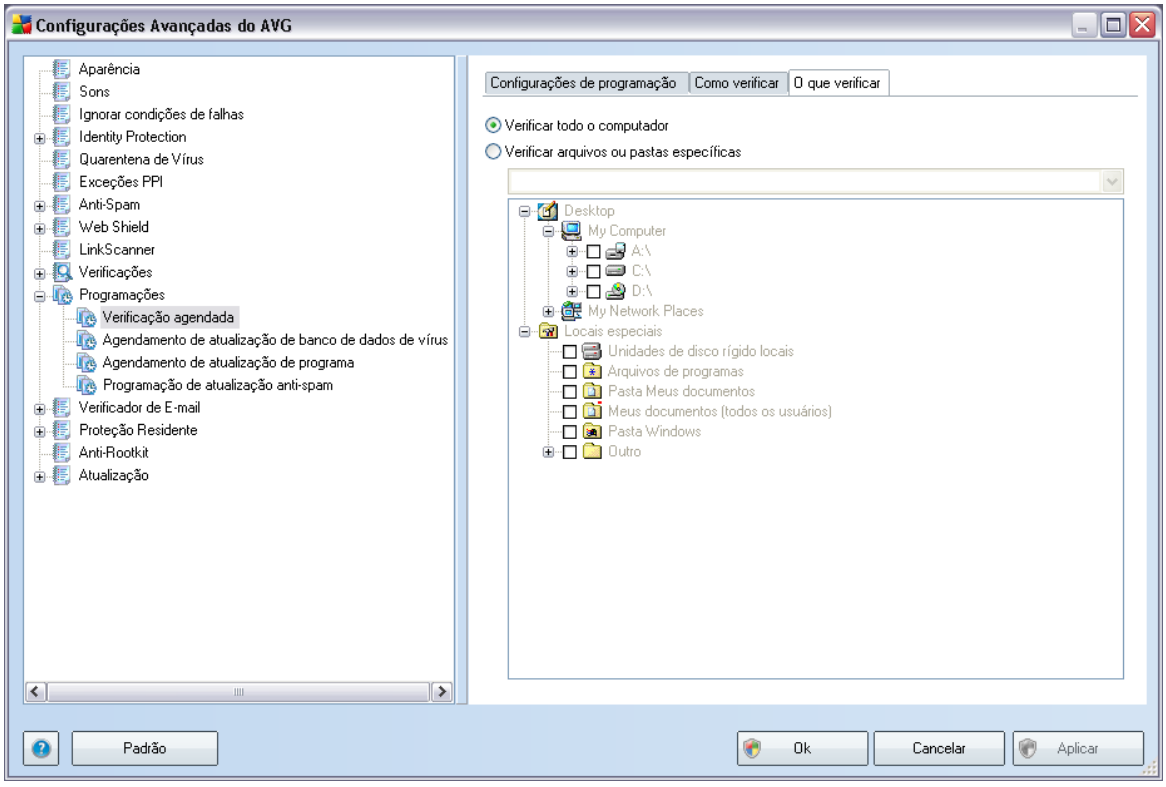
Na seção ***Verificar prioridade do processo*** , você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível médio de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos 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***).

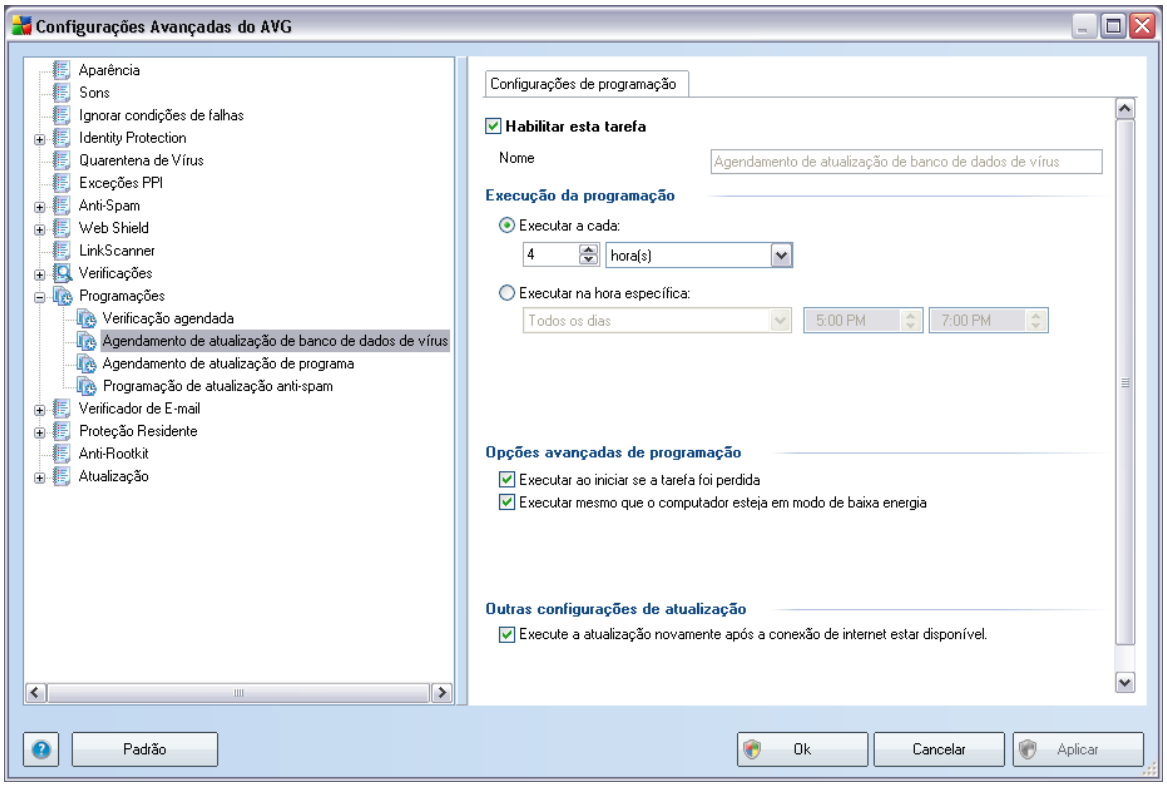




Na guia ***O que verificar***, você pode definir se deseja programar a [verificação de todo](#)

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.

10.7.2. 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. Para programações recém-adicionadas (*é possível adicionar uma nova programação clicando com o botão direito no item* ***Programação de atualizações do banco de***

dados de vírus *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 breves, descritivos e apropriados para as suas programações, para facilitar o seu reconhecimento no futuro.

Execução da programação

Nessa seção, especifique os intervalos de tempo para a inicialização da atualização do banco de dados de vírus recém-agendada. 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

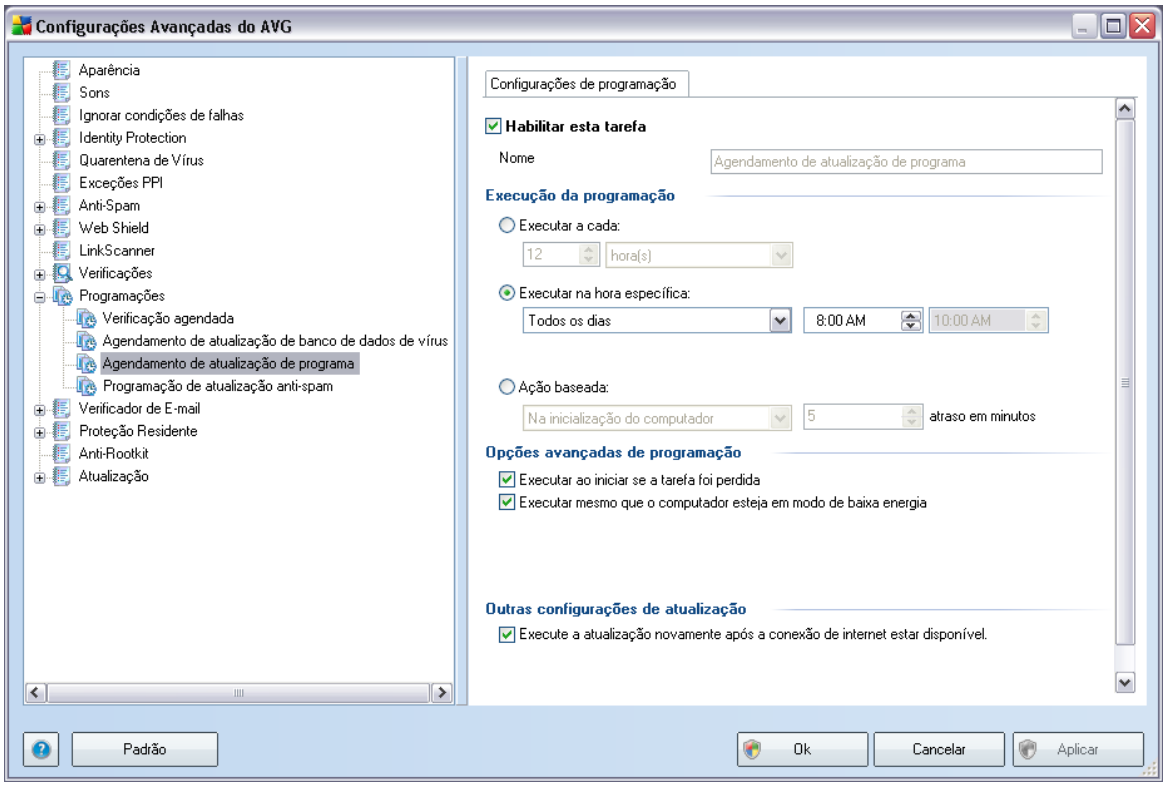
Essa seção permite definir sob quais condições a atualização do banco de dados de vírus deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

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****).*

10.7.3. Agendamento de atualização de programa



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. Para programações recém-adicionadas (*é possível adicionar uma nova programação clicando com o botão direito no item* ***Programação de atualizações do programa*** *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 breves, descritivos e apropriados para as suas programações, para facilitar o seu reconhecimento no futuro.

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.

