



AVG Internet Security 2011

Manual do Usuário

Revisão do documento 2011.21 (16.5.2011)

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

Este produto usa o RSA Data Security, Inc. Algoritmo de Compilador de Mensagem MD5, Copyright (C) 1991-2, RSA Data Security, Inc. Criado em 1991.

Este produto usa o código da biblioteca C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Este produto usa a biblioteca de compactação zlib, Copyright (c) 1995-2002 Jean-loup Gailly e Mark Adler.
Este produto usa a biblioteca de compactação libbzip2, Copyright (c) 1996-2002 Julian R. Seward.



Conteúdo

1. Introdução	8
2. Requisitos de instalação do AVG	9
2.1 Sistemas operacionais suportados	9
2.2 Requisitos de HW mínimos e recomendados	9
3. Opções de instalação do AVG	10
4. Processo de instalação do AVG	11
4.1 Bem-vindo	11
4.2 Ativar sua licença do AVG	12
4.3 Selecionar tipo de instalação	13
4.4 Opções personalizadas	14
4.5 Instalar a Barra de Ferramentas de Segurança do AVG	15
4.6 Progresso da Instalação	16
4.7 Instalação bem sucedida	16
5. Após a instalação	18
5.1 Registro do produto	18
5.2 Acesso à interface do usuário	18
5.3 Verificação de todo o computador	18
5.4 Teste Eicar	18
5.5 Configuração padrão do AVG	19
6. Interface de usuário do AVG	20
6.1 Menu do sistema	21
6.1.1 Arquivo	21
6.1.2 Componentes	21
6.1.3 Histórico	21
6.1.4 Ferramentas	21
6.1.5 Ajuda	21
6.2 Informações sobre status de segurança	24
6.3 Links rápidos	25
6.4 Visão geral dos componentes	25
6.5 Estatísticas	27
6.6 Ícone da bandeja do sistema	27
6.7 Gadget AVG	28



7. Componentes do AVG	31
7.1 Antivírus	31
7.1.1 <i>Princípios do Antivírus</i>	31
7.1.2 <i>Interface do Antivírus</i>	31
7.2 Anti-Spyware	32
7.2.1 <i>Princípios do Anti-Spyware</i>	32
7.2.2 <i>Interface do Anti-Spyware</i>	32
7.3 Anti-Spam	34
7.3.1 <i>Princípios do Anti-Spam</i>	34
7.3.2 <i>Interface do Anti-Spam</i>	34
7.4 Firewall	35
7.4.1 <i>Princípios do Firewall</i>	35
7.4.2 <i>Perfis do Firewall</i>	35
7.4.3 <i>Interface do Firewall</i>	35
7.5 Link Scanner	39
7.5.1 <i>Princípios do Link Scanner</i>	39
7.5.2 <i>Interface do Link Scanner</i>	39
7.5.3 <i>Search-Shield</i>	39
7.5.4 <i>Surf-Shield</i>	39
7.6 Proteção Residente	43
7.6.1 <i>Princípios da Proteção Residente</i>	43
7.6.2 <i>Interface da Proteção Residente</i>	43
7.6.3 <i>Deteção da Proteção Residente</i>	43
7.7 Family Safety	48
7.8 AVG LiveKive	48
7.9 Verificador de E-mail	48
7.9.1 <i>Princípios do Verificador de E-mail</i>	48
7.9.2 <i>Interface do Verificador de E-mail</i>	48
7.9.3 <i>Deteção de Verificador de E-mail</i>	48
7.10 Gerenciador de atualizações	52
7.10.1 <i>Princípios do Gerenciador de Atualizações</i>	52
7.10.2 <i>Interface do Gerenciador de atualizações</i>	52
7.11 Licença	54
7.12 Administração Remota	55
7.13 Proteção On-line	56
7.13.1 <i>Princípios da Proteção On-line</i>	56
7.13.2 <i>Interface da Proteção On-line</i>	56



7.13.3 Detecção da Proteção On-line	56
7.14 Anti-Rootkit	59
7.14.1 Princípios do Anti-Rootkit	59
7.14.2 Interface do Anti-Rootkit	59
7.15 Ferramentas do Sistema	61
7.15.1 Processos	61
7.15.2 Conexões da Rede	61
7.15.3 Início automático	61
7.15.4 Navegador de Extensões	61
7.15.5 Visualizador LSP	61
7.16 PC Analyzer	66
7.17 ID Protection	68
7.17.1 Princípios do ID Protection	68
7.17.2 Interface do ID Protection	68
7.18 Barra de ferramentas de segurança	70
8. Barra de Ferramentas de Segurança do AVG	72
8.1 Interface da Barra de Ferramentas de Segurança do AVG	72
8.1.1 Botão do logotipo AVG	72
8.1.2 Caixa de pesquisa do AVG Secure Search (powered by Google)	72
8.1.3 Status da Página	72
8.1.4 Notícias do AVG	72
8.1.5 Notícias	72
8.1.6 Excluir histórico	72
8.1.7 Notificador de e-mail	72
8.1.8 Informações do Tempo	72
8.1.9 Facebook	72
8.2 Opções da Barra de Ferramentas de Segurança do AVG	79
8.2.1 Guia Geral	79
8.2.2 Guia Botões úteis	79
8.2.3 Guia Segurança	79
8.2.4 Guia Opções avançadas	79
9. Configurações avançadas do AVG	84
9.1 Aparência	84
9.2 Sons	86
9.3 Ignorar condições de falhas	88
9.4 Identity Protection	89
9.4.1 Configurações do Identity Protection	89

9.4.2 Lista de permissões	89
9.5 Quarentena de vírus	93
9.6 Exceções PPI	93
9.7 Anti-Spam	95
9.7.1 Configurações	95
9.7.2 Desempenho	95
9.7.3 RBL	95
9.7.4 Lista de exceções	95
9.7.5 Lista negra	95
9.7.6 Configurações avançadas	95
9.8 Proteção On-line	107
9.8.1 Proteção da Web	107
9.8.2 Mensagens Instantâneas	107
9.9 Link Scanner	111
9.10 Verificações	112
9.10.1 Verificar todo o computador	112
9.10.2 Verificação da extensão shell	112
9.10.3 Verificar arquivos ou pastas específicos	112
9.10.4 Verificação de dispositivo removível	112
9.11 Programações	117
9.11.1 Verificação programada	117
9.11.2 Programação de atualização de banco de dados de vírus	117
9.11.3 Agendamento de atualização de programa	117
9.11.4 Agendamento de atualização do anti-spam	117
9.12 Verificador de e-mail	129
9.12.1 Certificação	129
9.12.2 Filtragem de correio	129
9.12.3 Servidores	129
9.13 Proteção Residente	138
9.13.1 Configurações avançadas	138
9.13.2 Itens excluídos	138
9.14 Servidor de cache	142
9.15 Anti-Rootkit	143
9.16 Atualizar	144
9.16.1 Proxy	144
9.16.2 Dial-up	144
9.16.3 URL	144
9.16.4 Gerenciar	144



9.17 Desativar temporariamente a proteção do AVG	151
9.18 Programa de Aprimoramento de Produto	152
10. Configurações de Firewall	155
10.1 Geral	155
10.2 Segurança	156
10.3 Perfis de áreas e adaptadores	157
10.4 IDS	158
10.5 Logs	160
10.6 Perfis	162
11. Verificação do AVG	164
11.1 Interface da verificação	164
11.2 Verificações predefinidas	165
11.2.1 Verificação de todo o computador	165
11.2.2 Verificar arquivos ou pastas específicos	165
11.2.3 Verificação Anti-Rootkit	165
11.3 Verificando o Windows Explorer	175
11.4 Verificação de linha de comando	176
11.4.1 Parâmetros de verificação CMD	176
11.5 Programação de verificação	178
11.5.1 Configurações de programação	178
11.5.2 Como verificar	178
11.5.3 O que verificar	178
11.6 Visão geral dos resultados da verificação	188
11.7 Detalhes dos resultados da verificação	189
11.7.1 Guia Visão geral dos resultados	189
11.7.2 Guia Infecções	189
11.7.3 Guia Spyware	189
11.7.4 Guia Avisos	189
11.7.5 Guia Rootkits	189
11.7.6 Guia Informações	189
11.8 Quarentena de vírus	197
12. Atualizações do AVG	199
12.1 Níveis de atualização	199
12.2 Tipos de atualização	199
12.3 Processo de atualização	199



13. Histórico de eventos	201
14. Perguntas Frequentes e Suporte Técnico	203



1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG Internet Security 2011**.

Parabéns pela aquisição do AVG Internet Security 2011!

O AVG Internet Security 2011 **é um dos vários produtos AVG premiados criados para fornecer a você paz de espírito e total segurança para o seu computador**. Como ocorreu com todos os produtos do AVG, o **AVG Internet Security 2011** foi completamente reprojeto para fornecer a proteção e a segurança certificada e renomada do AVG em uma nova forma, mais eficiente e amigável. Seu novo produto AVG Internet Security 2011 **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 opções para 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.

Todos os produtos AVG oferecem

- Proteção relevante para a forma como você usa seu computador e a Internet: transações bancárias e compras, navegação e pesquisa, bate-papo e envio de email ou download de arquivos e redes sociais - a AVG tem o produto de proteção certo para você
- Proteção isenta de problemas confiável usada por mais de 110 milhões de pessoas em todo o mundo e alimentada por uma rede global de pesquisadores altamente experientes
- Proteção com suporte especializado



2. Requisitos de instalação do AVG

2.1. Sistemas operacionais suportados

O **AVG Internet Security 2011** destina-se à proteção de estações de trabalho com os seguintes sistemas operacionais:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64, todas as edições)
- Windows 7 (x86 e x64, todas as edições)

(e possíveis service packs posteriores para sistemas operacionais específicos)

Observação: o componente [ID Protection](#) não é suportado no Windows e XP x64. Nesses sistemas operacionais, é possível instalar AVG Internet Security 2011, mas sem o componente IDP.

2.2. Requisitos de HW mínimos e recomendados

Requisitos mínimos de hardware para **AVG Internet Security 2011**:

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

Requisitos recomendados de hardware para **AVG Internet Security 2011**:

- CPU Intel Pentium 1,8 GHz
- 512 MB de memória RAM
- 1400 MB de espaço livre em disco rígido (para fins de instalação)



3. Opções de instalação do AVG

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

Antes de começar a instalar o AVG, é 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 ter certeza de instalar a versão mais recente disponível de AVG Internet Security 2011.

Durante o processo de instalação, será solicitado 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 sua cópia do AVG on-line, o número da licença foi enviado para você por e-mail.



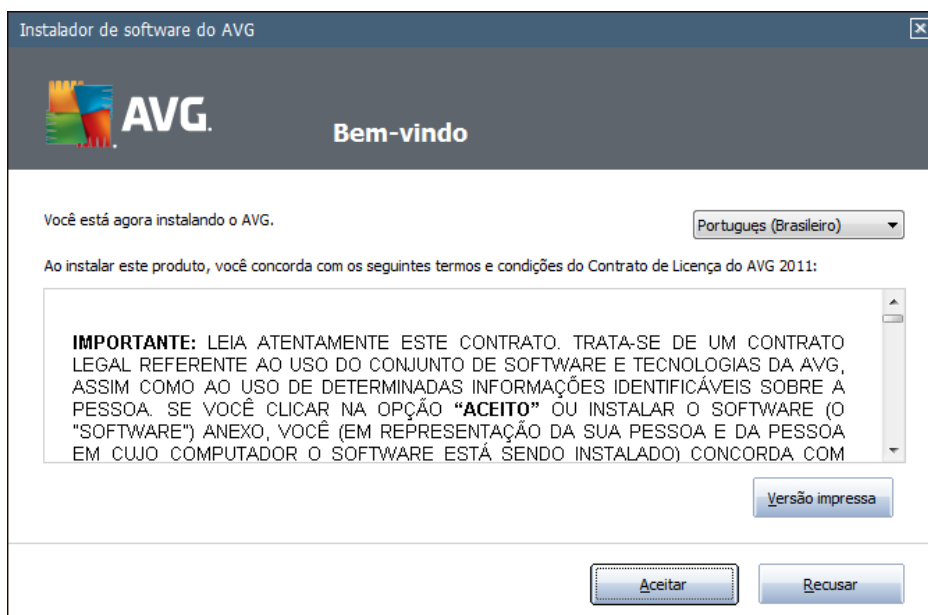
4. Processo de instalação do AVG

Para instalar o **AVG Internet Security 2011** em seu computador, você precisa obter o arquivo de instalação mais recente. Você pode usar o arquivo de instalação do CD que é parte da edição, mas o arquivo pode estar desatualizado. Dessa forma, é recomendável obter a versão mais recente do arquivo de instalação on-line. Você pode fazer download do arquivo no site da AVG <http://www.avg.com/>, seção [Suporte e Download](#).

A instalação é uma sequência 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:

4.1. Bem-vindo

O processo de instalação é iniciado com a janela da caixa de diálogo **Boas-vindas**. Aqui, é possível selecionar o idioma usado para o processo de instalação e o idioma padrão da interface do usuário do AVG. Na seção superior da janela da caixa de diálogo, localize o menu suspenso com a lista dos idiomas que podem ser escolhidos:



Atenção: aqui você está selecionando o idioma para o processo de instalação. O idioma selecionado será instalado como padrão para a interface do usuário do AVG, junto com inglês, que é instalado automaticamente. Se você quiser instalar outros idiomas para a interface do usuário, defina-os em uma das seguintes caixas de diálogo de configuração nomeadas [Opções Personalizadas](#).

Além disso, essa caixa de diálogo fornece o contrato de licença completo do AVG. Leia-o com atenção. Para confirmar que leu, compreendeu e aceita o contrato, pressione o botão **Aceitar**. Se você não concordar com o contrato de licença, pressione o botão **Recusar** e o processo de instalação será encerrado imediatamente.



4.2. Ativar sua licença do AVG

Na caixa de diálogo **Ativar sua Licença**, você deverá fornecer o número da sua licença no campo de texto fornecido.

O número de vendas pode ser encontrado no CD fornecido na embalagem do **AVG Internet Security 2011**. O número da licença está no e-mail de confirmação recebido depois da aquisição do AVG Internet Security 2011 **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.

4.3. Selecionar tipo de instalação



A caixa de diálogo **Selecionar tipo de instalação** oferece duas opções de instalação: **Instalação Rápida** e **Instalação Personalizada**.

Para a maioria dos usuários, é altamente recomendável manter a **Instalação Rápida** 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. Se você tiver selecionado a opção **Instalação Rápida**, pressione o botão **Próximo** para avançar para a caixa de diálogo [Instalar a Barra de Ferramentas de Segurança do AVG](#) seguinte.

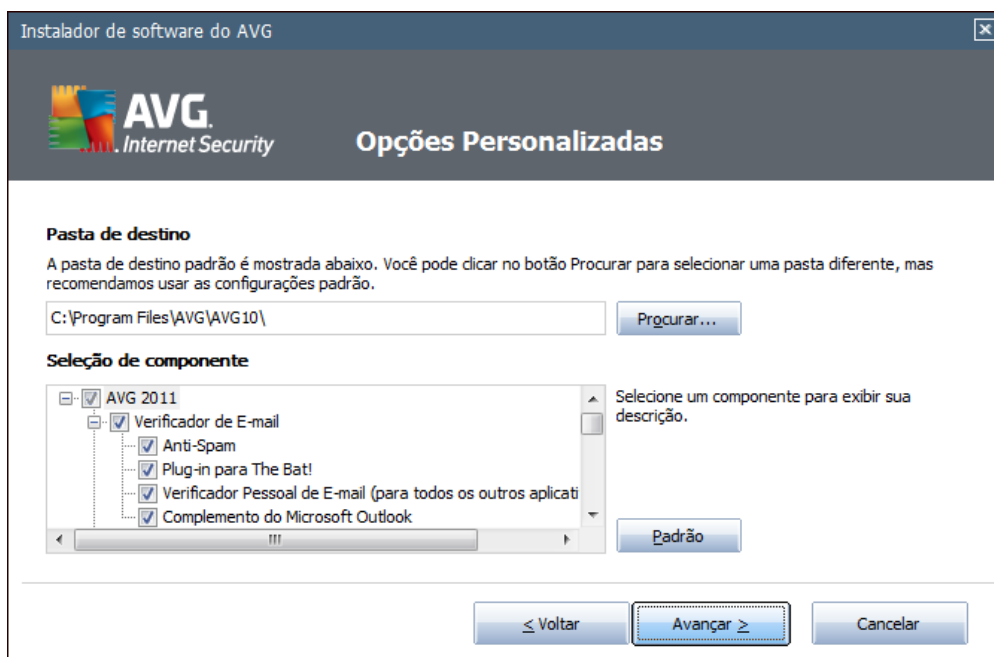
A **instalação personalizada** só deve ser usada por usuários experientes que tenham um motivo válido para instalar o AVG com configurações diferentes das padrão, ou seja, para se ajustar aos requisitos específicos do sistema. Após selecionar esta opção, pressione o botão **Próximo** para avançar para a caixa de diálogo [Opções Personalizadas](#).

Na seção direita da caixa de diálogo, você pode encontrar a caixa de seleção relacionada ao [gadget AVG](#) (com suporte no Windows Vista/Windows 7). Se quiser instalar esse gadget, marque a respectiva caixa de seleção. O [gadget AVG](#) poderá ser acessado pela barra lateral do Windows, proporcionando-lhe um acesso imediato aos recursos mais importantes do seu **AVG Internet Security 2011**, por exemplo, [verificação](#) e [atualização](#).



4.4. Opções personalizadas

A caixa de diálogo **Opções Personalizadas** permite configurar dois parâmetros da instalação:



Pasta de destino

Na seção **Pasta de Destino** da caixa de diálogo, você deve especificar o local onde o **AVG Internet Security 2011** deve ser instalado. Por padrão, o AVG será instalado na pasta Arquivos de programas da unidade C:. Se você desejar alterar esse local, use o botão **Procurar** para exibir a estrutura da unidade e selecionar a respectiva pasta.

Seleção de componente

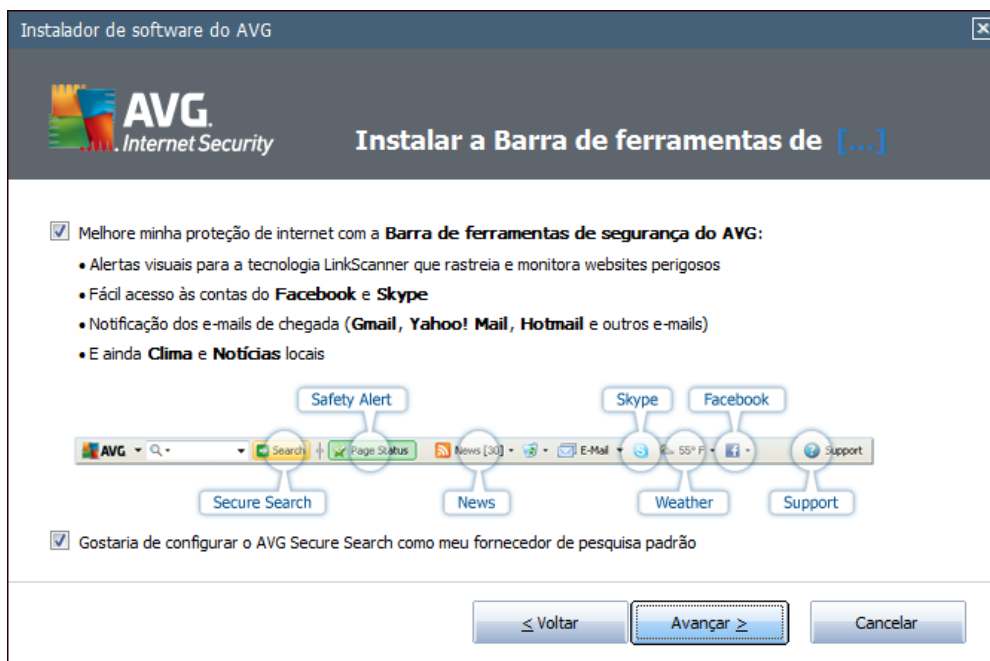
A seção **Seleção de Componente** exibe uma visão geral de todos os componentes **AVG Internet Security 2011** que podem ser instalados. Se as configurações padrão não forem adequadas a você, será possível remover/adicionar componentes específicos.

Entretanto, só é possível selecionar os componentes incluídos na edição do AVG que você adquiriu!

Selecione qualquer item na lista **Seleção de Componente**, e uma breve descrição do respectivo componente será exibida no lado direito desta seção. Para informações detalhadas sobre a funcionalidade de cada componente, consulte o capítulo [Visão Geral de Componentes](#) dessa documentação. Para reverter para a configuração padrão predefinida pelo fornecedor do software, use o botão **Padrão**.

Pressione o botão **Avançar** para continuar.

4.5. Instalar a Barra de Ferramentas de Segurança do AVG



Na caixa de diálogo **Instalar a Barra de Ferramentas de Segurança AVG**, decida se deseja instalar a **Barra de Ferramentas de Segurança AVG**. Se você não alterar as configurações padrão, esse componente será instalado automaticamente no navegador da Internet (*navegadores atualmente suportados são Microsoft Internet Explorer v. 6.0 ou mais recente e Mozilla Firefox v. 3.0 ou mais recente*), para lhe fornecer proteção online abrangente enquanto estiver navegando pela Internet.

Além disso, você tem a opção de decidir se quer escolher o **AVG Secure Search (powered by Google)** como o provedor de pesquisa padrão. Em caso afirmativo, mantenha a respectiva caixa de seleção marcada.



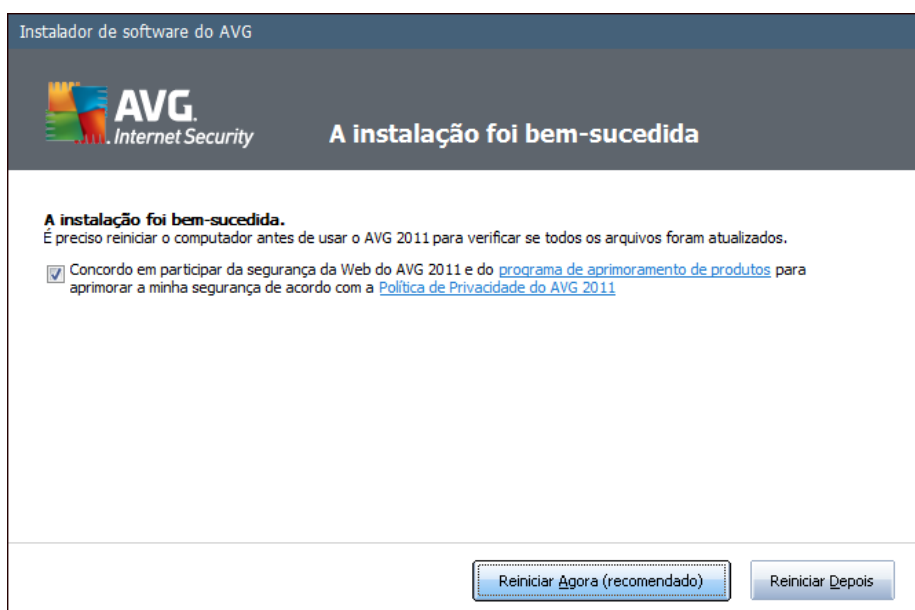
4.6. Progresso da Instalação

A caixa de diálogo **Progresso da Instalação** 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.

4.7. Instalação bem sucedida





A caixa de diálogo **Instalação realizada com êxito** confirma que o **AVG Internet Security 2011** foi totalmente instalado e configurado.

Nessa caixa de diálogo, forneça suas informações de contato para que possa receber todas as informações e notícias relacionadas ao produto. Abaixo do formulário de registro, você encontrará as duas seguintes opções:

- **Sim, manter-me informado sobre notícias de segurança e ofertas especiais do AVG 2011 por email** - marque a caixa de seleção para mencionar que gostaria de ser informado sobre as novidades na esfera de segurança de Internet e receber informações sobre ofertas especiais, aprimoramentos e atualizações do produto AVG etc.
- **Concordo em participar do Programa de Aprimoramento de Produto e Segurança na Web do AVG 2011 ...** - marque esta caixa de seleção para concordar que deseja participar do Programa de Aprimoramento de Produto (para mais detalhes, veja o capítulo [Configurações Avançadas/Programa de Aprimoramento de Produto AVG](#)) que coleta informações anônimas sobre ameaças detectadas para aumentar o nível de segurança geral na Internet.

Para finalizar o processo de instalação, é preciso reiniciar o computador: selecione se deseja **Reiniciar Agora** ou adiar essa ação - **Reiniciar Depois**.

Observação: se estiver usando alguma licença comercial do AVG e no caso de você ter selecionado anteriormente o item *Administração remota* a ser instalado (consulte [Opções Personalizadas](#)), a caixa de diálogo *Instalação realizada com êxito* será exibida na seguinte interface:

É preciso especificar os parâmetros do AVG DataCenter - forneça a string de conexão para o AVG DataCenter, no formato *servidor:porta*. Se essas informações não estiverem disponíveis no momento, deixe o campo em branco, e você poderá definir a configuração mais tarde, na caixa de diálogo **Configurações avançadas / Administração remota**. Para obter informações detalhadas sobre a administração remota do AVG, consulte o manual do usuário do AVG Business Edition, que pode ser baixado no site do AVG (<http://www.avg.com/>).



5. Após a instalação

5.1. Registro do produto

Ao concluir a instalação do **AVG Internet Security 2011**, 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.

5.2. Acesso à interface do usuário

A [Interface do Usuário do AVG](#) pode ser acessada de várias formas:

- clique duas vezes no [ícone da bandeja de sistema do AVG](#)
- clique duas vezes no ícone do AVG na área de trabalho
- clique duas vezes na linha de status localizada na seção inferior do [gadget AVG](#) (se [instalado](#); com suporte no Windows Vista/ Windows 7)
- no menu **Iniciar/Programas/AVG 2011/Interface do Usuário do AVG**
- da [Barra de Ferramentas de Segurança do AVG](#) por meio da opção **Iniciar AVG**

5.3. 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 Internet Security 2011**. 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](#).

5.4. Teste Eicar

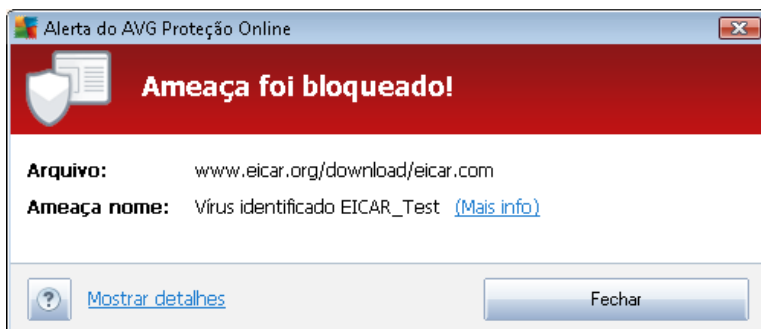
Para confirmar que **AVG Internet Security 2011** foi instalado corretamente, você pode executar o teste EICAR.

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

Tente baixar o arquivo **eicar.com** e salve-o em seu disco local. Logo após a confirmação do download do arquivo de teste, o [Proteção Online](#) reagirá a ele com um aviso. Esse aviso demonstra



que o AVG está instalado corretamente em seu computador.



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

5.5. Configuração padrão do AVG

A configuração padrão (isto é, como o aplicativo é configurado logo após a instalação) de **AVG Internet Security 2011** é definida pelo fornecedor do software, de forma que todos os componentes e funções sejam ajustados para obter um desempenho ideal.

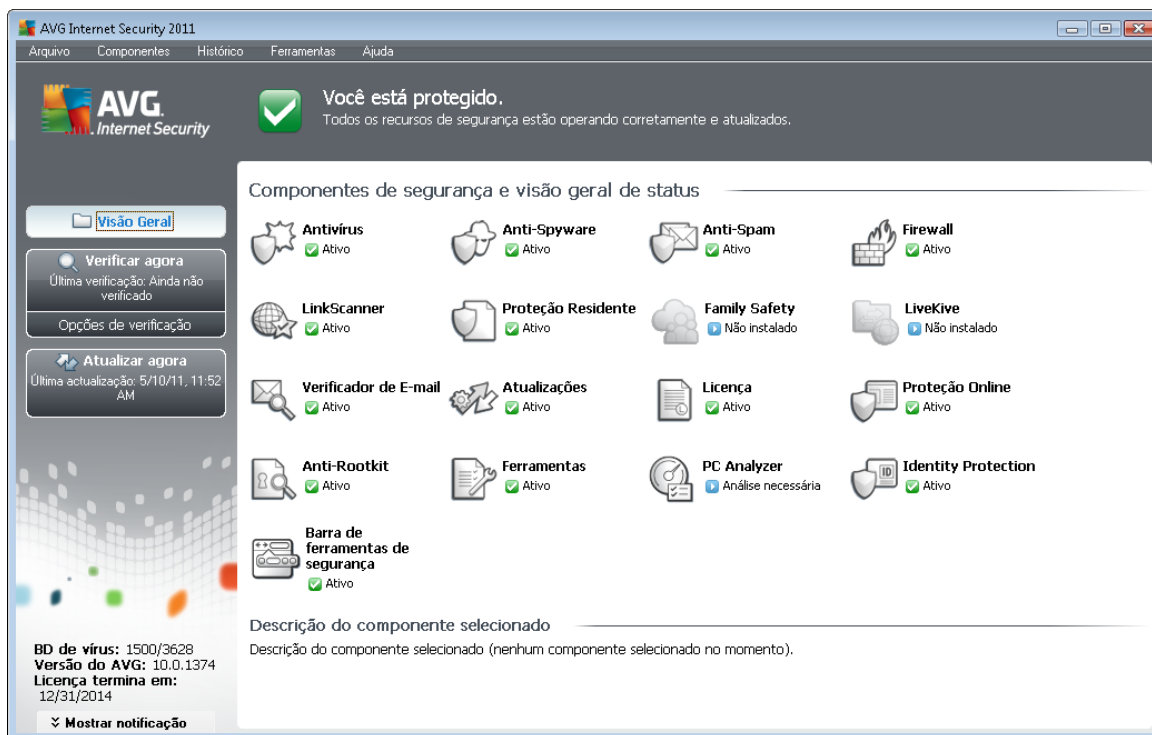
A menos que você tenha um motivo real para isso, não mude as configurações do AVG! Alterações nas configurações devem ser realizadas somente por um usuário experiente.

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**.



6. Interface de usuário do AVG

O AVG Internet Security 2011 é aberto com a janela principal:



A janela principal é dividida em várias seções:

- **Menu do Sistema** (linha do sistema superior da janela) é a navegação padrão que permite acessar todos os componentes, serviços e recursos do AVG - [detalhes >>](#)
- **Informações do Status de Segurança** (seção inferior da janela) fornece informações sobre o status atual do programa AVG - [detalhes >>](#)
- **Links Rápidos** (seção esquerda da janela) permite acessar rapidamente as tarefas mais importantes e mais utilizadas do AVG - [detalhes >>](#)
- **Visão Geral dos Componentes** (seção central da janela) oferece uma visão geral de todos os componentes AVG instalados - [detalhes >>](#)
- **Estatísticas** (seção inferior esquerda da janela) fornece todos os dados estatísticos referentes à operação dos programas - [detalhes >>](#)
- **Ícone da Bandeja do Sistema** (canto inferior direito do monitor, na bandeja do sistema) indica o status atual do AVG - [detalhes >>](#)
- **O gadget AVG** (barra lateral do Windows, oferecida no Windows Vista/7) permite acesso rápido à atualização e à verificação do AVG - [detalhes >>](#)



6.1. Menu do sistema

O **Menu do sistema** é a navegação padrão usada em todos os aplicativos Windows. Está localizado horizontalmente, na parte superior da janela principal do AVG Internet Security 2011. 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:

6.1.1. Arquivo

- **Sair** - fecha a interface do usuário do **AVG Internet Security 2011**. Entretanto, o aplicativo AVG continuará sendo executado em segundo plano e seu computador continuará protegido.

6.1.2. 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](#)
- **O Antivírus** garante que o computador seja protegido de vírus que tentam entrar nele - [detalhes >>](#)
- **Anti-Spyware** garante que o seu computador esteja protegido contra spyware e adware - [detalhes >>](#)
- **O Anti-Spam** verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis como SPAM - [detalhes >>](#)
- **O Firewall** controla a forma como o computador troca dados com outros computadores na Internet ou na rede local [detalhes >>](#)
- **O LinkScanner** verifica os resultados de pesquisa exibidos no navegador da Internet - [detalhes >>](#)
- **O Verificador de E-mail** verifica todas as mensagens enviadas e recebidas para procurar vírus [detalhes >>](#)
- **Segurança da Família** ajuda a monitorar as atividades on-line dos seus filhos, e protegê-los de sites de conteúdo impróprio - [detalhes >>](#)
- **LiveKive** fornece backup automático de seus dados online - [detalhes >>](#)
- **A Proteção Residente** é executada em segundo plano e verifica os arquivos à medida que eles são copiados, abertos ou salvos [detalhes >>](#)
- **O Gerenciador de Atualizações** controla todas as atualizações do AVG - [detalhes >>](#)
- **Licença** exibe o número da licença, tipo e data de validade - [detalhes >>](#)



- **Proteção Online** verifica todos os dados baixados por um navegador da Web [detalhes>>](#)
- **O Anti-Rootkit** detecta programas e tecnologias que tentam camuflar malware - [detalhes>>](#)
- **Ferramentas do Sistema** oferece um resumo detalhado das informações do ambiente do AVG e do sistema operacional - [detalhes >>](#)
- O αναλυσαδop **PC Analyzer** fornece informações sobre o status do seu computador - [detalhes >>](#)
- **Identity Protection** - componente anti-malware cujo foco é evitar que ladrões de identidade roubem seus valiosos bens digitais pessoais - [detalhes >>](#)
- **Barra de Ferramenta de Segurança** permite que você use funcionalidade seleccionada do AVG diretamente do seu navegador Internet - [>> detalhes](#)
- **Administração Remota** é exibido apenas no AVG Business Editions, caso tenha especificado durante o [processo de instalação](#) que esse componente deve ser instalado

6.1.3. Histórico

- [Resultados da verificação](#) - alterna para a interface de teste do AVG, especificamente para a caixa de diálogo [Visão Geral dos Resultados da Verificação](#)
- [Detecção da Proteção Residente](#) - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela [Proteção Residente](#)
- [Detecção do Verificador de E-mail](#) - abre uma caixa de diálogo com uma visão geral dos anexos de e-mail detectados como perigosos pelo componente [Verificador de E-mail](#)
- [Detecção da Proteção Online](#) - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pelo [Proteção Online](#)
- [Quarentena de Vírus](#) - abre a interface do espaço de quarentena ([Quarentena de Vírus](#)) no qual o AVG remove todas as infecções detectadas que, por algum motivo, não podem ser resolvidas automaticamente. No espaço de quarentena, os arquivos infectados são isolados e a segurança do computador é preservada, e, ao mesmo tempo, os arquivos infectados são armazenados para possível reparo futuro
- [Log de histórico de eventos](#) - abre a interface de log de histórico com uma visão geral de todas as ações registradas **AVG Internet Security 2011** .
- [Firewall](#) - abre a interface de configurações do firewall na guia [Logs](#) com uma visão geral detalhada de todas as ações do firewall

6.1.4. Ferramentas

- [Verificar computador](#) - alterna para a [interface de verificação do AVG](#) e inicia a verificação em todo o computador.
- [Verificar pasta seleccionada](#) - 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** - inicia automaticamente o processo de atualização **AVG Internet Security 2011**.
- **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 Internet Security 2011**. Em geral, é recomendável manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.
- **Configurações do Firewall** - abre uma caixa de diálogo independente para configuração avançada do componente **Firewall**.

6.1.5. 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
- **Sua Web AVG** - 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.

Observação: Se estiver utilizando a versão de teste do **AVG Internet Security 2011**, os dois últimos itens aparecem como **Comprar agora** e **Ativar**, permitindo que você compre a versão completa do programa imediatamente. Para **AVG Internet Security 2011** instalado com um número de vendas, os itens são exibidos como **Registrar** e **Ativar**. Para obter mais informações, visite a seção **Licença** deste documento.



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

6.2. 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 Internet Security 2011**. 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 com status crítico! Um ou mais componentes não estão funcionando adequadamente 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](#).

No caso de o AVG não ser ajustado para o desempenho ideal, um novo botão denominado **Corrigir** (ou **Corrigir tudo**, se o problema envolver mais de um componente) aparecerá perto das informações do status de segurança. Pressione o botão para iniciar um processo automático de Clique com o botão direito no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e configuração do programa. Essa é uma forma fácil de ajustar o AVG para o desempenho ideal e alcançar o nível de segurança máximo!

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!



Observação: as informações sobre o status do AVG também podem ser obtidas a qualquer momento no [ícone da bandeja do sistema](#).

6.3. Links rápidos

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



- **Visão geral** - use este 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 >>](#)
- **Verificar agora** - por padrão, o botão fornece informações (*tipo de verificação, data da última verificação*) sobre a última verificação feita. Você pode executar o comando **Verificar agora** para iniciar a mesma verificação novamente ou pode seguir o link **Opções de verificação** para abrir a interface de verificação do AVG, onde é possível realizar verificações, programar verificações ou editar seus parâmetros. Consulte o capítulo [Verificação do AVG >>](#)
- **Atualizar agora** - o link fornece a data da última execução do processo de atualização. Pressione o botão para abrir a interface de atualização e executar o processo de atualização do AVG - 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.

6.4. Visão geral dos componentes

A seção **Visão geral dos componentes** está localizada na parte central da [Interface do usuário do AVG](#). A seção é dividida em duas partes:

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



No **AVG Internet Security 2011a** seção **Visão geral dos componentes** contém informações sobre os seguintes componentes:

- **O Antivírus** garante que o computador seja protegido de vírus que tentam entrar nele - [detalhes >>](#)
- **Anti-Spyware** garante que o seu computador esteja protegido contra spyware e adware - [detalhes >>](#)
- **O Anti-Spam** verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis como SPAM - [detalhes >>](#)
- **O Firewall** controla a forma como o computador troca dados com outros computadores na Internet ou na rede local [detalhes >>](#)
- **O LinkScanner** verifica os resultados de pesquisa exibidos no navegador da Internet - [detalhes >>](#)
- **O Verificador de E-mail** verifica todas as mensagens enviadas e recebidas para procurar vírus [detalhes >>](#)
- **A Proteção Residente** é executada em segundo plano e verifica os arquivos à medida que eles são copiados, abertos ou salvos [detalhes >>](#)
- **Segurança da Família** ajuda a monitorar as atividades on-line dos seus filhos, e protegê-los de sites de conteúdo impróprio - [detalhes >>](#)
- **LiveKive** fornece backup automático de seus dados online - [detalhes >>](#)
- **O Gerenciador de Atualizações** controla todas as atualizações do AVG - [detalhes >>](#)
- **Licença** exibe o número da licença, tipo e data de validade - [detalhes >>](#)
- **Proteção Online** verifica todos os dados baixados por um navegador da Web [detalhes >>](#)
- **O Anti-Rootkit** detecta programas e tecnologias que tentam camuflar malware - [detalhes >>](#)
- **Ferramentas do Sistema** oferece um resumo detalhado das informações do ambiente do AVG e do sistema operacional - [detalhes >>](#)
- **O PC Analyzer** fornece informações sobre o status do seu computador - [detalhes >>](#)
- **Identity Protection** - componente anti-malware cujo foco é evitar que ladrões de identidade roubem seus valiosos bens digitais pessoais - [detalhes >>](#)
- **Barra de Ferramenta de Segurança** [permite que você use funcionalidades selecionadas do AVG diretamente do seu navegador Internet](#)
- **Administração Remota** exibida apenas no AVG Business Editions, caso você tenha especificado durante o [processo de instalação](#) que esse componente deve ser instalado



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

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

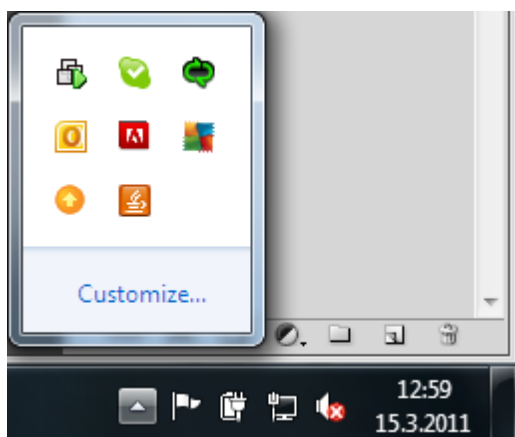
6.5. Estatísticas

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:

- **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 10.0.xxxx, onde 10.0 é a versão da linha do produto, e xxxx indica o número da compilação)
- **Vencimento da licença** - fornece a data de vencimento da licença do AVG

6.6. Ícone da bandeja do sistema

O **Ícone da bandeja do sistema** (na barra de tarefas do Windows) indica o status atual do AVG Internet Security 2011. Ele fica visível sempre na bandeja do sistema, independentemente de a janela principal do AVG estar aberta ou fechada:

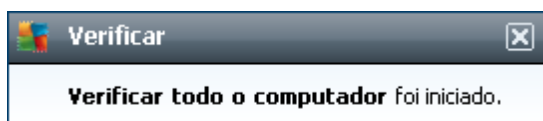


Se colorido , o **Ícone da bandeja do sistema** indica que todos os componentes do AVG estão ativos e completamente funcionais. Da mesma forma, o ícone AVG na bandeja do sistema pode ser exibido em sua cor normal caso o AVG esteja em estado de erro mas que você esteja completamente ciente desta situação e tenha deliberadamente decidido [ignorar o estado do componente](#). Um ícone com um sinal de exclamação  indica um problema (*componente inativo*,



status de erro, etc.). Clique duas vezes no **Ícone da Bandeja do Sistema** para abrir a tela principal e editar um componente.