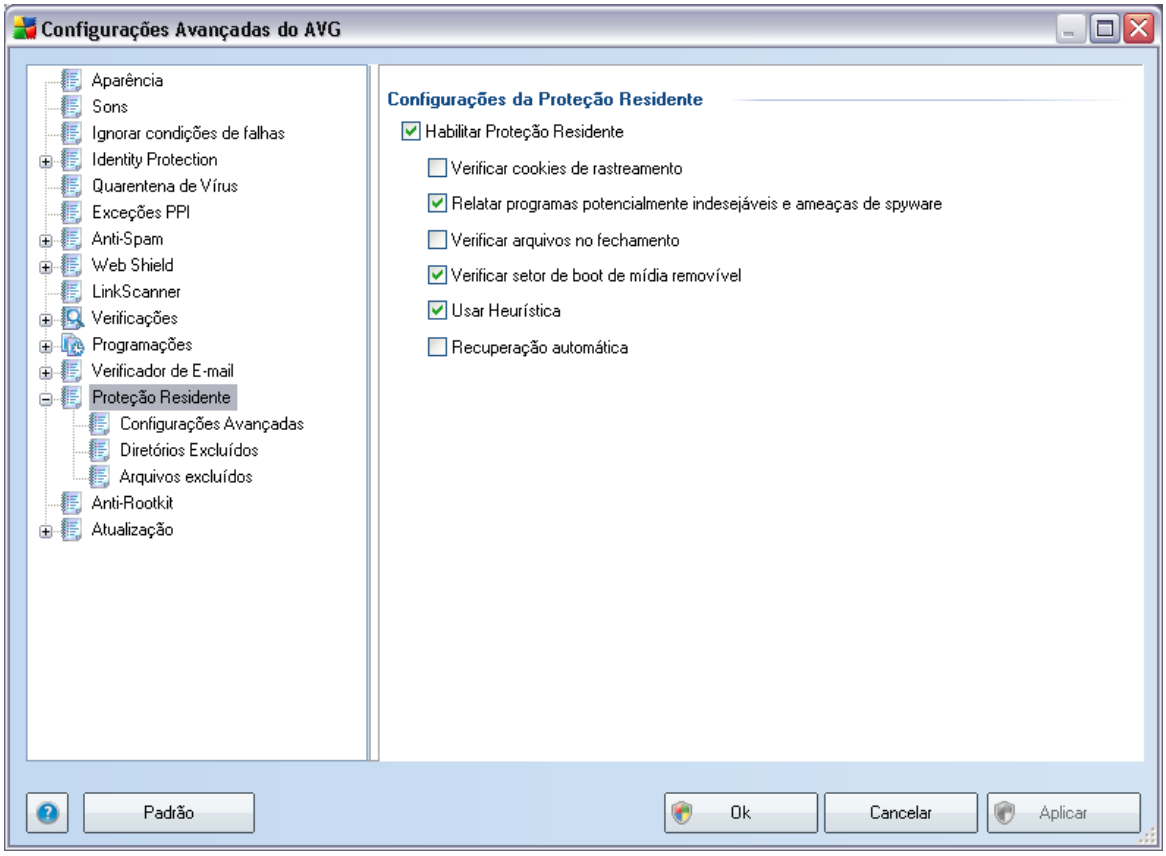
Outras configurações de atualização

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***).

10.8. 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 indesejados e ameaças de spyware*** - (*ativada por padrão*) verificação de programas potencialmente indesejados (

aplicativos executáveis que se comportam como vários tipos de spyware ou adware.

- ***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.

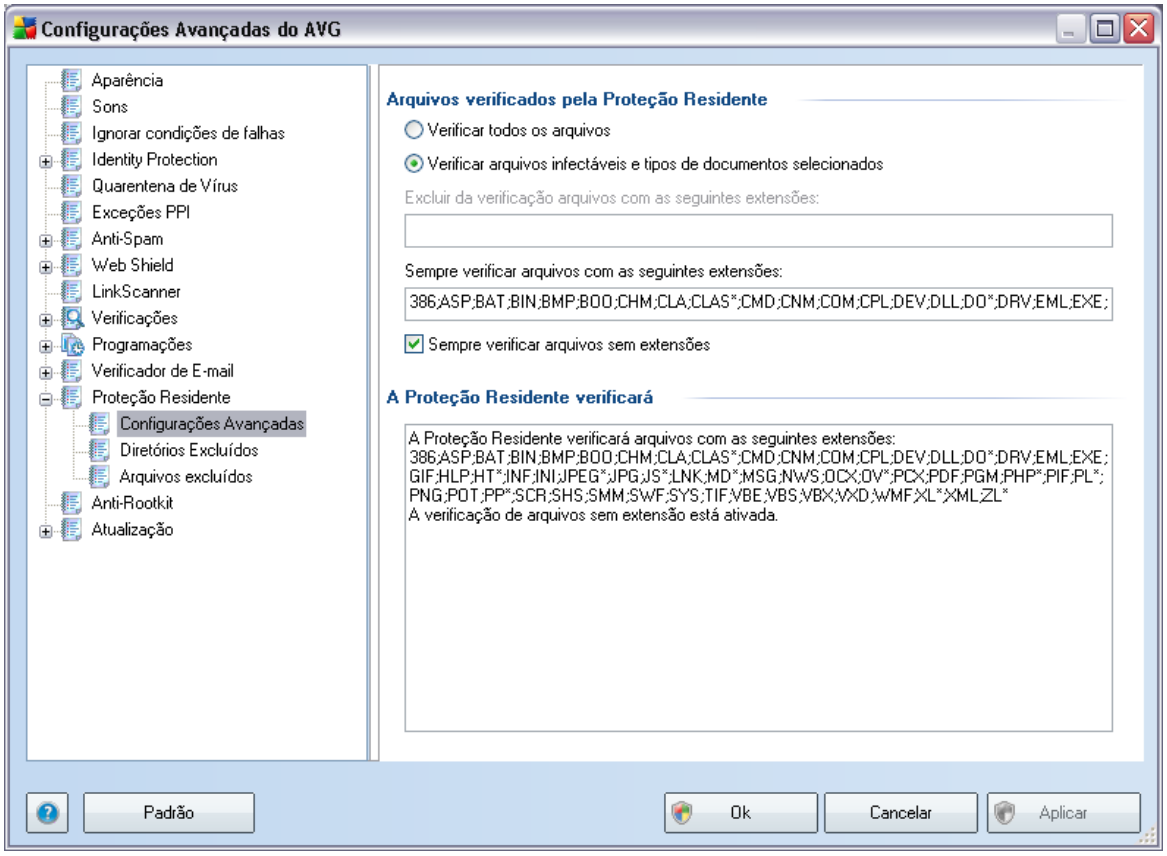
- ***Verificar setor de inicialização de mídia removível*** - (*ativado por padrão*)

- ***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

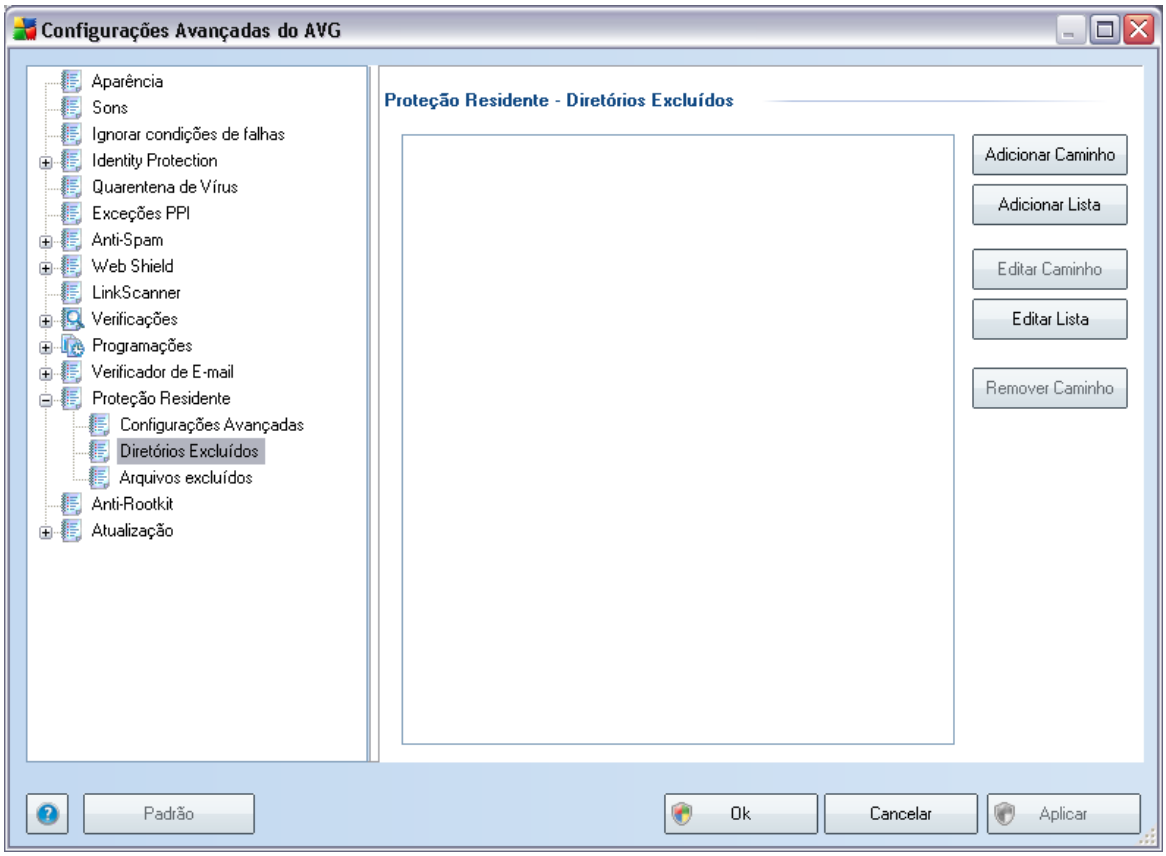
10.8.1. Configurações Avançadas

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.

10.8.2. 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.

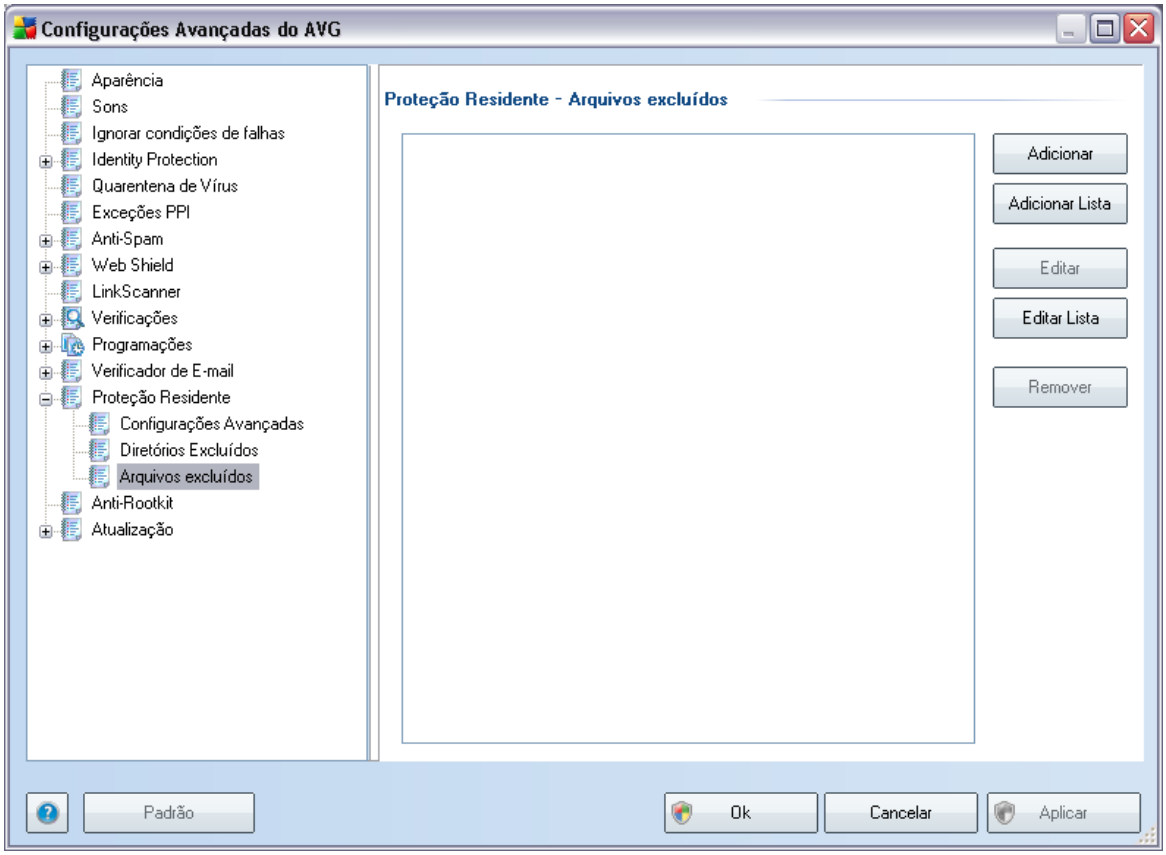
Essa caixa de diálogo fornece os seguintes botões de controle:

- ***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

10.8.3. Arquivos excluídos



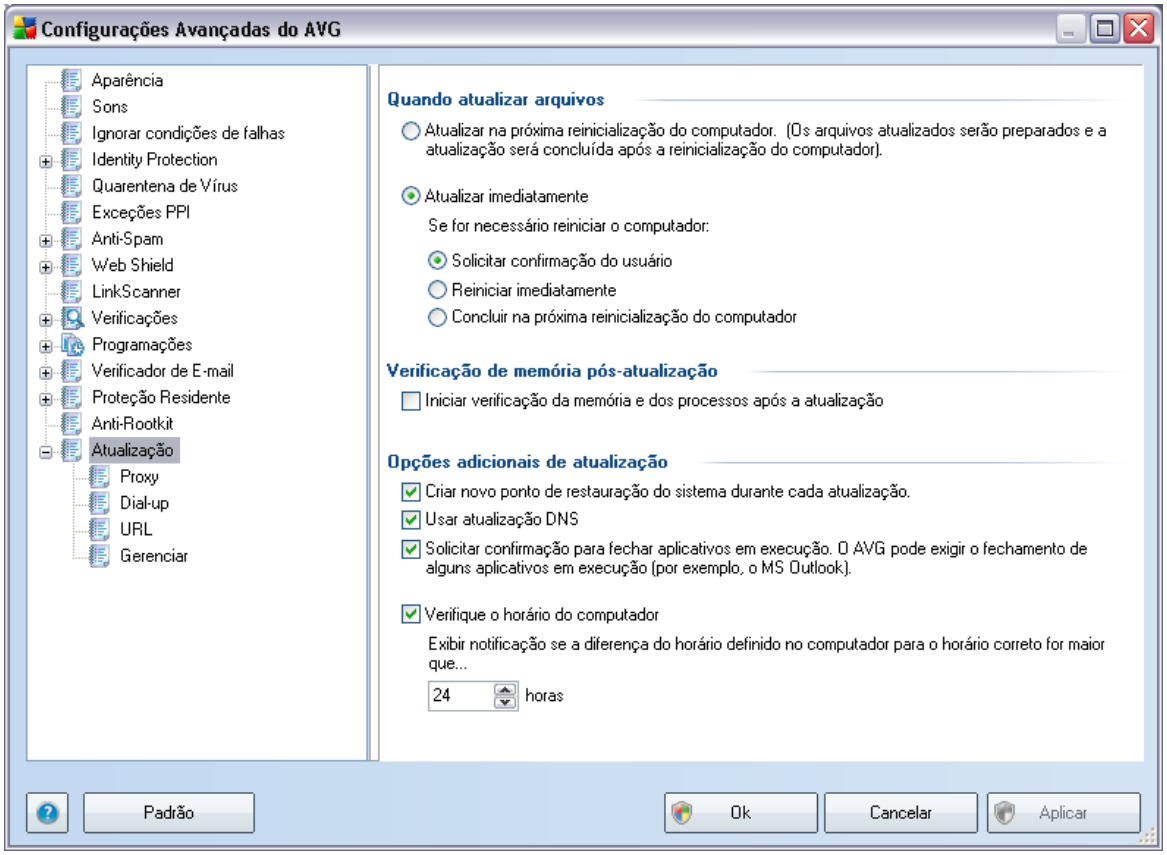
A caixa de diálogo ***Proteção Residente - Arquivos excluídos*** tem um comportamento idêntico ao da caixa de diálogo ***Proteção Residente - Exclusões de diretórios*** previamente descrita. Porém, em vez de pastas, você pode agora definir arquivos específicos que devem ser excluídos da verificação da ***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 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*** - permite editar o caminho especificado para uma pasta selecionada
- ***Editar Lista*** - permite editar a lista de pastas
- ***Remover*** - permite excluir o caminho para uma pasta selecionada da lista

10.9. 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

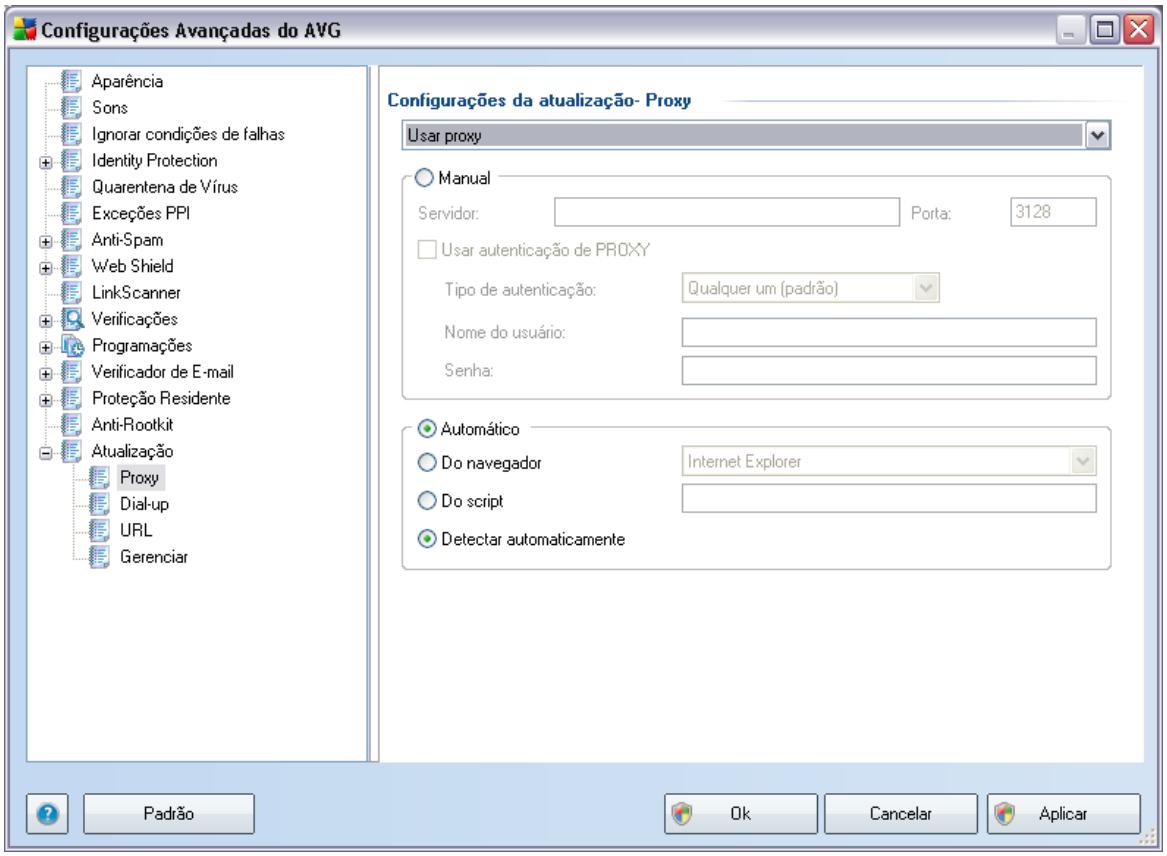
configuração original deste ponto. Esta opção está disponível em Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauração do Sistema, mas quaisquer alterações podem ser recomendadas apenas para usuários experientes! Mantenha esta caixa de seleção marcada se quiser usar o recurso.

- ***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.

10.9.1. 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 ocorrer 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***
- ***Tentar conectar usando proxy e, se falhar, conectar diretamente*** - configurações padrão

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*).