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



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

- **Abrir Interface do Usuário do AVG** - clique para abrir a [Interface do Usuário do AVG](#)
- **Verificações** - clique para abrir o menu de contexto do
- **Firewall** - clique para abrir o menu de contexto das opções de configurações de [Firewall](#), onde é possível editar os principais parâmetros: [status do Firewall](#) (*Firewall ativado/Firewall desativado/modo Emergência*), [mudança de modos de jogoe](#) [perfis de Firewall](#)
- **Executar o PC Analyzer** - clique para iniciar o componente [PC Analyzer](#)
- **Executando verificações** - este item será exibido apenas se uma verificação estiver atualmente em execução no computador. Para essa verificação, você pode definir sua prioridade ou, como segunda opção, interromper ou pausar a verificação em execução. Além disso, as seguintes ações estão acessíveis: *Definir prioridade para todas as verificações*, *Pausar todas as verificações* ou *Interromper todas as verificações*.
- **Atualizar agora** - inicia uma atualização [imediate](#)
- **Ajuda** - abre o arquivo de ajuda da página de inicialização

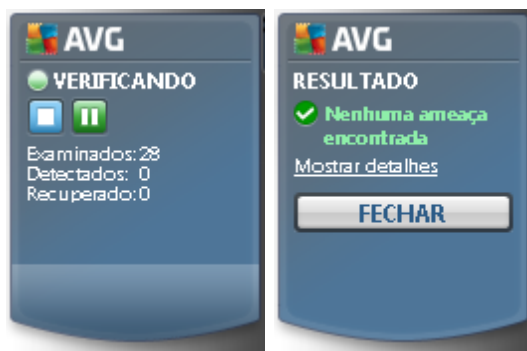
6.7. Gadget AVG

O **gadget AVG** é exibido na área de trabalho do Windows (*barra lateral do Windows*). Esse aplicativo tem suporte apenas nos sistemas operacionais Windows Vista e Windows 7. O **gadget AVG** oferece um acesso imediato às funções mais importantes do **AVG Internet Security 2011**, por exemplo, [verificação](#) e [atualização](#):



O **gadget AVG** fornece as seguintes opções de acesso rápido:

- **Verificar agora** - clique no link **Verificar agora** para iniciar a [verificação de todo o computador](#) diretamente. Você pode acompanhar o progresso do processo de verificação na interface do usuário alternativa do gadget. Uma breve visão geral de estatísticas fornece informações sobre o número de objetos verificados, ameaças detectadas e ameaças reparadas. Durante a verificação, você pode sempre pausar  ou interromper  o processo de verificação. Para obter dados detalhados relacionados aos resultados da verificação, consulte a caixa de diálogo padrão [Visão geral da verificação](#) que pode ser aberta diretamente do dispositivo pela opção **Mostrar detalhes**(os resultados respectivos de verificação serão listados na **Barra lateral do gadget de verificação**).



- **Atualizar agora** - clique no link **Atualizar agora** para iniciar a atualização do AVG diretamente do gadget:



- **Link no Twitter**  - abre uma nova interface do **gadget AVG**, fornecendo uma visão geral dos feeds mais recentes da AVG postados no Twitter. Siga o link **Ver todos os feeds da AVG no Twitter** para abrir o navegador em uma nova janela, e você será redirecionado diretamente ao site do Twitter, especificamente à página dedicada às notícias relacionadas à AVG:



- **Link do Facebook**  - abre o navegador no site do Facebook, especificamente na página da **Comunidade da AVG**
- **LinkedIn**  - esta opção só está disponível na instalação de rede (*ou seja, desde que você tenha instalado o AVG usando uma das licenças do AVG Business Editions*), e ele abre o seu navegador de internet no site **Comunidade AVG SMB** dentro da rede social LinkedIn
- **PC Analyzer**  - abre a interface do usuário no componente [PC Analyzer](#)
- **Caixa Procurar** - digite uma palavra-chave e obtenha os resultados da pesquisa imediatamente em uma nova janela aberta com o seu navegador padrão



7. Componentes do AVG

7.1. Antivírus

7.1.1. Princípios do Antivírus

O mecanismo de verificação do software antivírus verifica se há vírus conhecidos em todos os arquivos e atividades de arquivo (abertura/fechamento de arquivos, etc.) . Todo e qualquer vírus detectado será bloqueado e não poderá executar nenhuma ação. Ele também será limpo e colocado em quarentena. A maioria dos softwares antivírus usa a verificação heurística, em que 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 vírus novo e desconhecido se este contiver algumas características típicas dos vírus existentes.

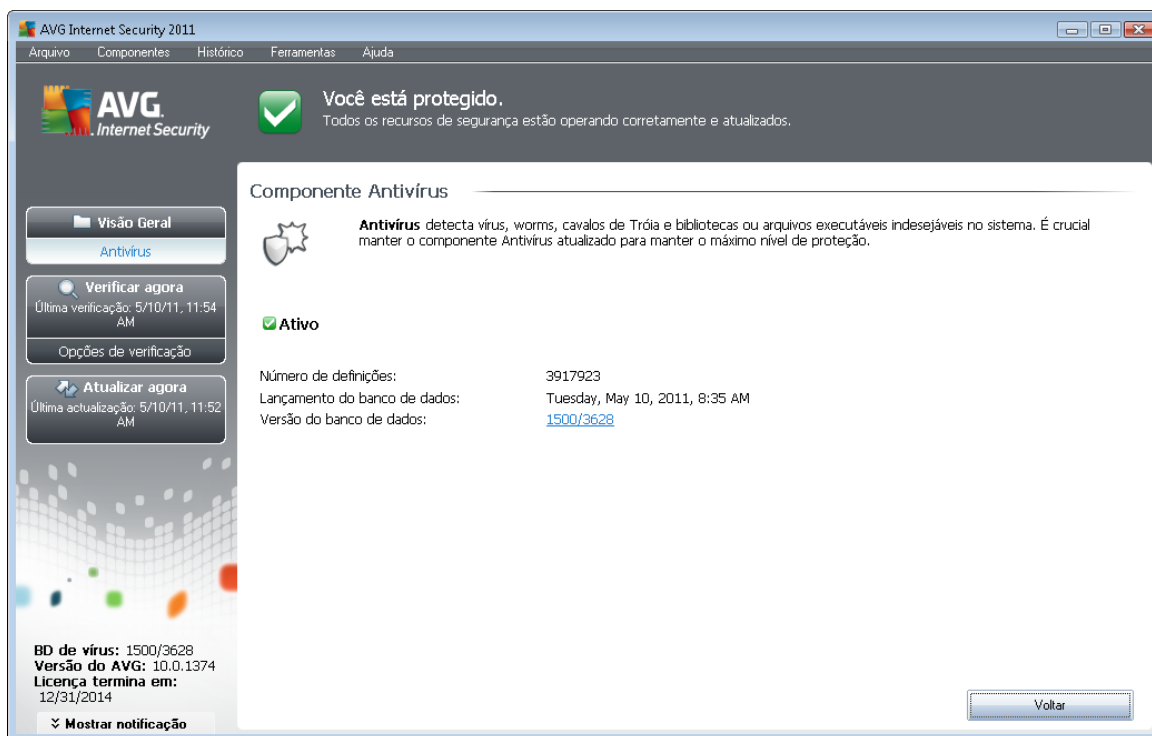
O recurso importante da proteção antivírus é que nenhum vírus conhecido pode ser executado no computador!

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 típicas 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, além de permitir o tratamento de todos os itens potencialmente prejudiciais como qualquer outra infecção.

7.1.2. 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:

- **Número de definições de spyware** - o número fornece a contagem de vírus definidos na versão atualizada do banco de dados de vírus.
- **Lançamento de banco de dados** - especifica quando e a que horas o banco de dados de vírus foi atualizado pela última vez
- **Versão do banco de dados** - define o número da versão do banco de dados de vírus atualmente instalada. 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 à [interface do usuário do AVG](#) padrão (*visão geral dos componentes*).

7.2. Anti-Spyware

7.2.1. Princípios do Anti-Spyware

Normalmente, o spyware é definido como um tipo de malware, ou seja, software que coleta informações a partir do computador do usuário sem o conhecimento ou consentimento dele. Alguns aplicativos de spyware também podem ser instalados propositalmente e, em geral, contêm

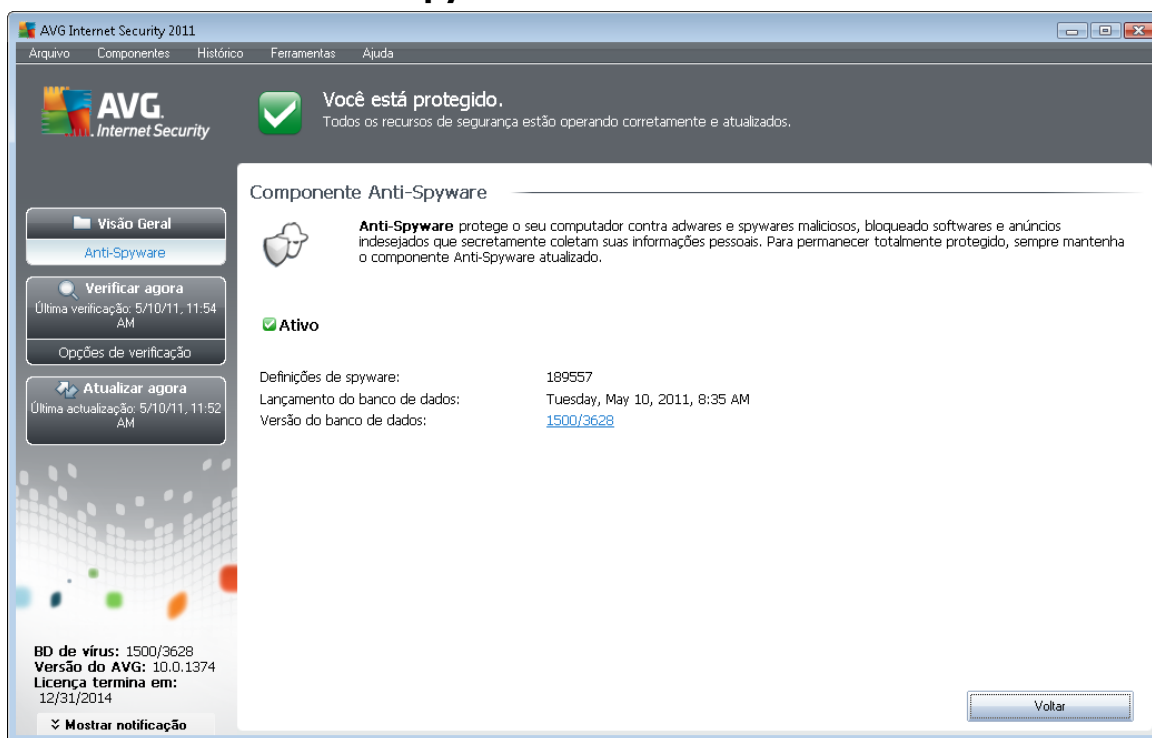


anúncios, janelas pop-up ou tipos diferentes de softwares inoportunos.

Atualmente, a fonte mais comum de infecção são sites com conteúdo potencialmente perigoso. Outros métodos de transmissão, como e-mail ou 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 AVG Internet Security 2011 [atualizações de banco de dados e programas](#). Por essa 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.

7.2.2. Interface do Anti-Spyware



A interface do componente **Anti-Spyware** fornece uma breve visão geral da funcionalidade do componente, informações sobre o status atual do componente e algumas estatísticas de **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.
- **Lançamento de 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 à [interface do usuário do AVG](#) padrão (*visão geral dos componentes*).

7.3. Anti-Spam

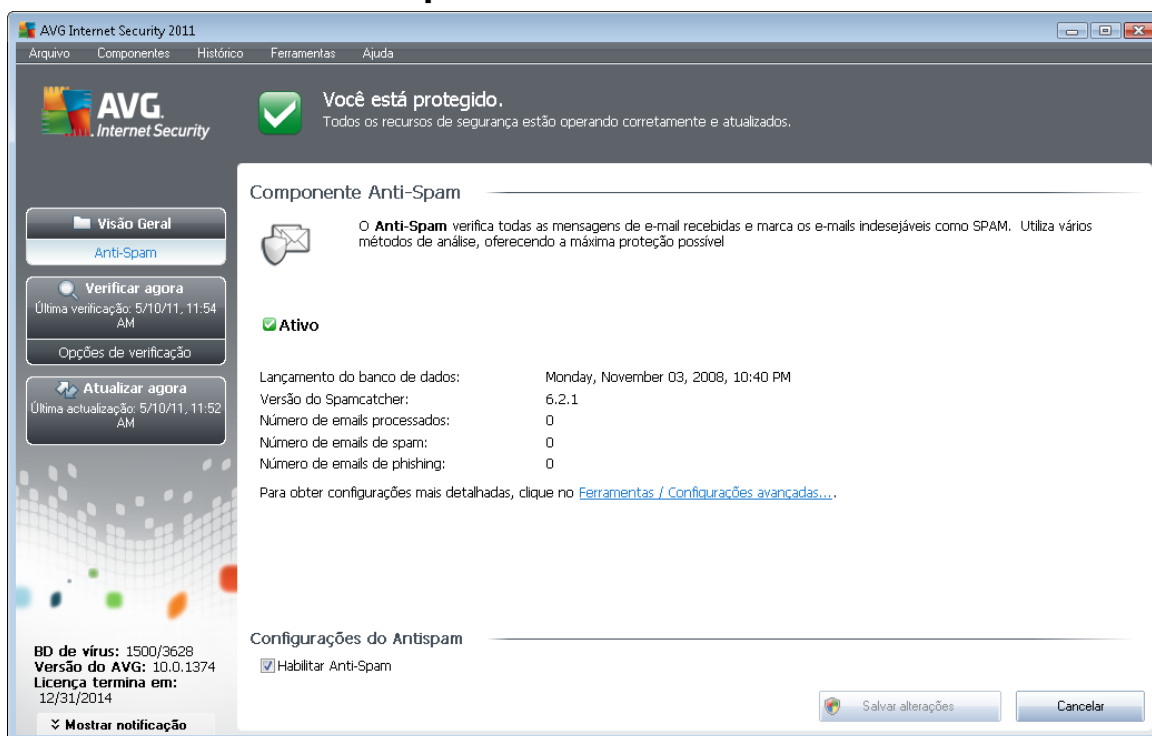
Spam refere-se a e-mail não solicitado, a maioria referente a propaganda de produto ou de serviço, enviada em grande quantidade para um grande número de endereços de e-mail ao mesmo tempo, enchendo as caixas de correio. O Spam não se refere a e-mail comercial válido, cujo envio conta com o consentimento por parte dos clientes. O spam não é apenas inoportuno, mas também pode ser fonte de fraudes, vírus ou conteúdo ofensivo.

7.3.1. Princípios do Anti-Spam

O **AVG Anti-Spam** verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis como spam. O **AVG Anti-Spam** pode modificar o assunto do e-mail (*que foi identificado como spam*), adicionando uma string de texto especial. Dessa forma, é possível filtrar facilmente os seus e-mails no cliente de e-mail.

O **componente AVG Anti-Spam** usa diversos métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejáveis. O **AVG Anti-Spam** usa um banco de dados regularmente atualizado para a detecção de spam. Também é possível usar [servidores RBL](#) (bancos de dados públicos de endereços de e-mail de "spammers conhecidos") e adicionar manualmente endereços de e-mail à sua [Lista de exceções](#) (nunca marcar como spam) e à sua [Lista negra](#) (sempre marcar como spam).

7.3.2. Interface do Anti-Spam



Na caixa de diálogo do componente **Anti-Spam**, você encontrará um texto curto descrevendo a



funcionalidade do componente, informações sobre seu status atual e as seguintes estatísticas:

- **Versão do banco de dados** - especifica quando e a que horas o banco de dados de spam foi atualizado e publicado
- **Versão do Spamcatcher** - define o número da versão mais recente do mecanismo anti-spam
- **Número de emails processados** - especifica quantas mensagens de email foram verificadas desde a última ativação do mecanismo antispam
- **Número de emails spam** - de todos os emails verificados, especifica quantas mensagens foram marcadas como spam
- **Número de emails phishing** - de todos os emails verificados, especifica quantas mensagens foram marcadas como tentativas de phishing

A caixa de diálogo **Anti-Spam** apresenta também o link [Ferramentas/Configurações Avançadas](#). Use o link para ser redirecionado ao ambiente de configuração avançada de todos os componentes do **AVG Internet Security 2011**.

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.

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

7.4. Firewall

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

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

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

Recomendação: geralmente, não é recomendável usar mais de um firewall em um computador individual. A segurança do computador não é aumentada se você instalar mais firewalls. É mais



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

7.4.1. Princípios do Firewall

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

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

O que o AVG Firewall pode fazer:

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

7.4.2. Perfis do Firewall

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

Perfis disponíveis

- **Permitir tudo** - um perfil do sistema de [Firewall](#) que foi predefinido pelo fabricante e está sempre presente. Quando esse perfil é ativado, toda a comunicação de rede é permitida e não se aplicam as regras da política de segurança, como se a proteção do [Firewall](#) estivesse desativada (isto é, todos os aplicativos são permitidos, mas os pacotes ainda estão sendo verificados; para desabilitar completamente qualquer filtragem, é preciso desabilitar o firewall). Esse perfil do sistema não pode ser duplicado, excluído e suas configurações não podem ser modificadas.
- **Bloquear tudo** - um perfil do sistema de [Firewall](#) predefinido pelo fabricante e que está sempre presente. Quando o perfil é ativado, toda a comunicação de rede é bloqueada e o computador não fica acessível para redes externas, nem pode se comunicar com ambientes externos. Esse perfil do sistema não pode ser duplicado, excluído e suas configurações não podem ser modificadas.



- **Perfis personalizados:**

- o **Conectado diretamente à Internet** – adequada para PCs comuns conectados diretamente à Internet ou notebooks conectando-se à Internet fora da rede segura da empresa. Selecione essa opção se estiver se conectando de casa ou se estiver em uma rede de pequena empresa sem controle central. Além disso, selecione essa opção quando estiver viajando e conectando seu notebook a partir de vários locais possivelmente perigosos (*internet café, quarto de hotel, etc.*). Serão criadas regras mais restritas, pois se parte do princípio que esses computadores não possuem proteção adicional e, portanto, requerem proteção máxima.
- o **Computador no domínio** – adequado para computadores em uma rede local, como rede de uma empresa ou escola. Presume-se que a rede esteja protegida por algumas medidas adicionais, de modo que o nível de segurança pode ser inferior para um computador isolado.
- o **Rede doméstica ou corporativa pequena** – adequado para computadores em uma rede pequena, como uma rede doméstica ou de uma pequena empresa, geralmente vários computadores conectados entre si, sem um administrador "central".

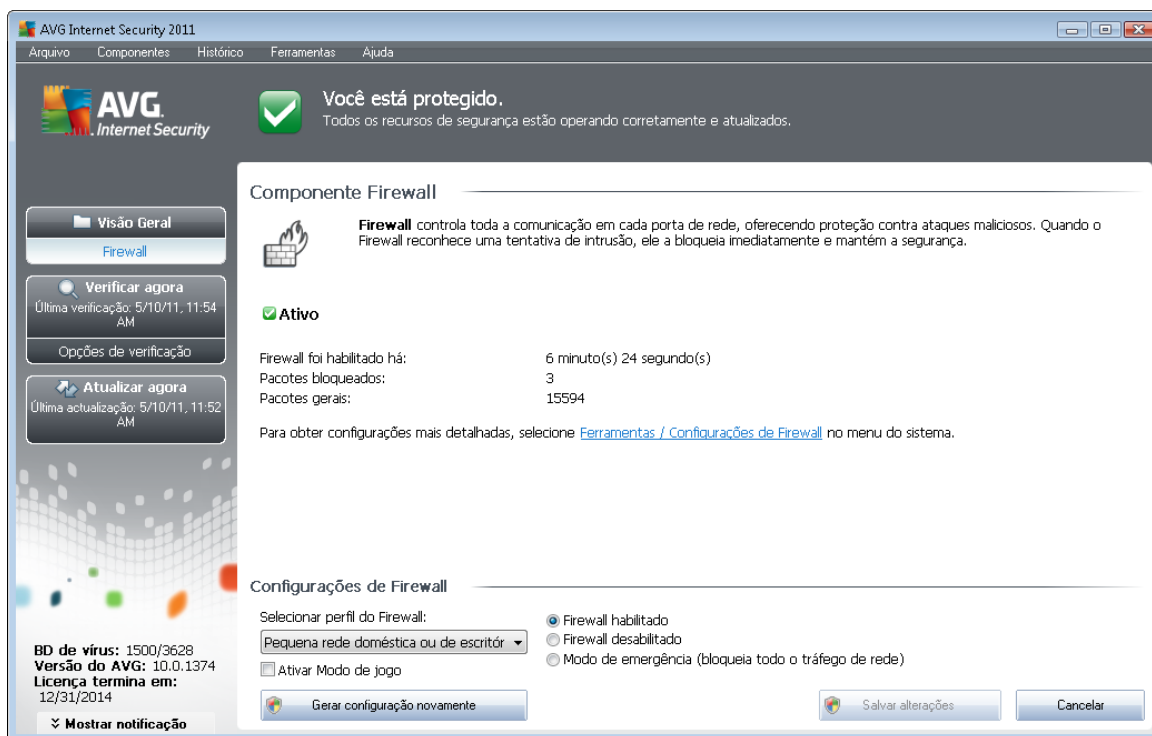
Alternância de perfil

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

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

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

7.4.3. Interface do Firewall



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

- **Firewall ficou habilitado por** - tempo decorrido desde que o Firewall foi iniciado
- **Pacotes bloqueados** - número de pacotes bloqueados do volume total de pacotes verificados
- **Pacotes gerais** - número de todos os pacotes verificados durante a execução do Firewall

Configurações de Firewall

- **Selecionar perfil do Firewall** - no menu suspenso, selecione um dos perfis definidos - dois perfis estão disponíveis sempre (os perfis padrão denominados **Permitir tudo e Bloquear tudo**), outros perfis foram adicionados manualmente por meio da edição do perfil na caixa de diálogo **Perfis** em **Configurações do Firewall**.
- **Ativar modo de jogo** - selecione esta opção para garantir que, quando aplicativos em tela cheia estiverem em execução (*jogos, apresentações, filmes etc.*), o **Firewall** não exiba caixas de diálogo solicitando se você deseja bloquear ou permitir a comunicação com aplicativos desconhecidos. No caso de um aplicativo desconhecido tentar comunicar-se pela rede neste momento, o **Firewall** permitirá ou bloqueará a tentativa automaticamente, de acordo com as configurações no perfil atual. **Nota:** Quando o modo de jogo está ativado, todas as tarefas programadas (verificações, atualizações) são adiadas até que o aplicativo



seja fechado.

- **Status do Firewall:**

- o **Firewall ativado** - selecione esta opção para permitir a comunicação com os aplicativos indicados como 'permitidos' no conjunto de regras definidas no perfil do [Firewall](#) selecionado
- o **Firewall desativado** - esta opção desativa totalmente o [Firewall](#), todo o tráfego da rede é permitido mas não verificado!
- o **Modo de emergência (bloquear todo o tráfego de Internet)** - selecione esta opção para bloquear todo o tráfego em cada porta de rede; o [Firewall](#) ainda está em execução, mas todo o tráfego da rede foi interrompido

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

Botões de controle

- **Gerar configuração novamente** - pressione este botão para substituir a configuração de **Firewall** existente e reverter para a configuração padrão com base na detecção automática.
- **Salvar alterações** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- **Cancelar** - pressione este botão para retornar à [interface do usuário do AVG](#) padrão (visão geral dos componentes)

7.5. Link Scanner

7.5.1. Princípios do Link Scanner

O **LinkScanner** protege contra o crescente número de ameaças atuais e que estão surgindo na Web. Essas ameaças podem estar escondidas em qualquer tipo de site, de governamentais a grandes marcas bem conhecidas, a pequenas empresas, e raramente permanecem nesses locais mais de 24 horas. O **LinkScanner** protege analisando as páginas da web que estão por trás de todos os links em qualquer página da Web que esteja vendo e garantindo que são seguras só no momento que importa – quando você está prestes a clicar nesse link.

A tecnologia do **LinkScanner** consiste em dois recursos, o [Search-Shield](#) e o [Surf-Shield](#):

- O [Search-Shield](#) contém a lista de sites ((endereços de URL) que são conhecidos por



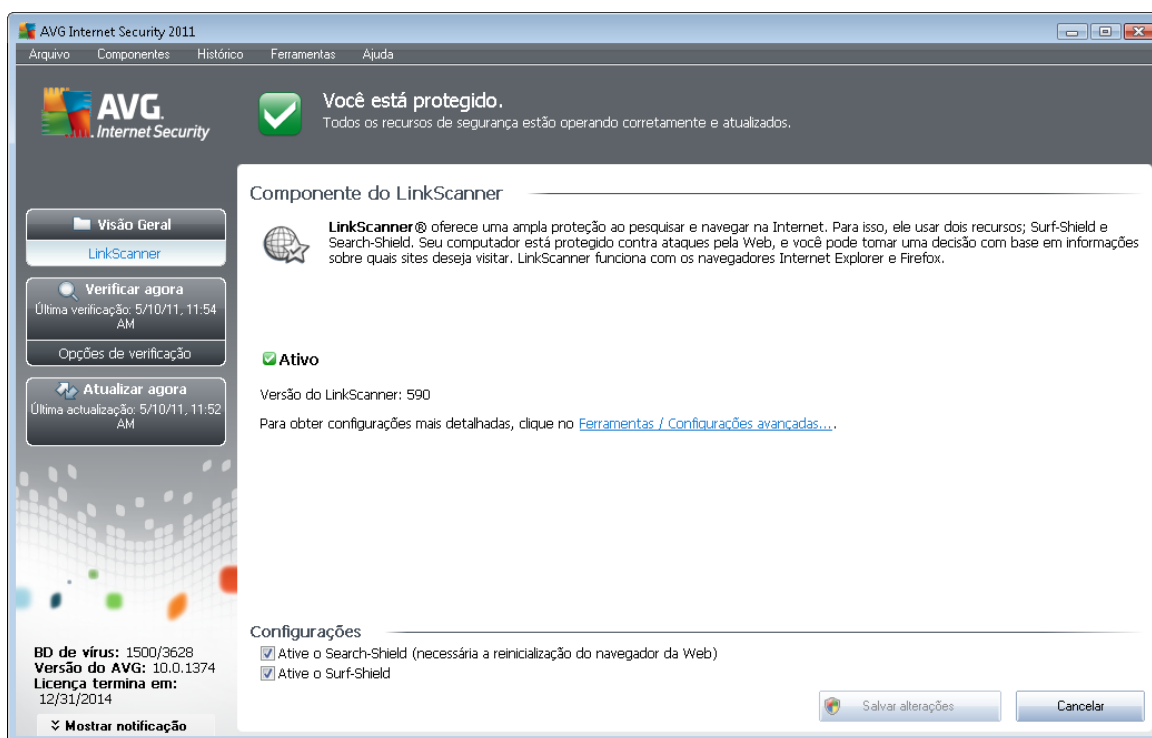
serem perigosos. Ao pesquisar no Google, Yahoo! Em pesquisas no JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ouSlashDot, todos os resultados são verificados de acordo com essa lista, e é mostrado um ícone de veredito (*nos resultados de busca do Yahoo são exibidos somente os ícones de veredito do "site explorado"*).

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

Observação: o LinkScanner não se destina a plataformas de servidores!

7.5.2. Interface do Link Scanner

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



Configurações do LinkScanner

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

- **Habilitar o Search-Shield** - (por padrão): ícones de notificação consultiva em buscas



realizadas com o Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ou SlashDot: verificarão além o conteúdo de sites retornados pelo mecanismo de busca.

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

7.5.3. Search-Shield

Ao pesquisar na Internet com o **Search-Shield** ativado, todos os resultados retornam dos mecanismos de busca mais conhecidos, como *Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, and SlashDot* são analisados com relação a links perigosos ou suspeitos. Ao verificar esses links e marcar os perigosos, o **AVG Link Scanner** indicará o problema antes de você clicar em links suspeitos ou perigosos, portanto você poderá ter certeza de que acessará apenas sites seguros.

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

 A página do link é segura (*este ícone não será exibido para resultados de pesquisa seguros resultados de pesquisa JP*).

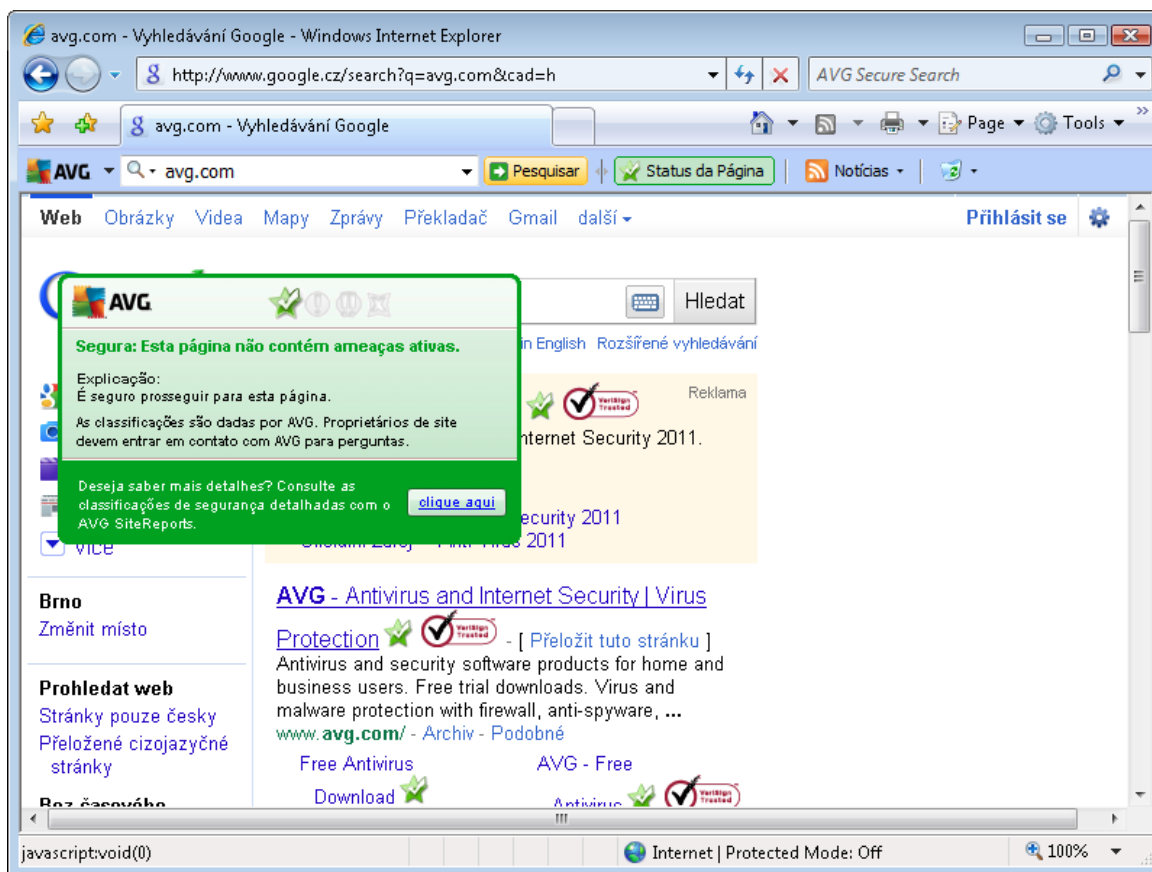
 A página do link não contém ameaças, mas é suspeita (*de origem ou intenção duvidosa, portanto, não é recomendada para compras online etc.*).

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

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

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

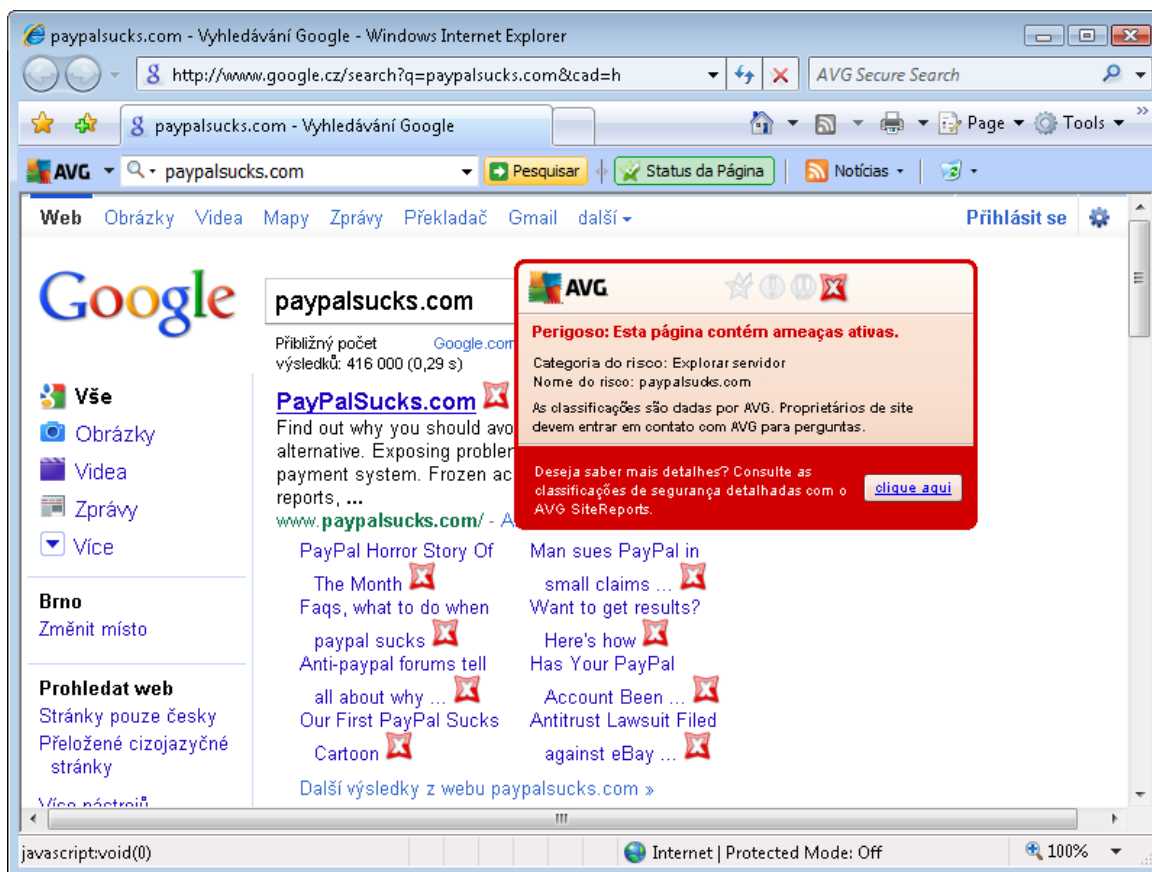
Passar o mouse sobre um ícone de classificação individual exibirá detalhes sobre o link específico em questão. As informações incluem detalhes adicionais da ameaça (*se existir alguma*):



7.5.4. Surf-Shield

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

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



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

7.6. Proteção Residente

7.6.1. 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.

O que a Proteção Residente pode fazer:

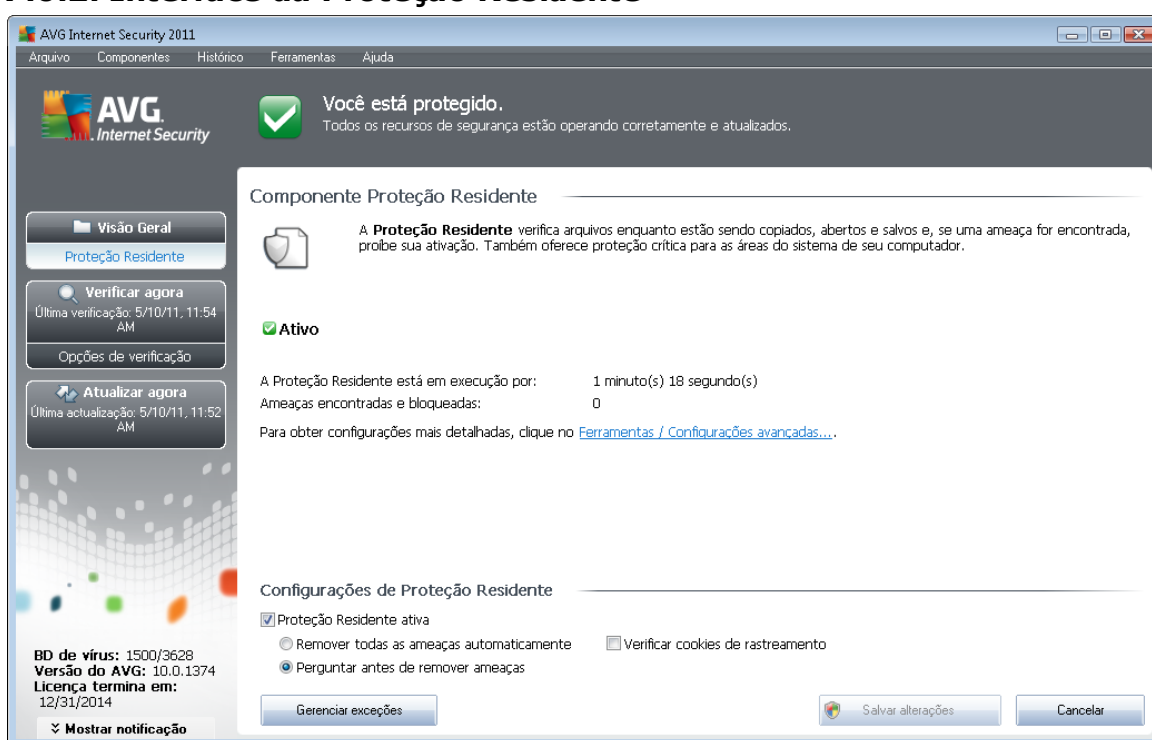
- Verificar tipos específicos de possíveis ameaças
- Verificar mídia removível (*disco flash etc.*)



- Verificar arquivos com extensões específicas ou sem nenhuma extensão
- Permitir exceções de verificação – especificar arquivos ou pastas que nunca devem ser verificados

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

7.6.2. Interface da Proteção Residente



Além de uma visão geral da funcionalidade **Proteção Residente** e das informações sobre o status do componente, a interface da **Proteção Residente** oferecerá também alguns dados estatísticos:

- **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*)

Configurações da Proteção Residente

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):

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

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

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

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

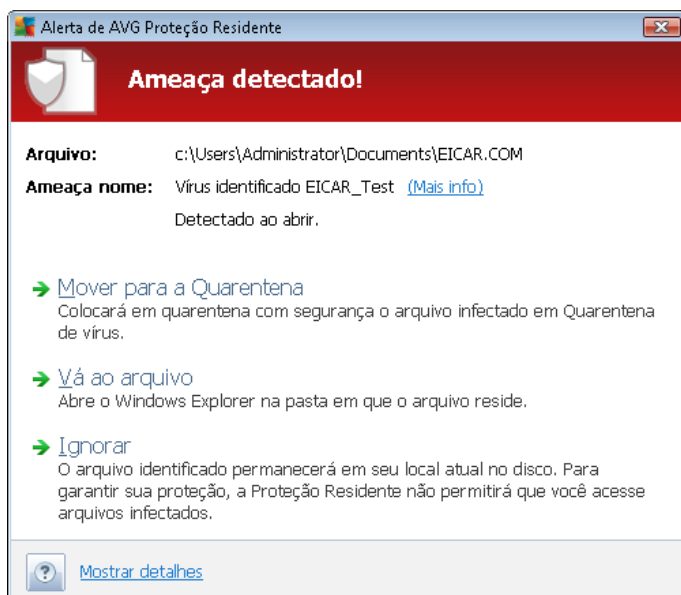
Botões de controle

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

- **Gerenciar exceções** - abre a caixa de diálogo [Proteção Residente - Itens Excluídos](#), 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 este botão para retornar à [interface do usuário do AVG](#) padrão (visão geral dos componentes)

7.6.3. 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 é alertado imediatamente por meio da seguinte caixa de diálogo:



Nessa caixa de diálogo de aviso, você encontrará dados sobre o arquivo detectado e considerado infectado (*Nome do arquivo*), o nome da infecção reconhecida (*Nome da ameaça*) e um link para a [Enciclopédia de vírus](#), na qual você pode encontrar informações detalhadas sobre a infecção detectada, se conhecida (*Mais informações*).

Além disso, você precisa decidir qual ação deve ser executada agora - as seguintes opções estão disponíveis:

Observe que, em condições específicas (o tipo de arquivo infectado e sua localização), nem todas as opções estarão sempre disponíveis!

- **Remover ameaça como Usuário avançado** – marque a caixa se supor que pode não ter direitos suficientes para remover a ameaça como um usuário comum. Usuários avançados possuem direitos de acesso amplos e se a ameaça estiver localizada em uma certa pasta do sistema, você pode precisar usar essa caixa de seleção para removê-la com sucesso.
- **Reparar** - este botão será exibido apenas se a infecção detectada puder ser reparada. Em seguida, ela é removida do arquivo e restaura o estado original do arquivo. Se o próprio arquivo for um vírus, use esta função para excluí-lo (*por exemplo, removido para a [Quarentena](#)*)
- **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!

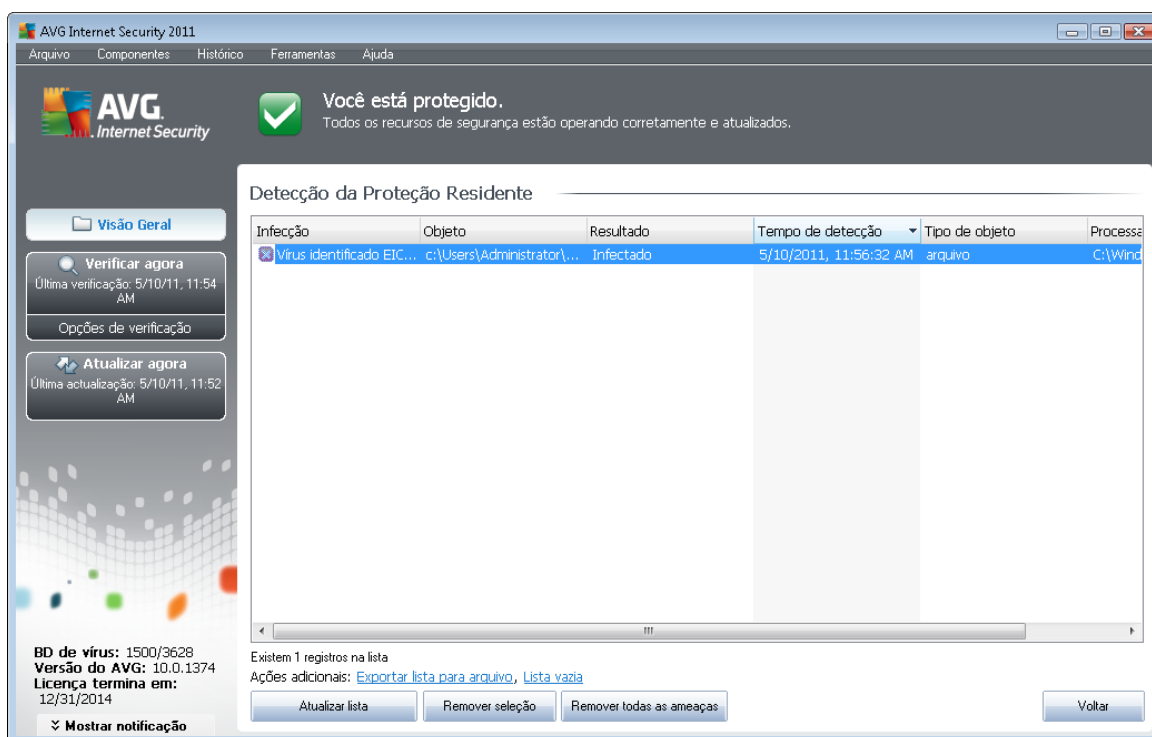
Nota: Pode acontecer do tamanho do objeto detectado exceder o limite de espaço livre na Quarentena de Vírus. Nesse caso, uma mensagem de aviso será exibida informando sobre o problema enquanto você tenta mover o objeto infectado para a Quarentena de Vírus. No entanto, o tamanho da Quarentena de Vírus pode ser editado. Ele é definido como uma porcentagem ajustável



do tamanho real do disco rígido. Para aumentar o tamanho da Quarentena de Vírus, vá para a caixa de diálogo [Quarentena de vírus](#) dentro de [Configurações avançadas do AVG](#), na opção "Limitar o tamanho da Quarentena de Vírus".