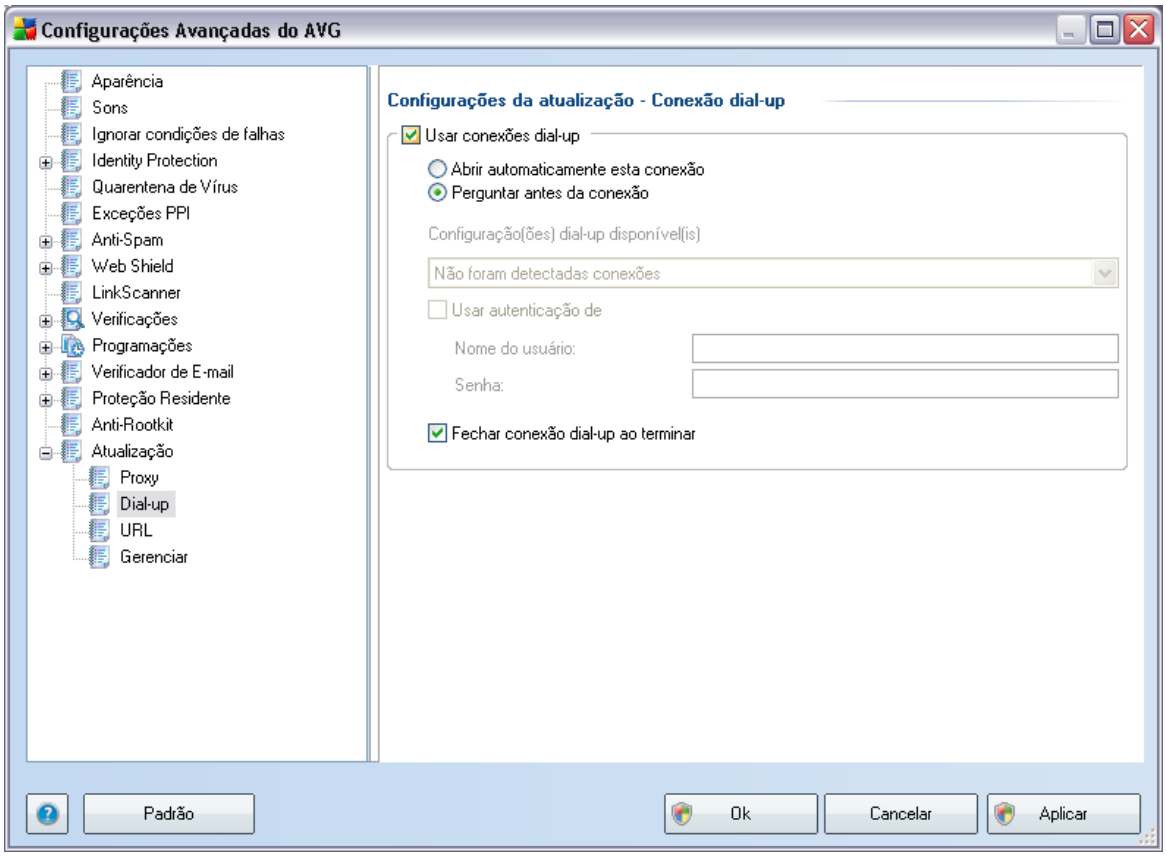
O servidor proxy também pode ter configurado regras especificas para cada usuário. Se o servidor proxy estiver configurado dessa forma, selecione a opção ***Usar autenticação PROXY*** para verificar se o nome de usuário e a senha são válidos para conexão à Internet por meio do servidor proxy.

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

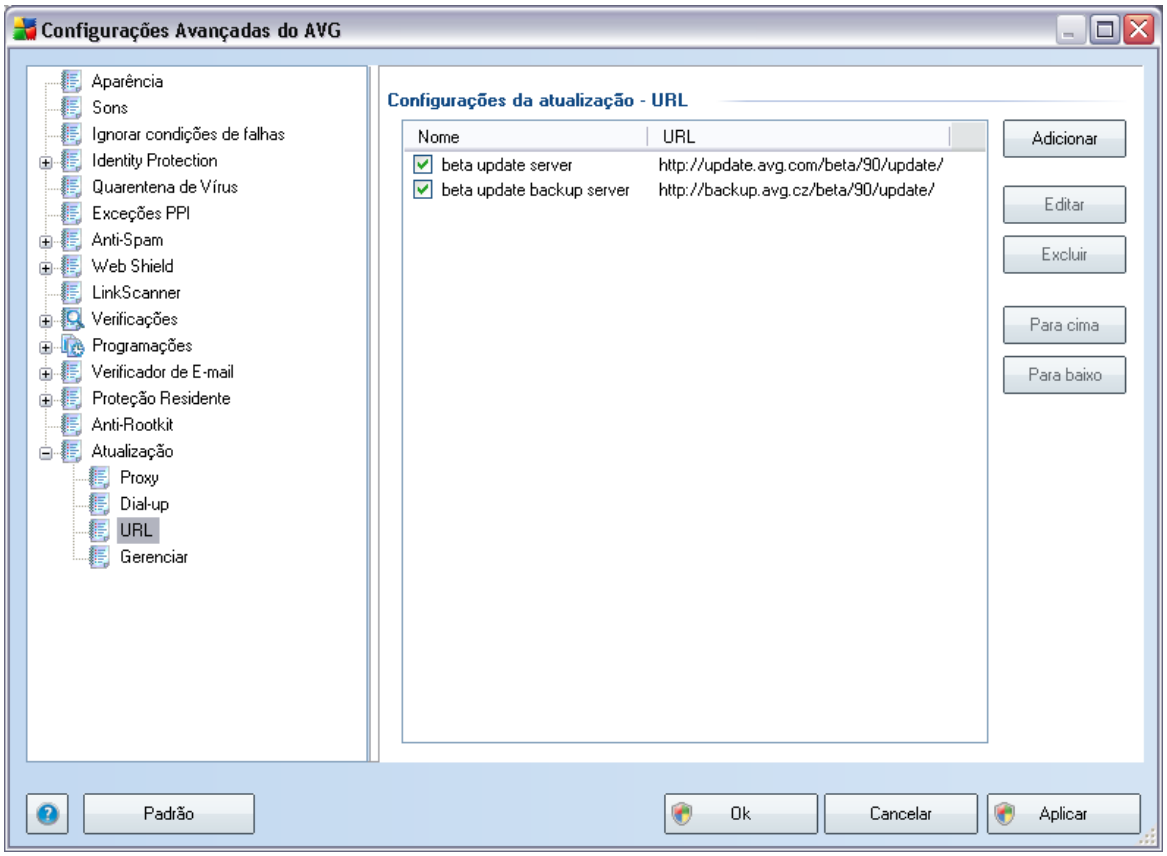
10.9.2. Dial-up



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***).

10.9.3. URL

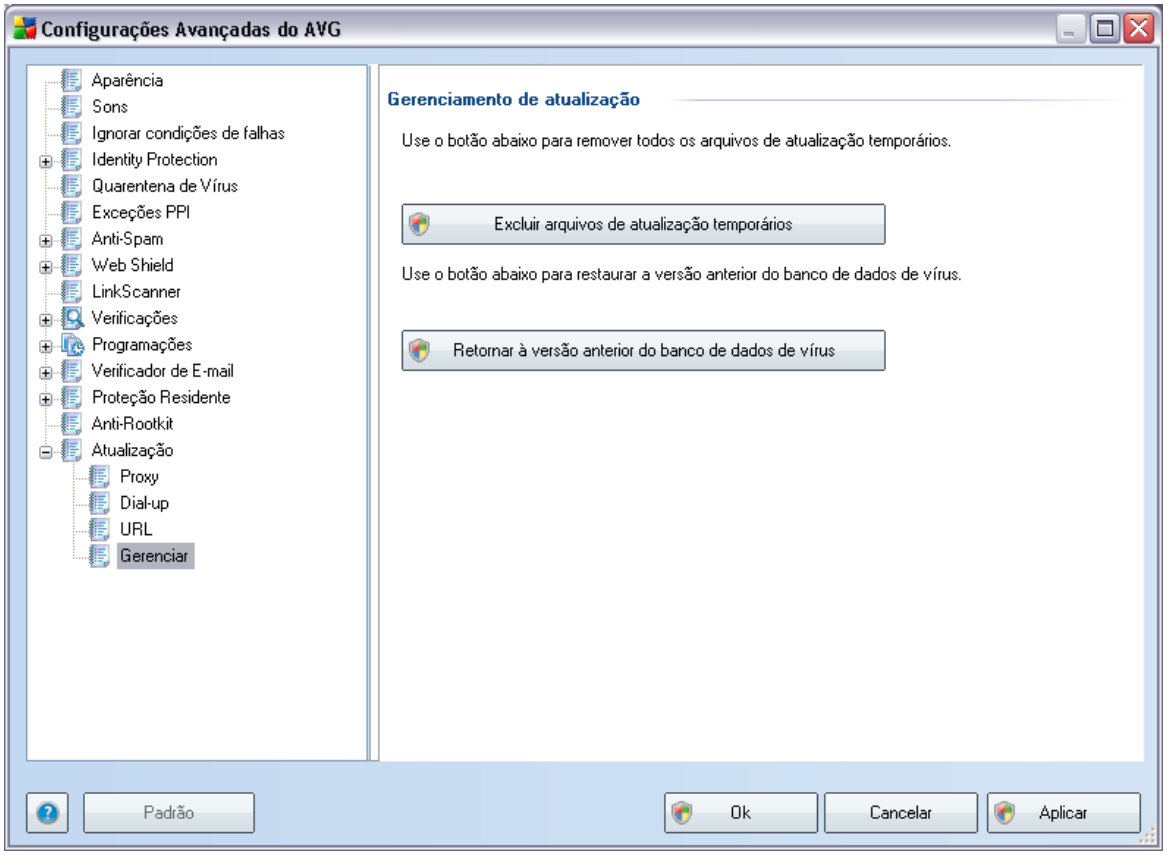


A caixa de diálogo ***URL*** oferece uma lista de endereços da Internet, de onde você poderá baixar os arquivos de atualização. A lista e os itens podem ser modificados por meio dos seguintes botões de controle:

- ***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.

10.9.4. Gerenciar

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



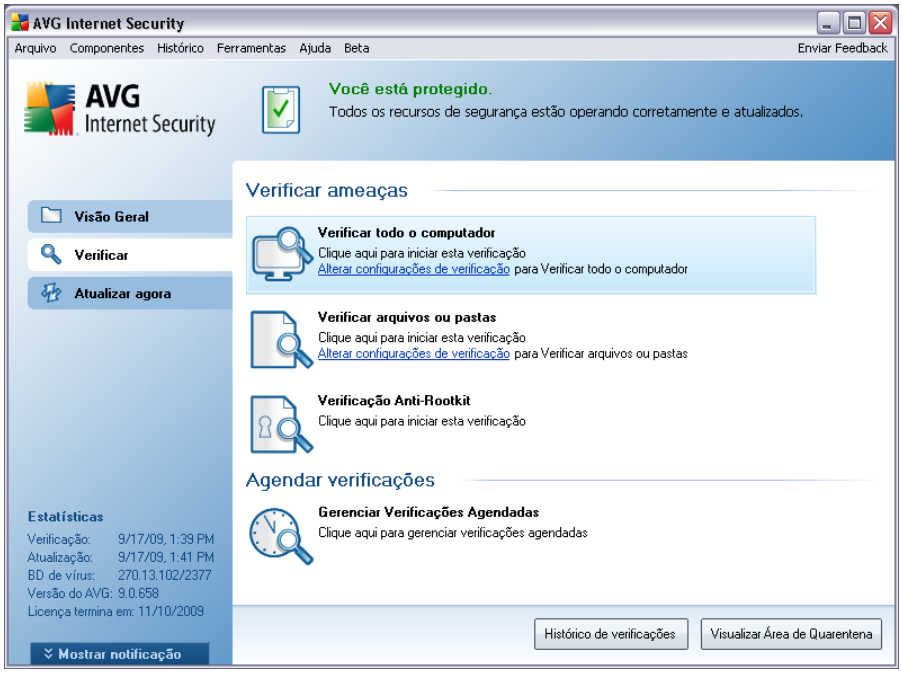
- ***Excluir arquivos de atualização temporários*** - pressione este botão para excluir todos os arquivos de atualização redundantes do seu disco rígido (*por padrão, eles são armazenados por 30 dias*)

- ***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*)

11. Verificação do AVG

A verificação é parte crucial da funcionalidade **AVG 9.0 File Server**. Você pode executar testes sob demanda ou programá-los para serem executados periodicamente , em momentos de sua conveniência.