Na seção inferior da caixa de diálogo, você encontrará o link **Mostrar detalhes** - clique nele para abrir uma janela popup com informações detalhadas sobre o processo em execução enquanto a infecção foi detectada e a identificação do processo.

A visão geral completa de todas as ameaças detectadas pela [Proteção Residente](#) está disponível na caixa de diálogo **Deteção da Proteção Residente**, acessível por meio da opção de menu do sistema [Histórico/deteção da Proteção Residente](#):



A **deteção 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)*.

7.7. Family Safety

A **Proteção AVG para a Família** ajuda a proteger seus filhos contra conteúdo de mídia, pesquisas on-line e sites inapropriados, além de enviar relatórios sobre as atividades que eles realizam on-line. Você pode definir o nível apropriado de proteção para cada um de seus filhos e monitorá-los individualmente por meio de logins exclusivos.

O componente é ativado somente quando o produto **Proteção AVG para a Família** é instalado em sua máquina. Se você não tiver o produto **Proteção AVG para a Família** instalado, clique no ícone correspondente na interface de usuário do **AVG Internet Security 2011** e você será redirecionado ao site do produto, onde poderá encontrar todos os detalhes necessários.

7.8. AVG LiveKive

O **AVG LiveKive** faz backup automático de todos os arquivos, fotos e músicas em um local seguro, permitindo que você os compartilhe com a família e amigos e os acesse de qualquer dispositivo habilitado da web, incluindo dispositivos iPhones e Android.

O componente é ativado somente quando o produto **AVG LiveKive** for instalado em sua máquina. Se você não tiver o produto **AVG LiveKive** instalado, clique no ícone correspondente na interface de usuário do **AVG Internet Security 2011** e será então redirecionado ao site do produto, onde poderá encontrar todos os detalhes necessários.

7.9. Verificador de E-mail

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

7.9.1. Princípios do Verificador de E-mail

Verificador de E-mail Pessoal verifica e-mails de entrada/saída automaticamente. É possível usá-lo com clientes de email que não têm seu próprio plugin no AVG (*mas pode também ser usado para verificar mensagens de email de clientes de email com os quais o AVG é compatível com um plugin específico, por exemplo, Microsoft Outlook e The Bat*). Ele é usado principalmente com aplicativos de email como Outlook Express, Mozilla, Incredimail etc.



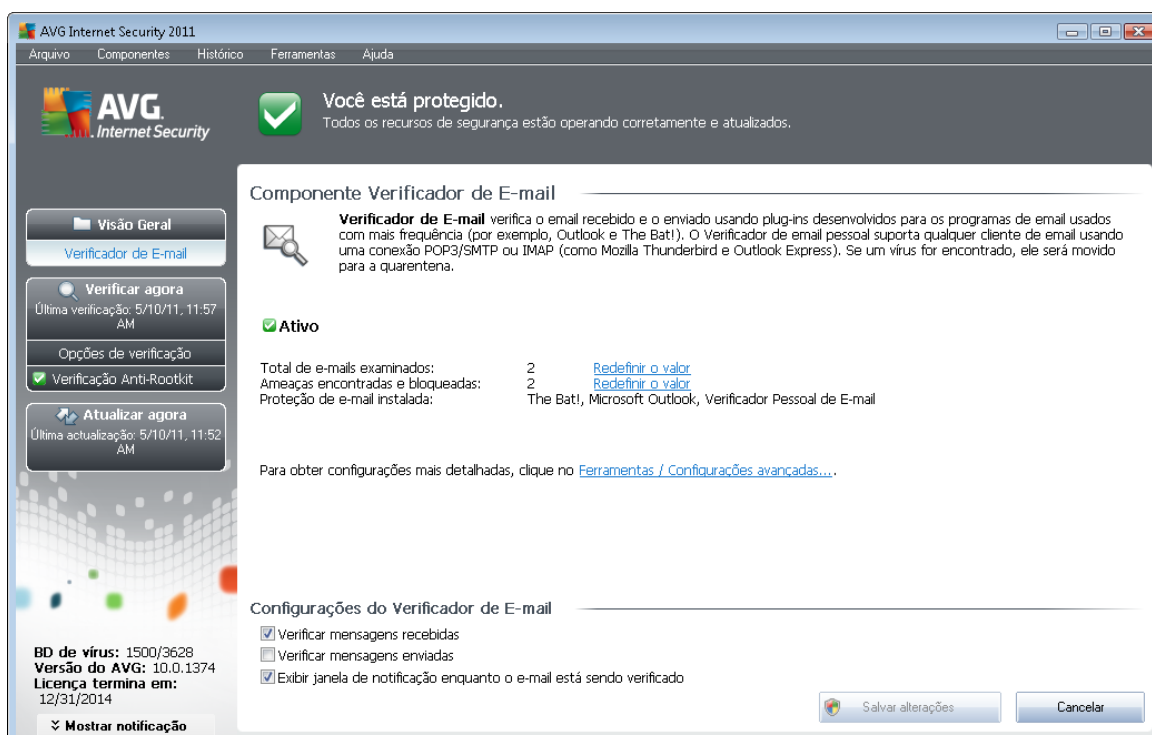
Durante a [instalação](#) do AVG, existem servidores automáticos criados para controle de e-mails: um para verificar e-mails de entrada e o segundo para verificar e-mails de saída. Utilizando esses dois servidores, os e-mails são automaticamente verificados nas portas 110 e 25 (*portas padrão para o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

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

- **E-mails de entrada:** ao receber uma mensagem do servidor, o componente **Verificador de e-mail** a testa em busca de vírus, remove anexos infectados e adiciona uma certificação. Quando detectados, os vírus são movidos para a [Quarentena de Vírus](#) imediatamente. Então a mensagem é passada para o cliente de e-mail.
- **E-mails de saída:** a mensagem é enviada a partir do cliente de e-mail para o Verificador de e-mail; ele testa essa mensagem e seus anexos em busca de vírus e, em seguida, envia a mensagem ao servidor SMTP (a *verificação de e-mails de saída está desativada por padrão e pode ser configurada manualmente*).

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

7.9.2. Interface do Verificador de E-mail



Na caixa de diálogo do componente **Verificador de E-mail**, você poderá encontrar um texto curto descrevendo a funcionalidade do componente, informações sobre seu status atual e as seguintes estatísticas:

- **Total de e-mails verificados**- quantas mensagens de e-mail foram verificadas desde que foi lançado o **Verificador de E-mail** mais recente (se necessário, este valor pode ser



redefinido; para fins de estatística, por exemplo - Redefinir valor)

- **Ameaças encontradas e bloqueadas** - fornece o número de infecções detectadas nas mensagens de e-mail desde que o **Verificador de E-mail** foi iniciado pela última vez.
- **Proteção de e-mail instalada** - informações sobre um plug-in de proteção de e-mail específico referente ao seu cliente de e-mail padrão instalado.

Configurações do Verificador de E-mail

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

- **Verificar mensagens de entrada** - marque esse item para especificar que todos os e-mails enviados à sua conta devem ser verificados em busca de vírus. Esse item está ativado por padrão e não convém alterar essa configuração!
- **Verificar mensagens de saída** - marque o item para confirmar a verificação de vírus em todos os e-mails enviados a partir da sua conta. Esse item está desativado por padrão.
- **Exibir janela de notificação enquanto o e-mail for verificado** – marque o item para confirmar que deseja ser informado através da caixa de diálogo de notificação exibida sobre o ícone AVG na bandeja do sistema durante a verificação de seu e-mail através do componente [Verificador de E-mail](#). Esse item está ativado por padrão e não convém alterar essa configuração!

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

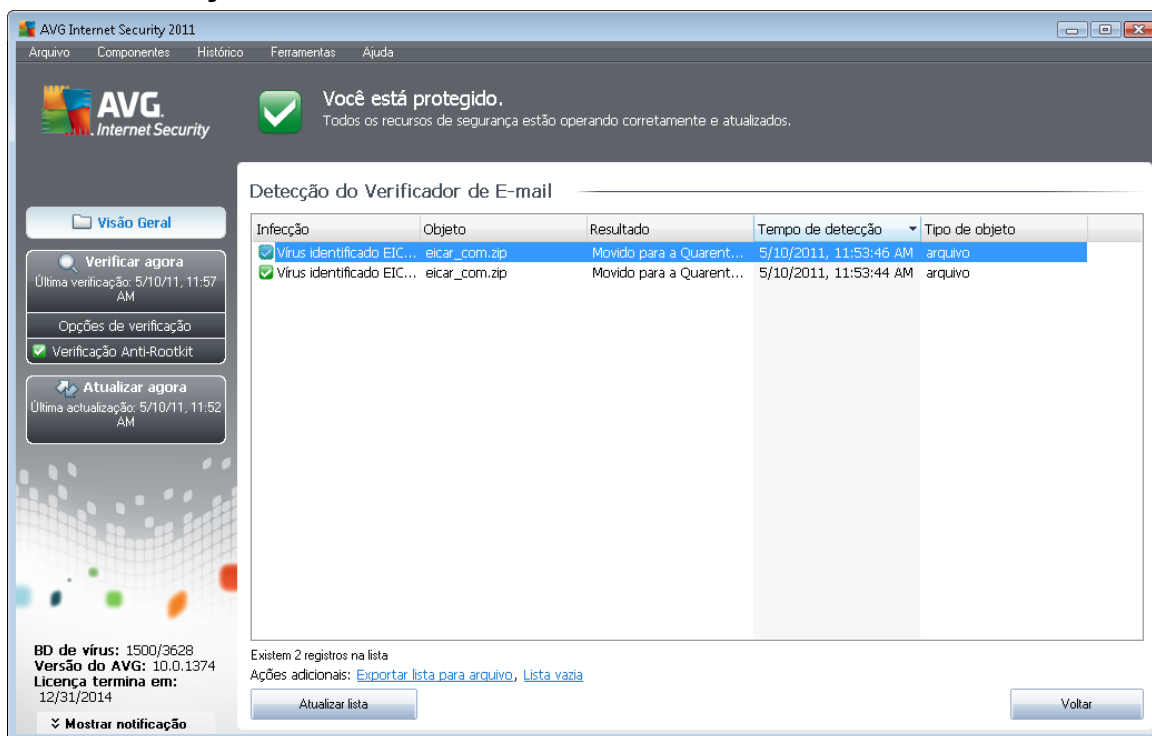
Nota: o fornecedor do software configurou todos os componentes do AVG para proporcionar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar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

Botões de controle

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

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

7.9.3. Detecção de Verificador de E-mail



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

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

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

Botões de controle

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



- **Atualizar listas** - atualiza a lista de ameaças detectadas
- **Voltar** - leva você de volta à caixa de diálogo exibida anteriormente

7.10. Gerenciador de atualizações

7.10.1. Princípios do Gerenciador de Atualizações

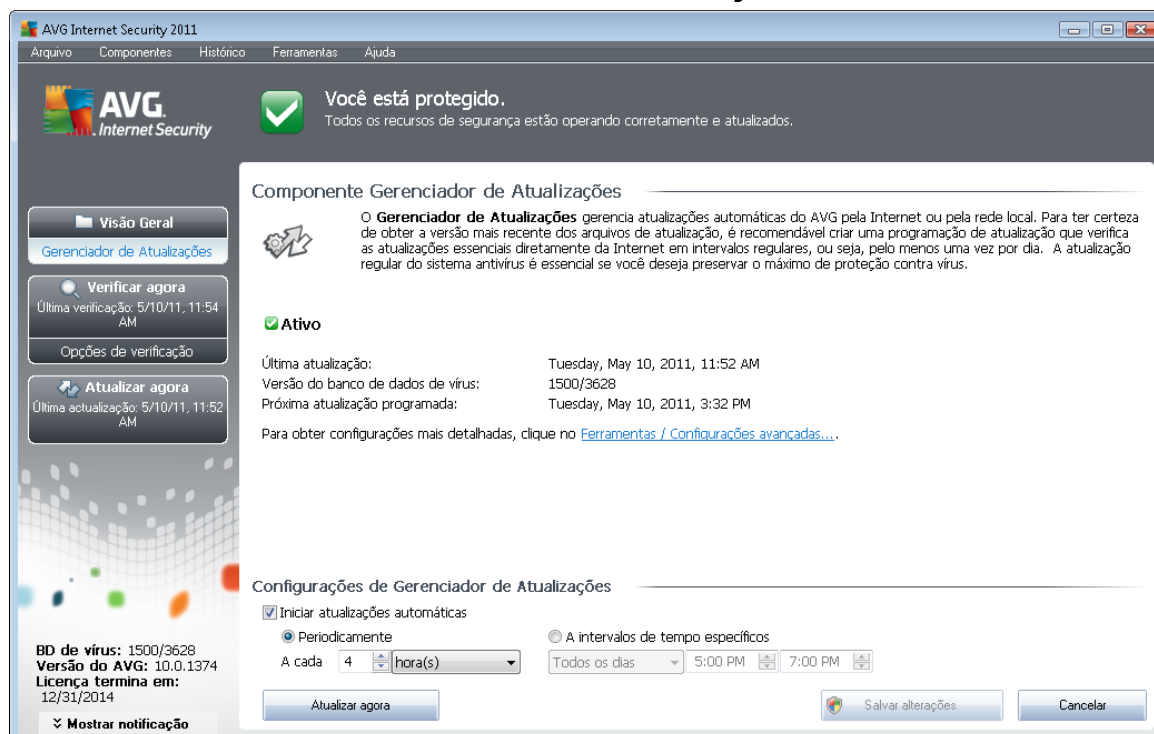
Nenhum software de segurança pode garantir proteção real de vários tipos de ameaças se não for regularmente atualizado! Os criadores de vírus estão sempre em busca de novas brechas que possam explorar em softwares e sistemas operacionais. Novos vírus, novos malwares, novos ataques de hackers surgem diariamente.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

É fundamental atualizar o AVG regularmente!

O **Gerenciador de atualizações** 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.

Observação: consulte o capítulo [Atualizações do AVG](#) para obter mais informações sobre os tipos e níveis de atualização!

7.10.2. Interface do Gerenciador de atualizações





A interface do **Gerenciador de Atualizações** exibe informações sobre a funcionalidade do componente e seu status atual e fornece os dados estatísticos relevantes:

- **Atualização mais recente** - especifica a data e a hora da última atualização do banco de dados
- **Versão do banco de dados de vírus** - define o número da versão do banco de dados de vírus atualmente instalada. Esse número aumenta a cada atualização da base de vírus
- **Próxima atualização programada** - especifica a data e a hora da próxima atualização do banco de dados

Configurações de Gerenciador de Atualizações

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:

- o **Periodicamente** - define o intervalo de tempo
- o **Em um intervalo de tempo específico** - defina a hora do dia exata que a atualização deve ser feita

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

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

Botões de controle

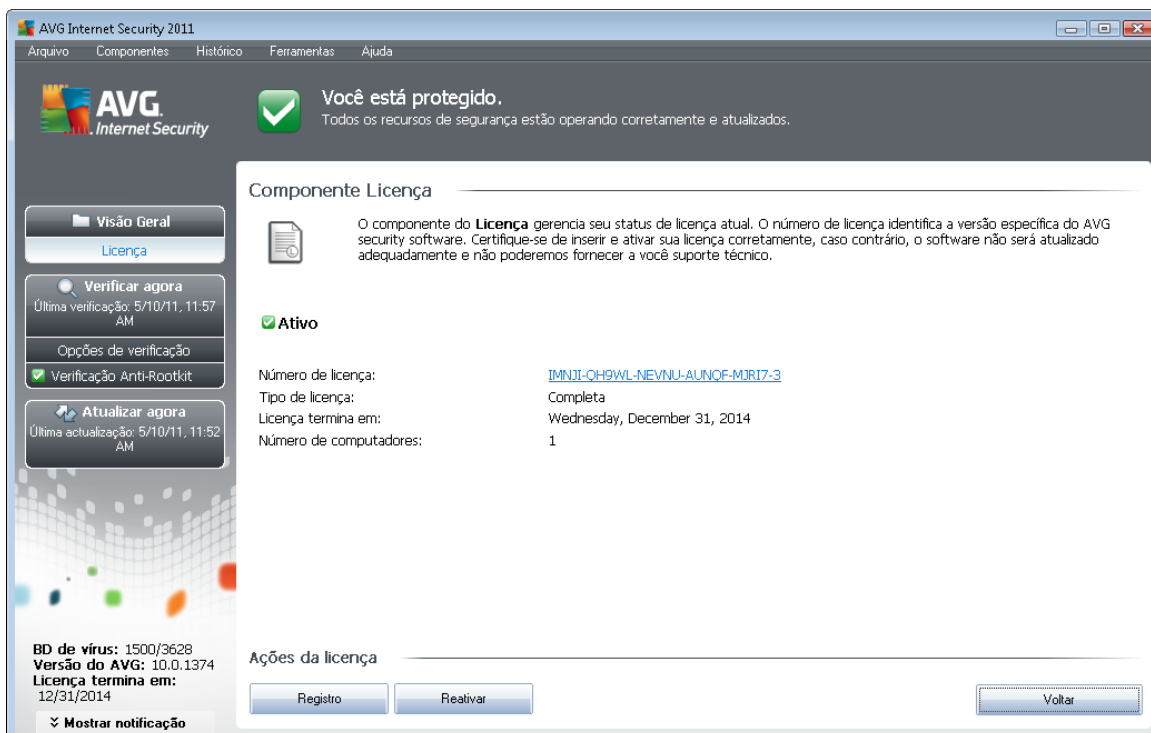
Os botões de controle disponíveis na interface do **Gerenciador de Atualizações** são os seguintes:

- **Atualizar agora** - inicializa uma [atualização imediata](#) sob demanda.
- **Salvar alterações** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo



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

7.11. Licença



Na interface do componente **Licença**, você encontrará um texto curto descrevendo a funcionalidade do componente, informações sobre seu status atual e as seguintes informações:

- **Número da licença** - apresenta a forma reduzida do número da licença (*por motivos de segurança, os últimos quatro símbolos estão faltando*). 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 Internet Security 2011** depois dessa data, terá que renovar a licença. A renovação da licença pode ser realizada online, no [site da AVG](#).
- **Número de computadores** - a quantidade de estações de trabalho em que você tem permissão para instalar o **AVG Internet Security 2011**.

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.

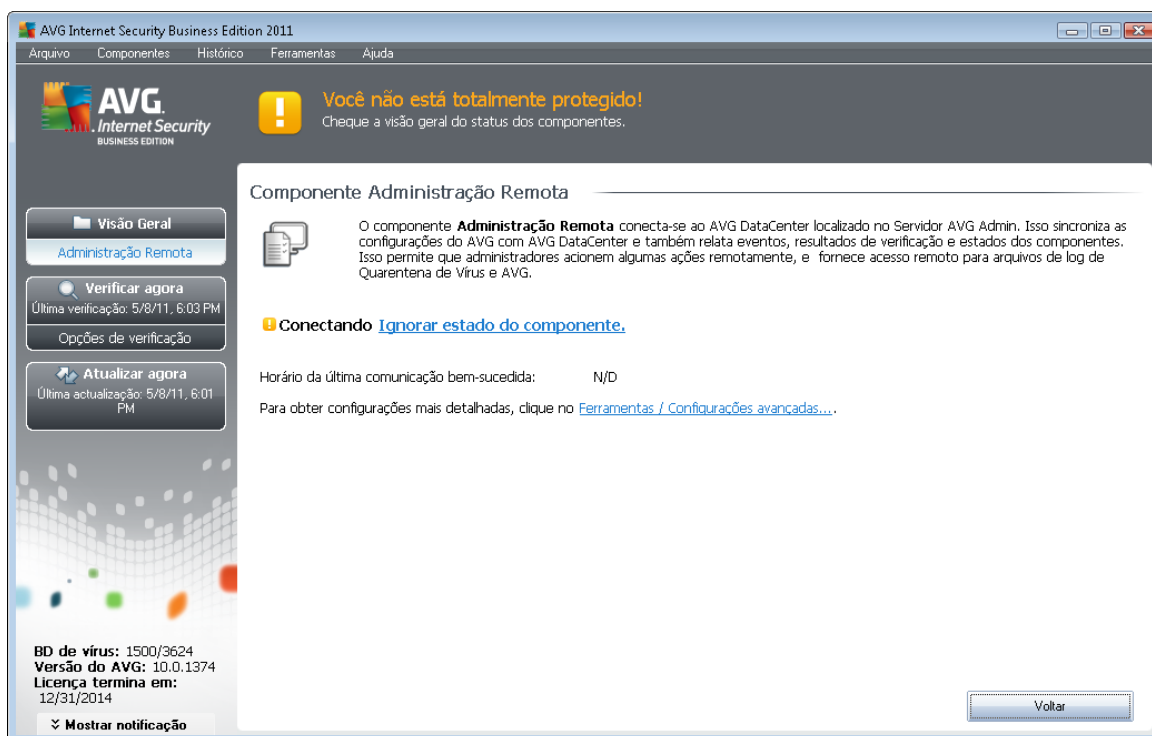


- **Reativar** - abre a caixa de diálogo **Ativar AVG** com os dados inseridos na caixa de diálogo [Personalizar AVG](#) do [processo de instalação](#). Nessa caixa de diálogo é possível inserir o número da licença para substituir o número de vendas (o número com o qual você instalou o AVG) ou para substituir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

Observação: Se estiver utilizando a versão do AVG Internet Security 2011, os botões aparecem como **Comprar agora** e **Ativar**, permitindo que você compre a versão completa do programa imediatamente. Para AVG Internet Security 2011 instalado com um número de vendas, os botões são exibidos como **Registrar** e **Ativar**.

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

7.12. Administração Remota



O componente **Administração Remota** aparece apenas na interface do usuário do **AVG Internet Security 2011** se o Business Edition do seu produto foi instalado (veja no componente [Licença](#)). Na caixa de diálogo **Administração Remota**, você pode encontrar informações relativas ao componente, ou seja, se ele está ativo e conectado ao servidor. Todas as configurações do componente **Administração Remota** devem ser feitas em **Configurações Avançadas/ Administração Remota**.

Para obter uma descrição detalhada das opções e da funcionalidade do componente no sistema Administração Remota do AVG, consulte a documentação específica dedicada a esse tópico exclusivamente. Esta documentação está disponível para download no [Site do AVG \(www.avg.com\)](http://www.avg.com), na seção **Centro de suporte/Download/Documentação**.



Botões de controle

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

7.13. Proteção On-line

7.13.1. Princípios da Proteção On-line

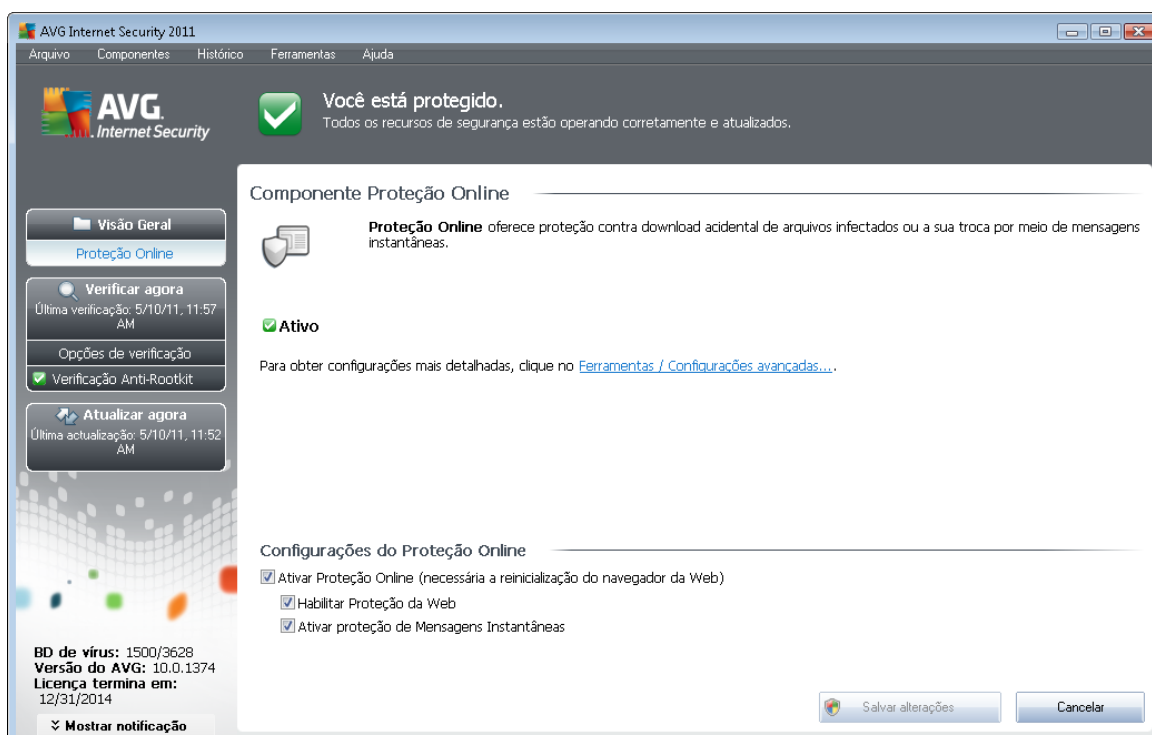
A **Proteção Online** é um tipo de proteção residente em tempo real. Ela verifica o conteúdo de páginas da Web visitadas (e possíveis arquivos incluídos nelas) mesmo antes destas serem exibidas no navegador da Web ou baixadas no computador.

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

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

7.13.2. Interface da Proteção On-line

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





Configurações da Proteção Online

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

- **Ativar Proteção da Web** - essa opção confirma que **Proteção Online** deve realizar a verificação do conteúdo do site.
- **Ativar a Proteção de Mensagens Instantâneas** - marque este item se quiser que a **Proteção On-line** verifique se a comunicação de mensagens instantâneas (*por exemplo, ICQ, MSN Messenger, ...*) está sem vírus.

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

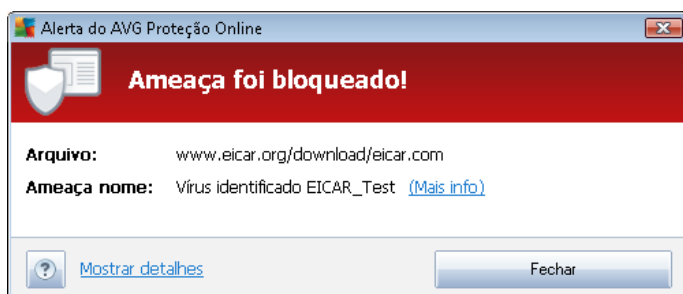
Botões de controle

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

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

7.13.3. Detecção da Proteção On-line

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

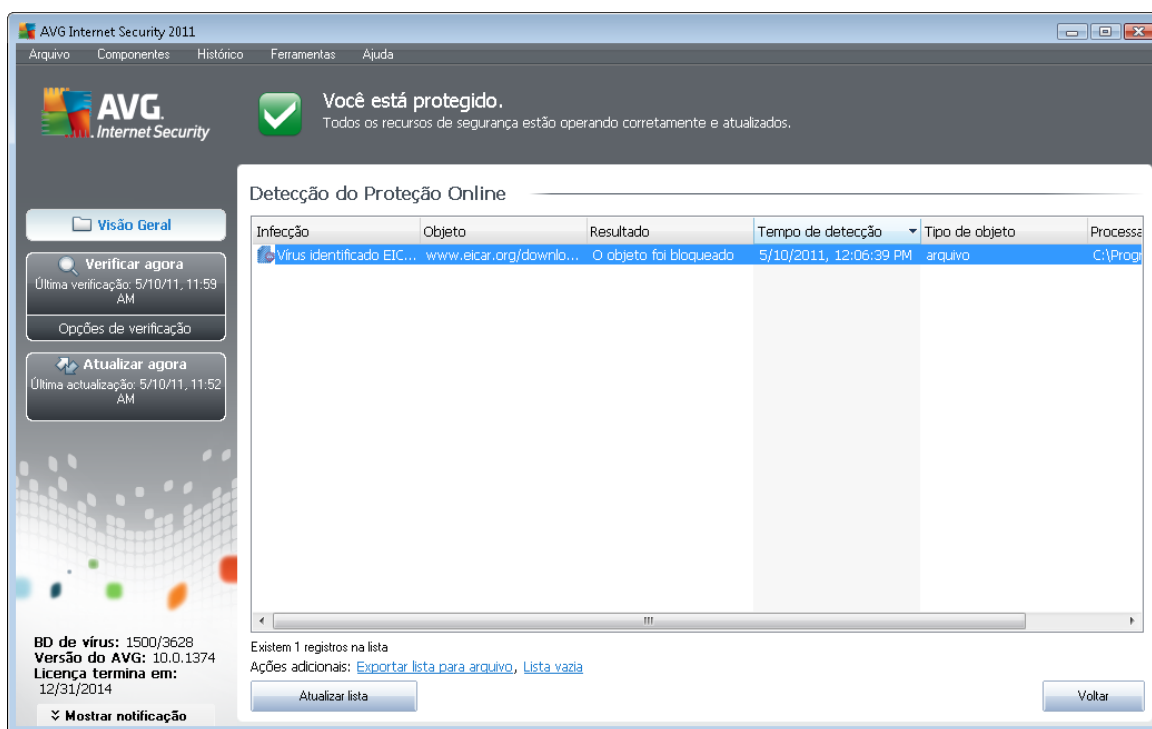




Nessa caixa de diálogo de aviso, você encontrará dados sobre o arquivo detectado e considerado infectado (*Nome do arquivo*), o nome da infecção reconhecida (*Nome da ameaça*) e um link para a [Enciclopédia de vírus](#), na qual você pode encontrar informações detalhadas sobre a infecção detectada (se conhecida). Essa caixa de diálogo fornece os seguintes botões:

- **Mostrar detalhes** - clique no botão **Mostrar detalhes** para abrir uma nova janela popup, na qual você pode encontrar informações sobre o processo em execução enquanto a infecção foi detectada e a identificação do processo.
- **Fechar** - clique no botão para fechar a caixa de diálogo de aviso.

A página da Web suspeita não será aberta, e a detecção da ameaça será registrada na lista de **Deteções da Proteção Online** - essa visão geral de ameaças detectadas está acessível no menu do sistema [Histórico/deteções da Proteção Online](#).



Em cada objeto detectado, são fornecidas as seguintes informações:

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



permitir que fosse detectado

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

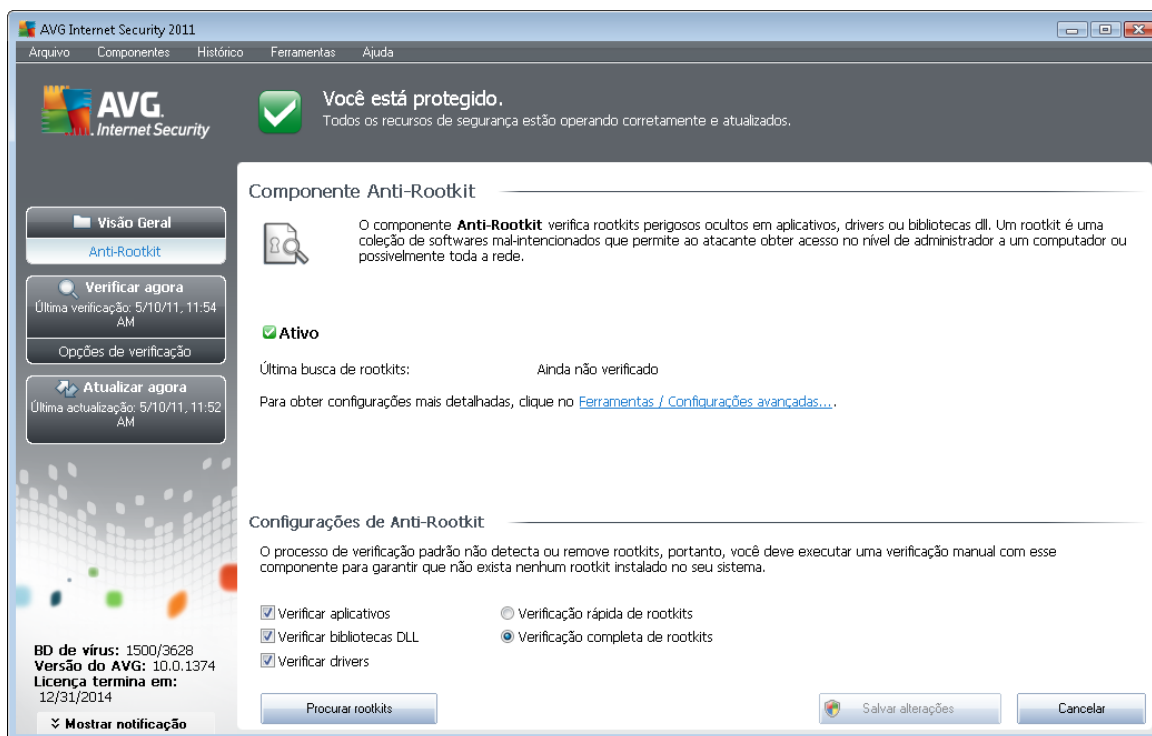
7.14. Anti-Rootkit

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

7.14.1. Princípios do Anti-Rootkit

O **AVG Anti-Rootkit** é uma ferramenta especializada para detectar e remover efetivamente rootkits perigosos, isto é, programas e tecnologias que podem camuflar a presença de software malicioso no seu computador. O **AVG Anti-Rootkit** é capaz de detectar rootkits com base em um conjunto de regras predefinidas. Observe que são detectados todos os rootkits (*não apenas os infectados*). Se o **AVG Anti-Rootkit** encontrar um rootkit, isso não quer dizer necessariamente que esse rootkit está infectado. Algumas vezes os rootkits são usados como drivers ou fazem parte de aplicativos corretos.

7.14.2. Interface do Anti-Rootkit



A interface do usuário do **Anti-Rootkit** fornece uma breve descrição da funcionalidade do componente, informa o status atual do componente e também traz informações sobre a última vez que o teste do **Anti-Rootkit** foi iniciado (**Última pesquisa do rootkit**). A caixa de diálogo **Anti-Rootkit** apresenta também o link [Ferramentas/Configurações Avançadas](#). Use o link para ser redirecionado ao ambiente de configuração avançada do componente **Anti-Rootkit**.

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.

Configurações de Anti-Rootkit

Na parte inferior da caixa de diálogo, você localizará a seção **Configurações do Anti-Rootkit**, onde é possível configurar funções elementares da verificação de presença do rootkit. Primeiro, marque as respectivas caixas de seleção para especificar objetos que devem ser verificados:

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

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



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

Botões de controle

- **Pesquisar rootkits** - como a verificação do rootkit não é parte implícita de [Verificar todo o computador](#), você pode executar a verificação do rootkit diretamente da interface do **Anti-Rootkit** usando esse botão.
- **Salvar alterações** - pressione este botão para salvar todas as alterações feitas nessa interface e voltar para a [interface do usuário do AVG padrão](#) (*visão geral dos componentes*)
- **Cancelar** - pressione este botão para voltar para a [interface do usuário AVG padrão](#) (*visão geral dos componentes*) sem salvar as alterações feitas

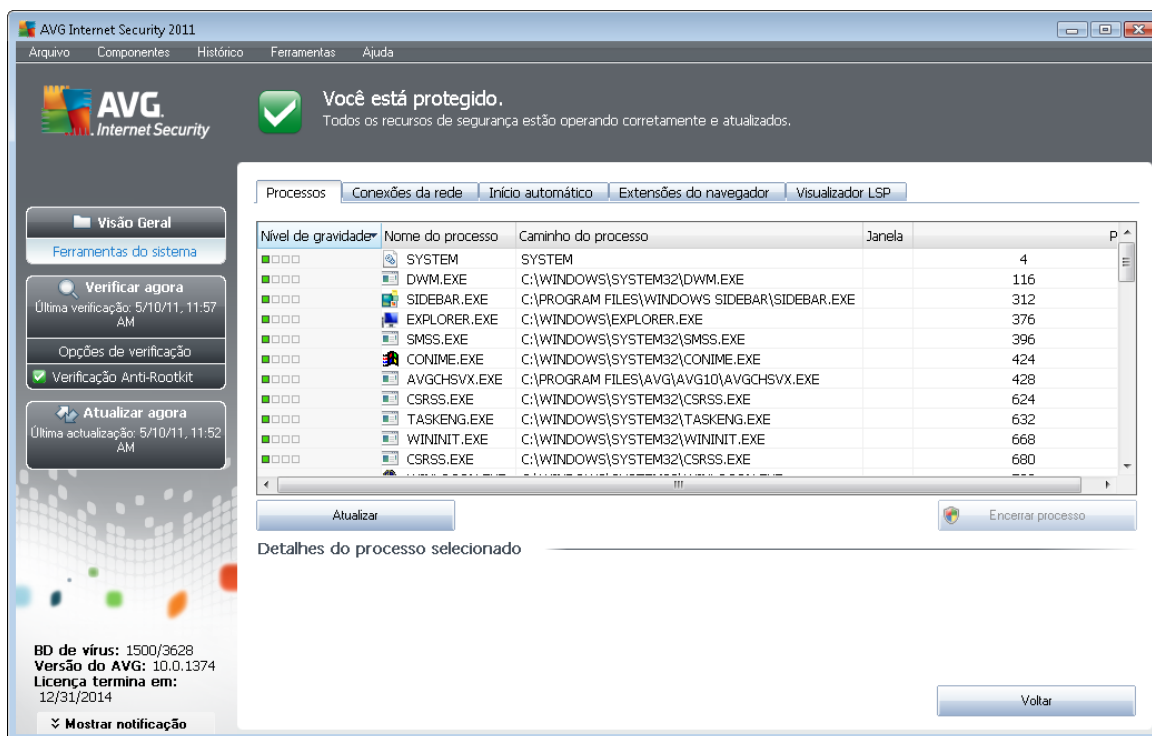
7.15. Ferramentas do Sistema

Ferramentas do Sistema refere-se a ferramentas que oferecem um resumo detalhado do sistema operacional e do ambiente do AVG Internet Security 2011. O componente exibe uma visão geral de:

- [Processos](#) - lista de processos (*isto é, aplicativos em execução*) que estão ativos no momento no computador
- [Conexões de rede](#) - lista de conexões ativas no momento
- [Inicialização automática](#) - lista todos os aplicativos que são executados durante a inicialização do sistema Windows
- [Extensões do navegador](#) - lista de plug-ins (*ou seja, aplicativos*) instalados no navegador da Internet
- [Visualizador de LSPs](#) - lista de provedores de serviços em camadas (LSP)

As visões gerais específicas também podem ser editadas, mas isso é recomendado somente a usuários bem experientes!

7.15.1. Processos



A caixa de diálogo **Processos** contém uma lista de processos (isto é, aplicativos em execução) que estão ativos no momento no computador. A lista é dividida em várias colunas:

- **Nível de segurança** – identificação gráfica da respectiva severidade do processo em uma escala de quatro níveis, variando do menos importante (■□□□) até o mais crítico (■■■■)
- **Nome do processo** - nome do processo em execução
- **Caminho do processo** - indica um caminho físico para o processo em execução
- **Janela** - se aplicável, indica o nome da janela do aplicativo
- **PID** - o número de identificação do processo é um identificador exclusivo do processo interno do Windows

Botões de controle

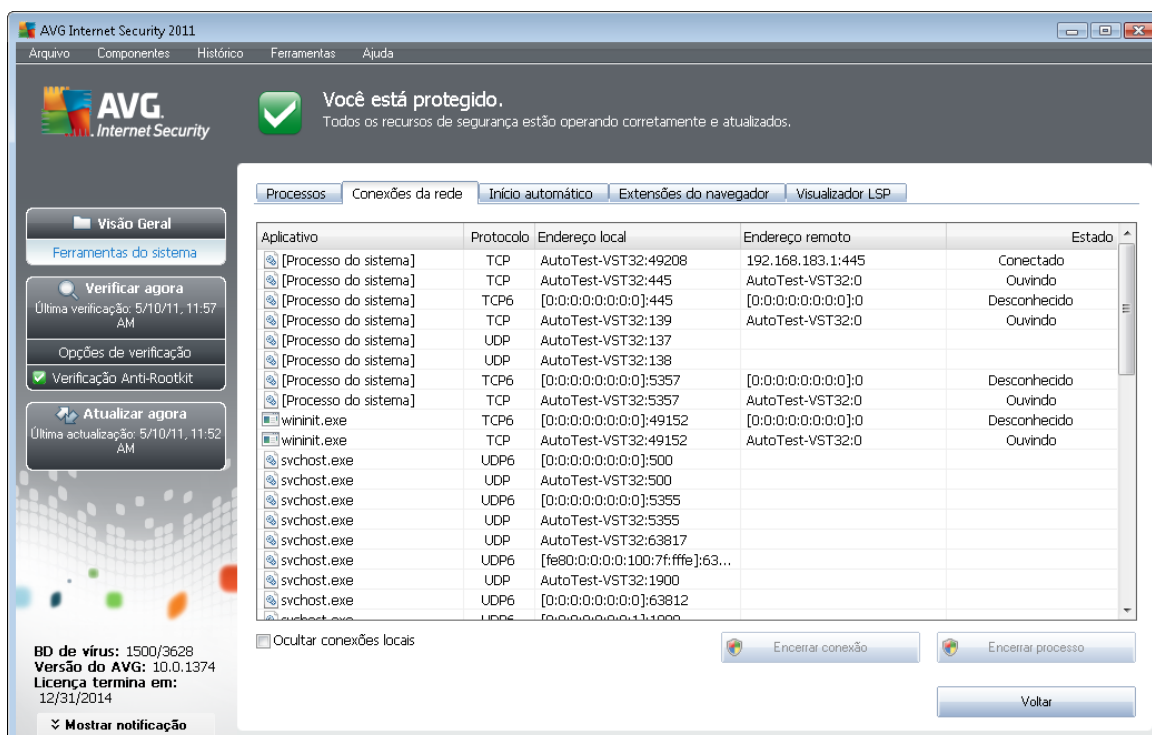
Os botões de controle disponíveis na interface de **Ferramentas do sistema** são os seguintes:

- **Atualizar** - atualiza a lista de processos de acordo com o status atual
- **Finalizar processo** - você pode selecionar um ou mais aplicativos e depois finalizá-los pressionando esse botão. **Nós sugerimos não encerrar nenhum aplicativo, a menos que você tenha certeza absoluta de que eles representam uma ameaça real!**



- **Voltar** - leva você de volta à interface do usuário padrão [do AVG](#) (visão geral dos componentes)

7.15.2. Conexões da Rede



A caixa de diálogo **Conexões de Rede** contém uma lista das conexões ativas no momento. A lista é dividida nas seguintes colunas:

- **Aplicativo** - nome do aplicativo associado à conexão (com exceção do Windows 2000 em que as informações não estão disponíveis)
- **Protocolo** - tipo de protocolo de transmissão usado na conexão:
 - o TCP - protocolo usado junto com o protocolo de Internet (IP) para transmitir informações pela Internet
 - o UDP - alternativa para o protocolo TCP
- **Endereço local** - endereço IP do computador local e o número de porta usado
- **Endereço remoto** - endereço IP do computador remoto e o número da porta à qual está conectado. Se possível, procurará também o nome do host do computador remoto.
- **Estado** - indica o estado atual mais provável (Conectado, Servidor fechado, Escuta, Ativo fechado concluído, Passivo fechado, Ativo fechado)

Para listar apenas as conexões externas, marque a caixa de seleção **Ocultar conexões locais** na



seção inferior da caixa de diálogo, abaixo da lista.