11.1. 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

11.2. Verificações predefinidas

Um dos recursos principais do **AVG 9.0 File Server 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.

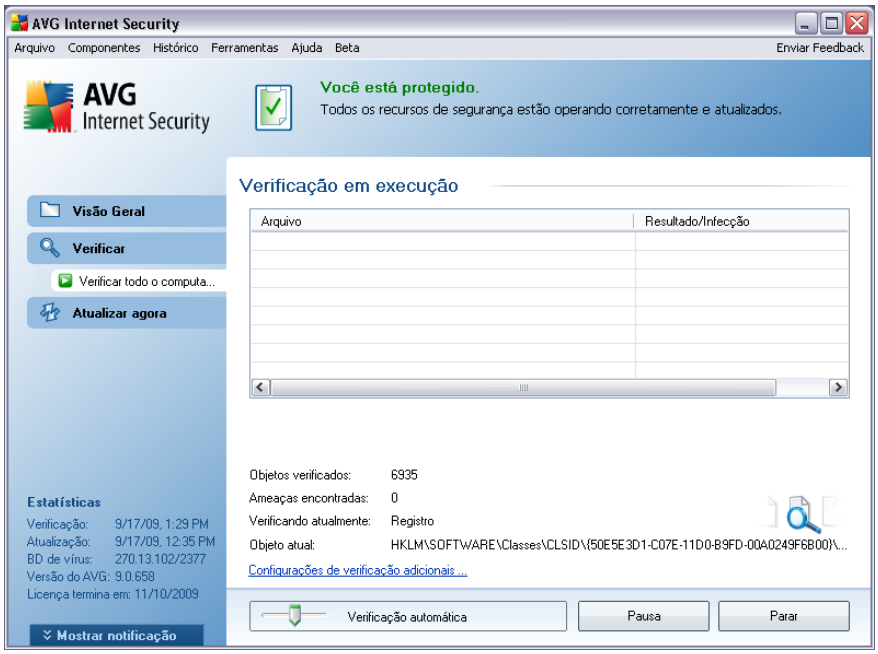
No **AVG 9.0 File Server**, você encontrará os seguintes tipos de verificação predefinidas pelo fornecedor do software:

11.2.1. 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.

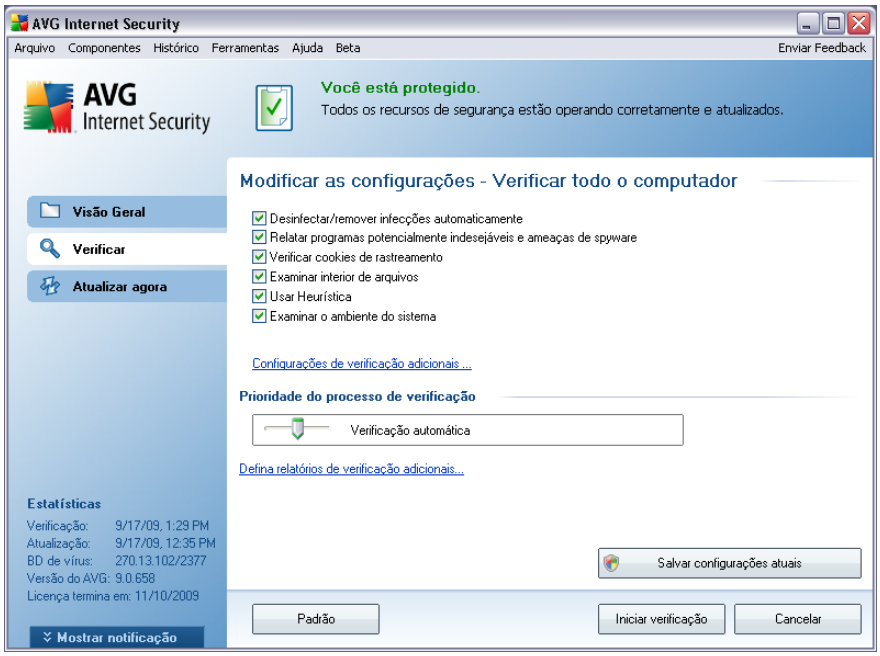
Iniciar verificação

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.



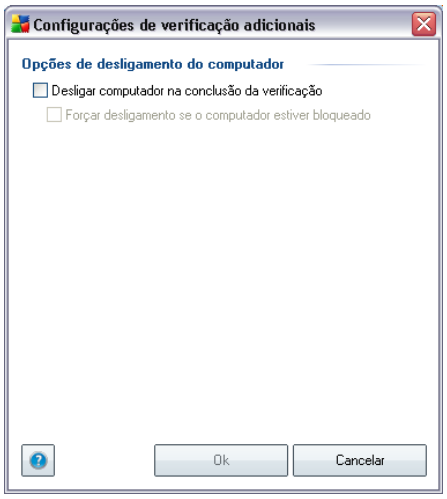
Verificar edições de configuração

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; ou

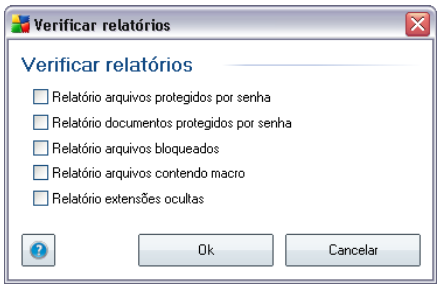
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*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.*

11.2.2. Verificar arquivos ou pastas específicos

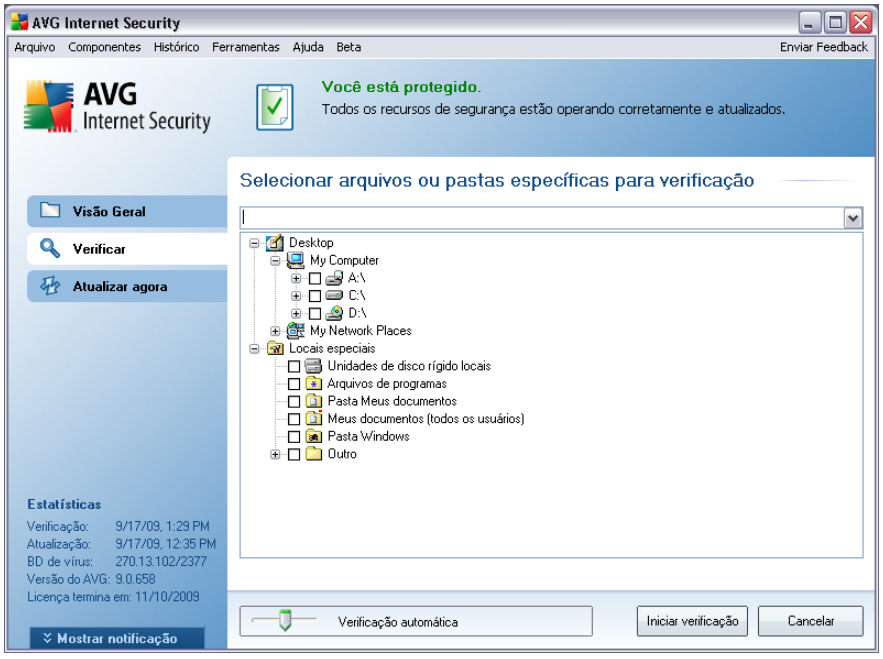
Verificar arquivos ou pastas específicas - verifica somente as áreas do computador que você tenha selecionado para verificação (*pastas selecionadas, disco rígido, unidades de disquete, CDs etc.*). O andamento da verificação em caso de detecção e tratamento de vírus é o mesmo da verificação de todo o 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 "!" .

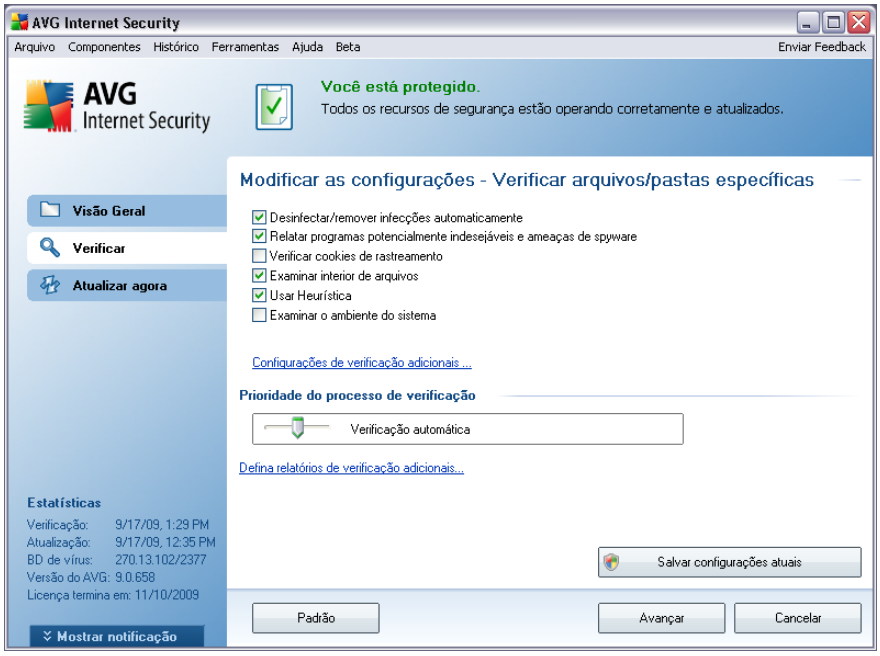
Finalmente, para iniciar a verificação, pressione o botão ***Iniciar verificação***; o processo de verificação será basicamente idêntico à verificação de todo o conteúdo do computador.