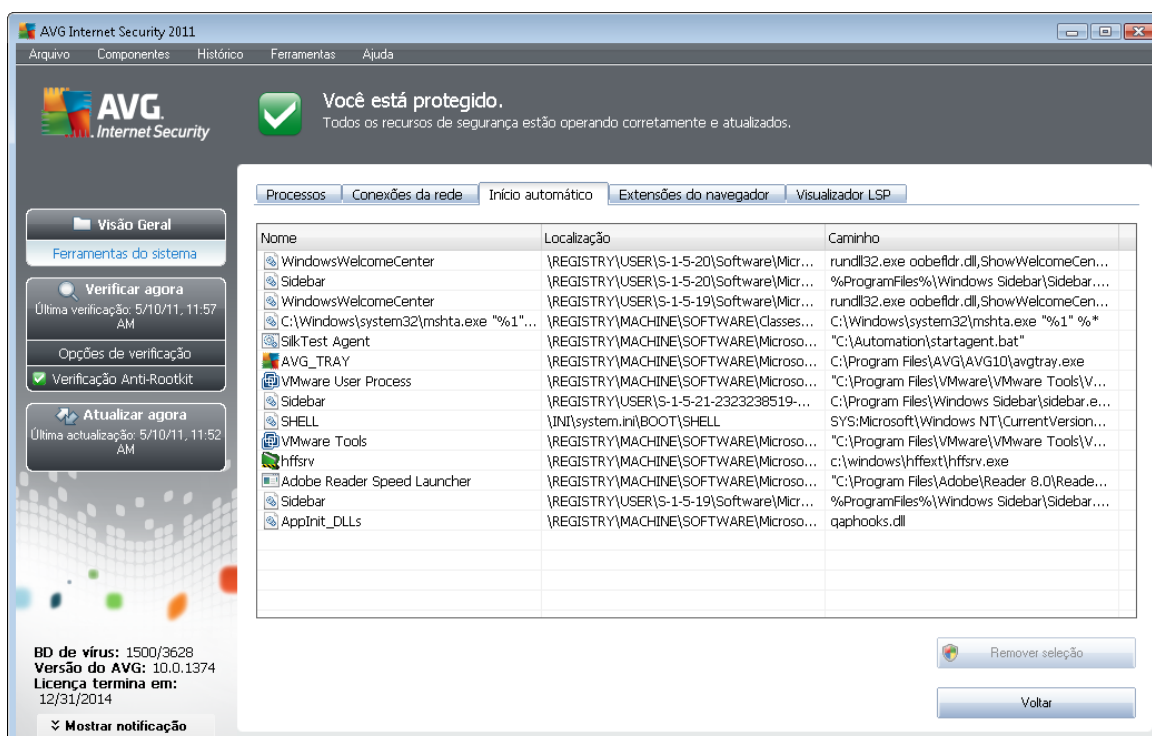
Botões de controle

Os botões de controle disponíveis são:

- **Encerrar Conexão** - fecha uma ou mais conexões selecionadas na lista
- **Terminar processo** - fecha um ou mais aplicativos associados às conexões selecionadas na lista
- **Voltar** - volta para a [interface do usuário do AVG](#) padrão (visão geral dos componentes).

Às vezes só é possível encerrar aplicativos que estejam no estado conectado no momento. Nós sugerimos não encerrar nenhuma conexão, a menos que você tenha certeza absoluta de que elas representam uma ameaça real!

7.15.3. Início automático



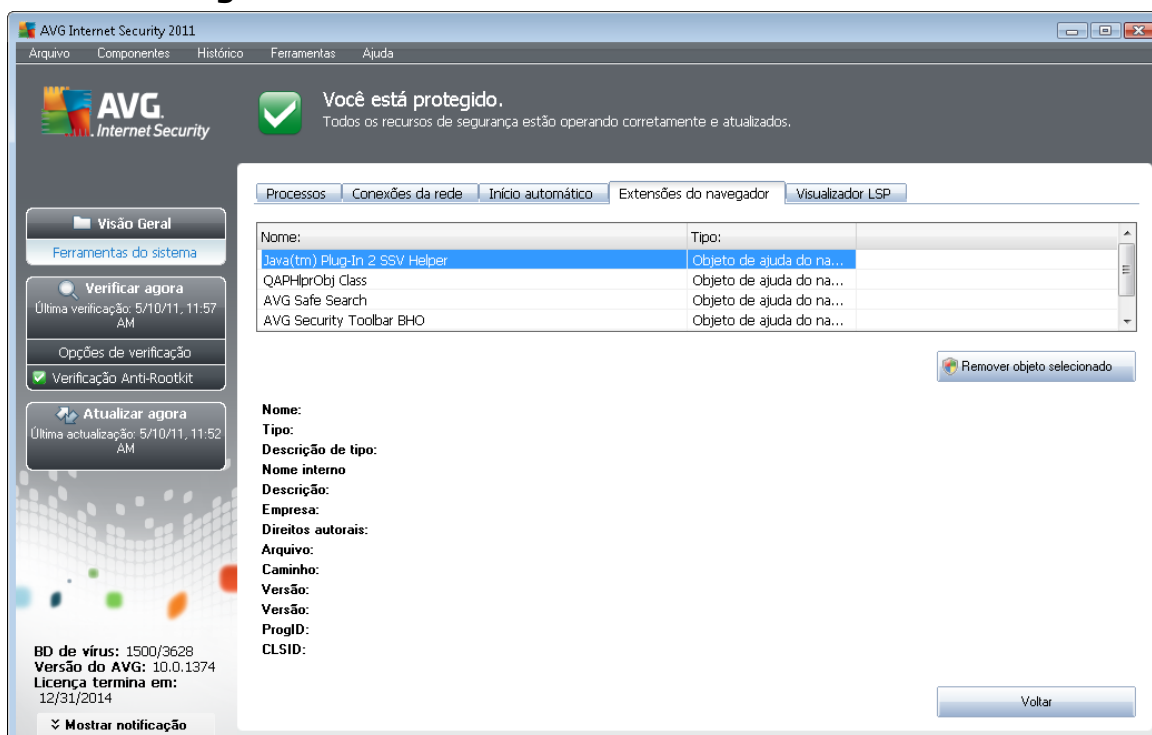
A caixa de diálogo **Inicialização automática** mostra uma lista de todos os aplicativos executados durante a inicialização do sistema Windows. Muito frequentemente, vários aplicativos malware são adicionados automaticamente na entrada do registro de inicialização.

Você pode excluir uma ou mais entradas selecionando-as e pressionando o botão **Remover selecionados**. O botão **Voltar** leva você de volta à interface do usuário do AVG padrão (visão geral dos componentes).



Nós sugerimos não excluir nenhum aplicativo da lista, a menos que você tenha certeza absoluta de que eles representam uma ameaça real!

7.15.4. Navegador de Extensões



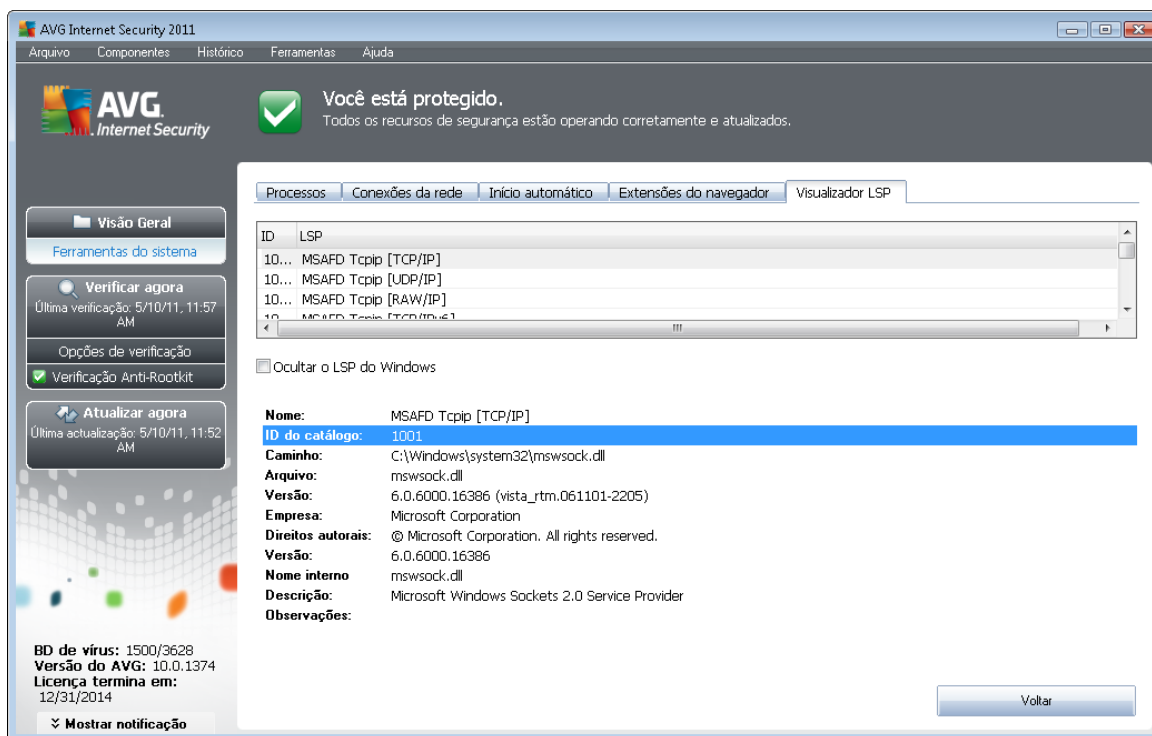
A caixa de diálogo **Extensões do Navegador** contém uma lista de plug-ins (como aplicativos) instalados no navegador da Internet. Esta lista pode conter os plug-ins normais, assim como programas malware potenciais. Clique em um objeto na lista para obter informações detalhadas sobre o plug-in selecionado que será exibido na seção inferior da caixa de diálogo.

Botões de controle

Os botões de controle disponíveis na guia **Extensão do navegador** são:

- **Remover objeto selecionado** - remove o plug-in atualmente realçado na lista. **Nós sugerimos não excluir nenhum plug-in da lista, a menos que você tenha certeza absoluta de que eles representam uma ameaça real!**
- **Voltar** - leva você de volta à [interface do usuário do AVG](#) padrão (visão geral dos componentes)

7.15.5. Visualizador LSP



A caixa de diálogo **Visualizador de LSP** mostra uma lista de provedores de serviços em camadas (LSP, Layered Service Providers).

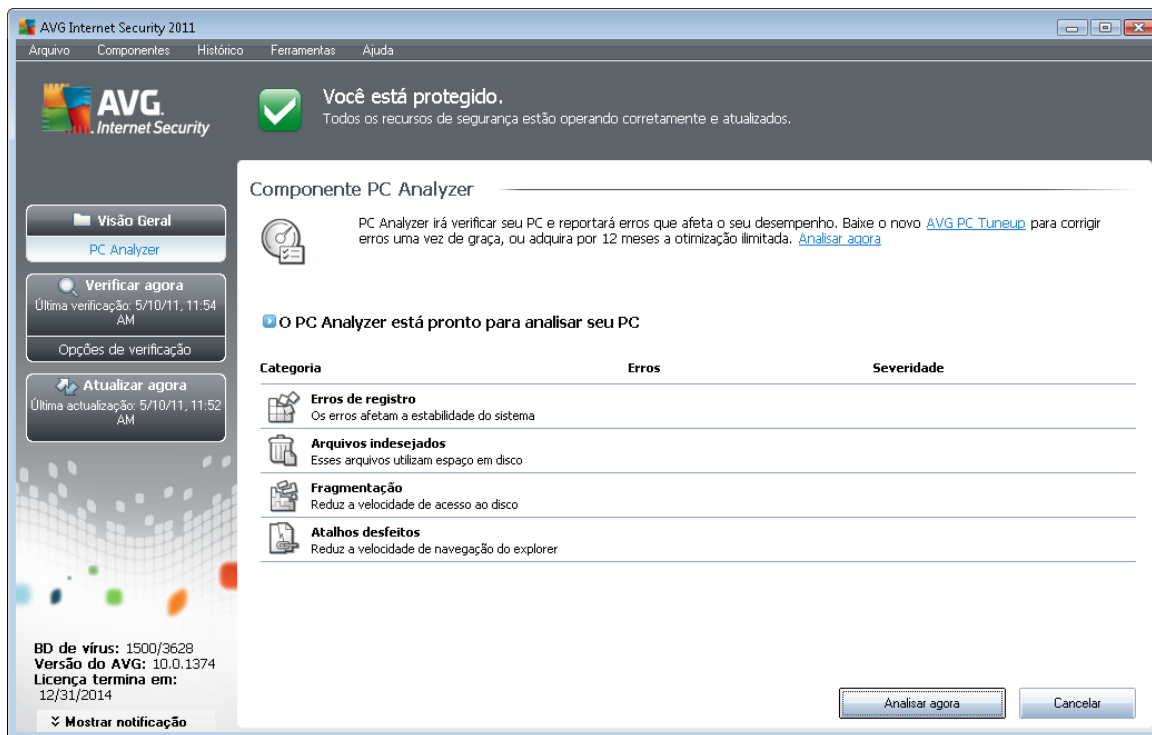
Um **LSP** é um driver de sistema vinculado aos serviços de rede do sistema operacional Windows. Ele tem acesso a todos os dados enviados e recebidos no computador e pode modificar esses dados. Alguns LSPs são necessários para permitir que o Windows conecte você a outros computadores, inclusive à Internet. No entanto, certos aplicativos malware também podem se instalar como LSPs, tendo acesso a todos os dados transmitidos pelo seu computador. Portanto, essa análise pode ajudá-lo a verificar todas as ameaças de LSP possíveis.

Em determinadas circunstâncias, também é possível reparar LSPs danificados (*por exemplo, quando o arquivo foi removido mas as entradas de registro permanecem intocadas*). Um novo botão para corrigir o problema é exibido quando um LSP reparável é descoberto.

Para incluir o LSP do Windows na lista, desmarque a caixa de seleção **Ocultar LSP do Windows**. O botão **Voltar** leva você de volta à interface do usuário do AVG padrão (visão geral dos componentes).

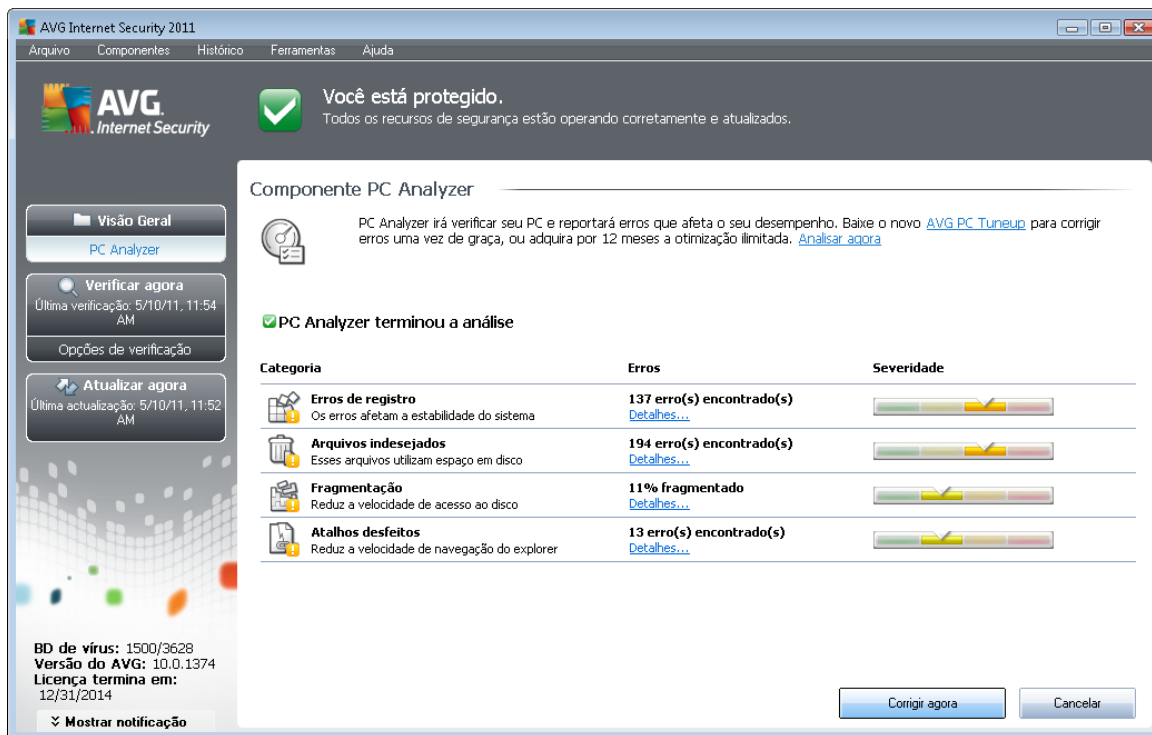
7.16. PC Analyzer

O componente **PC Analyzer** verifica o seu computador quanto a problemas de sistema e apresenta uma visão geral transparente do que pode estar afetando o desempenho geral do computador. Na interface do usuário do componente, é possível ver um gráfico dividido em quatro linhas relacionadas às respectivas categorias:



- **Erros do Registro** exibirá o número de erros no Registro do Windows. Como corrigir o Registro requer conhecimento avançado, não é recomendável que você tente corrigi-lo sozinho.
- **Arquivos indesejados** exibirá o número de arquivos que muito provavelmente podem ser gerados externamente. Geralmente, há muitos tipos de arquivos temporários e arquivos na Lixeira.
- **Fragmentação** calculará a porcentagem de disco rígido que está fragmentada, ou seja, usada por muito tempo para que a maioria dos arquivos agora seja dividida em partes diferentes do disco físico. Você pode usar uma ferramenta de desfragmentação para corrigir isso.
- **Atalhos desfeitos** notificará você sobre atalhos que não funcionam mais, que levam a locais não existentes, etc.

Para iniciar a análise do seu sistema, pressione o botão **Analisar agora**. Você poderá acompanhar o progresso da análise e os seus resultados diretamente no gráfico:



A visão geral de resultados apresenta o número de problemas de sistema detectados (**Erros**) divididos de acordo com as respectivas categorias testadas. Os resultados da análise serão também exibidos graficamente em um eixo na coluna **Gravidade**.

Botões de controle

- **Analisar agora** (é exibido antes do início da análise)- pressione este botão para iniciar a análise imediata do seu computador
- **Corrigir agora** (exibido quando a análise é finalizada) - pressione o botão para acessar o site da AVG (<http://www.avg.com/>) na página que fornece informações detalhadas e atualizadas relacionadas ao componente **PC Analyzer**
- **Cancelar** - pressione este botão para interromper a análise em execução ou retornar à [interface do usuário do AVG](#) padrão (visão geral dos componentes) quando a análise estiver concluída

7.17. ID Protection

O **AVG Identity Protection** é um produto anti-malware cujo objetivo é evitar que ladrões de identidade roubem suas senhas, informações de contas bancárias, números de cartões de crédito e outros dados pessoais digitais de valor a partir de todos os tipos de softwares mal-intencionados (*malware*) que visam ao seu PC. Ele garante que todos os programas em execução no seu PC estejam funcionando corretamente. O **AVG Identity Protection** aponta e bloqueia comportamento suspeito em base contínua, além de proteger seu computador de todos os novos malware.

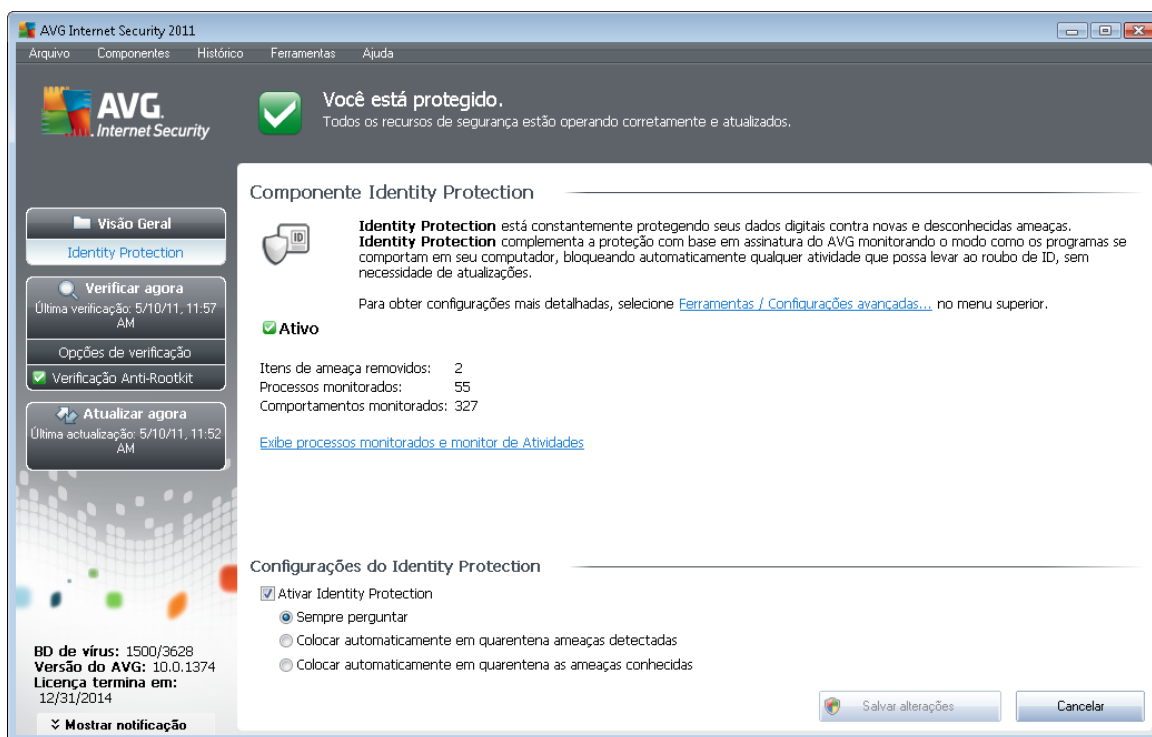


7.17.1. Princípios do ID Protection

O **AVG Identity Protection** é um componente anti-malware que o protege de todos os tipos de malware (*spyware, robôs, roubo de identidade...*) usando tecnologias comportamentais e que fornece proteção imediata contra novos vírus. Como os malware se tornam cada vez mais sofisticados e vêm na forma de programas normais que podem ser abertos em seu PC, permitindo o atacante remoto roubar sua identidade, o **AVG Identity Protection** o protegerá destes novos malware com base em seu funcionamento. Trata-se de uma proteção complementar ao [AVG Anti-Virus](#), que o protege de vírus conhecidos e baseados em arquivos usando um mecanismo de assinatura e verificação.

É extremamente recomendável que você tenha os componentes [AVG Anti-Virus](#) e AVG Identity Protection, para obter proteção completa para o seu PC.

7.17.2. Interface do ID Protection



A interface do componente **Identity Protection** fornece uma breve descrição da funcionalidade básica do componente, seu status e alguns dados estatísticos:

- **Itens de malware removidos** - fornece o número de aplicativos detectados como malware e removidos
- **Processos monitorados** - número de aplicativos atualmente em execução que estão sendo monitorados pelo IDP
- **Comportamentos monitorados** - número de ações específicas em execução com os aplicativos monitorados



Abaixo, você pode encontrar o link [Exibir processos monitorados e monitor de Atividades](#), que o levará para a interface do usuário do componente [Ferramentas do sistema](#), em que é possível localizar uma visão geral detalhada de todos os processos monitorados.

Configurações do Identity Protection

Na parte inferior da caixa de diálogo, você pode encontrar a seção **Configurações do Identity Protection**, onde é possível editar alguns recursos básicos da funcionalidade do componente:

- **Ativar Identity Protection** - (ativada por padrão): marque para ativar o componente IDP e abrir opções de edição adicionais.

Em alguns casos, o **Identity Protection** pode relatar que alguns arquivos autênticos são suspeitos ou perigosos. Como o **Identity Protection** detecta ameaças com base em seu comportamento, isso normalmente ocorre quando algum programa tenta controlar as teclas, instalar outros programas ou quando um novo driver é instalado no computador. Portanto, selecione uma das opções a seguir, que especificam o comportamento do componente **Identity Protection** se ele detectar uma atividade suspeita:

- o **Sempre avisar** - se um aplicativo for detectado como malware, você deverá determinar se ele deve ou não ser bloqueado (essa opção está ativada por padrão, e convém não alterá-la, a não ser que você tenha um motivo concreto para isso)
- o **Colocar ameaças detectadas automaticamente em quarentena** - todos os aplicativos detectados como malware serão bloqueados automaticamente
- o **Colocar ameaças detectadas automaticamente em quarentena** - todos os aplicativos detectados com certeza absoluta como malware serão bloqueados

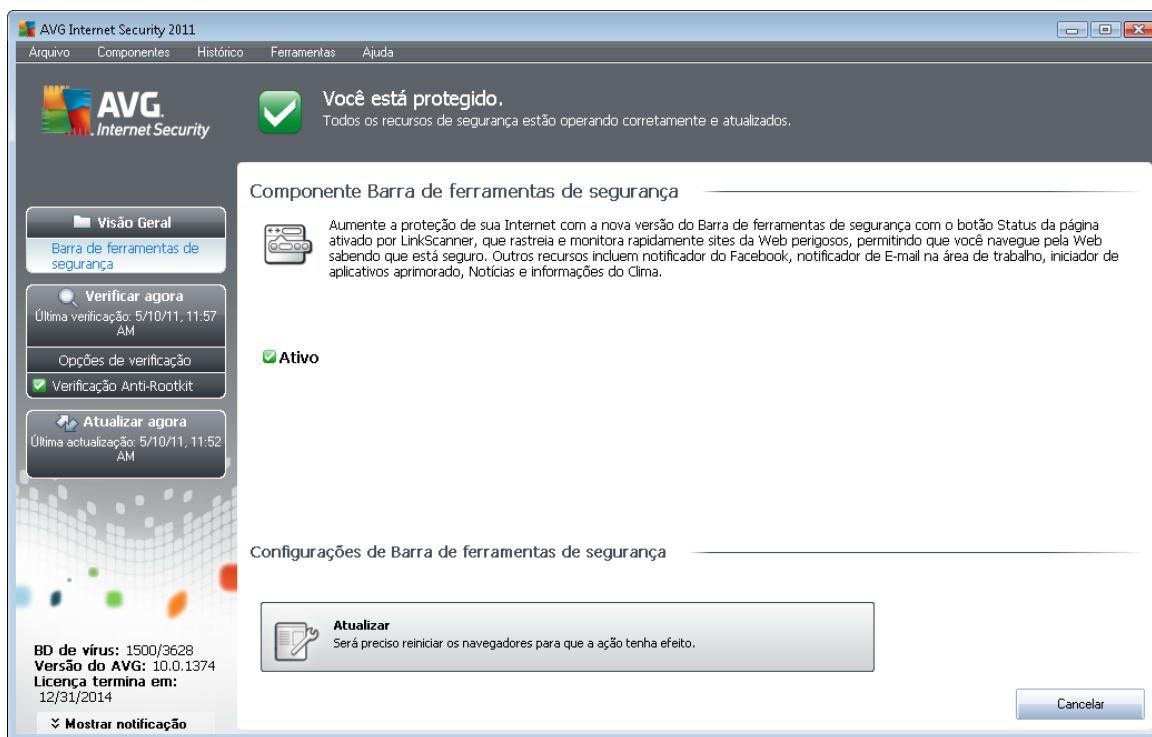
Botões de controle

Os botões de controle disponíveis na interface do **Identity Protection** são os seguintes:

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

7.18. Barra de ferramentas de segurança

A **Barra de Ferramentas de Segurança** é uma barra de ferramentas opcional no navegador da Web, que oferece maior proteção do AVG e diversos recursos e ferramentas práticos enquanto você navega na Web. Atualmente, a **Barra de Ferramentas de Segurança** é compatível com os navegadores Internet Explorer (6.0 ou superior) e Mozilla Firefox (3.0 ou superior):



Todas as configurações do componente **Barra de ferramentas de segurança** podem ser acessadas diretamente em [Barra de ferramentas de segurança](#) pelo seu navegador.



8. Barra de Ferramentas de Segurança do AVG

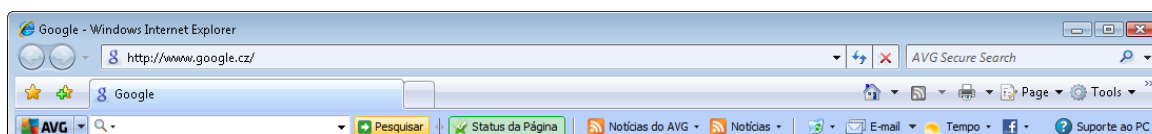
Barra de Ferramentas de Segurança do AVG é uma nova ferramenta que funciona junto com o componente [LinkScanner](#). A **Barra de Ferramentas de Segurança AVG** pode ser usada para controlar as funções do [LinkScanner](#) e ajustar seu comportamento.

Se você optar por instalar a barra de ferramentas durante a instalação do **AVG Internet Security 2011**, ela será adicionada ao navegador (*Internet Explorer 6.0 ou mais recente e Mozilla Firefox 3.0 ou mais recente*) automaticamente. Outros navegadores de Internet não são suportados no momento.

Observação: se você estiver usando um navegador da Internet alternativo (por exemplo, o Avant Browser), poderá perceber um comportamento inesperado.

8.1. Interface da Barra de Ferramentas de Segurança do AVG

A **Barra de Ferramentas de Segurança do AVG** foi desenvolvida para funcionar com o **MS Internet Explorer** (versão 6.0 ou mais recente) e **Mozilla Firefox** (versão 3.0 ou mais recente). Quando você decidir que deseja instalar a **Barra de Ferramentas de Segurança do AVG** (durante o [processo de instalação](#) do AVG, será necessário decidir se deseja ou não instalar o componente), o componente estará localizado no navegador da Web, abaixo da barra de endereços:



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

8.1.1. Botão do logotipo AVG

Este oferece acesso a itens gerais da barra de ferramentas. Clique no botão do logotipo para ser redirecionado ao [site do AVG](#). Clicar no ponteiro ao lado do ícone do AVG abrirá o seguinte:

- **Informações da barra de ferramentas** - link para a página inicial da **Barra de Ferramentas de Segurança do AVG** que contém informações detalhadas sobre a proteção da barra de ferramentas
- **Iniciar AVG** - abre a [interface de usuário](#) do **AVG Internet Security 2011**
- **Informações AVG** - abre um menu de contexto com os seguintes links com informações de segurança importantes relacionadas a **AVG Internet Security 2011**:
 - o **Sobre Ameaças** - abre o [site da AVG](#) na página que fornece os dados mais importantes sobre as ameaças principais, recomendações de remoção de vírus, informações de atualização do AVG, acesso ao [Banco de dados de vírus](#) e mais informações relevantes
 - o **Notícias do AVG** - abre a página da Web que fornece as publicações mais recentes relacionadas ao AVG



o *Nível atual de ameaças* - abre a página da Web do AVG Virus Lab, com uma exibição gráfica do nível atual de ameaças na Web

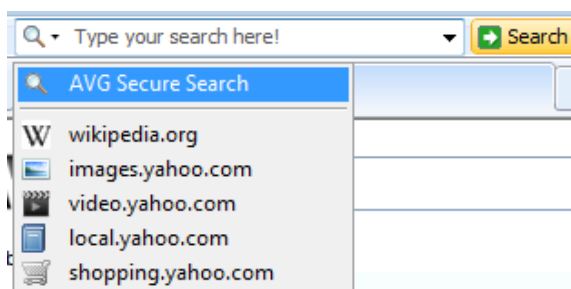
o *AVG Threat Labs* - abre o site [AVG Site Reports](#), em que você pode pesquisar as ameaças específicas por nome e obter informações detalhadas sobre cada uma

- **Opções** - abre uma caixa de diálogo de configuração na qual você pode ajustar as configurações do **AVG Security Toolbar** para que elas atendam às suas necessidades - consulte o capítulo [Opções da Barra de Ferramentas de Segurança AVG](#)
- **Excluir histórico** - permite, na **Barra de Ferramentas de Segurança do AVG**, excluir o histórico completo ou, separadamente, excluir cookies, o histórico de pesquisa, o histórico do navegador e o histórico de downloads.
- **Atualizar** - verifica se há novas atualizações para a **Barra de Ferramentas de Segurança do AVG**
- **Ajuda** - oferece opções para abrir o arquivo de ajuda, entrar em contato com o [Suporte Técnico AVG](#), enviar seu feedback relacionado ao produto ou exibir detalhes da versão atual da barra de ferramentas

8.1.2. Caixa de pesquisa do AVG Secure Search (powered by Google)

A caixa de diálogo **AVG Secure Search (powered by Google)** é uma maneira fácil e segura de pesquisar na Web usando o AVG Secure Search (powered by Google). Digite uma palavra ou frase na caixa de pesquisa e pressione o botão **Pesquisar** ou a tecla **Enter** para começar a pesquisa no servidor do AVG Secure Search (powered by Google) diretamente, seja qual for a página exibida no momento. A caixa de pesquisa também lista o histórico de pesquisa. As pesquisas feitas com a caixa de pesquisa são analisadas usando a proteção [Search-Shield](#).

Como segunda opção, no campo de pesquisa, você pode alternar para a Wikipédia ou algum outro serviço de pesquisa específico - veja a figura:



8.1.3. Status da Página

Diretamente na barra de ferramentas, este botão exibe a avaliação da página da Web exibida no momento, com base nos critérios do componente [Surf-Shield](#):

-  - A página de link é segura

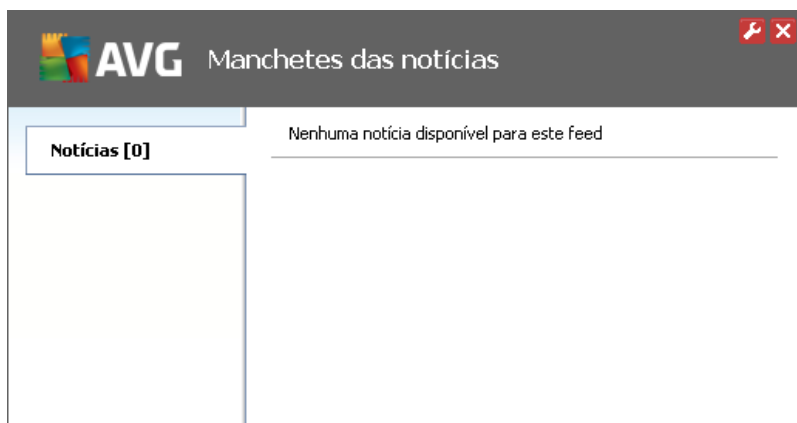


-  - A página é um tanto suspeita.
-  - A página contém links para páginas potencialmente perigosas.
-  - A página de link contém ameaças ativas! Para sua própria segurança, você não poderá visitar esta página.
-  - A página não está acessível e não pôde ser verificada.

Clique no botão para abrir um painel de informações com dados detalhados na página da Web especificada.

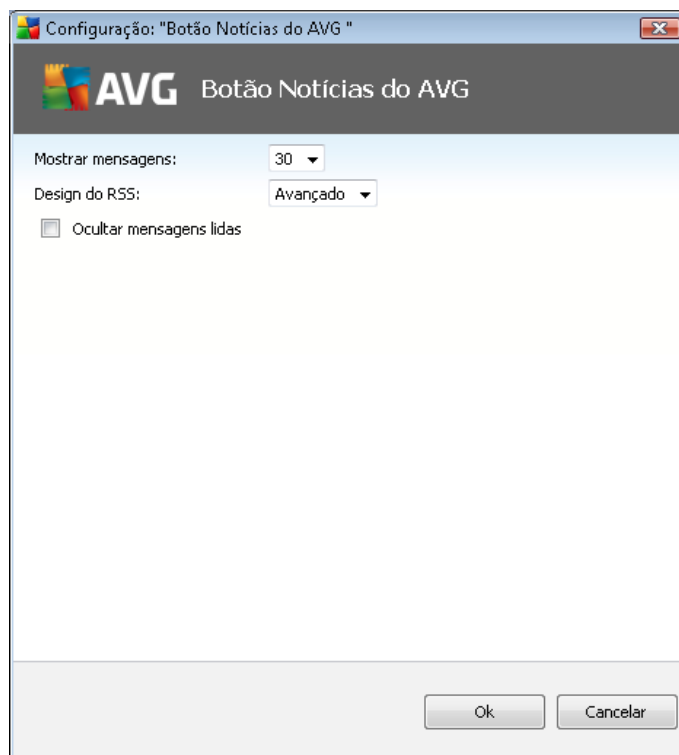
8.1.4. Notícias do AVG

Diretamente da **Barra de Ferramentas de Segurança do AVG**, este botão abre uma visão geral das **Manchetes** mais recentes relacionadas à AVG, tanto notícias da imprensa quando press releases da empresa:



No canto superior direito, é possível ver dois botões de controle vermelhos:

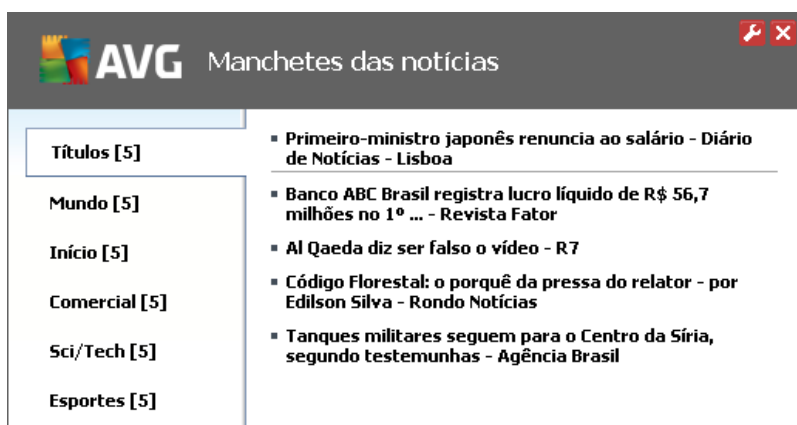
-  - o botão abre a caixa de diálogo de edição, na qual é possível especificar parâmetros do botão **Notícias da AVG** exibido na **Barra de Ferramentas de Segurança do AVG**:



- o **Mostrar mensagens** - altere o número desejado de mensagens que devem ser exibidas por vez
- o **Design RSS** - selecione entre o modo Avançado/Básico da exibição atual da visão geral de notícias (*por padrão, o modo Avançado fica selecionado - veja a figura acima*)
- o **Ocultar mensagens lidas** - marque este item para confirmar que toda mensagem lida não deve mais ser exibida, para que novas mensagens possam ser fornecidas
-  - clique neste botão para fechar a visão geral de notícias aberta atualmente

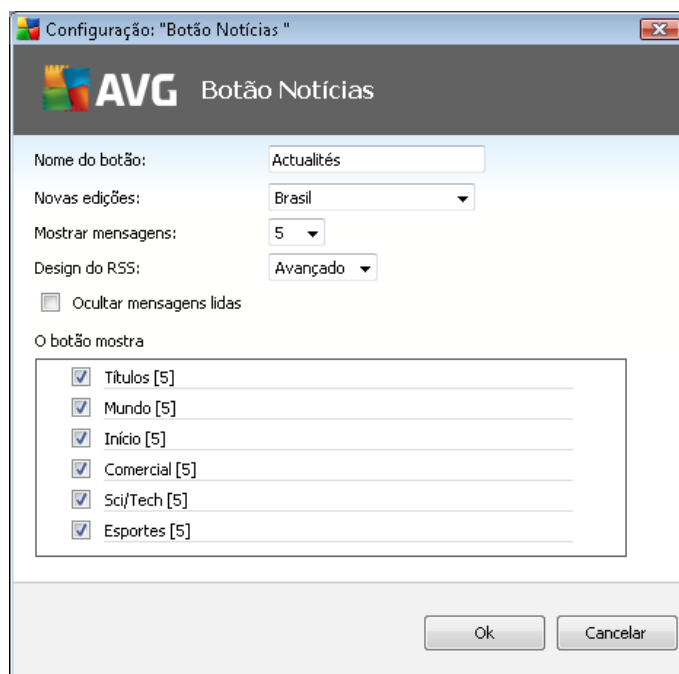
8.1.5. Notícias

Da mesma forma, diretamente na **Barra de Ferramentas de Segurança do AVG**, este botão abre uma visão geral das notícias mais recentes da mídia selecionada divididas em várias seções:



No canto superior direito, é possível ver dois botões de controle vermelhos:

-  - o botão abre a caixa de diálogo de edição, na qual é possível especificar parâmetros do botão **Notícias** exibido na **Barra de Ferramentas de Segurança do AVG**:



o **Nome do botão** - você tem a opção de alterar o nome do botão exibido na **Barra de Ferramentas de Segurança do AVG**

o **Edição de notícias** - escolha um país na lista para exibir notícias da região selecionada

o **Mostrar mensagens** - especifique o número desejado de mensagens que devem ser exibidas por vez



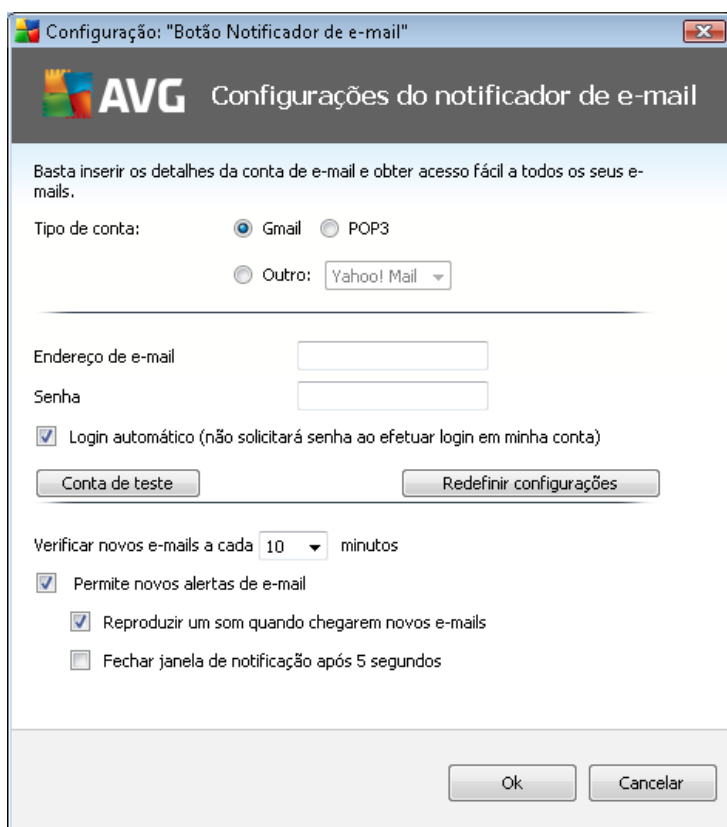
- o **Design RSS** - alterne entre a opção Básico/Avançado para selecionar o design da visão geral de notícias (*o design avançado é definido por padrão, consulte a imagem acima*)
- o **Ocultar mensagens lidas** - marque este item para confirmar que todas as mensagens lidas não devem mais ser exibidas na visão geral de notícias e devem ser substituídas por uma nova manchete
- o **Mostrar** - neste campo, você pode atribuir qual tipo de notícia deve ser exibido na visão geral de notícias da **Barra de Ferramentas de Segurança do AVG**
 -  - clique neste botão para fechar a visão geral de notícias aberta atualmente

8.1.6. Excluir histórico

Usando esse botão, você pode excluir o histórico do navegador exatamente como via opção **Logotipo AVG -> Excluir histórico**.

8.1.7. Notificador de e-mail

O botão **Notificador de Email** permite ativar a opção de ser informado sobre mensagens de email recém-recebidas diretamente na interface da [Barra de Ferramentas de Segurança do AVG](#). O botão abre a seguinte caixa de edição, na qual você pode definir os parâmetros de sua conta de email e das regras de exibição de email. Siga as instruções na caixa de diálogo:



- **Tipo de conta** - Especifique o tipo de protocolo que a sua conta de email usa. Você pode selecionar uma das seguintes alternativas: *Gmail*, *POP3* ou selecionar o nome do servidor no menu suspenso no item *Outro* (no momento, você poderá usar essa opção caso a sua conta esteja no *Yahoo! JP Mail* ou *Hotmail*). Se não tiver certeza do tipo de servidor de



email que sua conta usa, tente localizar as informações do provedor de email ou o seu provedor de serviços de Internet.

- **Login** - na seção abaixo, forneça a forma exata do seu *endereço de e-mail* e a *senha correspondente*. Mantenha a opção *Login Automático* marcada para que você não precise preencher os dados repetidamente.
- **Testar conta** - use este botão para testar os detalhes inseridos.
- **Restaurar configurações** - remove rapidamente os detalhes do endereço de e-mail inseridos acima.
- **Verificar se há novos emails a cada ... minutos** - Defina o intervalo de tempo a ser usado para verificar se há novas mensagens de email (*no intervalo de 5 a 120 minutos*) e especifique se e como quer ser informado sobre a chegada de uma nova mensagem.
- **Permitir novos alertas de e-mail** - desmarque esta opção para desabilitar as notificações visuais na chegada de novas mensagens de e-mail.
 - o **Reproduzir um som quando chegarem novos e-mails** - desmarque esta opção para desabilitar as notificações sonoras na chegada de novas mensagens de e-mail.
 - o **Fechar a janela de notificação após 5 segundos** - selecione esta opção para fechar automaticamente a janela de notificação visual na chegada de novas mensagens de e-mail após 5 segundos.

8.1.8. Informações do Tempo

O botão **Tempo** exibe as informações sobre a temperatura atual (*atualizada a cada 3 a 6 horas*) no seu destino selecionado diretamente na interface da **Barra de Ferramentas de Segurança do AVG**. Clique no botão para abrir um novo painel de informações com visão geral detalhada do tempo:

Brno, CZ
[[alterar localização](#)]

20° C
Velocidade do vento: 3.22 km/h
Nascer do Sol: 05:16
Pôr do Sol: 20:21

TER Máx.: 24 °C Mín: 12 °C	QUA Máx.: 24 °C Mín: 9 °C
---	--

Atualizado 05/10/2011 10:38:45 **YAHOO! NEWS** [Previsão completa >](#)

A seguir, localize as opções de edição:



- **Alterar local** - clique no texto **Alterar local** para exibir uma nova caixa de diálogo denominada **Pesquisar por sua localização**. Preencha o nome da sua localidade desejada no campo de texto e confirme clicando no botão **Pesquisar**. Em seguida, na lista de todas as localidades de mesmo nome, selecione o destino que está procurando. Por fim, o painel de informações será exibido novamente, fornecendo as informações sobre o tempo do local selecionado.
- **Conversor Fahrenheit / Celsius** - no canto superior direito do painel de informações, você pode escolher entre as escalas Fahrenheit e Celsius. Com base na sua escolha, as informações de temperatura serão fornecidas na escala selecionada.
- **Previsão Completa** - se você estiver interessado em uma previsão detalhada e completa, use o link **Previsão Completa** para acessar o site especializado em previsão de tempo.

8.1.9. Facebook

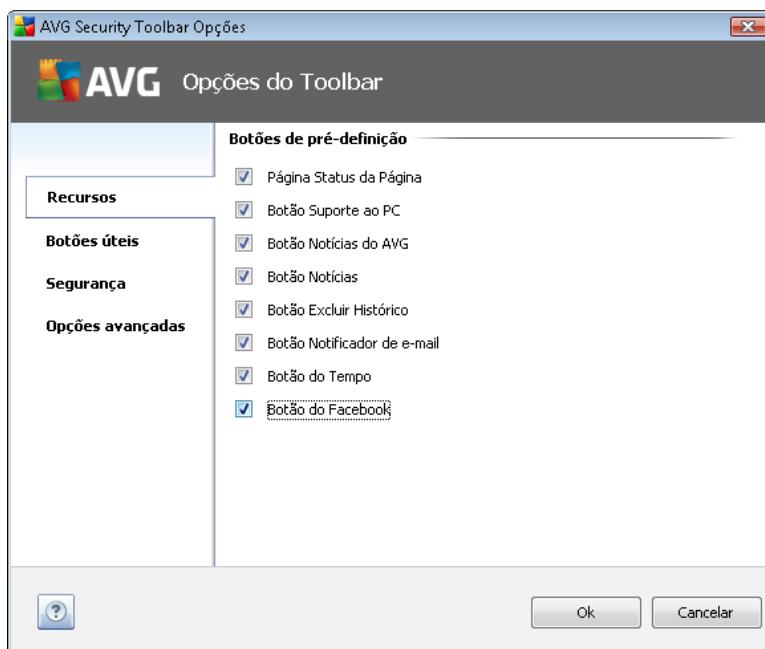
O botão **Facebook** permite se conectar à rede social [Facebook](#) diretamente pela **Barra de Ferramentas de Segurança do AVG**. Clique no botão, e o convite de login aparece; clique novamente para abrir a caixa de diálogo **Login do Facebook**. Forneça seus dados de acesso e pressione o botão **Conectar**. Se ainda não tiver uma conta do [Facebook](#), você poderá criar uma diretamente usando o link **Inscriver-se no Facebook**.

Durante o processo de registro no [Facebook](#), você será convidado a permitir o aplicativo **Extensão Social AVG**. A funcionalidade desse aplicativo é essencial para a barra de ferramentas (conexão com [Facebook](#)), por isso que se recomenda permitir a sua ativação, portanto, certifique-se de permiti-la. Em seguida, a conexão com o [Facebook](#) será ativada, e o botão **Facebook** na **Barra de Ferramentas de Segurança do AVG** agora oferece as opções de menu do [Facebook](#) padrão.

8.2. Opções da Barra de Ferramentas de Segurança do AVG

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

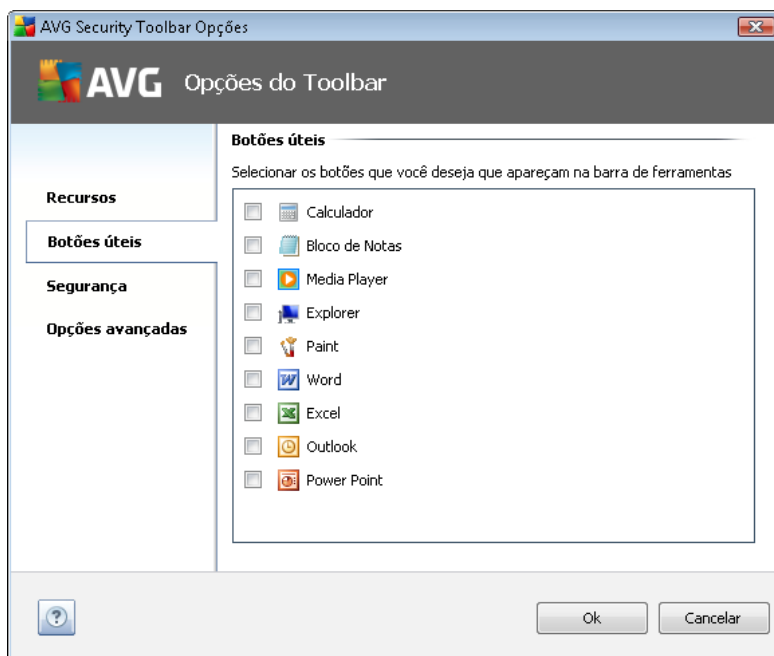
8.2.1. Guia Geral



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

- **Botão de Status da Página** - o botão oferece a possibilidade de exibir as informações sobre o status de segurança da página aberta no momento **Barra de Ferramentas de Segurança do AVG**
- **Botão Notícias do AVG** - o botão abre a página da Web que fornece as publicações mais recentes relacionadas ao AVG
- **Botão Notícias** - o botão fornece uma visão geral estruturada das notícias atuais através da imprensa diária
- **Botão Excluir histórico** - esse botão permite Excluir o histórico inteiro ou Excluir o histórico de pesquisas, Excluir o histórico do navegador, Excluir o histórico de downloads ou Excluir cookies diretamente do painel AVG Security Toolbar
- **Botão Notificador de Email** - o botão permite exibir as mensagens de email recém-recebidas na interface da **Barra de Ferramentas de Segurança do AVG**
- **Botão Tempo** - o botão oferecer informações imediatas sobre a situação do tempo em um local selecionado
- **Botão Facebook** - o botão oferece uma conexão direta com a rede social [Facebook](https://www.facebook.com)

8.2.2. Guia Botões úteis



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

8.2.3. Guia Segurança



A guia **Segurança** está dividida em duas seções, **AVG Browser Security** e **Classificações**, onde é

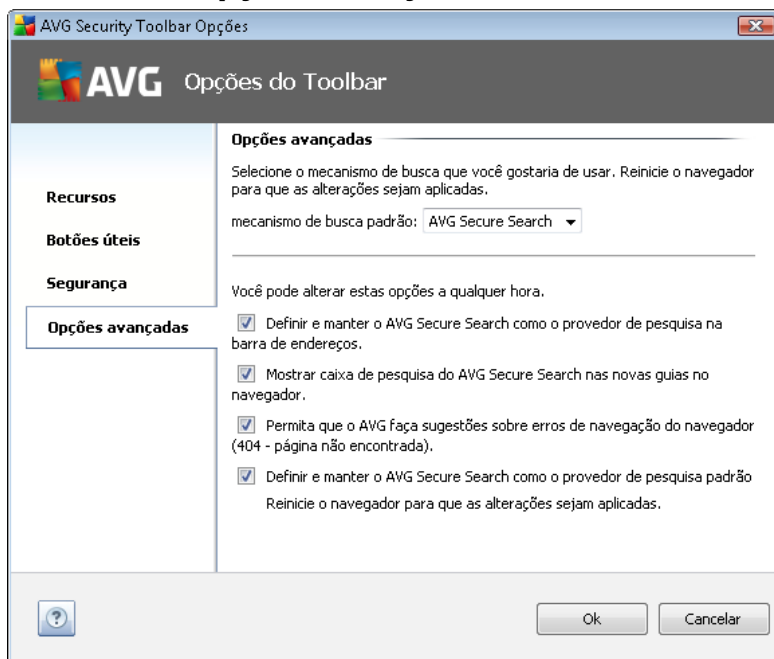


possível marcar caixas de seleção específicas para atribuir a funcionalidade da **Barra de Ferramentas de Segurança AVG** que você deseja usar:

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

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

8.2.4. Guia Opções avançadas





Na guia **Opções avançadas** selecione primeiro qual o mecanismo de pesquisa você deseja usar como padrão. Você pode escolher entre *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* e *Yahoo! JP*. Tendo alterado o mecanismo de busca padrão, reinicie o seu navegador de internet para que as alterações tenham efeito.

Além disso, você pode ativar ou desativar outras configurações específicas da **Barra de Ferramentas de Segurança do AVG** (a legenda indicada se refere às configurações padrão do *AVG Secure Search (powered by Google)*):

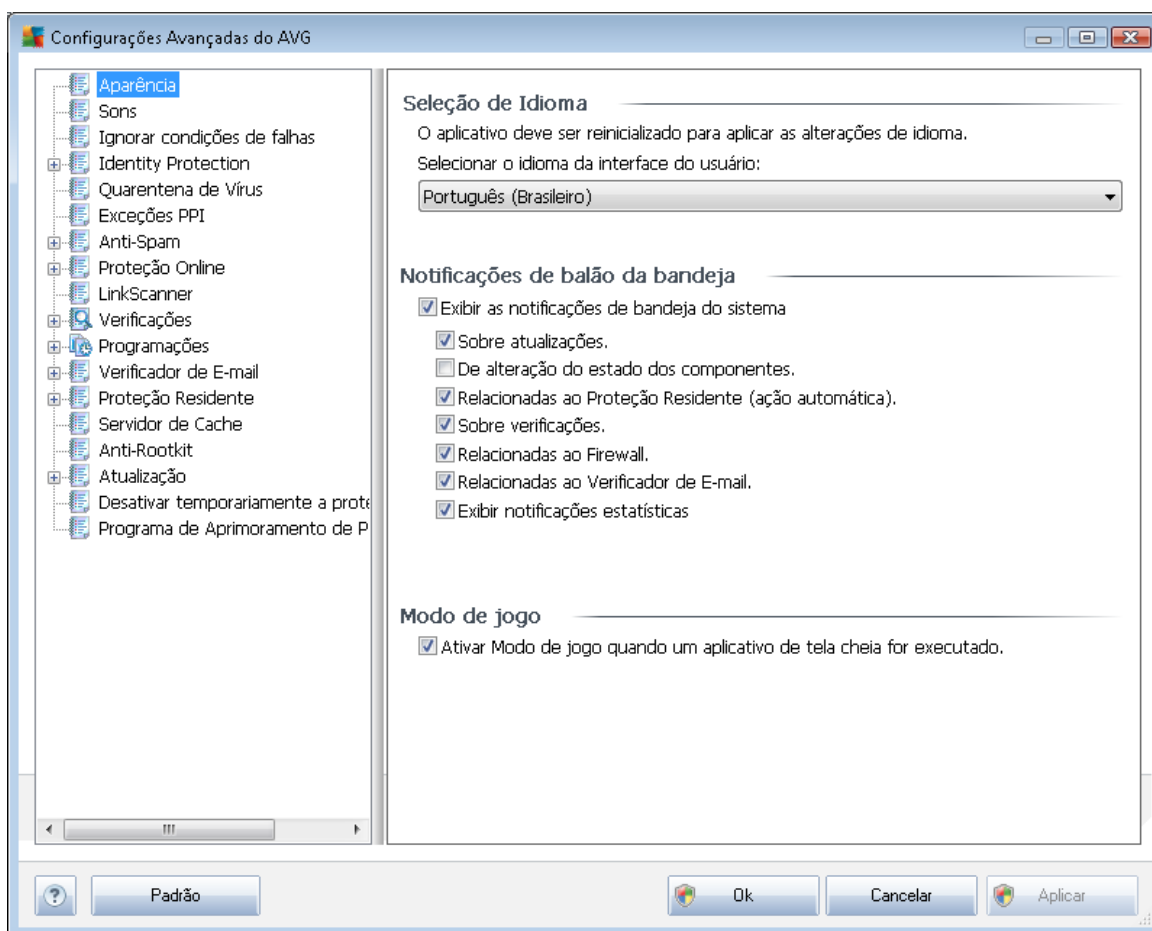
- **Definir e manter o AVG Secure Search (powered by Google) como o provedor de pesquisa da barra de endereços** - se esta opção for selecionada, ela permitirá que você digite uma palavra-chave de pesquisa diretamente na barra de endereços do navegador de Internet, e o serviço Google será usado automaticamente para pesquisar sites relevantes.
- **Deixar que o AVG faça sugestões no caso de erros de navegação do navegador (404/DNS)** - ao pesquisar na Web, se acessar uma página inexistente ou uma página que não pode ser exibida (erro 404), você será redirecionado automaticamente a uma página da Web que permite selecionar a partir de uma visão geral de páginas alternativas relacionadas ao tópico.
- **Definir e manter o AVG Secure Search (powered by Google) como o provedor de pesquisa padrão** - o Google é o mecanismo de pesquisa padrão da Web na **Barra de Ferramentas de Segurança do AVG** e, se essa opção for ativada, ele também poderá se tornar o mecanismo de pesquisa padrão do navegador da Web.

9. Configurações avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG Internet Security 2011** 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.

9.1. Aparência

O primeiro item na árvore de navegação, **Aparência**, refere-se às configurações gerais da [interface de usuário do AVG](#) e algumas opções básicas do comportamento do aplicativo:

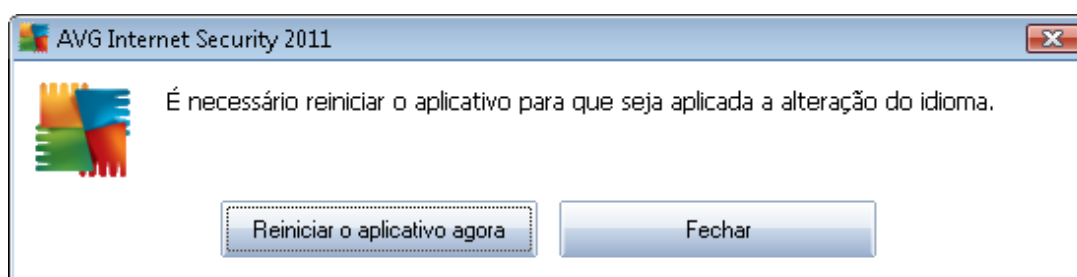


Seleção de idioma

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 [Opção Personalizada](#)), além do inglês (*que vem instalado por padrão*). 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 de balão da bandeja no status do aplicativo. Por padrão, as notificações de balão podem ser exibidas e é recomendável manter essa configuração! As notificações de balão geralmente informam sobre alguma alteração de status do componente do AVG e você deve prestar atenção nelas.

Entretanto, se por alguma razão você optar por não exibir essas notificações 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 fica marcado (*como ativado*) e as notificações são exibidas. Desmarque este item para desativar completamente a exibição de todas as notificações de balão. Quando ativado, é possível selecionar quais notificações específicas devem ser exibidas:
 - o **Exibir notificações da bandeja sobre atualizações** - defina se as informações referentes ao início, andamento ou finalização do processo de atualização do AVG devem ser exibidas;
 - o **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;
 - o **Exibir notificações referentes a Proteção Residente (ação automática)** - decida se as informações relativas a salvar, copiar e abrir processos devem ser exibidas ou omitidas (*esta configuração apenas demonstra se a opção [Reparo automático](#) de*



Proteção Residente está ativada);

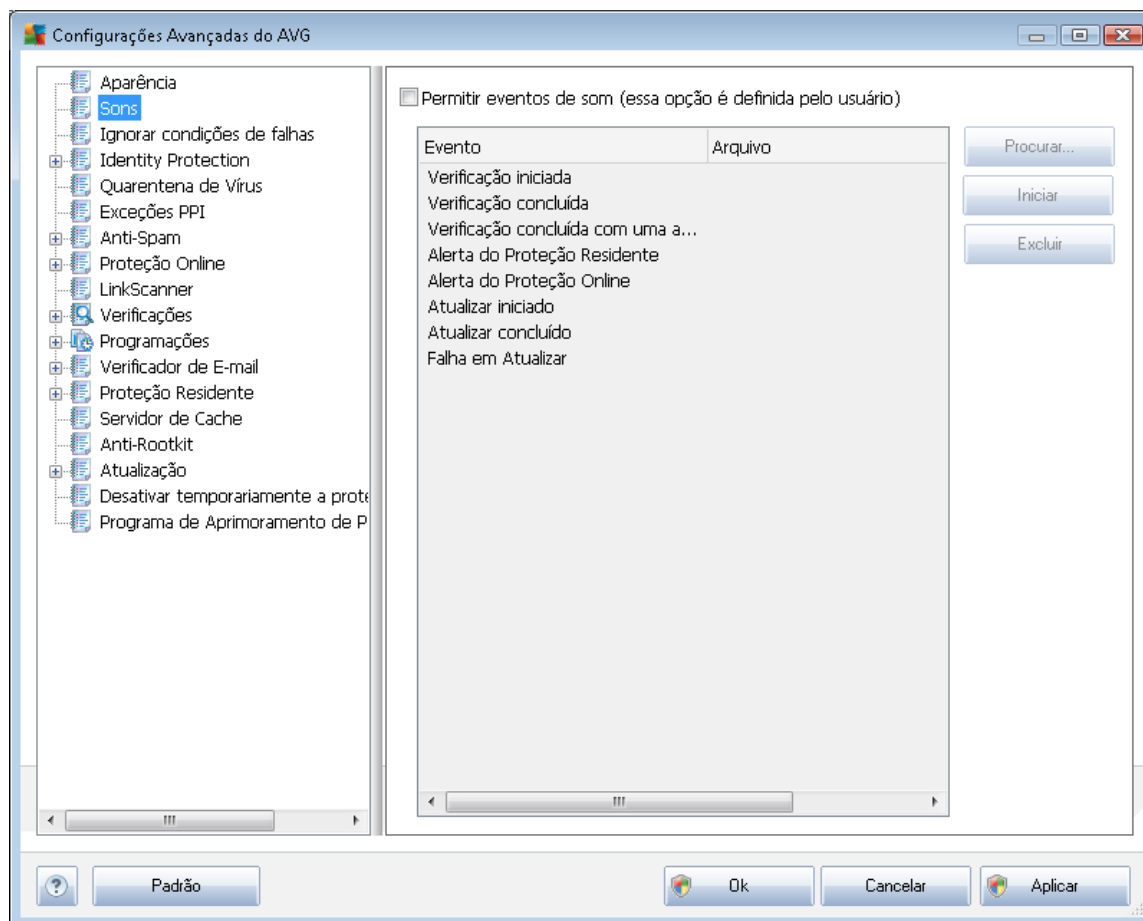
- o **Exibir notificações sobre verificação** - decida se as informações sobre início automático da verificação agendada, seu andamento e resultados devem ser exibidos;
- o **Exibir notificações na bandeja relativas ao Firewall** - decidir se as informações relativas ao status e processo do Firewall, como avisos de ativação/desativação do componente, possível bloqueio de tráfego etc. devem ser exibidas
- o **Exibir notificações da bandeja relacionadas ao Verificador de E-mail** - decida se as informações sobre a verificação de todas as mensagens de e-mail de entrada e saída serão exibidas..
- o **Exibir notificações estatísticas** - mantenha a opção selecionada para permitir que notificações regulares de análises estatísticas sejam exibidas na bandeja do sistema.

Modo de jogo

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

9.2. Sons

Na caixa de diálogo **Sons**, você pode especificar se deseja receber informações sobre ações específicas 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:

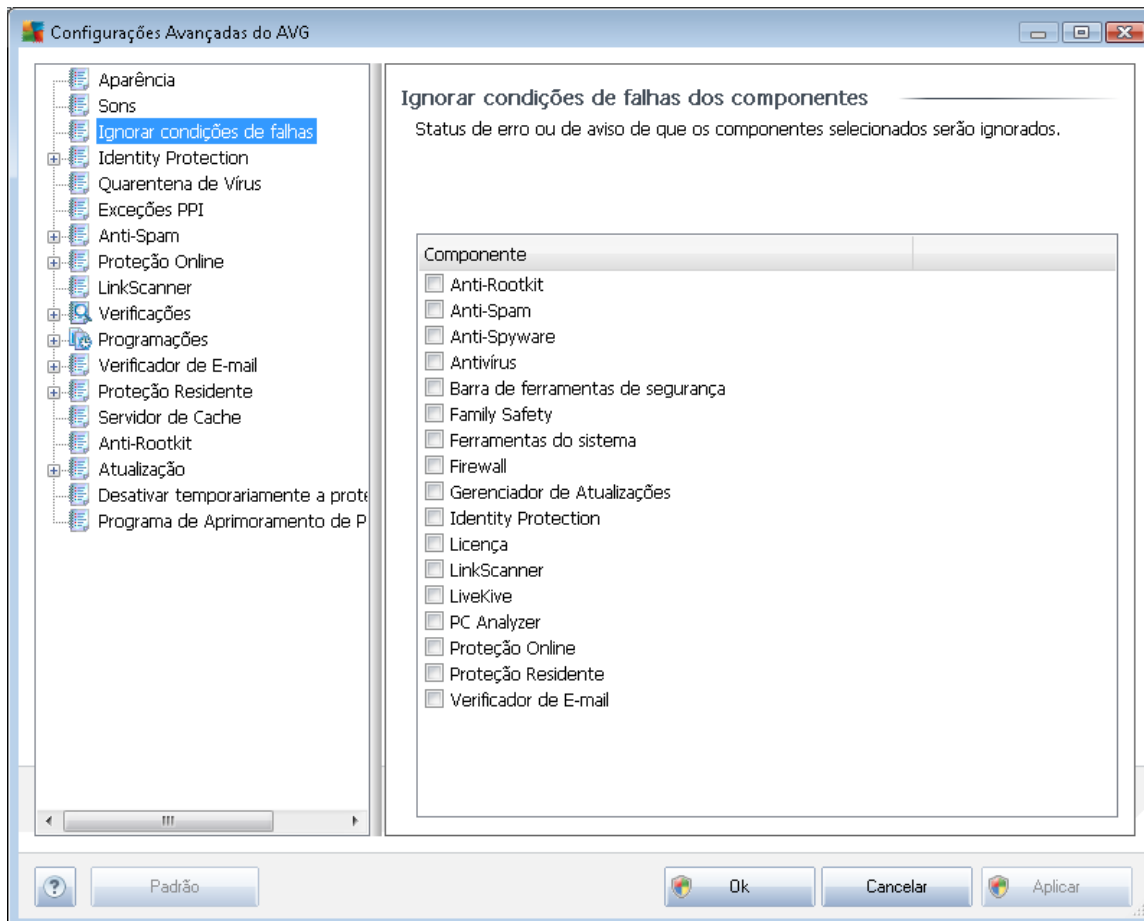


Em seguida, selecione o respectivo evento na lista e procure (usando a opção **Procurar**) um som apropriado no disco rígido que deseja atribuir a esse evento. Para ouvir o som selecionado, realce o evento na lista e pressione o botão **Reproduzir**. Use o botão **Excluir** para remover o som atribuído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

Observação: apenas sons *.wav podem ser usados!

9.3. 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



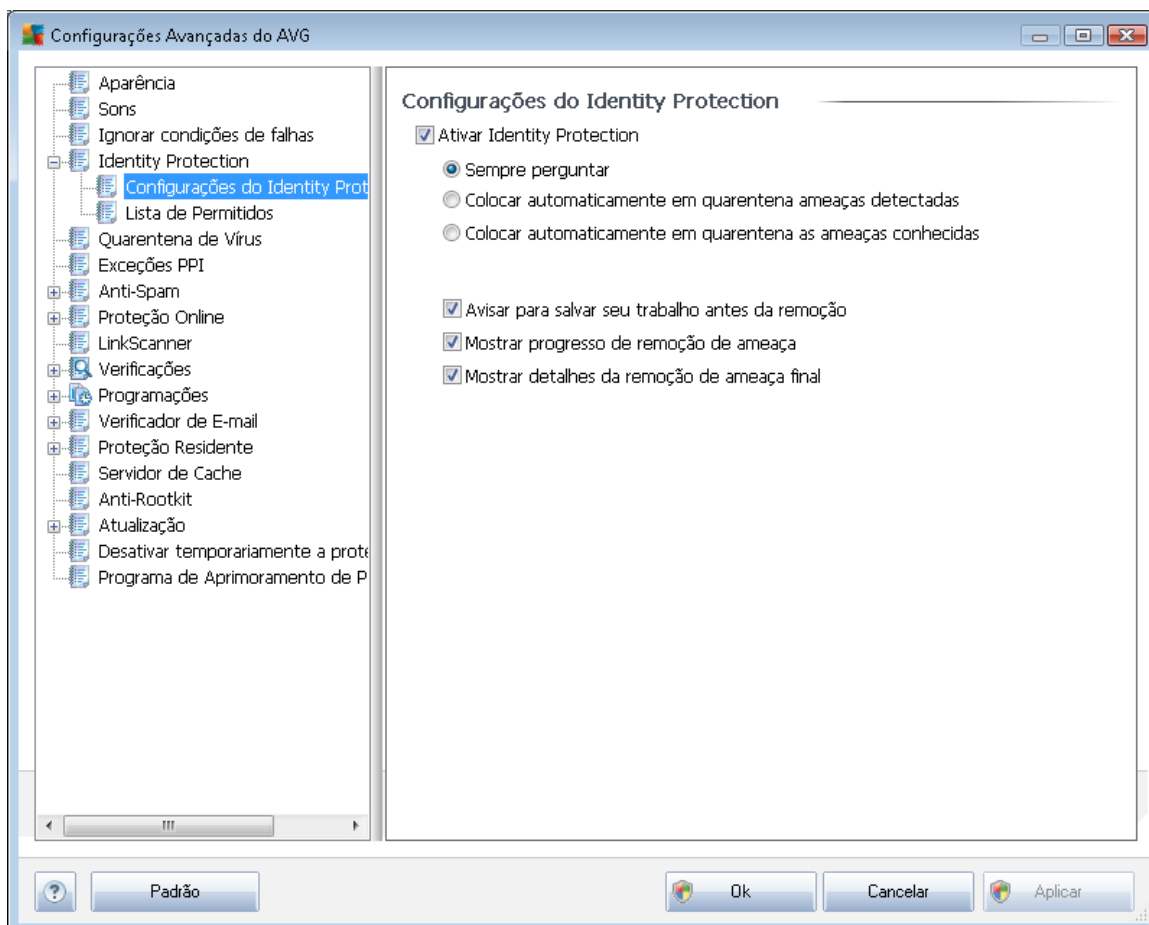
possa aparecer.

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](#).

9.4. Identity Protection

9.4.1. Configurações do Identity Protection

A caixa de diálogo [Configurações do Identity Protection](#) permite ativar/desativar os recursos elementares do componente [Identity Protection](#):



Ativar Identity Protection (ativada por padrão) – desmarque para desativar o componente [Identity Protection](#).

É altamente recomendável não fazer isso a menos que você precise!

Quando o [Identity Protection](#) está ativado, você pode especificar o que fazer quando uma ameaça



é detectada:

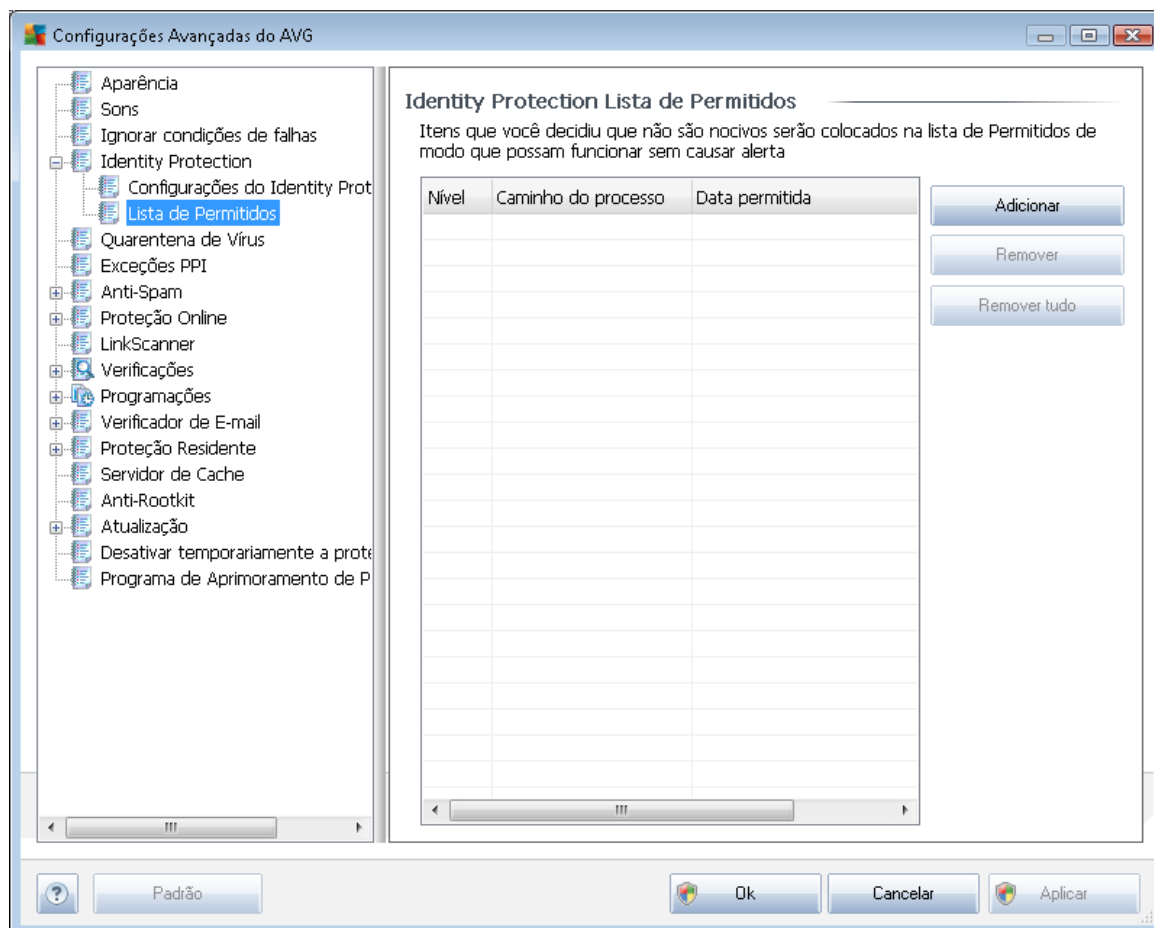
- **Perguntar sempre** (*ativado por padrão*) - quando uma ameaça for detectada, será perguntado se deseja movê-la para a quarentena para assegurar que aplicativos que você deseja executar não sejam removidos.
- **Colocar ameaças detectadas automaticamente em quarentena** - marque essa caixa para definir que deseja mover todas as ameaças possivelmente detectadas para um espaço seguro da [Quarentena de Vírus do AVG](#) imediatamente. Se você mantiver as configurações padrão, quando uma ameaça for detectada, será perguntado se você deseja movê-la para a quarentena para assegurar que aplicativos que você deseja executar não sejam removidos.
- **Colocar automaticamente em quarentena as ameaças detectadas** - marque esse item se desejar que todos os aplicativos detectados como possíveis malware sejam movidos automaticamente e imediatamente para a [Quarentena de Vírus do AVG](#).

Posteriormente você pode atribuir itens específicos para ativar de modo opcional mais recursos do [Identity Protection](#):

- **Solicitar salvar o trabalho antes da remoção** - (*ativado por padrão*) - marque esse item se desejar se avisado antes do aplicativo detectado como possível malware ser removido para quarentena. Caso você esteja trabalhando com o aplicativo, seu projeto poderá ser perdido e você deverá salvá-lo antes. Por padrão, este item está ativado e recomendamos fortemente mantê-lo assim.
- **Exibir progresso de remoção de malware** - (*somente por padrão*) - com esse item ativado, quando um malware potencial é detectado, uma nova caixa de diálogo é aberta para exibir o andamento do malware movido para quarentena.
- **Exibir detalhes finais de remoção de malware** - (*ativado por padrão*) - com esse item ativado, o Identity Protection exibe informações detalhadas sobre cada objeto movido para quarentena (*nível de gravidade, localização etc.*).

9.4.2. Lista de permissões

Na caixa de diálogo **Configurações do Identity Protection**, se você optar por manter o item **Colocar automaticamente em quarentena ameaças detectadas** desmarcado, sempre que um malware perigoso for detectado, será perguntado se você deseja removê-lo. Se depois você atribuir o aplicativo suspeito (*detectado com base em seu comportamento*) como seguro e confirmar que ele deve ser mantido no computador, o aplicativo será adicionado à chamada **Identity Protection - Lista de permitidos** e não será mais reportado como perigoso:



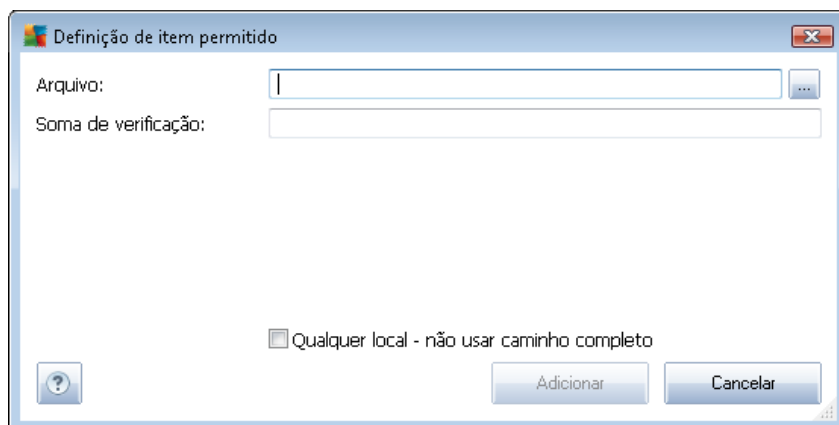
A **Identity Protection - Lista de permitidos** fornece as seguintes informações sobre cada aplicativo:

- **Nível** - identificação gráfica da respectiva severidade do processo em uma escala de quatro níveis, variando do menos importante (■□□□) até o mais crítico (■□■□)
- **Caminho do processo** - caminho para o local do arquivo executável do aplicativo (processo)
- **Data da permissão** - data na qual você atribuiu manualmente o aplicativo como seguro

Botões de controle

Os botões de controle disponíveis na caixa de diálogo **Lista de permissão do Identity Protection** são os seguintes:

- **Adicionar** - pressione esse botão para adicionar um novo aplicativo à lista de permissões. A caixa de diálogo a seguir é ativada:



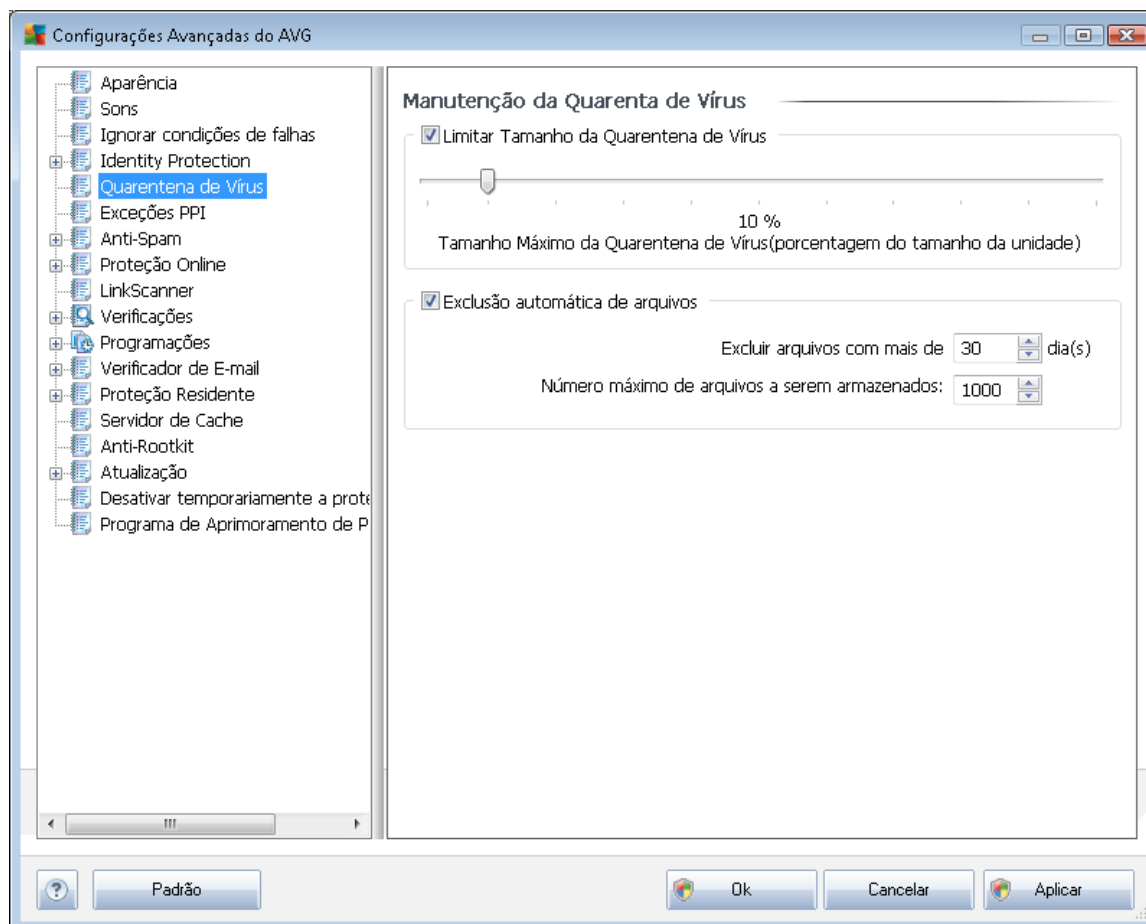
o **Arquivo** - digite o caminho completo para o arquivo (*aplicativo*) que você deseja marcar como exceção

o **Soma de Verificação** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string 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.