Verificar edições de configuração

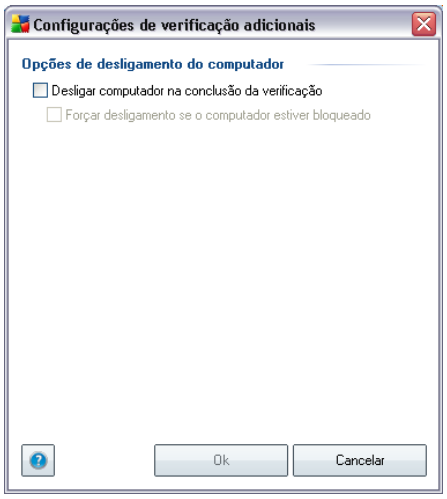
Você tem a opção de editar as configurações padrão predefinidas de ***Verificar***

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; ou

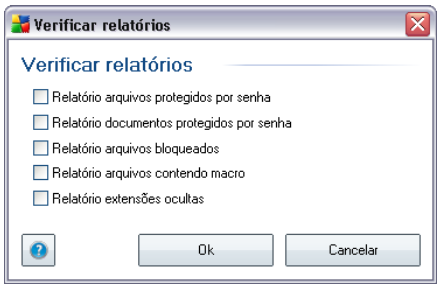
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*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:

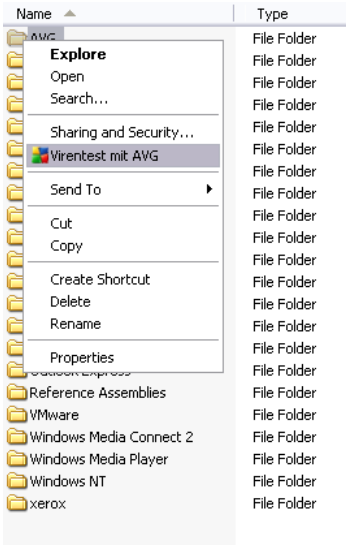


Aviso: *Essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo* ***Verificação do AVG / Programação da verificação / Como Verificar****. Se você decidir alterar as configurações padrão de* ***Verificar arquivos ou pastas específicas****, 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 verificações programadas (* *todas as verificações personalizadas são baseadas na configuração atual de Verificação de arquivos ou pastas selecionados* *).*

11.3. Verificando o Windows Explorer

Além das verificações predefinidas inicializadas em todo o computador ou em áreas selecionadas, o **AVG 9.0 File Server** 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

11.4. Verificação de linha de comando

Dentro de **AVG 9.0 File Server** 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 vírgulas, 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.

11.4.1. 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

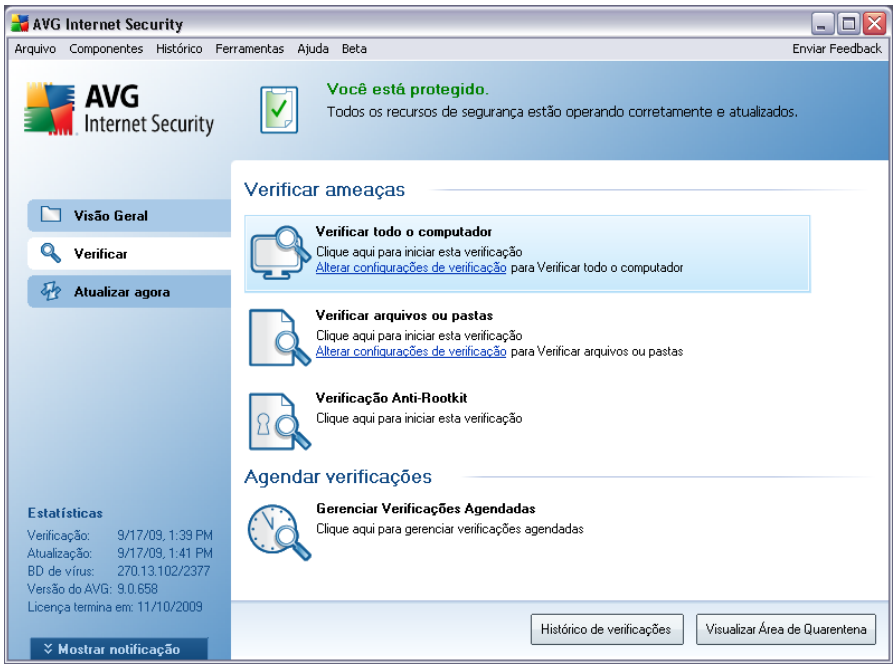
- ***/PUP*** Relatar "Programas potencialmente indesejáveis"
- ***/REG*** Verificar Registro
- ***/COO*** Verificar cookies
- ***/?*** Exibir ajuda neste tópico
- ***/HELP*** Exibir ajuda neste tópico
- ***/PRIORIDADE*** Definir prioridade de verificação /Baixa, Automática, Alta (veja Configurações avançadas / 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)

11.5. Programação de verificação

Com o **AVG 9.0 File Server**, 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.

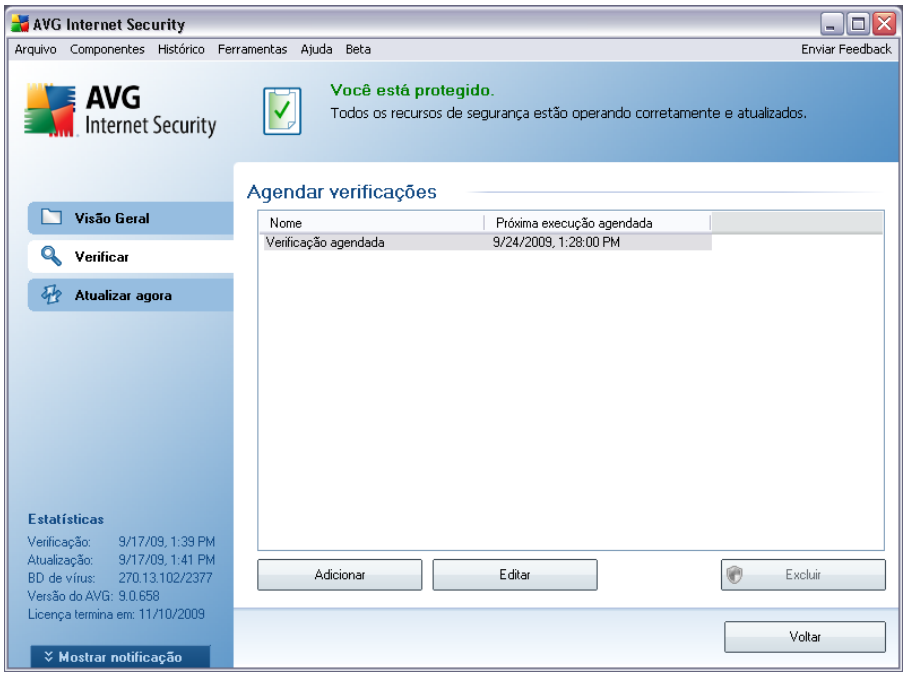
Inicialize a ***Verificação de todo o computador*** regularmente, pelo menos uma vez por semana. Se possível, inicialize a verificação de todo o computador diariamente, conforme definido na configuração padrão da programação da verificação.Se o computador estiver "sempre ligado", você poderá programar 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.

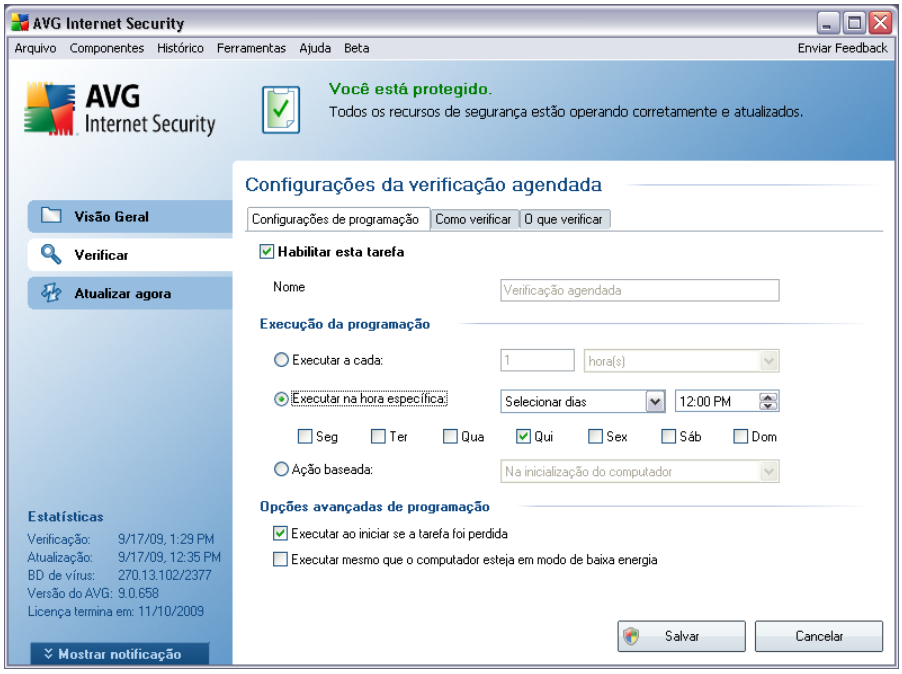
- ***Editar programa da verificação*** - esse botão só pode ser usado se você tiver selecionado um teste existente anteriormente na lista de testes programados. Nesse caso, o botão aparecerá ativo e você poderá clicar nele para passar para a caixa de diálogo ***Configurações da verificação programada***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

11.5.1. 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.

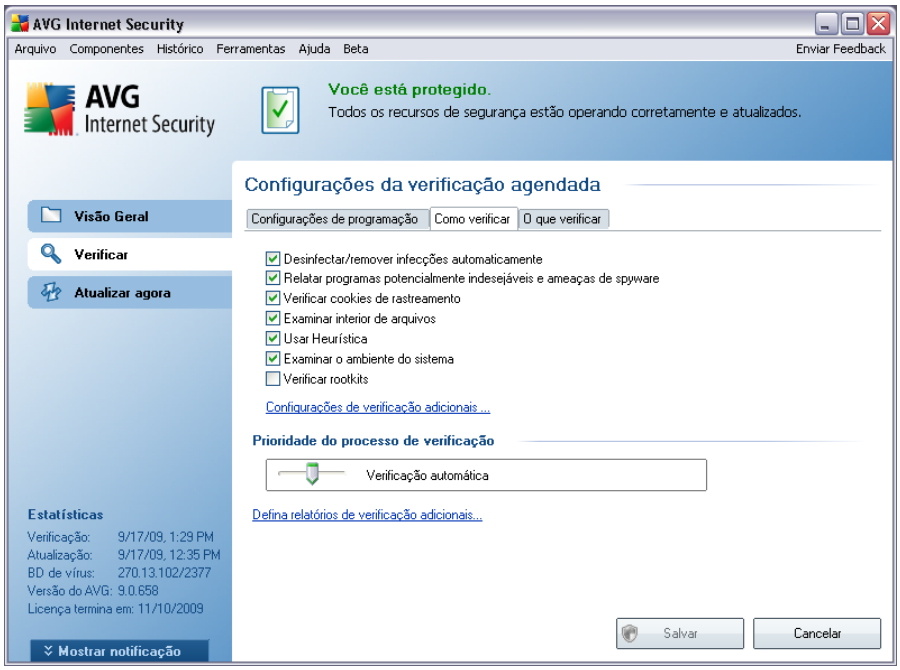
Botões de controle da caixa de diálogo Configurações para verificação programada

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações de 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 .

11.5.2. 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 e Spyware Potencialmente Indesejados*** - (*ativado por padrão*): esse parâmetro controla a funcionalidade ***Antivírus***, que permite detectar programas potencialmente indesejados (*arquivos executáveis que podem ser executados como spyware ou adware*), os quais poderão ser bloqueados ou removidos;

- ***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.