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

- **Remover** - pressione para remover o aplicativo selecionado da lista
- **Remover tudo** - pressione para remover todos os aplicativos listados

9.5. Quarentena de vírus



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

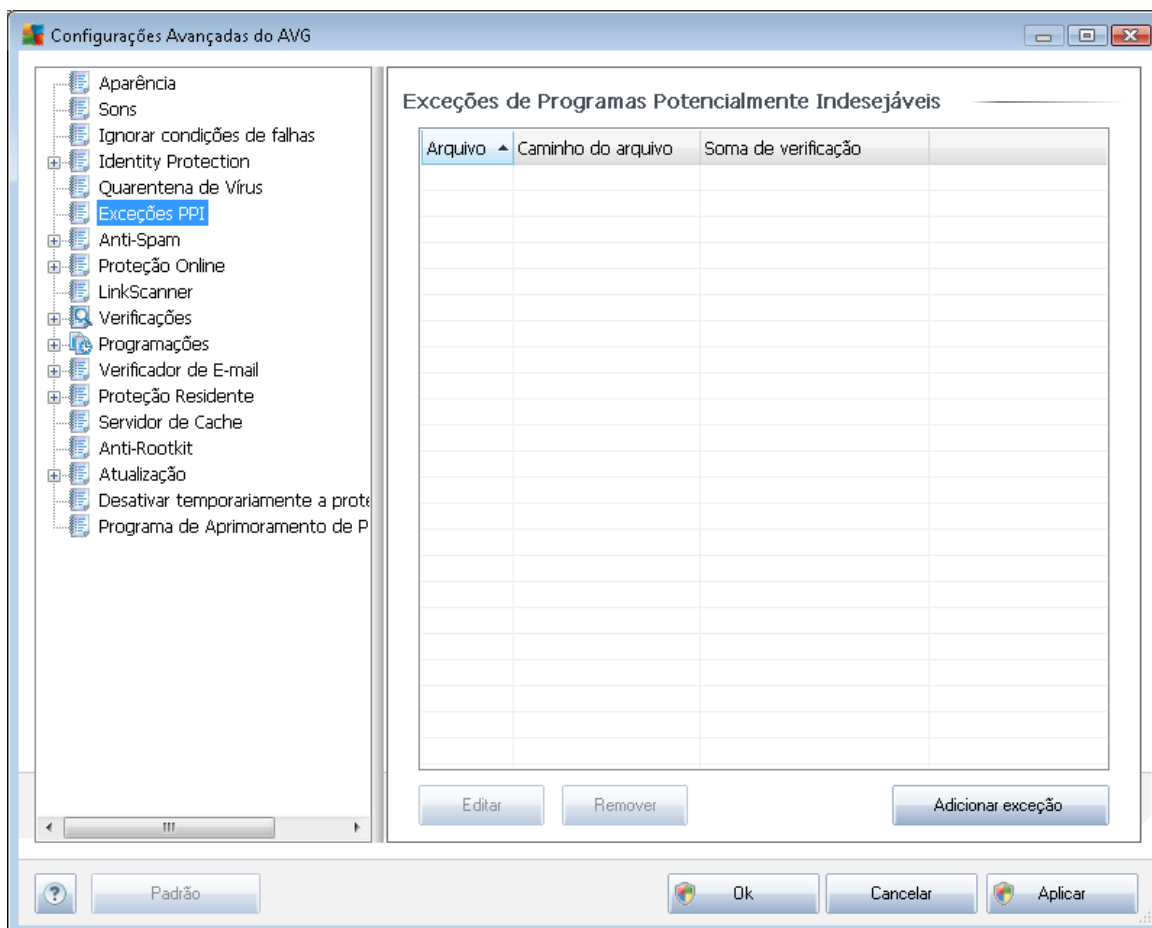
- **Limitar tamanho da Quarentena de vírus** - use o controle deslizante para definir o tamanho máximo da [Quarentena de vírus](#). O tamanho é especificado proporcionalmente ao tamanho do seu disco rígido local.
- **Exclusão automática de arquivo** - nessa seção, defina a duração máxima de armazenamento 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**).

9.6. Exceções PPI

O AVG Internet Security 2011 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:

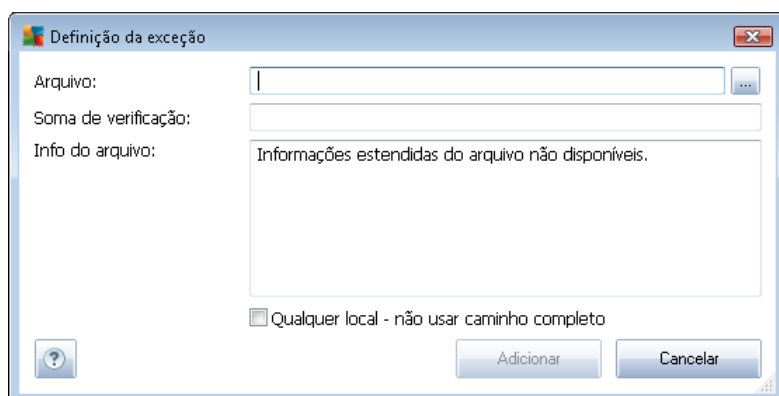
- **Arquivo** - fornece o nome do respectivo aplicativo
- **Caminho do arquivo** - mostra a localização do aplicativo
- **Soma de Verificação** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string de caracteres gerados automaticamente, que permite ao AVG diferenciar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

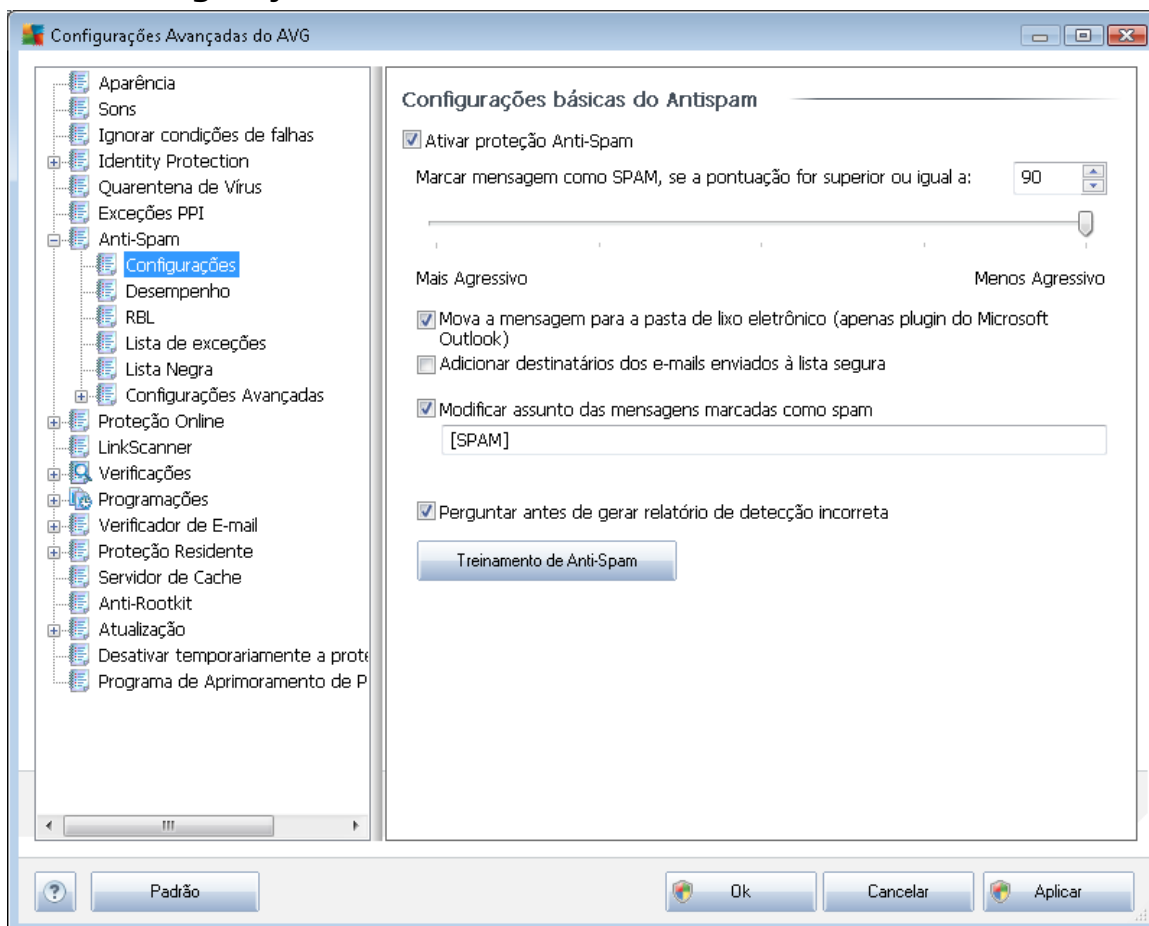
- **Remover** - exclui o item selecionado da lista de exceções
- **Adicionar exceção** - abre uma caixa de diálogo de exceção na qual é possível definir os parâmetros da nova exceção a ser criada:



- o **Arquivo** - digite o caminho completo para o arquivo que deseja marcar como uma exceção
- o **Soma de verificação** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string 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.
- o **Informações do arquivo** - exibe outras informações disponíveis sobre o arquivo (*informações de licença/versão etc.*)
- o **Qualquer local - não use caminhos completos** - se quiser definir o arquivo como uma exceção apenas no local específico, deixe a caixa de seleção desmarcada. Se a caixa de seleção estiver marcada, o arquivo especificado será definido como uma exceção, não importa onde esteja (*entretanto, você precisa especificar o caminho completo para o arquivo específico de qualquer forma; o arquivo será usado como um exemplo exclusivo para a possibilidade de que dois arquivos com o mesmo nome apareçam no sistema*).

9.7. Anti-Spam

9.7.1. Configurações



Na caixa de diálogo **Configurações básicas de anti-spam**, é possível marcar/desmarcar a caixa de seleção **Ativar proteção do Anti-Spam** para permitir/proibir a verificação anti-spam da comunicação por e-mail. Essa opção está ativada por padrão e, como sempre, convém manter essa configuração, a não ser que você tenha um motivo concreto para alterá-la.

Em seguida, você também pode selecionar medidas de pontuação mais ou menos agressivas. O **filtro Anti-Spam** atribui a cada mensagem uma pontuação (ou seja, o nível de semelhança entre um SPAM e o conteúdo da mensagem), com base em várias técnicas dinâmicas de verificação. É possível ajustar a configuração **Marcar mensagem como spam se o resultado for superior a** digitando o valor ou movendo o controle deslizante para a esquerda ou para a direita (o intervalo dos valores é limitado a 50 a 90).

Em geral, recomendamos a definição do limite entre 50 e 90 ou, em caso de dúvidas, como 90. Veja uma análise geral do limite de pontuação:

- **Valor entre 80 e 90** - As mensagens de e-mail que parecem ser [spam](#) serão filtradas. Algumas mensagens que não são SPAM poderão ser bloqueadas incorretamente.
- **Valor entre 60 e 79** - uma configuração considerada bastante agressiva. As mensagens de e-mail que provavelmente são [spam](#) serão filtradas. É provável que mensagens não spam



também sejam bloqueadas

- **Valor entre 50 e 59** - Configuração muito agressiva. É provável que mensagens de e-mail não spam sejam bloqueadas como verdadeiras mensagens [spam](#). Esse intervalo limite não é recomendado para uso normal.

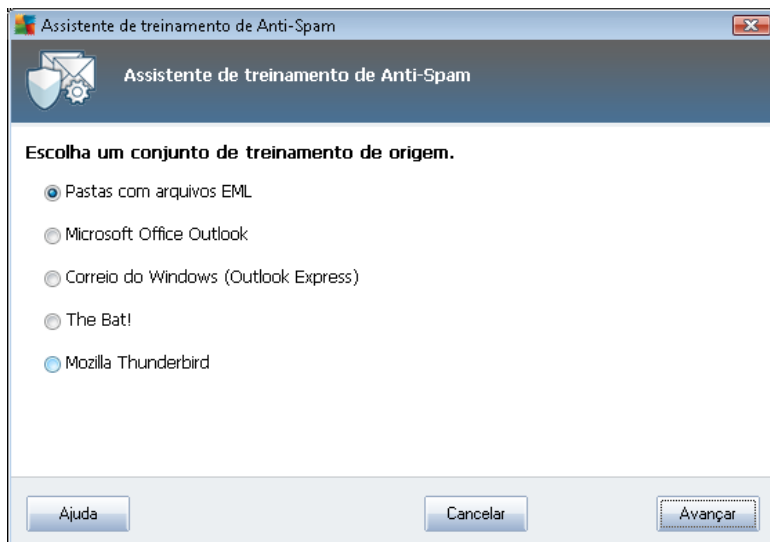
Na caixa de diálogo **Configurações básicas de anti-spam**, você pode definir com mais detalhes como as mensagens de e-mail de [spam](#) detectadas devem ser tratadas:

- **Mover mensagens para a pasta Lixo** - marque essa caixa de seleção para especificar se cada mensagem de spam deve ser automaticamente movida para a pasta de lixo específica dentro do cliente de e-mail;
- **Adicionar destinatários de e-mails enviados à [lista de exceções](#)** - marque essa caixa de seleção para confirmar que todos os destinatários de e-mails enviados são confiáveis e que todas as mensagens de e-mail provenientes das contas desses destinatários podem ser entregues;
- **Modificar assunto das mensagens marcadas como vírus** - marque essa caixa de seleção se quiser que todas as mensagens detectadas como [spam](#) sejam marcadas com uma palavra ou um caractere específico no campo de assunto do e-mail. O texto desejado pode ser digitado no campo de texto ativado.
- **Perguntar antes de gerar relatório de detecção incorreta** - contanto que, durante o [processo de instalação](#), você concorde em participar do [Programa de Aprimoramento de Produto](#). Se for o caso, você autoriza a geração de relatório de ameaças detectadas para a AVG. A geração de relatório é feita automaticamente. Entretanto, você pode marcar esta caixa de seleção para configurar que deseja que uma pergunta seja feita antes de relatar qualquer spam detectado à AVG, para ter certeza de que a mensagem deva realmente ser classificada como spam.

Botões de controle

Botão Treinamento Anti-Spam abre o [Assistente de treinamento Anti-Spam](#) descrito de maneira detalhada no [próximo capítulo](#).

A primeira caixa de diálogo do **Assistente de treinamento de anti-spam** solicita que você selecione a origem das mensagens de e-mail que deseja usar para treinamento. Normalmente, convém usar e-mails marcados incorretamente como SPAM ou mensagens de spam que não foram reconhecidas.



Existem as seguintes opções dentre as quais escolher:

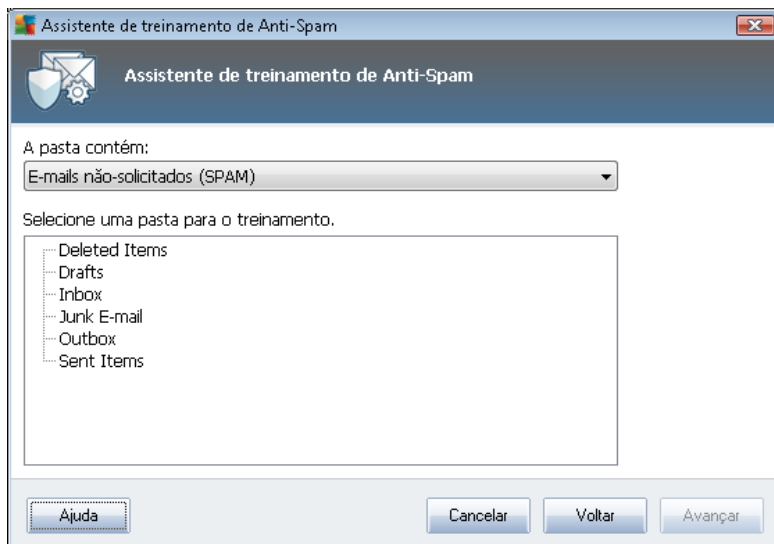
- **Um cliente de e-mail específico** - se você usa um dos clientes de e-mail listados (*MS Outlook, Outlook Express, The Bat!*), basta selecionar a opção correspondente
- **Pasta com arquivos EML** - se você usa qualquer outro programa de e-mail, salve primeiro as mensagens em uma pasta específica (*no formato .eml*) ou certifique-se de que conhece o local das pastas de mensagens do cliente de e-mail. Em seguida, selecione **Pasta com arquivos EML**, o que permitirá que você localize a pasta desejada na próxima etapa

Para um processo de treinamento mais rápido e fácil, é uma boa idéia organizar os e-mails nas pastas antecipadamente, para que a pasta que você usará para treinamento contenha apenas as mensagens de treinamento (desejadas ou indesejadas). Entretanto, isso não é necessário, uma vez que você poderá filtrar os e-mails posteriormente.

Selecione a opção apropriada e clique em **Avançar** para continuar com o assistente.

A caixa de diálogo exibida nesta etapa depende da seleção anterior.

Pastas com arquivos EML



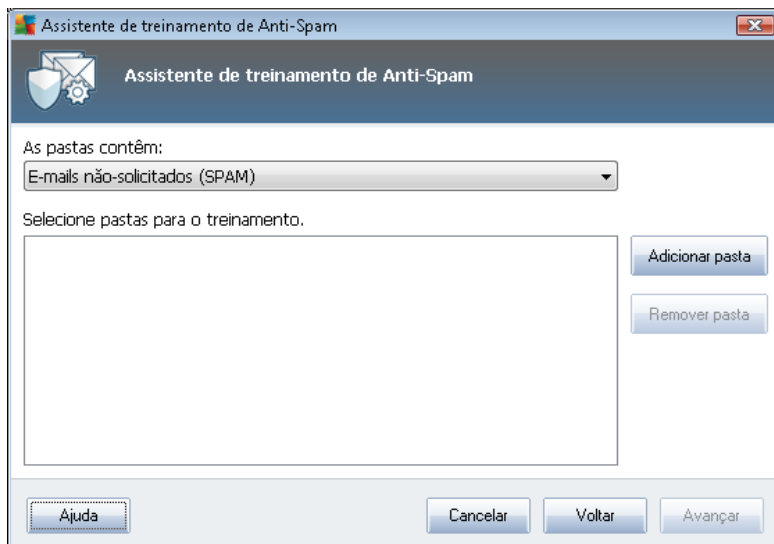
Nesta caixa de diálogo, selecione a pasta com as mensagens que deseja usar para treinamento. Pressione o botão **Adicionar pasta** para localizar a pasta com os arquivos .eml (*mensagens de e-mail salvas*). A pasta selecionada será então exibida na caixa de diálogo.

No menu suspenso **As pastas contêm**, defina uma das duas opções - se a pasta selecionada deve conter mensagens desejadas (*HAM*) ou mensagens não solicitadas (*SPAM*). Lembre-se de que você poderá filtrar as mensagens na próxima etapa, de modo que a pasta não precisa conter somente e-mails de treinamento. Você pode também remover as pastas selecionadas não desejadas da lista clicando no botão **Remover pasta**.

Quando terminar, clique em **Avançar** e passe para [Opções de filtragem de mensagem](#).

Cliente de e-mail específico

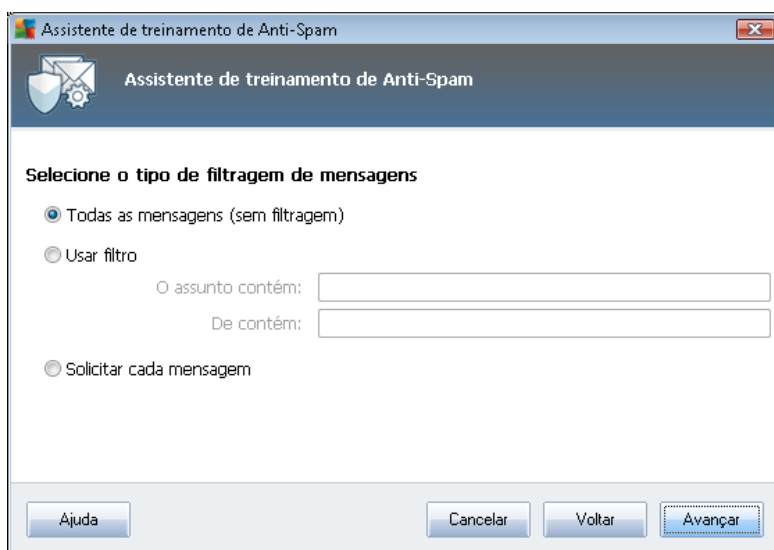
Após confirmar uma das opções, será exibida uma nova caixa de diálogo.



Observação: no caso do Microsoft Office Outlook, será necessário selecionar o perfil do MS Office Outlook primeiro.

No menu suspenso **As pastas contêm**, defina uma das duas opções - se a pasta selecionada deve conter mensagens desejadas (*HAM*) ou mensagens não solicitadas (*SPAM*). Lembre-se de que você poderá filtrar as mensagens na próxima etapa, de modo que a pasta não precisa conter somente e-mails de treinamento. Uma árvore de navegação do cliente de e-mail selecionado já está exibida na seção principal da caixa de diálogo. Localize a pasta desejada na árvore e realce-a com o seu mouse.

Quando terminar, clique em **Avançar** e passe para [Opções de filtragem de mensagem](#).



Nesta caixa de diálogo, você poderá definir a filtragem das mensagens de e-mail.



Se tiver certeza de que a pasta selecionada contém apenas as mensagens que deseja usar para treinamento, selecione a opção **Todas as mensagens (sem filtragem)**.

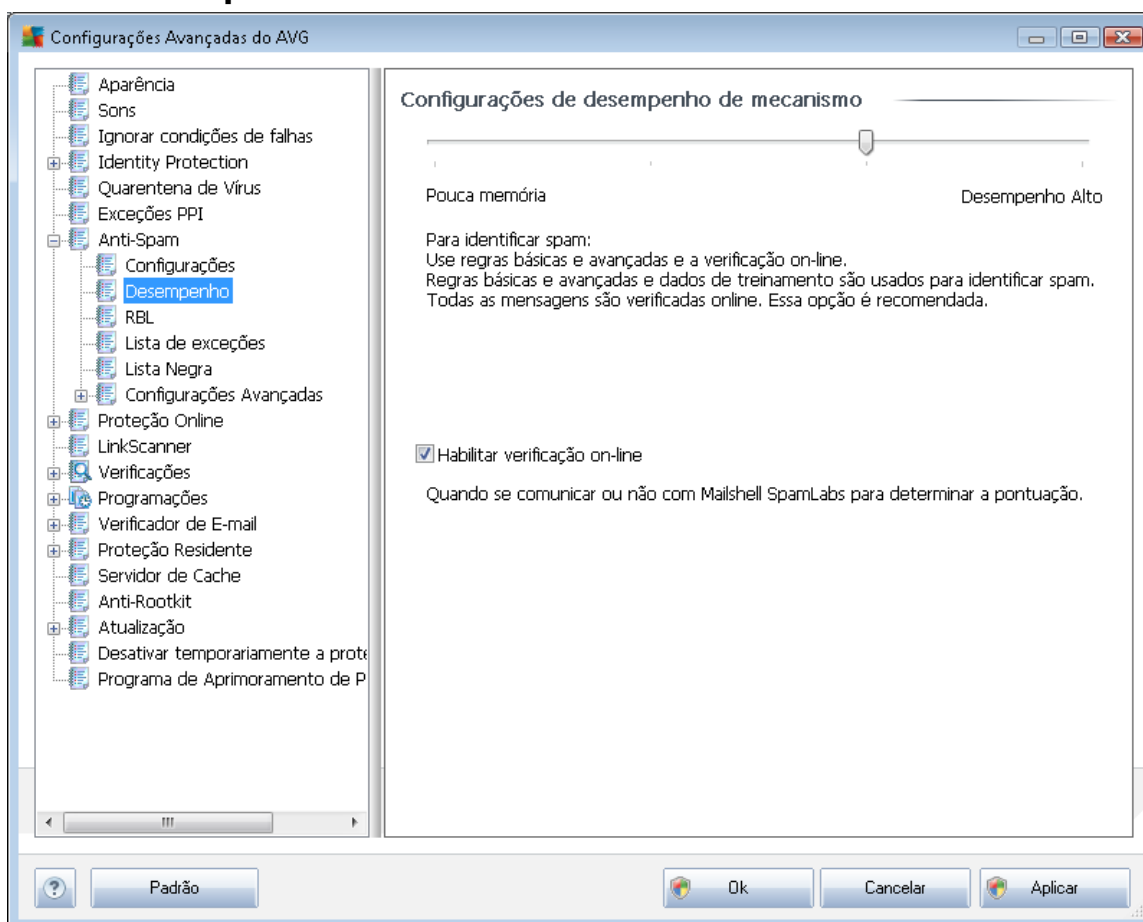
Se você não estiver certo sobre as mensagens contidas na pasta e quiser que o assistente faça perguntas sobre cada mensagem (para poder determinar se ela deve ser usada para treinamento ou não), selecione a opção **Perguntar em cada mensagem**.

Para uma filtragem mais avançada, selecione a opção **Usar filtro**. Você pode inserir uma palavra (nome), parte de uma palavra ou frase a ser pesquisada no assunto de e-mail e/ou no campo do remetente. Todas as mensagens que correspondem exatamente aos critérios inseridos serão usadas para o treinamento, sem solicitações adicionais.

Atenção!: Quando você preenche ambos os campos de texto, os endereços que correspondem a apenas uma das duas condições serão usados também!

Quando a opção apropriada for selecionada, clique em **Avançar**. A caixa de diálogo a seguir terá caráter apenas informativo, informando que o assistente está pronto para processar as mensagens. Para iniciar o treinamento, clique no botão **Avançar** novamente. O treinamento será iniciado de acordo com as condições selecionadas previamente.

9.7.2. Desempenho





A caixa de diálogo **Configurações de desempenho do mecanismo** (que pode ser acessada no link do item **Desempenho** do painel de navegação esquerdo) oferece as configurações de desempenho do componente **Anti-Spam**. Mova o controle deslizante para a esquerda ou para a direita para alterar o nível de intervalo de desempenho de verificação entre os modos **Pouca memória**/**Alto desempenho**.

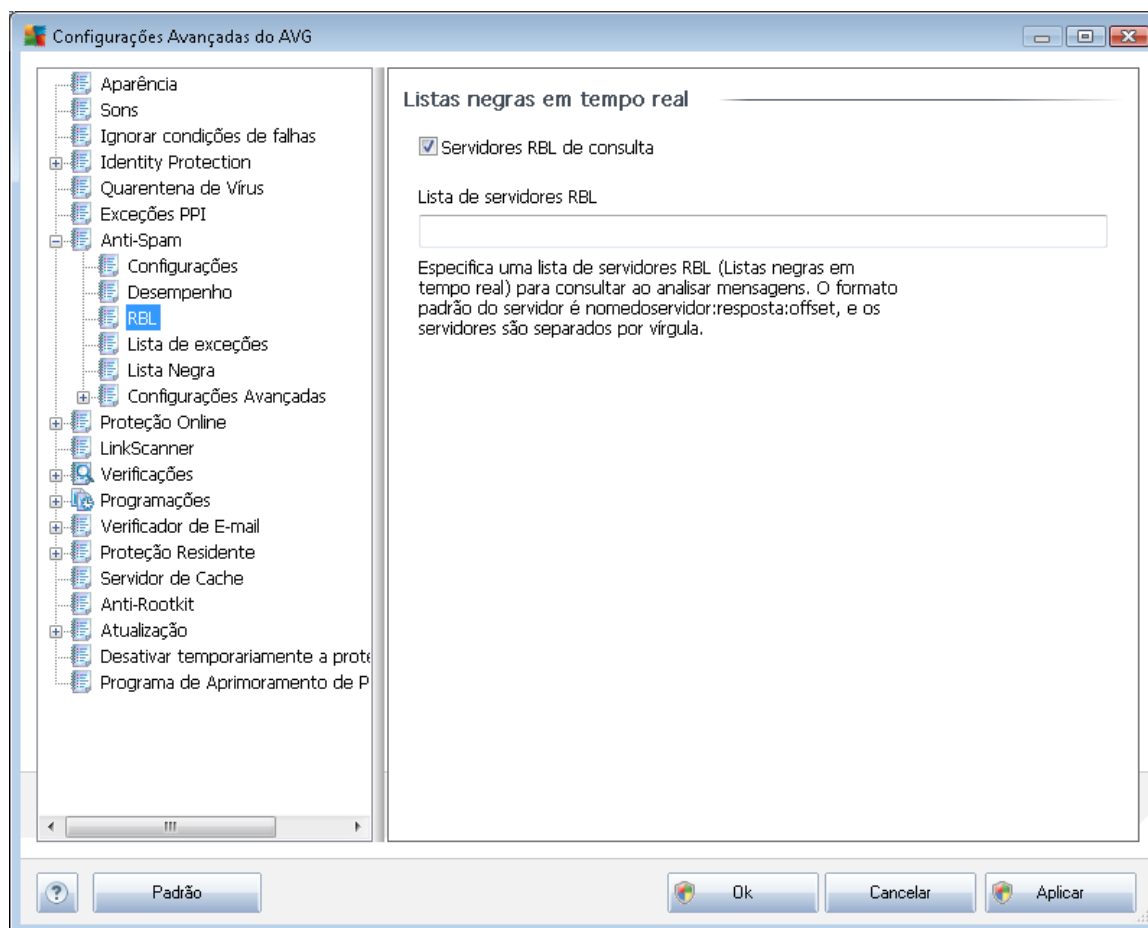
- **Pouca memória** - durante o processo de verificação para identificar [spam](#), nenhuma regra será usada. Apenas os dados de treinamento serão usados para identificação. Esse modo não é recomendado para uso comum, a menos que o hardware do computador seja realmente fraco.
- **Alto desempenho** - este modo consumirá muita memória. Durante o processo de verificação para identificar um [spam](#), os seguintes recursos serão usados: cache do banco de dados de regras e [spam](#), regras básicas e avançadas, endereços IP de spam e bancos de dados de spam.

O item **Habilitar verificação online** fica ativado por padrão. Ele resulta em uma detecção de [spam](#) mais precisa por meio da comunicação com os servidores [Mailshell](#), ou seja, os dados verificados serão comparados com o banco de dados [Mailshell](#) on-line.

Geralmente é recomendável manter as configurações padrão e alterá-las somente se houver um motivo para isso. Alterações na configuração devem ser feitas somente por usuários experientes!

9.7.3. RBL

O item **RBL** abre uma caixa de diálogo denominada **Realtime Blackhole Lists**:



Nessa caixa de diálogo, você pode ativar/desativar a função **Consultar servidores RBL**.

O servidor RBL (*Realtime Blackhole Lists*) é um servidor DNS com um amplo banco de dados de remetentes de spam. Quando esse recurso estiver ativado, todas as mensagens de e-mail serão verificadas no banco de dados do servidor RBL e marcadas como [spam](#), se forem idênticas a qualquer uma das entradas do banco de dados. Os bancos de dados dos servidores RBL contêm as impressões de spam atualizadas por minuto, mais recentes, para fornecer a melhor e mais precisa detecção de [spam](#). Este recurso é especialmente útil para usuários que recebem grandes quantidades de spam que não estão sendo detectados normalmente pelo mecanismo de [Anti-Spam](#).

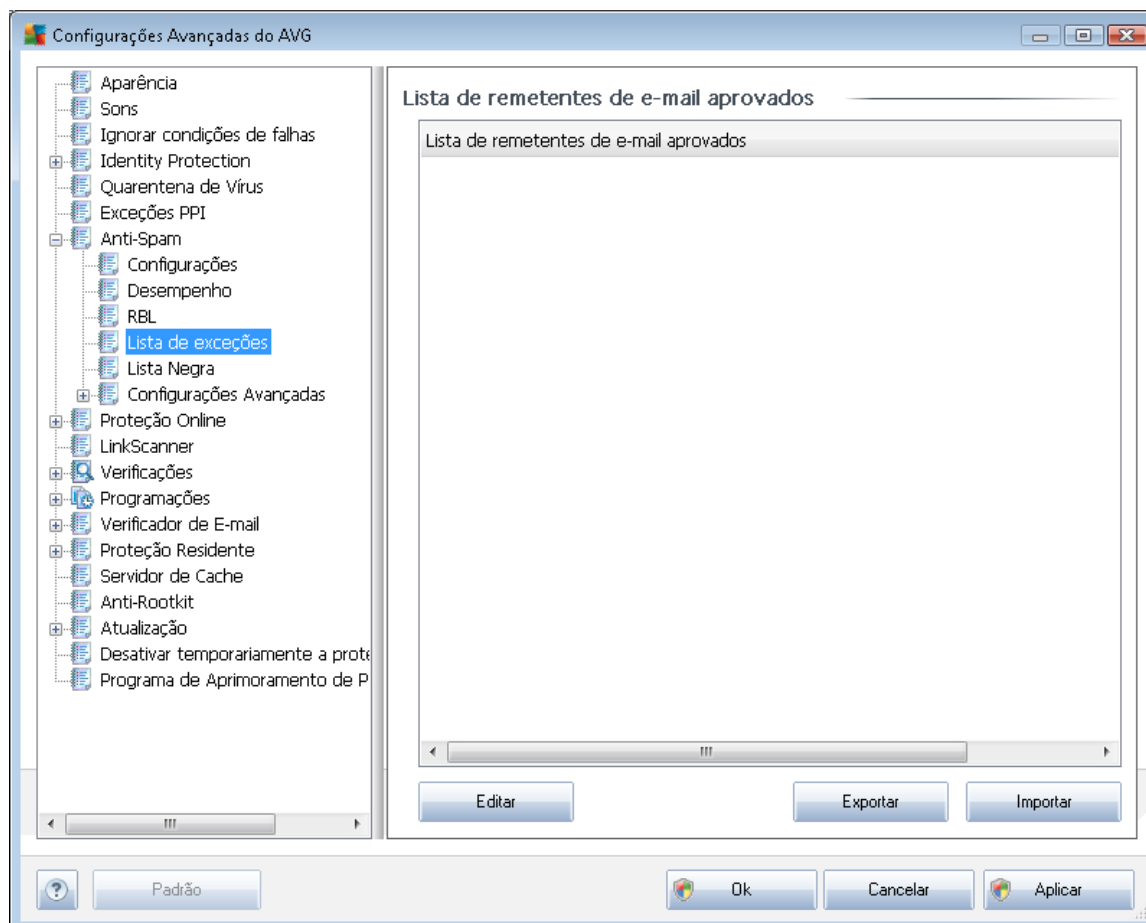
A **Lista de servidores RBL** permite definir locais de servidores RBL específicos.

Observação: ativar este recurso poderá reduzir a velocidade do processo de recebimento de e-mail em alguns sistemas e configurações, pois cada mensagem deve ser verificada no banco de dados do servidor RBL.

Nenhum dado pessoal é enviado ao servidor!

9.7.4. Lista de exceções

O item **Lista de exceções** abre uma caixa de diálogo denominada **Lista de remetentes de e-mail aprovados**, com uma lista global de endereços de e-mail e nomes de domínio de remetentes aprovados cujas mensagens nunca serão marcadas como [spam](#).



Na interface de edição, você pode compilar uma lista dos remetentes sobre os quais tem certeza de que não enviarão mensagens indesejáveis ([spam](#)). Você pode também compilar uma lista de nomes de domínio completos (como *avg.com*) que você sabe que não gera mensagens de spam.

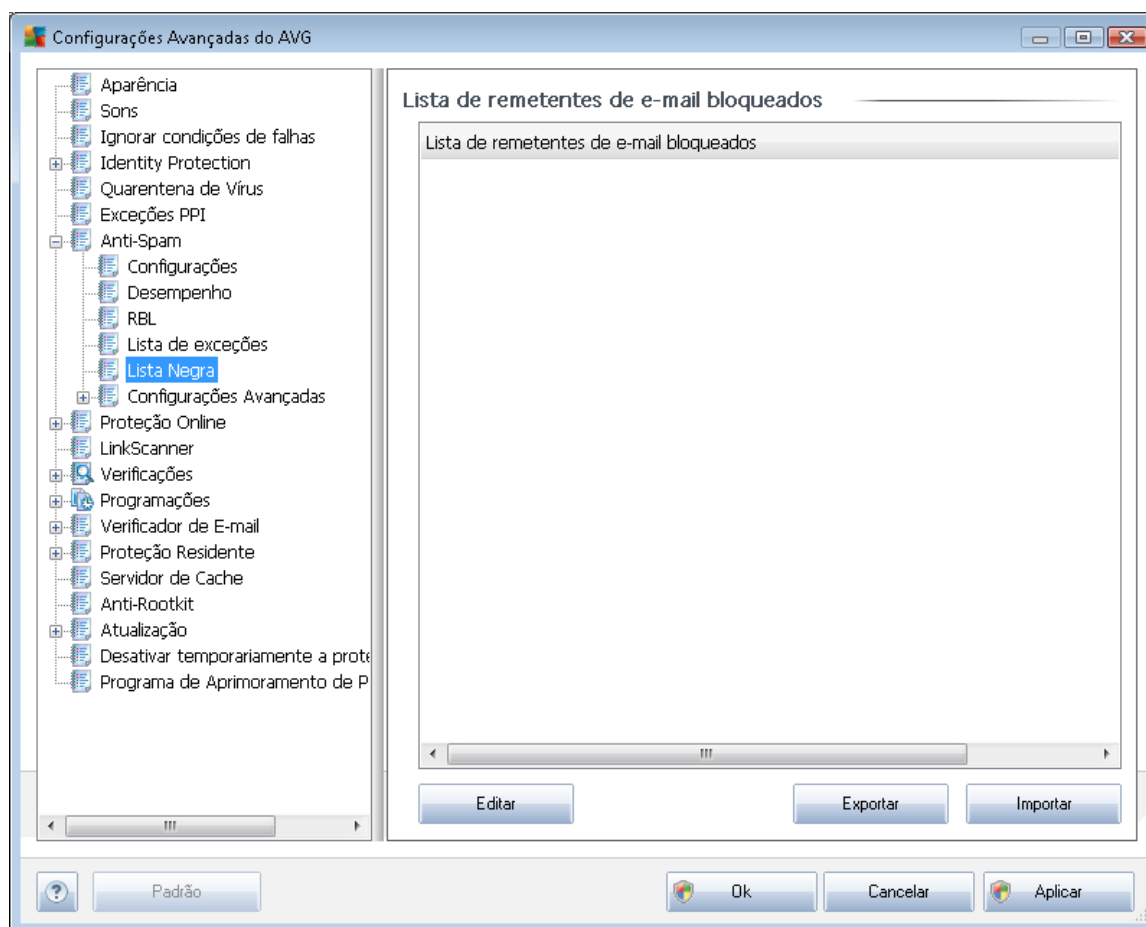
Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los digitando diretamente cada endereço de e-mail ou importando toda a lista de endereços de uma vez. Os seguintes botões estão disponíveis:

- **Editar** - pressione esse botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (*você também pode usar o método copiar/colar*). Insira um item (*remetente, nome do domínio*) por linha.
- **Exportar** - se, por algum motivo, você decidir exportar os registros, será possível fazê-lo pressionando esse botão. Todos os registros serão salvos em um arquivo de texto simples.
- **Importar** - se você já tiver um arquivo de texto com nomes de domínio/endereços de e-mail

preparado, poderá simplesmente importá-lo selecionando este botão. O conteúdo do arquivo deve conter somente um item (*endereço, nome de domínio*) por linha.

9.7.5. Lista negra

O item **Lista negra** abre uma caixa de diálogo com uma lista global de endereços de e-mail e nomes de domínio de remetentes bloqueados cujas mensagens sempre serão marcadas como [spam](#).



Na interface de edição, você pode compilar uma lista dos remetentes que você espera que enviem mensagens indesejáveis ([spam](#)). Você também pode compilar uma lista de nomes de domínio completos (*como [empresaqueenviaspam.com](#)*), dos quais espera receber mensagens de spam. Todos os endereços de e-mail/domínios listados serão identificados como spam.

Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los digitando diretamente cada endereço de e-mail ou importando toda a lista de endereços de uma vez. Os seguintes botões estão disponíveis:

- **Editar** - pressione esse botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (*você também pode usar o método copiar/colar*). Insira um item (*remetente, nome do domínio*) por linha.



- **Exportar** - se, por algum motivo, você decidir exportar os registros, será possível fazê-lo pressionando esse botão. Todos os registros serão salvos em um arquivo de texto simples.
- **Importar** - se você já tiver um arquivo de texto com nomes de domínio/endereços de e-mail preparado, poderá simplesmente importá-lo selecionando este botão.

9.7.6. Configurações avançadas

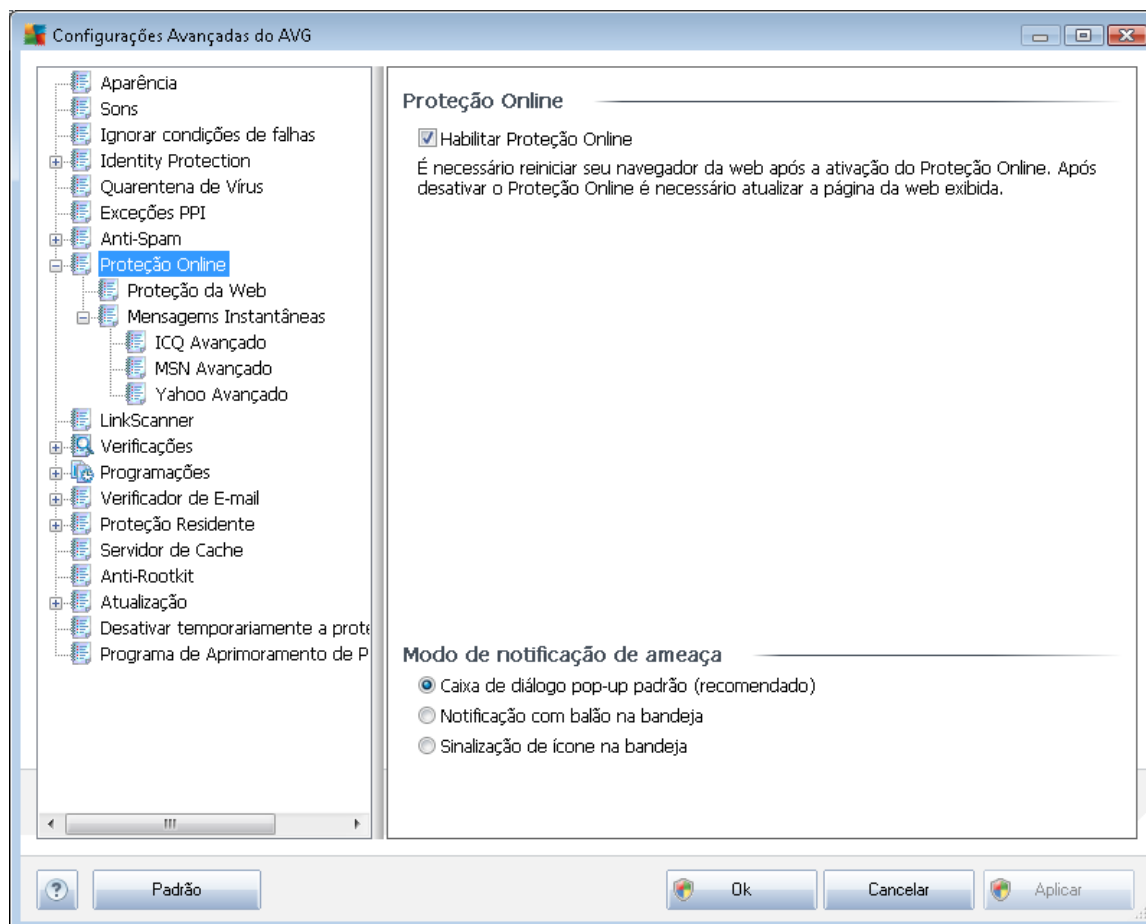
A seção Configurações avançadas contém várias opções de configuração para o componente Anti-Spam. Essas configurações se destinam a usuários experientes, principalmente administradores de rede que precisam configurar a proteção anti-spam em detalhes para a melhor proteção de servidores de e-mail. Por essa razão, não há ajuda adicional disponível para as caixas de diálogo individuais; entretanto, existe uma breve descrição de cada opção respectiva diretamente na interface do usuário.

É altamente recomendável não alterar as configurações, a menos que você esteja bastante familiarizado com as configurações avançadas do Spamcatcher (MailShell Inc.). Qualquer alteração inapropriada poderá resultar em mau desempenho ou no funcionamento incorreto do componente.

Se você ainda acredita que precisa alterar as configurações [Anti-Spam](#) no nível muito avançado, siga as instruções fornecidas diretamente na interface do usuário. Geralmente, em cada caixa de diálogo você encontrará um único recurso específico e poderá editá-lo. Sua descrição é sempre incluída na caixa.

- **Cache** - impressão digital, reputação do domínio, LegitRepute
- **Treinamento** - máximo de entradas de palavras, limite de treinamento automático, peso
- **Filtragem** - lista de idiomas, lista de países, IPs aprovados, IPs bloqueados, países bloqueados, conjunto de caracteres bloqueados, remetentes falsificados
- **RBL** - servidores RBL, vários acertos, limite, tempo limite, máximo de IPs
- **Conexão com a Internet** - tempo limite, servidor proxy, autenticação proxy

9.8. Proteção On-line



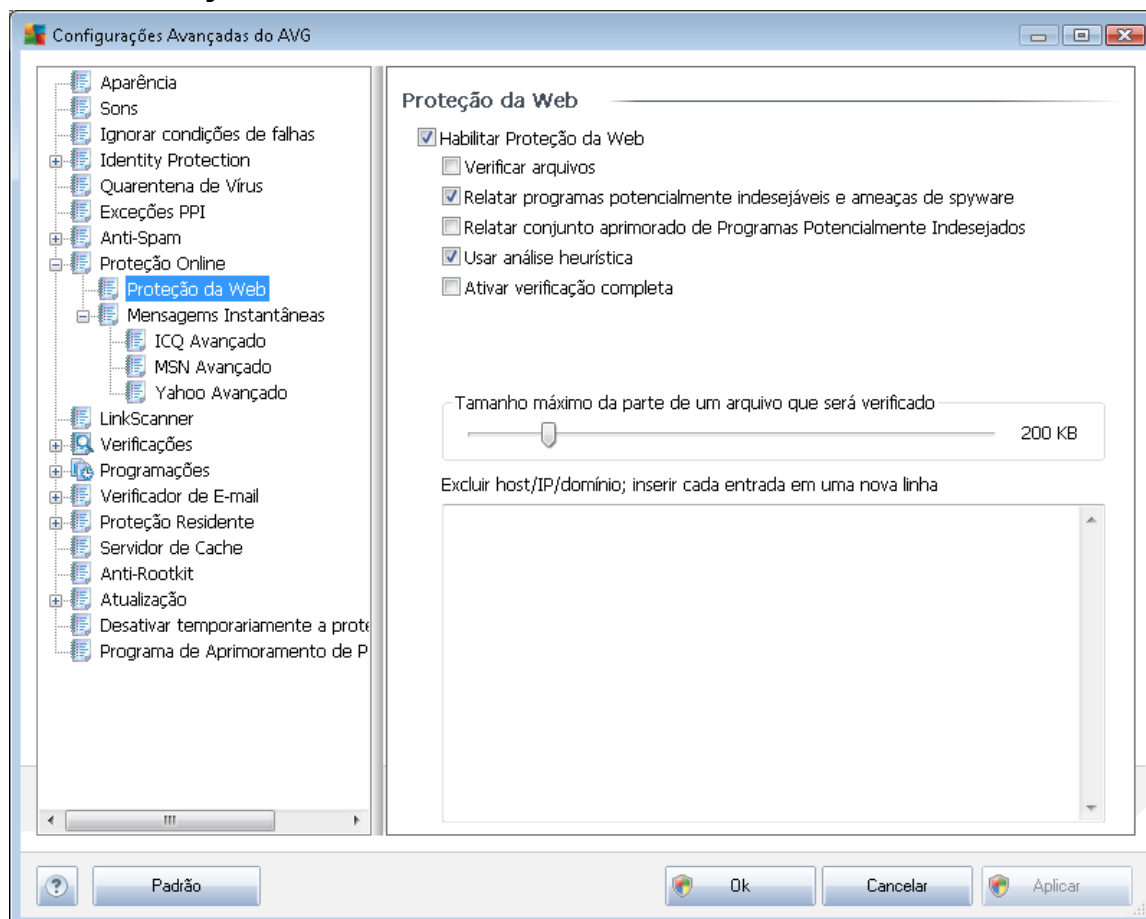
A caixa de diálogo **Proteção Online** permite ativar/desativar totalmente o componente **Proteção Online** por meio da opção **Ativar Proteção Online** (*ativada por padrão*). Para obter configurações mais avançadas sobre esse componente, continue nas caixas de diálogo seguintes, conforme relacionado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

- [Proteção da Web](#)
- [Mensagens Instantâneas](#)

Modo de notificação de ameaça

Na parte inferior da caixa de diálogo, selecione de que maneira você gostaria de ser informado sobre possíveis ameaças detectadas: por meio de uma caixa de diálogo pop-up, notificação de balão na bandeja ou nas informações de ícone na bandeja.

9.8.1. Proteção da Web



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

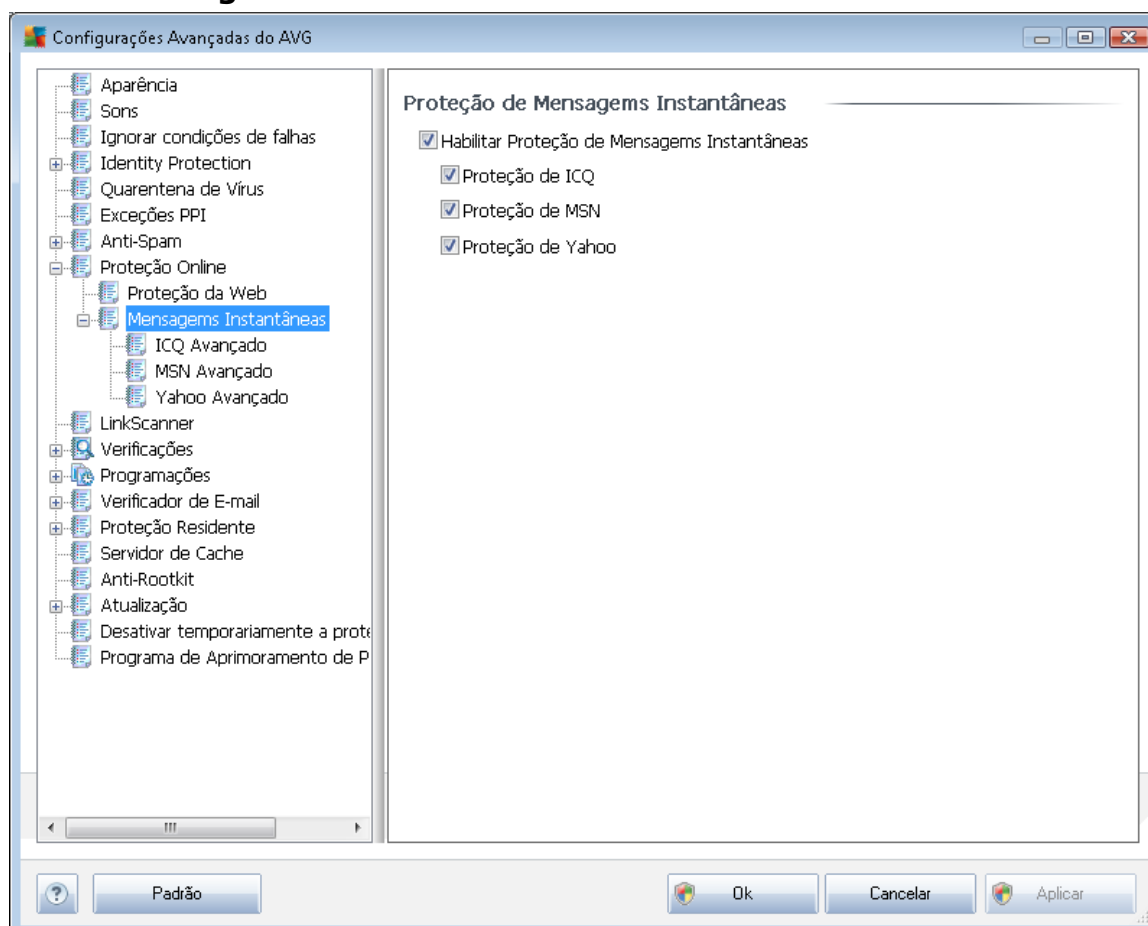
- **Ativar Proteção da Web** - essa opção confirma que o [Proteção Online](#) deve realizar a verificação do conteúdo das páginas www. Desde que essa opção esteja ativada (por padrão), você pode ativar/desativar estes itens:
 - o **Verificar arquivos** - (desativada por padrão): verifique o conteúdo dos arquivos possivelmente incluídos na página www a ser exibida.
 - o **Informar programas potencialmente indesejáveis e ameaças de spyware** – marque para ativar o mecanismo [Anti-Spyware](#) e [verificar spyware, bem como vírus](#). [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
 - o **Informar conjunto avançado de programas potencialmente indesejáveis** - (desativada por padrão): marque para detectar o pacote estendido de [spyware](#):



programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- o **Usar análise heurística** - (ativada por padrão): verifique o conteúdo da página a ser exibida usando o método de [análise heurística](#) (emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual).
- o **Ativar verificação completa** (desativada por padrão) - em situações específicas (suspeita de que seu computador foi infectado), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.
- o **Tamanho máximo de um arquivo a ser verificado** - se os arquivos incluídos estiverem presentes na página exibida, você também poderá verificar o conteúdo deles, mesmo antes que sejam baixados para seu computador. Entretanto, a verificação de arquivos grandes pode levar tempo e o download da página da Web pode ficar significativamente mais lento. Use a barra deslizante para especificar o tamanho máximo de um arquivo que ainda será verificado pela [Proteção Online](#). Mesmo se o arquivo baixado for maior que o especificado, deixando de ser verificado pela Proteção Online, você ainda estará protegido. Se o arquivo estiver infectado, a [Proteção Residente](#) o detectará imediatamente.
- o **Excluir host/IP/domínio** - no campo de texto você pode digitar o nome exato de um servidor (host, endereço IP, endereço IP com máscara ou URL) ou um domínio que não deve ser verificado pela [Proteção Online](#). Portanto, exclua apenas o host que você tenha certeza de que nunca permitirá conteúdo web perigoso.

9.8.2. Mensagens Instantâneas

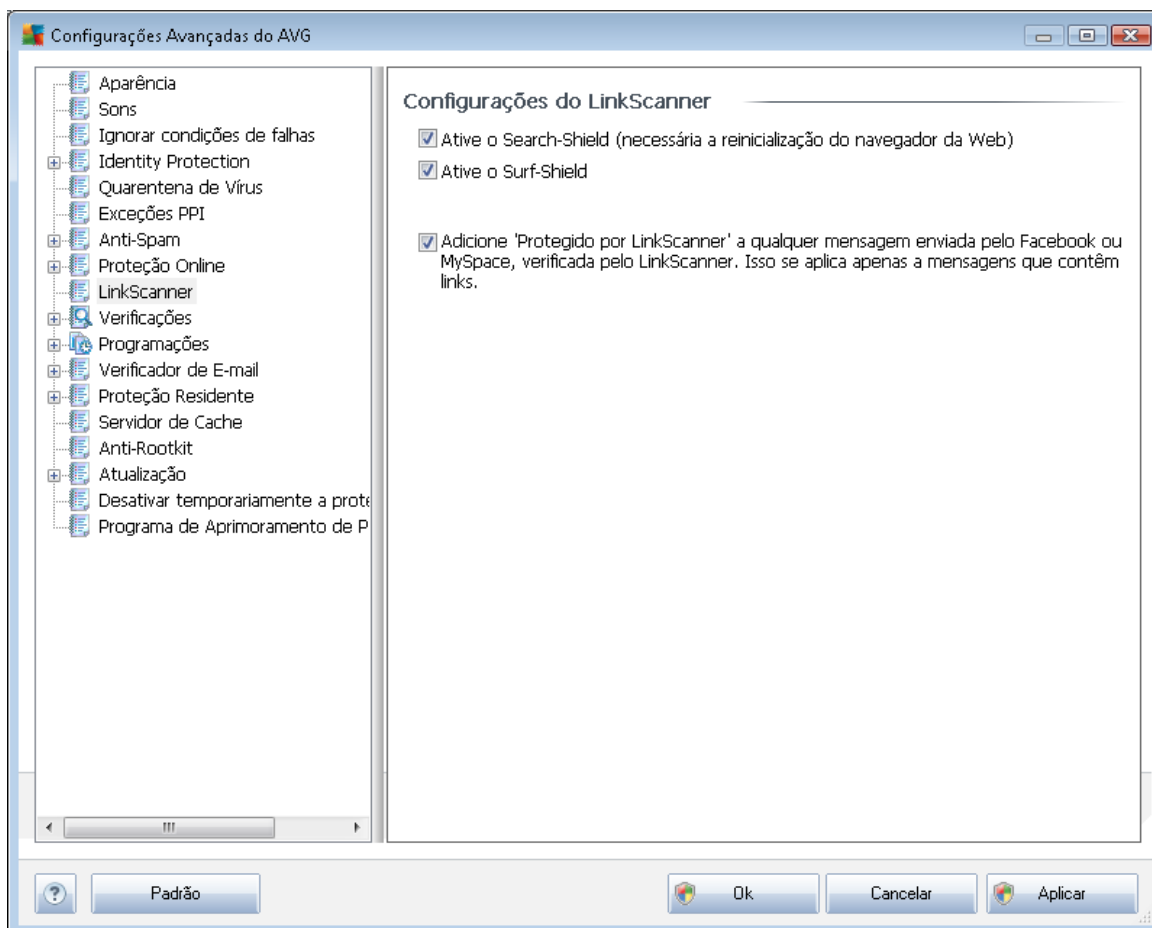


Na caixa de diálogo **Proteção de Mensagens Instantâneas**, é possível editar as configurações dos componentes da **Proteção Online** referentes à verificação de mensagens instantâneas. No momento, os três programas de mensagens instantâneas têm suporte: **ICQ**, **MSN** e **Yahoo** - marque o item apropriado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

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

9.9. Link Scanner

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



- **Habilitar o Search-Shield** - (*por padrão*): ícones de notificação consultiva em buscas realizadas com o Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ou SlashDot: verificarão adiante o conteúdo dos sites retornados pelo mecanismo de busca.
- **Ativar Surf-Shield** - (*ativo por padrão*): proteção ativa (*em tempo real*) contra sites exploradores à medida que são acessados. As conexões conhecidas com sites maliciosos e seu conteúdo exploratório são bloqueadas à medida que são acessados por meio de um navegador da Web ou outro aplicativo que utilize HTTP).
- **Adicionar "Protegido pelo LinkScanner" ...** - marque este item para confirmar que deseja inserir o aviso de certificação na verificação de todas as mensagens do **LinkScanner** que contêm hiperlinks ativos enviadas a partir das redes sociais Facebook e MySpace.



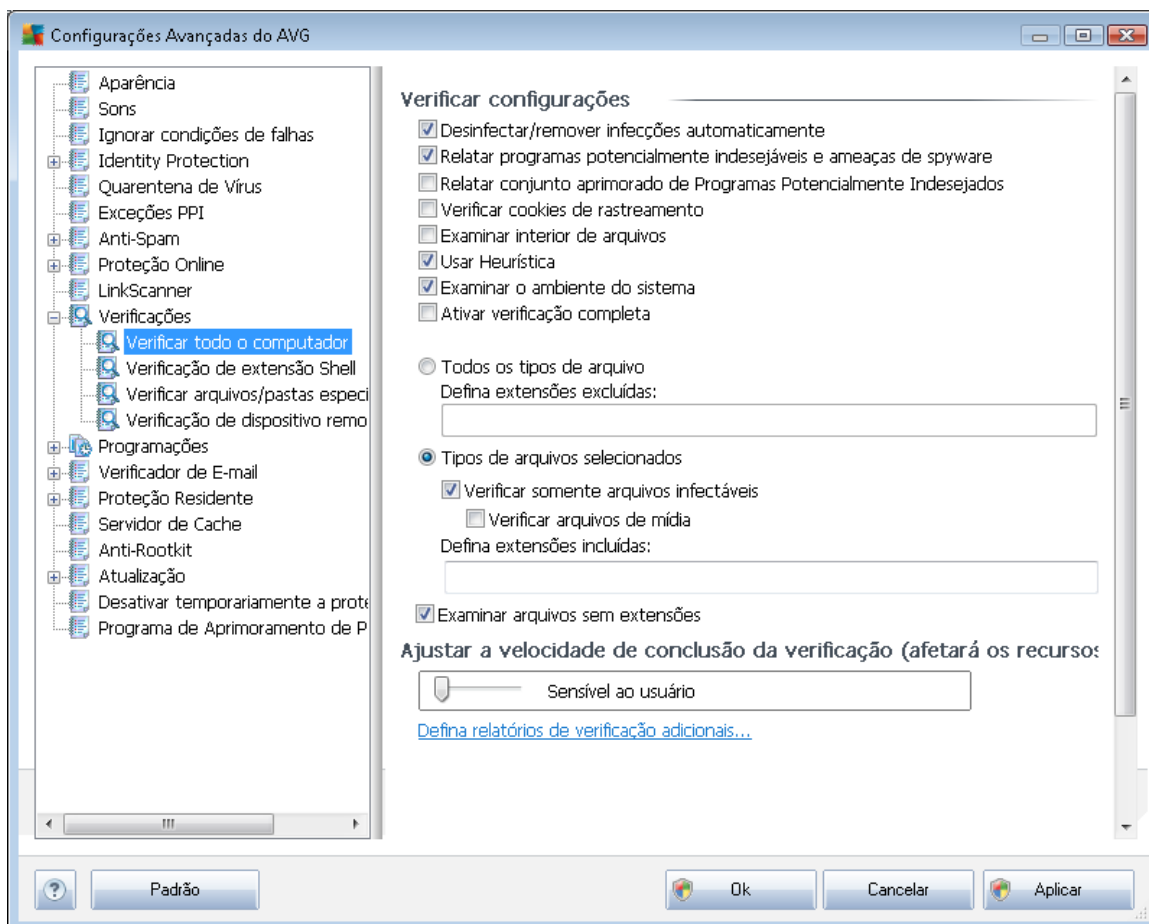
9.10. Verificações

As configurações de verificação avançadas 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 específicos](#) - verificação padrão predefinida de áreas selecionadas do computador
- [Verificação de dispositivos removíveis](#) - verificação específica de dispositivos removíveis conectados ao computador

9.10.1. 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** (ativada por padrão) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a [Quarentena de Vírus](#).
- **Informar programas potencialmente indesejáveis e ameaças de spyware** (ativada por padrão) - marque para ativar o mecanismo [Anti-Spyware](#) e verificar spyware, bem como vírus. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Informar conjunto avançado de programas potencialmente indesejáveis** (desativada por padrão) - marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.
- **Verificar cookies de rastreamento** (desativada por padrão) - este 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 de sites ou conteúdo de carrinhos de compras eletrônicas*)
- **Verificar dentro dos arquivos** (desativada por padrão) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.
- **Usar Heurística** (ativada 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** (ativada por padrão) - a verificação também atuará nas áreas do sistema do seu computador.
- **Ativar verificação completa** (desativada por padrão) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

Além disso, você deve decidir se deseja verificar

- **Todos os tipos de arquivos** com a possibilidade de definirem exceções a partir da

verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas) que não devem ser verificadas;

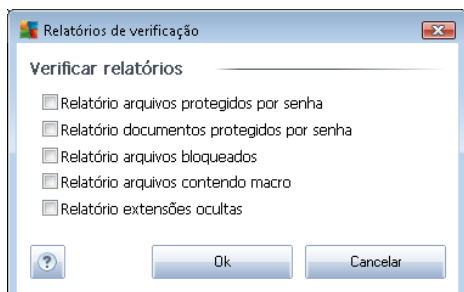
- **Tipos de arquivos selecionados** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
- Opcionalmente, você pode optar por **Verificar arquivos sem extensão** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

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

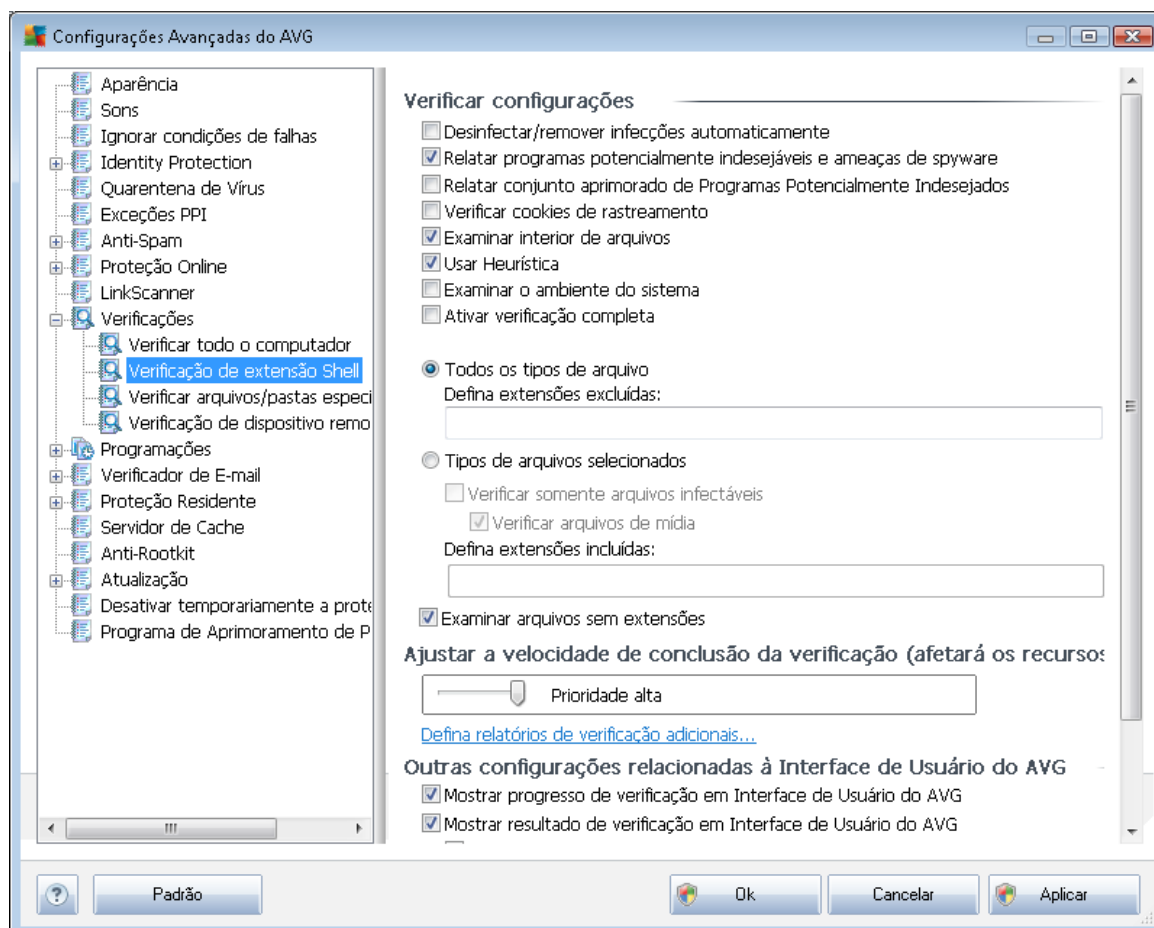
Defina relatórios de verificação adicionais...

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



9.10.2. Verificação da extensão shell

Da mesma forma que o item anterior, [Verificar todo o computador](#), este item, denominado **Verificação da extensão shell** também 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](#):



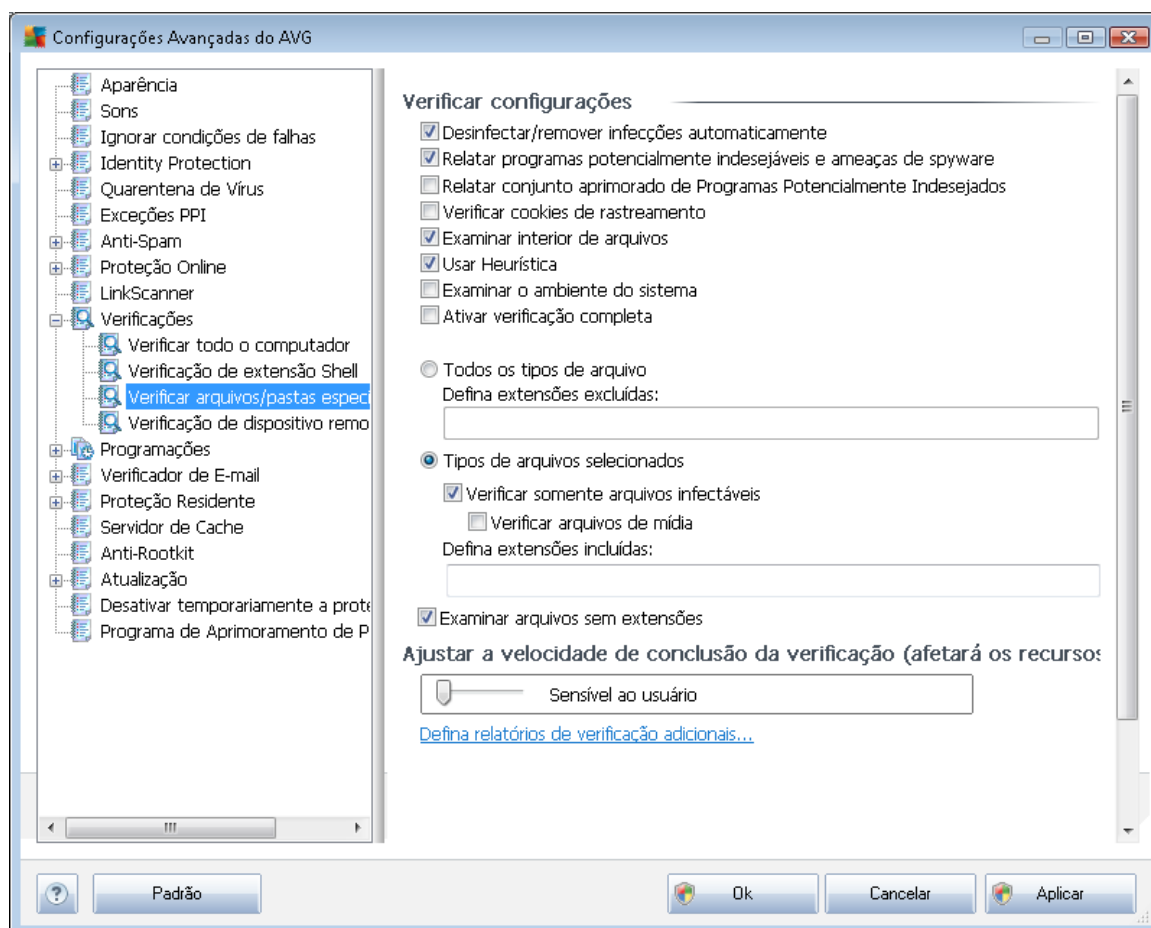
A lista de parâmetros é idêntica à disponível para [Verificar todo o computador](#). Entretanto, as configurações padrão são diferentes (por exemplo, *Verificar todo o computador*, por padrão, não verifica os arquivos, mas verifica o ambiente de sistema, ao passo que com a *Verificação da Extensão Shell*, é ao contrário).

Observação: para obter uma descrição dos parâmetros específicos, consulte o capítulo [Configurações avançadas do AVG/Verificações/Verificar todo o computador](#).

Em comparação com a caixa de diálogo [Verificar todo o computador](#), a caixa de diálogo *Verificação da extensão shell* também possui uma seção denominada **Outras configurações relacionadas à interface do usuário do AVG**, onde você pode especificar se deseja que o progresso da verificação e os resultados da verificação estejam acessíveis na interface do usuário do AVG. Além disso, você pode definir que o resultado da verificação seja exibido apenas se uma infecção for detectada durante a verificação.

9.10.3. Verificar arquivos ou pastas específicos

A interface de edição de *Verificar arquivos ou pastas específicos* é idêntica à caixa de diálogo de edição [Verificar todo o computador](#). Todas as opções de configuração são as mesmas, porém as configurações padrão são mais rigorosas em [Verificar todo o computador](#).

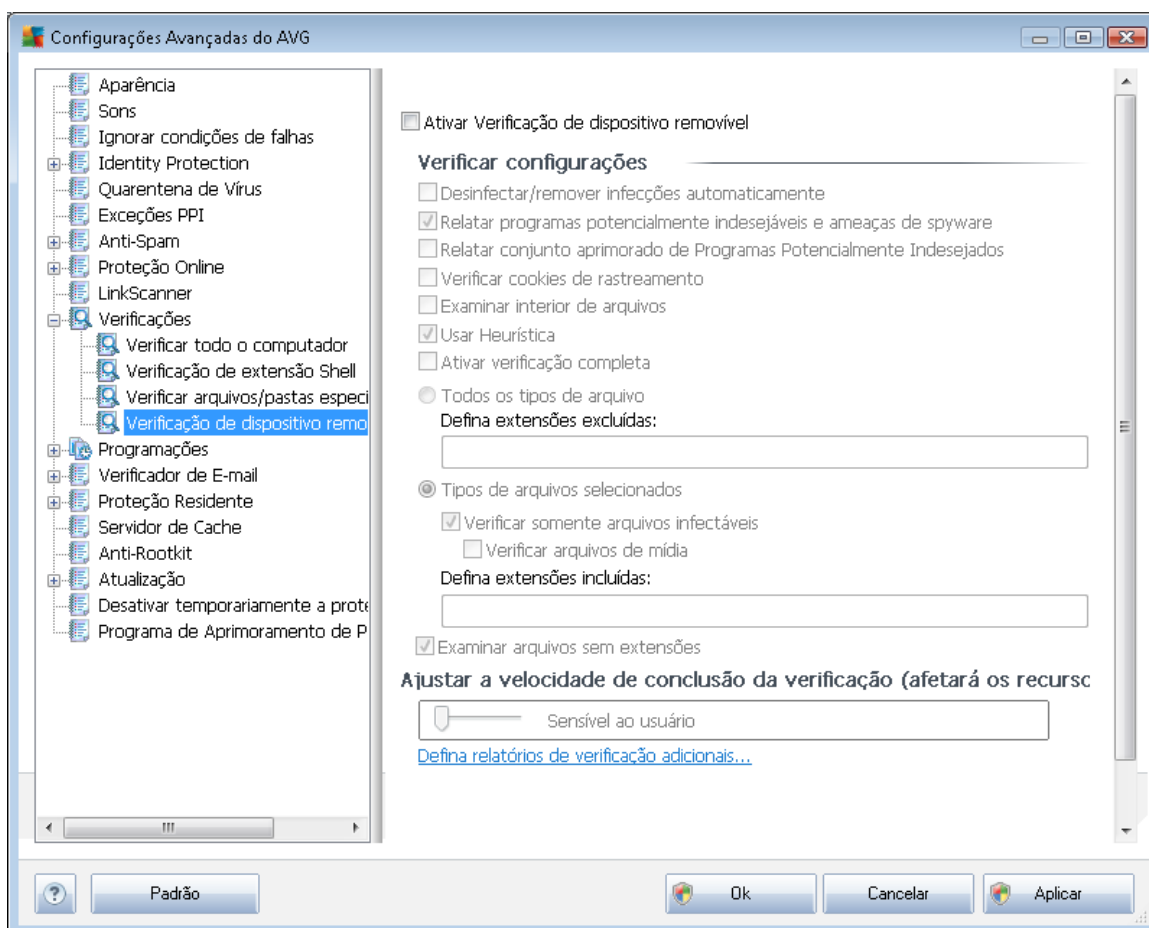


Todo os parâmetros definidos nesta caixa de diálogo de configuração são válidos somente para as áreas selecionadas para verificação com a [Verificação de arquivos ou pastas específicos](#)!

Observação: para obter uma descrição dos parâmetros específicos, consulte o capítulo [Configurações avançadas do AVG/Verificações/Verificar todo o computador](#).

9.10.4. 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](#).

9.11. Programações

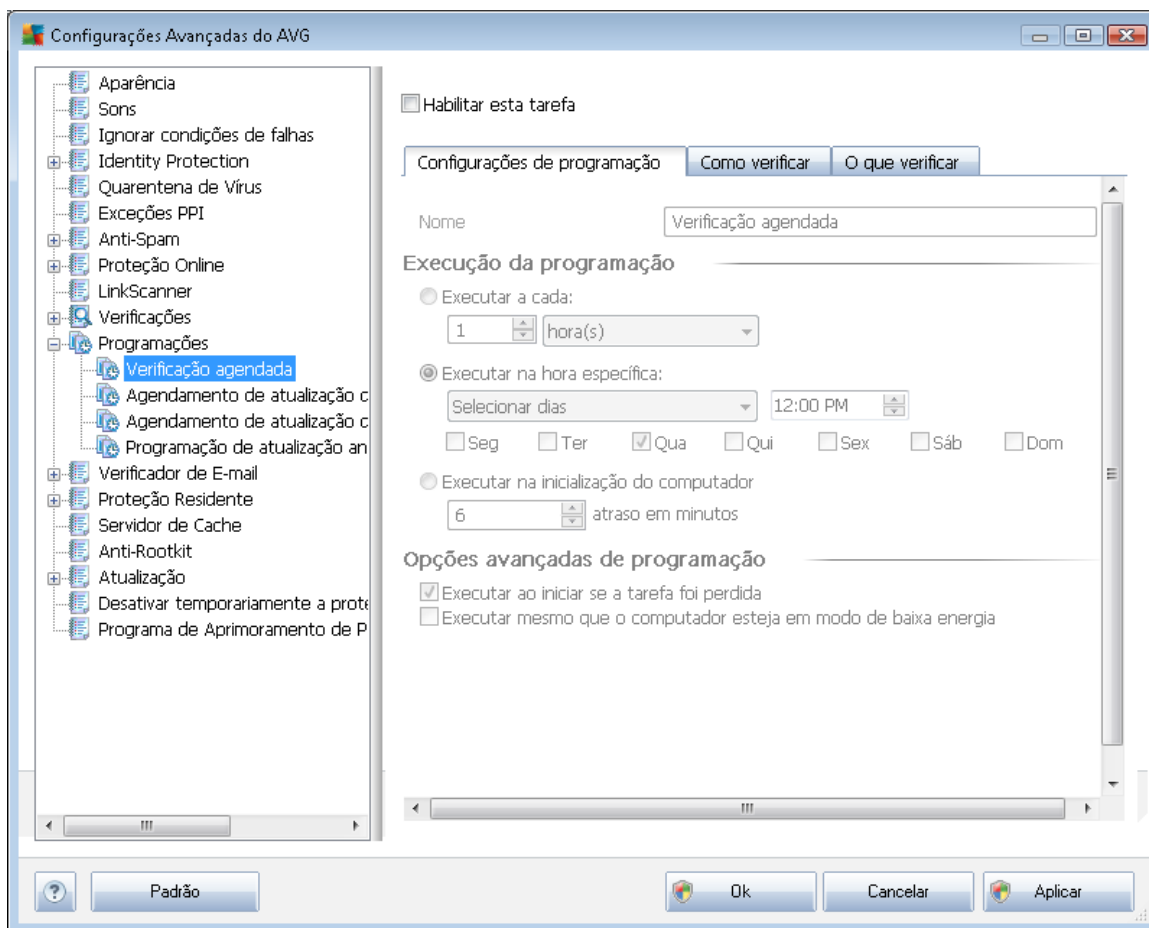
Na seção **Agendamentos**, é possível editar as configurações padrão de:

- [Verificação agendada](#)
- [Agendamento de atualização de banco de dados de vírus](#)

- [Agendamento de atualização de programa](#)
- [Agendamento de atualização do Anti-Spam](#)

9.11.1. Verificação programada

Os parâmetros da verificação agendada podem ser editados(*ou uma nova configuração de agenda*) em três guias. Em cada guia, você pode primeiro marcar/desmarcar o item **Habilitar esta tarefa** para simplesmente desativar temporariamente o teste agendado e ativá-lo novamente quando 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:

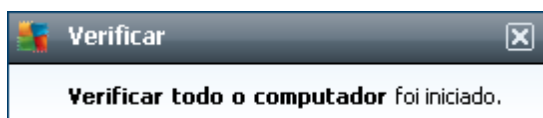
Execução da programação

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

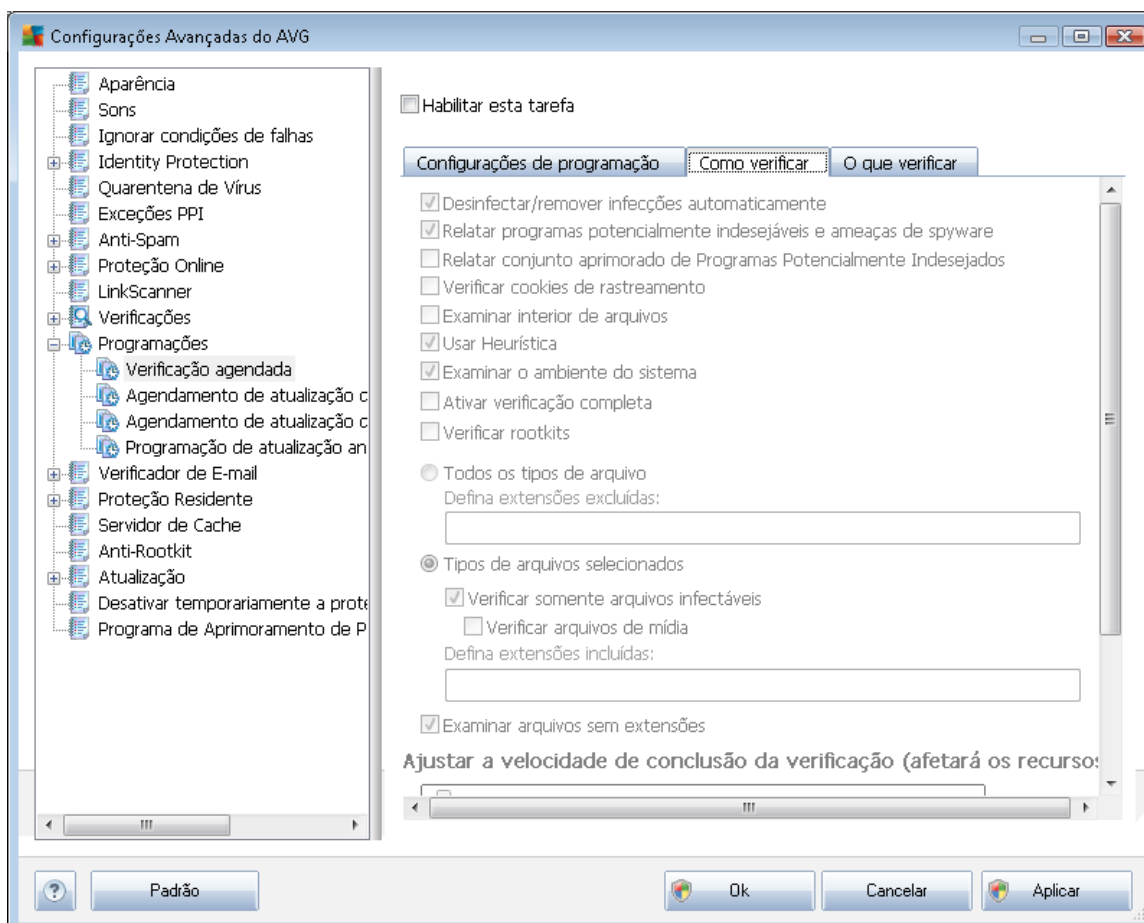
Essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

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 cores e com um holofote) informando que uma verificação agendada está em execução. Clique com o botão direito do mouse no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e também alterar a prioridade da verificação 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, ele poderá ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a [Quarentena de Vírus](#).
- **Informar programas potencialmente indesejáveis e ameaças de spyware** (ativada por padrão): marque para ativar o mecanismo [Anti-Spyware](#) e verificar se há spyware, bem como vírus. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Informar conjunto avançado de programas potencialmente indesejáveis** (desativada por padrão): marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas

podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- **Verificar cookies de rastreamento** (desativada por padrão): este 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 carrinhos de compras eletrônicas)
- **Verificar interior dos arquivos** (desativada por padrão): este parâmetro define que a verificação deve atuar em todos os arquivos, mesmo que eles estejam compactados em algum tipo de arquivo, como ZIP, RAR etc.
- **Usar Heurística** (ativada 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** (ativada por padrão): a verificação também atuará nas áreas do sistema do seu computador;
- **Ativar verificação completa** (desativada por padrão) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.
- **Verificar rootkits** (desativada por padrão): marque este item se desejar incluir a detecção de rootkit na verificação de todo o computador. A detecção de rootkit também está disponível por meio do componente [Anti-Rootkit](#);

Além disso, você deve decidir se deseja verificar

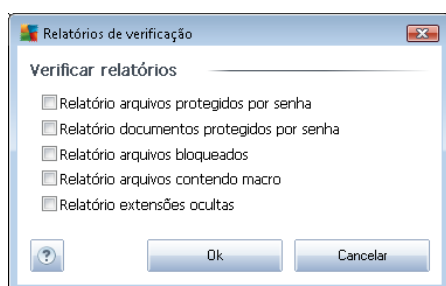
- **Todos os tipos de arquivos** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas)
- **Tipos de arquivos selecionados** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
- Opcionalmente, você pode optar por **Verificar arquivos sem extensão** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

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

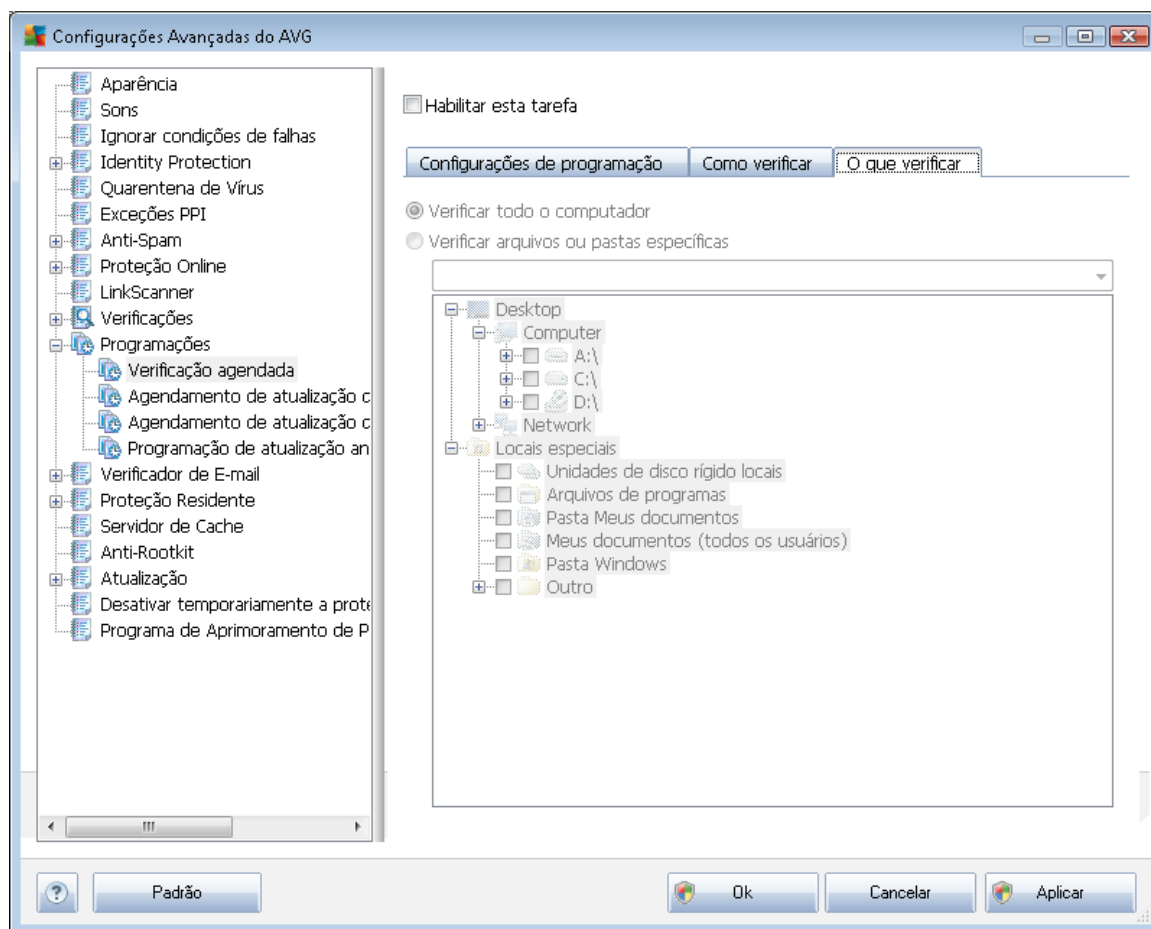
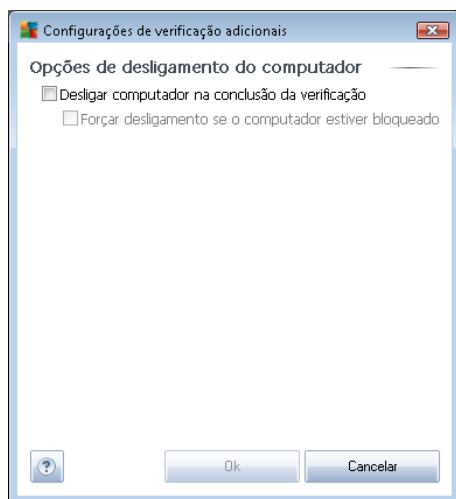
Defina relatórios de verificação adicionais

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



Configurações de verificação adicionais

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**).