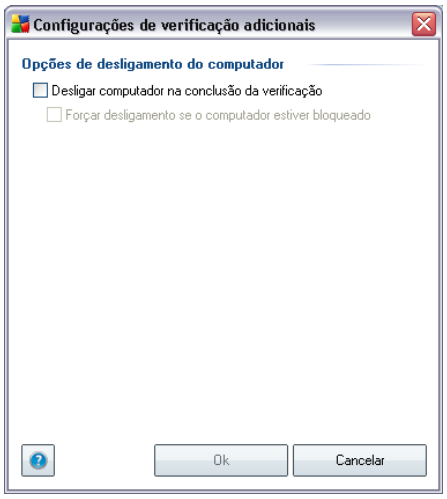
- ***Usar Heurística*** - (*ativado por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado,em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***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***;

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:



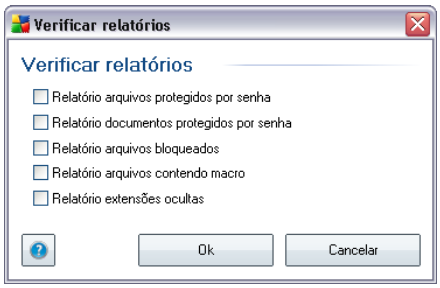
  - ***Opções de desligamento do computador*** - decida se o computador

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; ou
  - ***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****.*

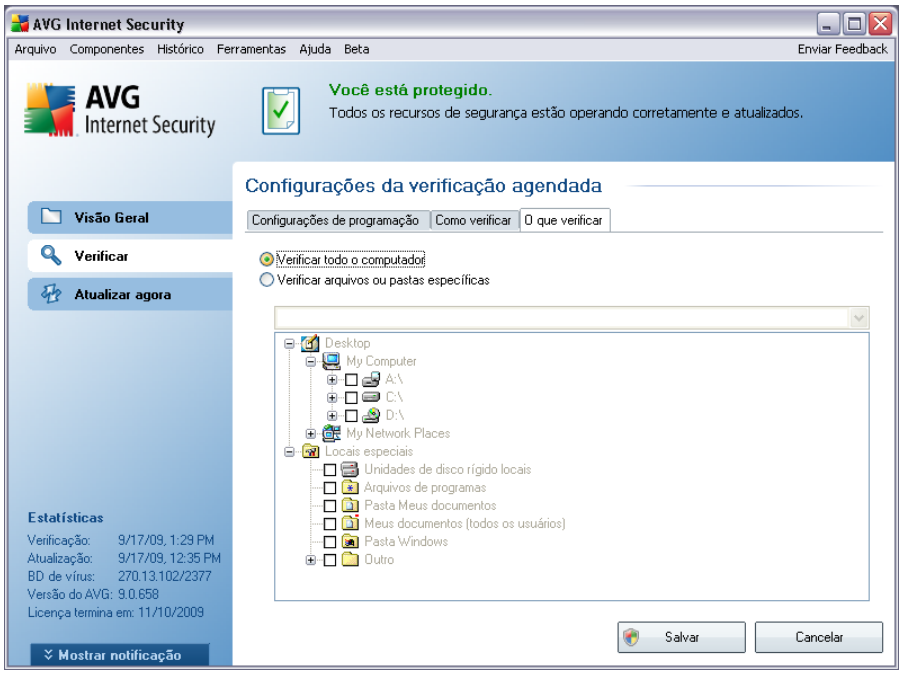
Botões de controle

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações de programação***, ***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 .

11.5.3. 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.

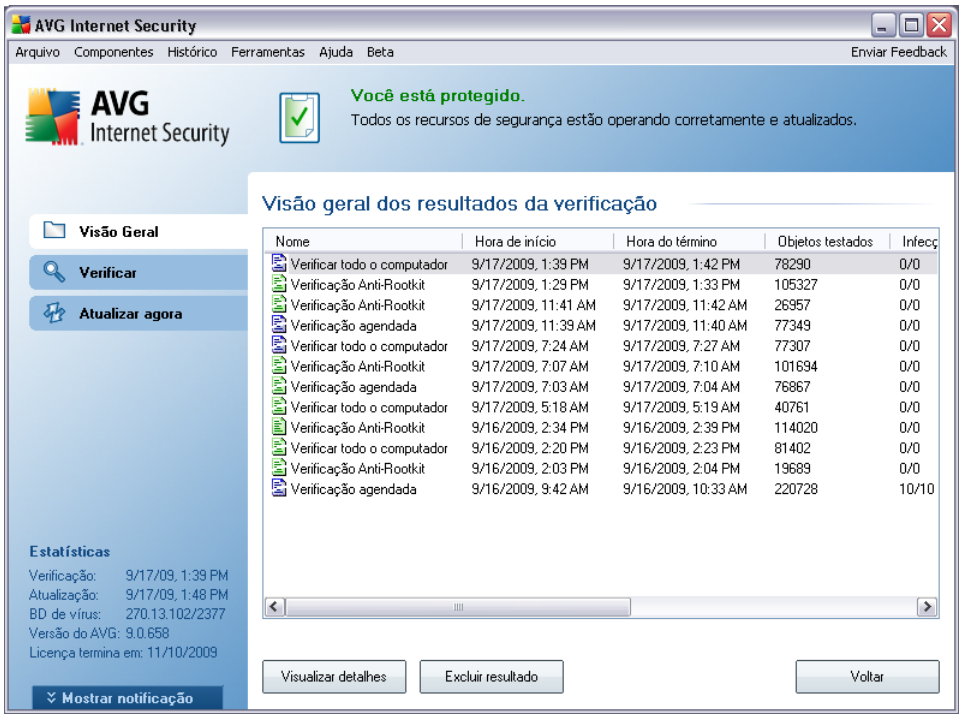
Botões de controle da caixa de diálogo Configurações para verificação programada

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações de 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 .

11.6. 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
- ***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*** - esse botão só fica ativo se uma verificação específica for selecionada na visão geral acima. Pressione-o para passar para a caixa de diálogo ***Resultados da verificação*** e exibir dados detalhados sobre a verificação selecionada
- ***Excluir resultado*** - esse botão só fica ativo se uma verificação específica for selecionada na visão geral acima. Pressione-o para remover o item selecionado da visão geral dos resultados de verificação
- ***Voltar*** - volta para a caixa de diálogo padrão da interface de verificação do AVG

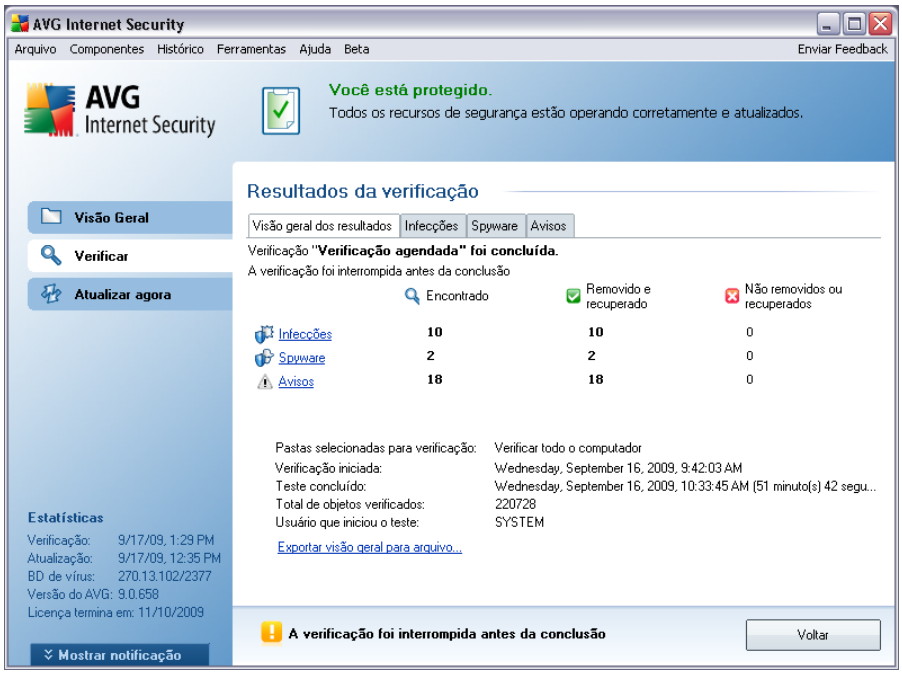
11.7. Detalhes dos resultados da verificação

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
- ***Avisos*** - essa guia é exibida somente se durante a verificação não tiver sido possível verificar alguns objetos
- ***Rootkits*** - essa guia é exibida somente se rootkits tiverem sido 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

11.7.1. Guia Visão geral dos resultados



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

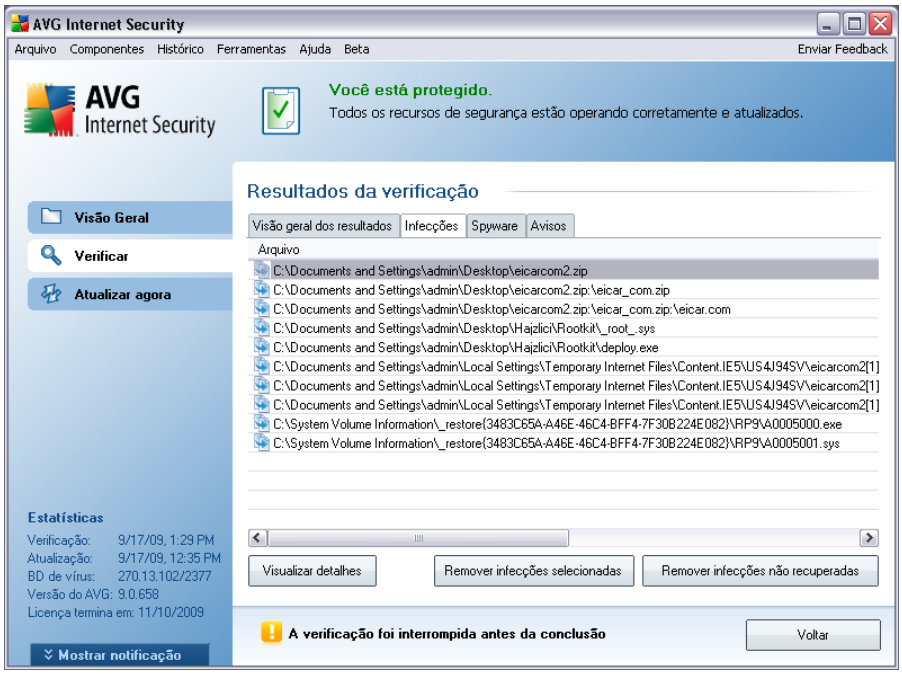
- infecções por vírus/spyware detectadas
- infecções por vírus/spyware removidas
- o número de infecções por vírus/spyware que não puderam ser removidas ou reparadas

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***.

11.7.2. 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:

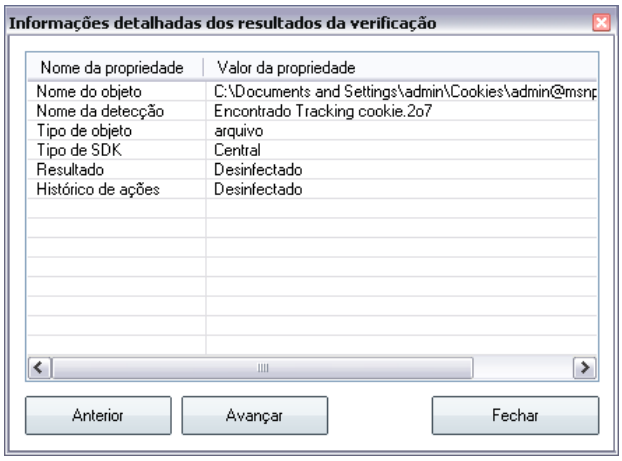
- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do vírus detectado (*para obter detalhes sobre o vírus específico, consulte a Enciclopédia de Vírus online*).
- ***Resultado*** - define o status atual do objeto infectado detectado durante a verificação.
    - ***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:

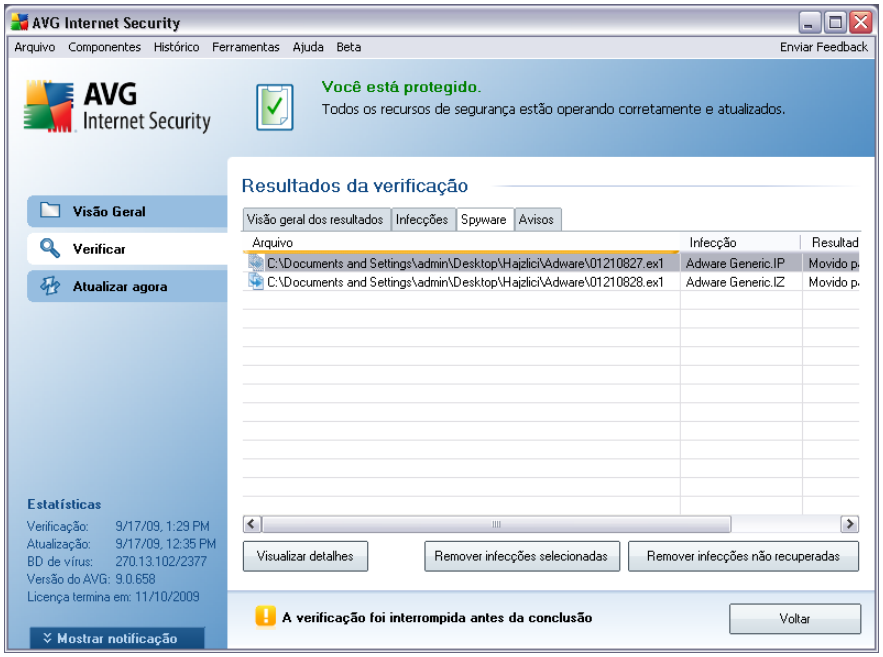
- ***Exibir detalhes*** - o botão abre uma nova janela de diálogo denominada ***Detalhes do resultado da verificação***:



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***.

11.7.3. 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

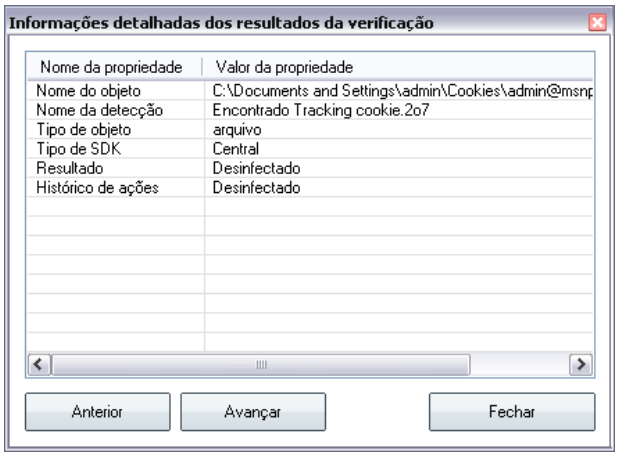
(por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica).

- **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***.

11.7.4. 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.

11.7.5. 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:

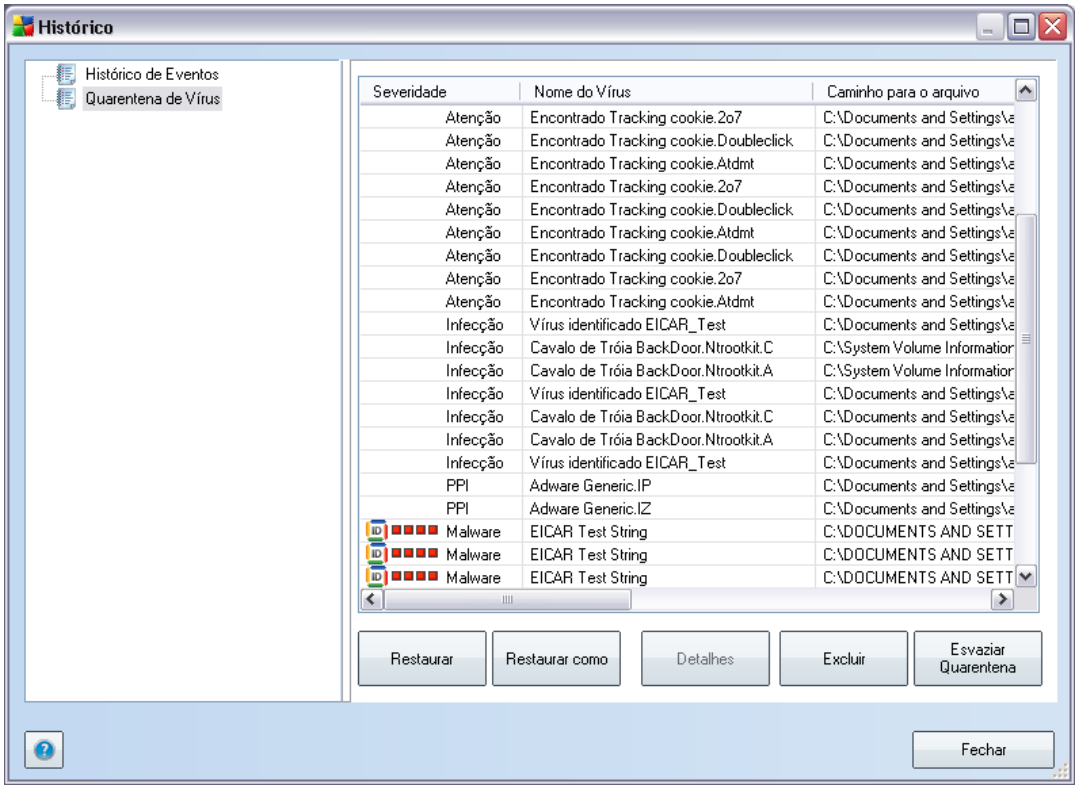
- ***Compactado em tempo de execução*** - o arquivo foi compactado com um dos compactadores menos comuns, o que pode indicar uma tentativa de impedir a verificação desse arquivo. Entretanto, nem todos os relatórios de tal arquivo indica um vírus.
- ***Compactado em tempo de execução com recorrência***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

11.8. 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.

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*** - fornece a identificação gráfica da respectiva severidade da descoberta, em uma escala de quatro níveis que varia desde incensurável (■□□□) até muito perigosa (■■■■)
- ***Tipo de infecção*** - distingue tipos de descoberta 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.

- ***Excluir*** - remove completamente o arquivo infectado da ***Quarentena de Vírus***
- ***Esvaziar a Quarentena*** - remove completamente todo o conteúdo da ***Quarentena de Vírus***

12. Atualizações do AVG

Manter o AVG atualizado é fundamental para garantir que todos os vírus recém-descobertos sejam detectados o mais rapidamente possível. 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 banco de vírus do AVG se mantenha atualizado também durante o dia.

12.1. Níveis de Atualização

O AVG oferece dois níveis de atualização à sua escolha:

- Asdefini|Jesdeatualiza|©o ***contêm 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.

12.2. 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.

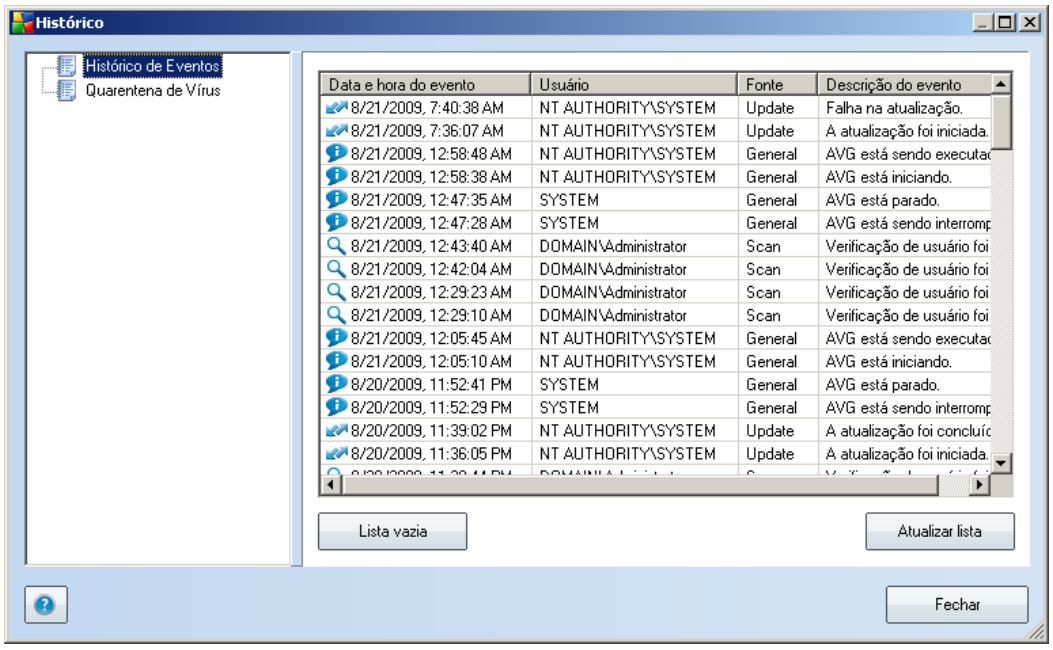
12.3. Processo de atualização

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. Recomendado apenas para usuários experientes!*

13. 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 9.0 File Server**. ***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

14. 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.avg.com).

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***.