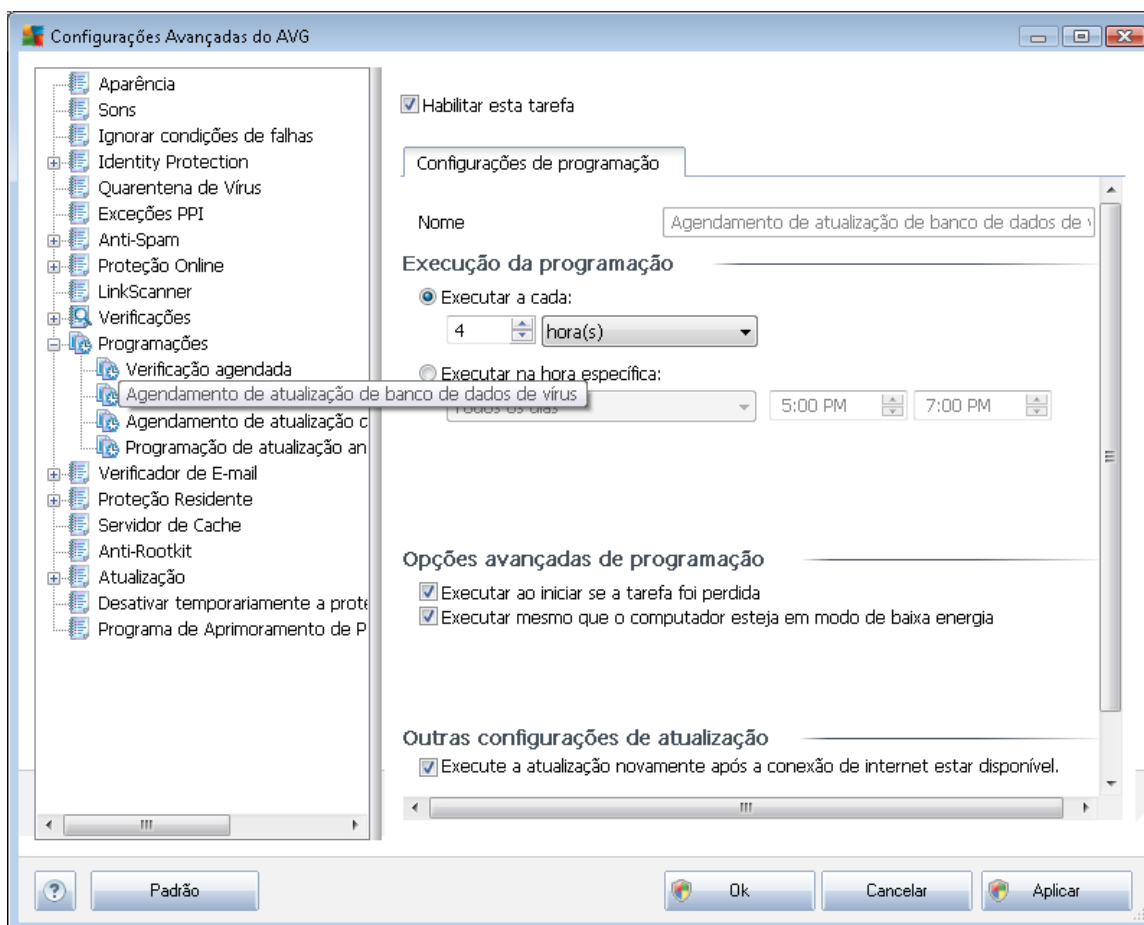
Na guia **O que verificar**, você pode definir se deseja programar a [verificação de todo o computador](#) ou a [verificação de arquivos ou pastas específicas](#). Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será



ativada e você poderá especificar as pastas para verificação.

9.11.2. Programação de atualização de banco de dados de vírus

Se for *realmente necessário*, você pode desmarcar o item **Ativar essa tarefa**, para simplesmente desativar temporariamente a atualização do banco de dados de vírus agendada, ativando-a mais tarde novamente:



O banco de dados básico de vírus é coberto no componente [Gerenciador de Atualização](#). Nessa caixa de diálogo, você pode configurar parâmetros detalhados de agendamento de atualização do banco de dados de vírus. No campo de texto denominado **Nome** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

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



Opções avançadas de programação

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

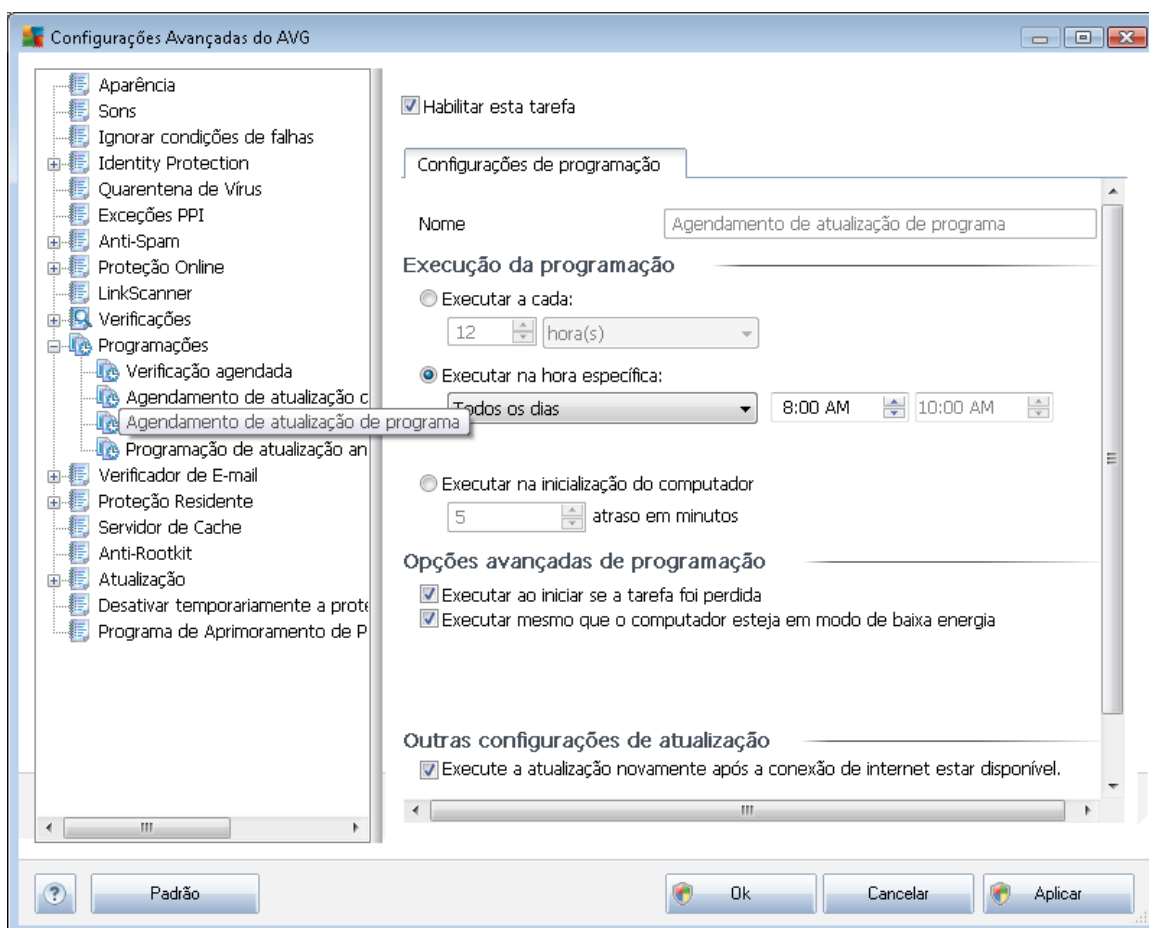
Outras configurações de atualização

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

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

9.11.3. Agendamento de atualização de programa

Se for *realmente necessário*, você pode desmarcar o item **Ativar essa tarefa** para simplesmente desativar temporariamente o programa de atualização agendado, ativando-o mais tarde novamente:



No campo de texto denominado **Nome** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

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

Opções avançadas de programação

Essa seção permite definir sob quais condições a atualização do programa deverá ou não ser



inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

Outras configurações de atualização

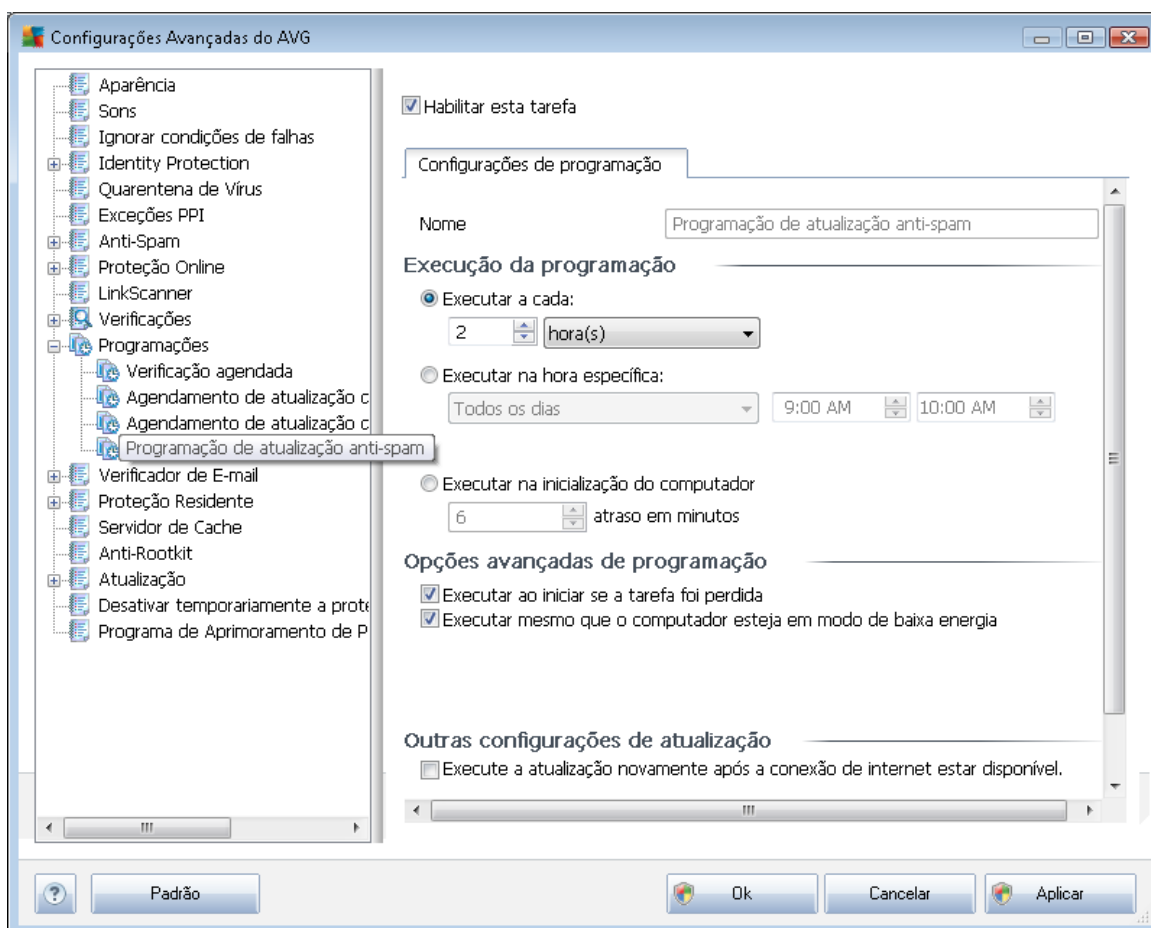
Marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

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

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

9.11.4. Agendamento de atualização do anti-spam

Se for **realmente necessário**, você pode desmarcar o item **Ativar essa tarefa** para desativar temporariamente a [atualização do Anti-Spam programada](#), e ligá-lo novamente mais tarde:



A programação da atualização básica do [Anti-Spam](#) é coberta no componente [Gerenciador de Atualizações](#). Nessa caixa de diálogo, você pode configurar parâmetros detalhados do programa de atualização. No campo de texto denominado **Nome** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Aqui, especifique os intervalos de tempo para a inicialização da atualização do [Anti-Spam](#) recém-programada. O tempo pode ser definido pela repetição da inicialização da atualização do [Anti-Spam](#) **depois de um certo 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 [Anti-Spam](#) deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

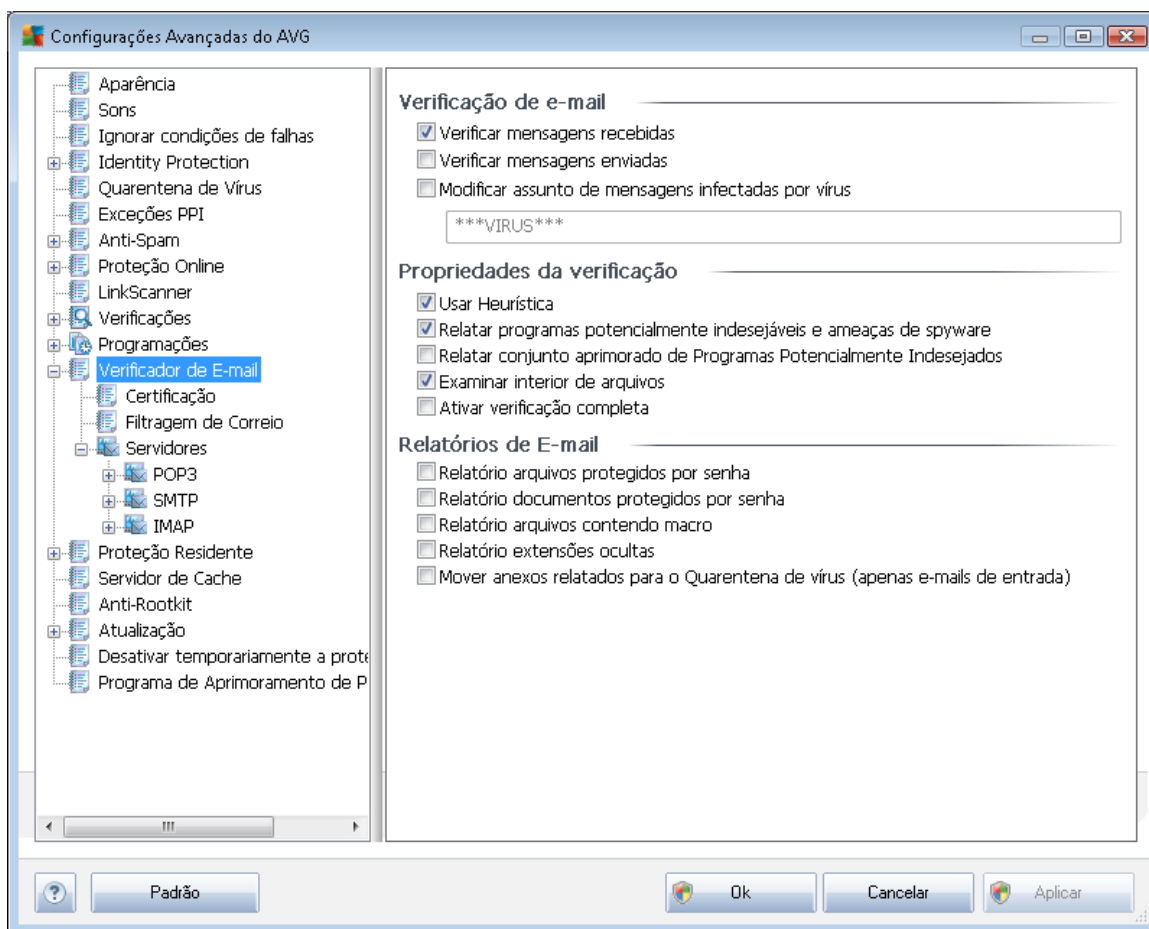
Outras configurações de atualização

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 do [Anti-Spam](#) falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

Assim que a verificação agendada 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](#)).

9.12. Verificador de e-mail

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





Verificação de e-mail

Nesta seção, você pode definir as funções básicas a seguir para mensagens de e-mail recebidas e/ou enviadas:

- **Verificar mensagens recebidas** (*ativada por padrão*) - marque para ativar/desativar a opção de verificação de todas as mensagens de email enviadas ao seu cliente de email
- **Verificar mensagens enviadas** (*desativada por padrão*) - marque para ativar/desativar a opção de verificação de todos os emails enviados de sua conta
- **Modificar assunto de mensagens infectadas por vírus** (*desativada por padrão*) - se quiser ser avisado de que a mensagem de email verificada foi considerada infecciosa, marque este item e digite o texto desejado no campo de texto. Esse texto será adicionado ao campo "Assunto" para cada mensagem de e-mail detectada para facilitar a identificação e filtragem. O valor padrão recomendável é *****VIRUS*****.

Propriedades da verificação

Nesta seção, você pode especificar como as mensagens de e-mail serão verificadas:

- **Usar Heurística** (*ativada por padrão*) - marque para usar o [método de detecção de heurística](#) ao verificar mensagens de e-mail. Quando essa opção está ativada, você pode filtrar anexos de e-mail não apenas por extensão, mas também o conteúdo real do anexo será considerado. A filtragem pode ser definida na caixa de diálogo [Filtragem de e-mail](#).
- **Informar programas potencialmente indesejáveis e ameaças de spyware** (*ativada por padrão*) - marque para ativar o mecanismo [Anti-Spyware](#) e verificar se há spyware e vírus. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Informar conjunto avançado de programas potencialmente indesejáveis** (*desativada por padrão*) - marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.
- **Verificar dentro de arquivos** (*ativada por padrão*) - marque para verificar os conteúdos de arquivos anexados às mensagens de e-mail.
- **Ativar verificação completa** (*desativada por padrão*) - em situações específicas (*por exemplo, suspeita de que seu computador foi infectado por vírus ou invadido*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.



Relatório de anexos de e-mail

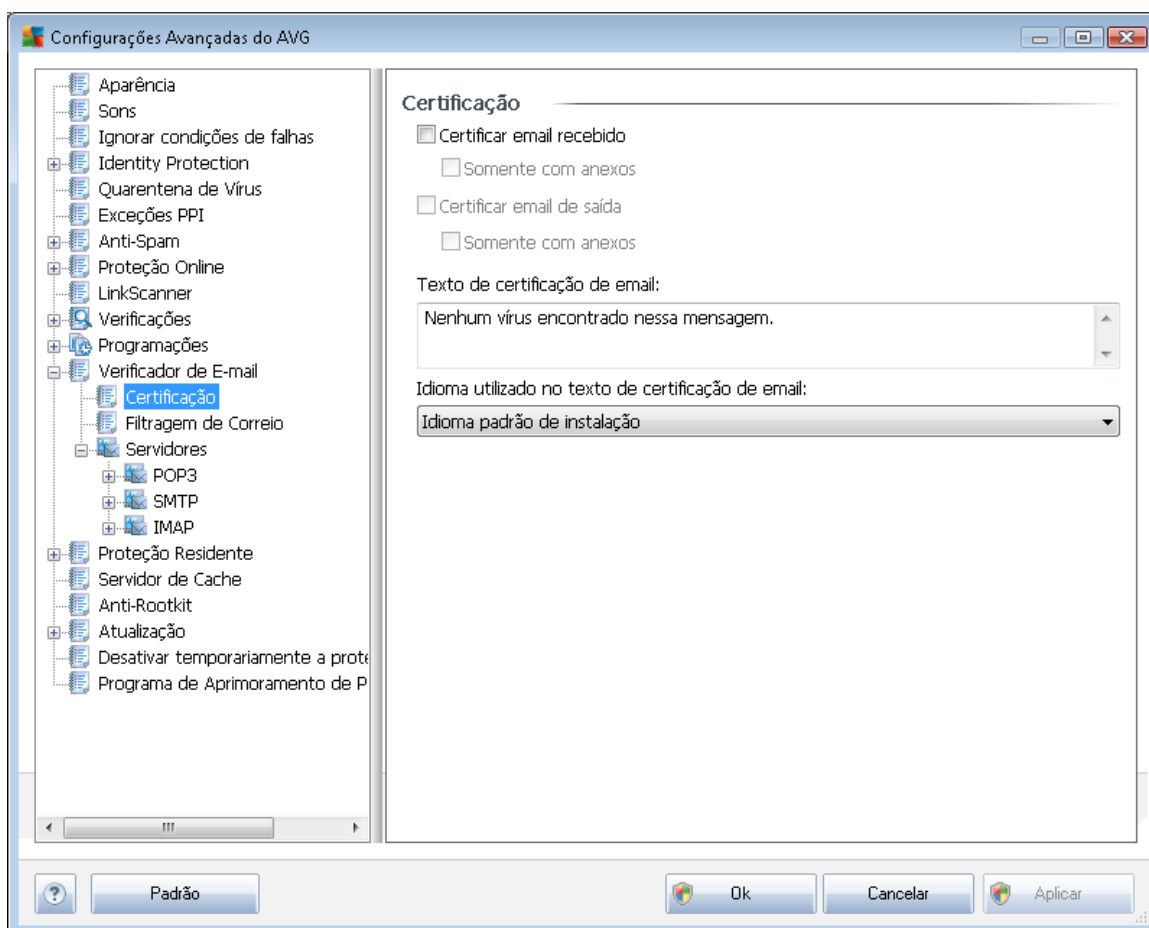
Nesta seção, você pode definir relatórios adicionais sobre arquivos potencialmente perigosos ou suspeitos. Observe que nenhuma caixa de diálogo de advertência será exibida, apenas um texto de certificação será adicionado ao final da mensagem de e-mail e todos esses relatórios serão listados na caixa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

- **Reportar arquivos protegidos por senha** – arquivos (ZIP, RAR etc.) protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa de seleção para reportá-los como potencialmente perigosos.
- **Reportar documentos protegidos por senha** – documentos protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa de seleção para reportá-los como potencialmente perigosos.
- **Reportar arquivos contendo macros** – uma macro é uma sequência predefinida de etapas com o objetivo de executar certas tarefas mais fáceis para um usuário (as macros do MS Word são amplamente conhecidas). Dessa forma, uma macro pode conter instruções potencialmente perigosas e convém você marcar a caixa de seleção para garantir que os arquivos com macros sejam reportados como suspeitos.
- **Reportar extensões ocultas** – extensões ocultas podem fazer um arquivo executável suspeito, "alguma coisa.txt.exe", por exemplo, parecer-se com um arquivo de texto comum inofensivo "alguma coisa.txt". Marque a caixa de seleção para reportá-los como potencialmente perigosos.
- **Mover anexos de e-mail informados para a área de Quarentena** - especifique se você deseja ser notificado por e-mail sobre arquivos protegidos por senha, documentos protegidos por senha, arquivos contendo macros e/ou arquivos com extensão oculta detectados como um anexo de uma mensagem de e-mail verificada. Se uma mensagem desse tipo for identificada durante a verificação, defina se o objeto infectado detectado deve ser movido para a [Quarentena](#).



9.12.1. Certificação

Na caixa de diálogo **Certificação**, você pode especificar o texto e o idioma da certificação para as mensagens recebidas e enviadas:



O texto de certificação consiste em duas partes, parte do usuário e parte do sistema - veja o seguinte exemplo: a primeira linha representa a parte do usuário, o restante é gerado automaticamente:

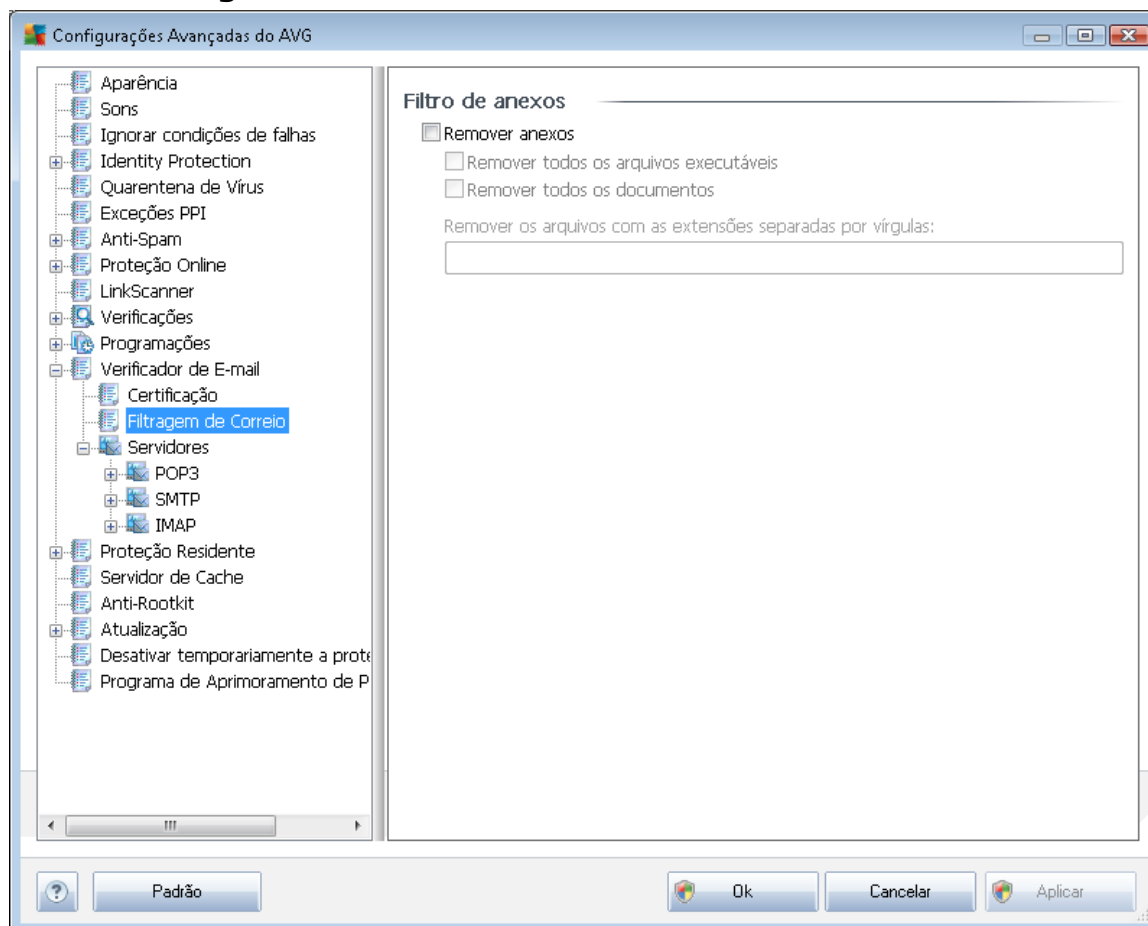
Nenhum vírus encontrado nessa mensagem.

Verificado pelo AVG.

Versão: x.y.zz / Banco de dados de vírus: xx.y.z - Data de lançamento: 12/9/2010

Se decidir usar a certificação das mensagens de email recebidas e enviadas, você poderá mais adiante nessa caixa de diálogo especificar o conteúdo exato da parte do usuário do texto de certificação (**Texto de certificação de email**) e escolher qual idioma deve ser usado para a parte gerada automaticamente pelo sistema da certificação (**Idioma usado para o texto de certificação de email**).

9.12.2. Filtragem de correio

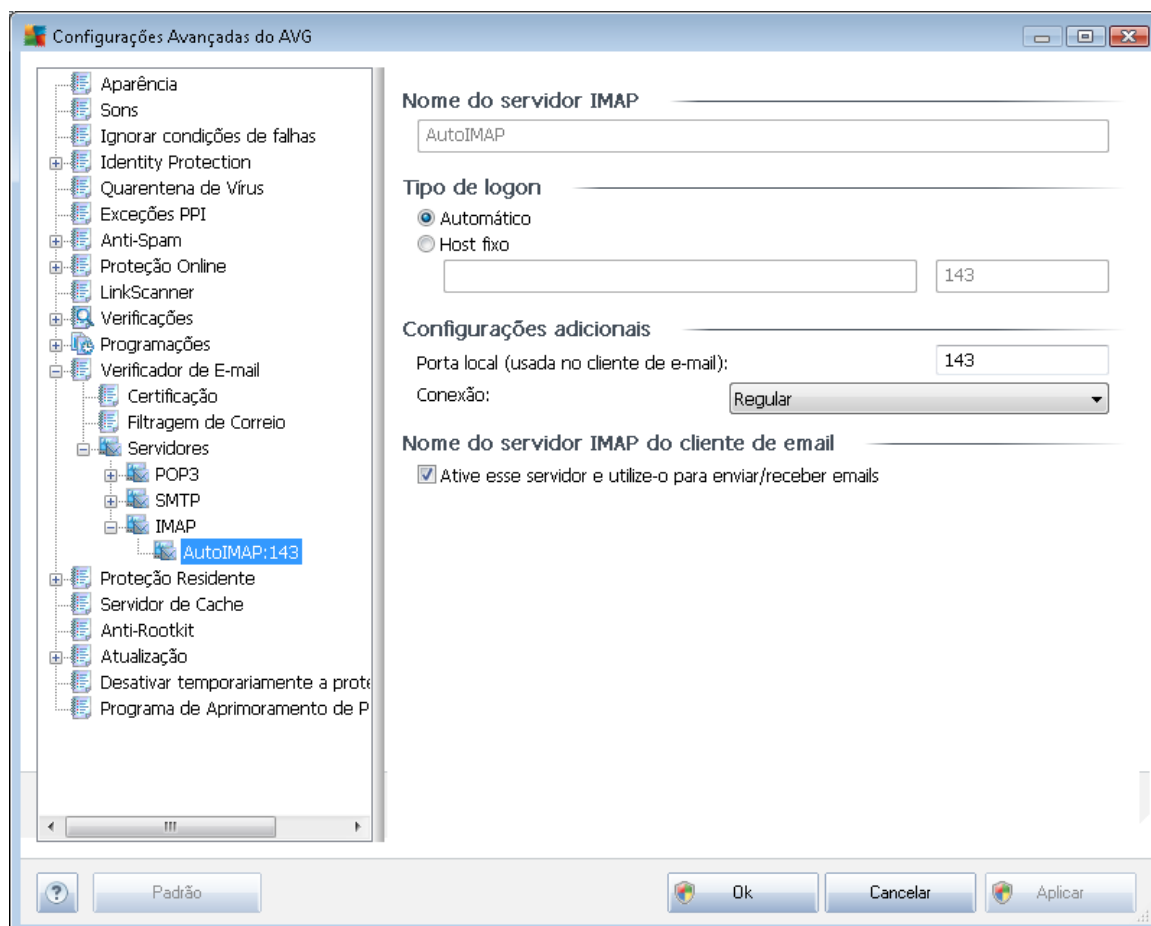


A caixa de diálogo **Filtro de anexo** permite configurar parâmetros para a verificação de anexos de mensagens de e-mail. Por padrão, a opção **Remover anexos** é desativada. Se você desejar ativá-la, todos anexos de mensagens de e-mail detectados como infectados ou potencialmente perigosos serão removidos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

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

9.12.3. Servidores

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

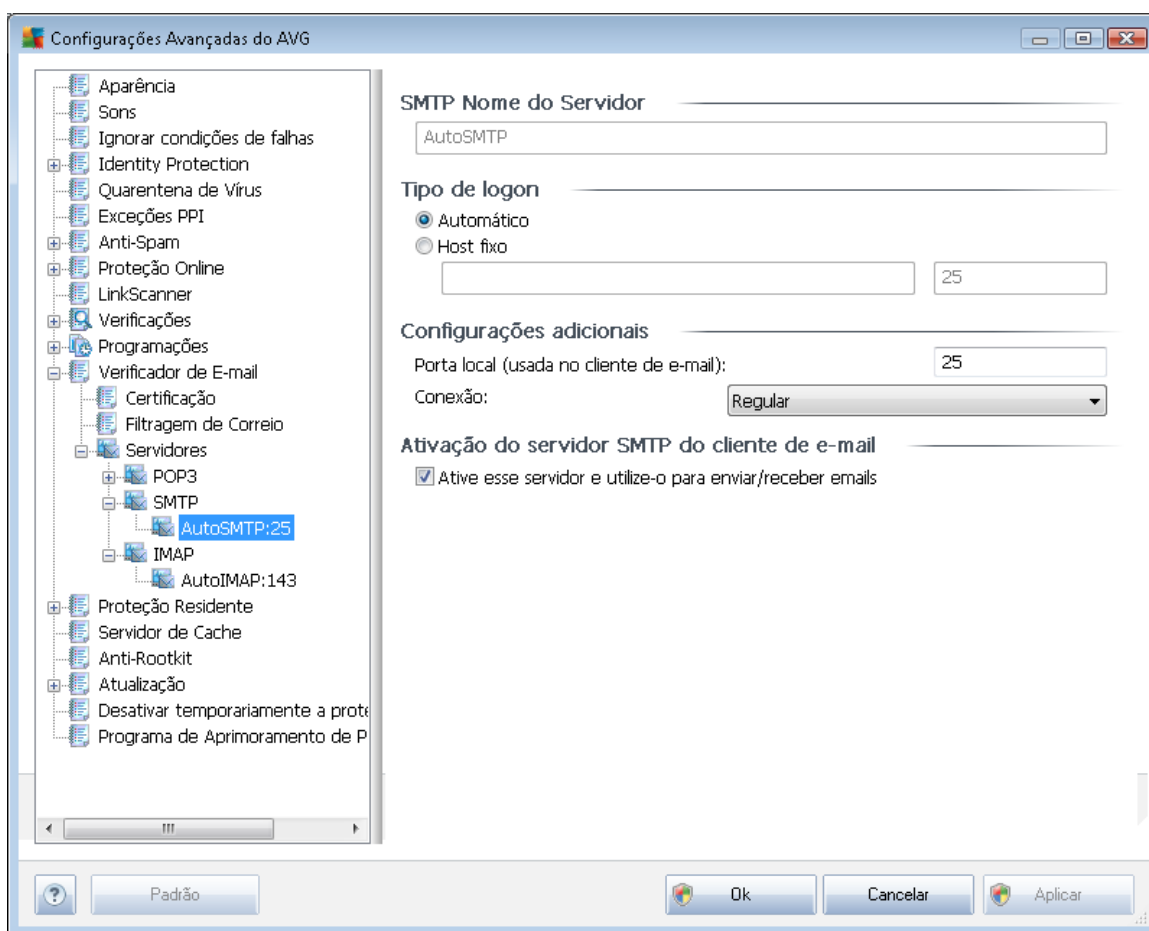


Nessa caixa de diálogo (aberta via **Servidores/POP3**), você pode configurar um novo servidor do **Verificador de E-mail** usando o protocolo POP3 para e-mails recebidos:

- **Nome do Servidor POP3** - neste campo, é possível especificar o nome dos servidores recém-adicionados (para adicionar um servidor POP3, clique com o botão direito do mouse sobre o item POP3 do menu de navegação esquerdo). Para o servidor "AutoPOP3" criado automaticamente, este campo fica desativado.
- **Tipo de login** - define o método para determinar o servidor de e-mail usado para e-mails recebidos:
 - o **Automático** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail.
 - o **Host fixo** - Nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mail. O nome de login permanecerá inalterado. Para um nome, você pode usar um nome de domínio (por exemplo, pop.acme.com) assim como um endereço IP (por exemplo, 123.45.67.89). Se o servidor de e-mail usar uma porta não padrão, você poderá especificar essa porta depois do nome do servidor usando um ponto-e-vírgula como delimitador (por

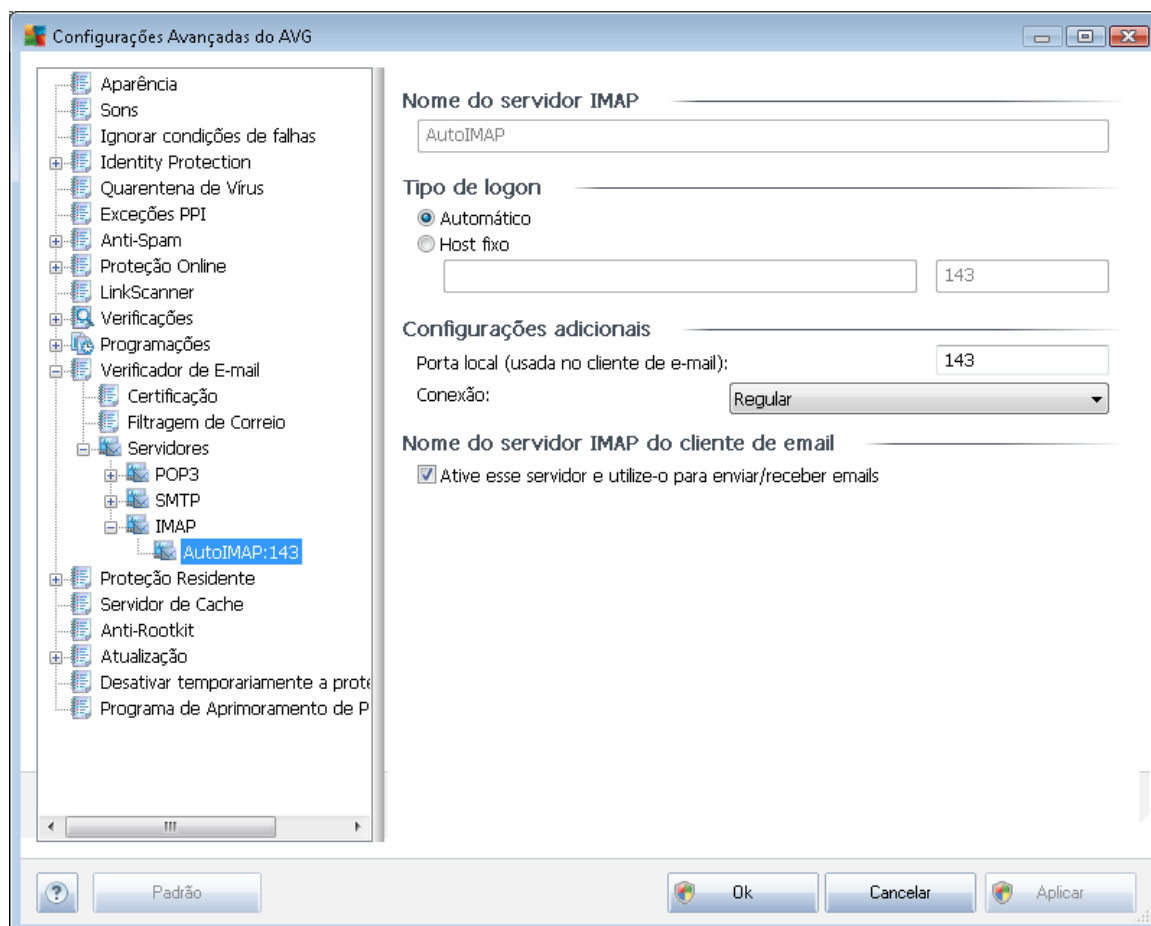
exemplo, *pop.acme.com:8200*). A porta padrão para a comunicação POP3 é 110.

- **Configurações adicionais** - especifica parâmetros mais detalhados:
 - o **Porta local** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação POP3.
 - o **Conexão** - no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso estará disponível somente quando houver suporte no servidor de e-mail de destino.
- **Ativação do servidor POP3 do cliente de e-mail** - marque/desmarque esse item para ativar ou desativar o servidor POP3 especificado



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

- **Nome do Servidor SMTP** - neste campo, é possível especificar o nome dos servidores recém-adicionados (*para adicionar um servidor SMTP, clique com o botão direito do mouse sobre o item SMTP do menu de navegação esquerdo*). Para o servidor "AutoSMTP" criado automaticamente, este campo fica desativado.
- **Tipo de login** - define o método para determinar o servidor de e-mail usado para e-mails enviados:
 - o **Automático** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail
 - o **Host fixo** - nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mails. Você pode usar um nome de domínio (*por exemplo, smtp.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de e-mail usar uma porta não padrão, você poderá digitar essa porta depois do nome do servidor usando dois pontos como delimitador (*por exemplo, smtp.acme.com:8200*). A porta padrão para a comunicação SMTP 25 é.
- **Configurações adicionais** - especifica parâmetros mais detalhados:
 - o **Porta local** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação SMTP.
 - o **Conexão** - no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso está disponível somente quando houver suporte no servidor de e-mail de destino.
- **Ativação do servidor SMTP do cliente de e-mail** - marque/desmarque esse item para ativar ou desativar o servidor SMTP especificado



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

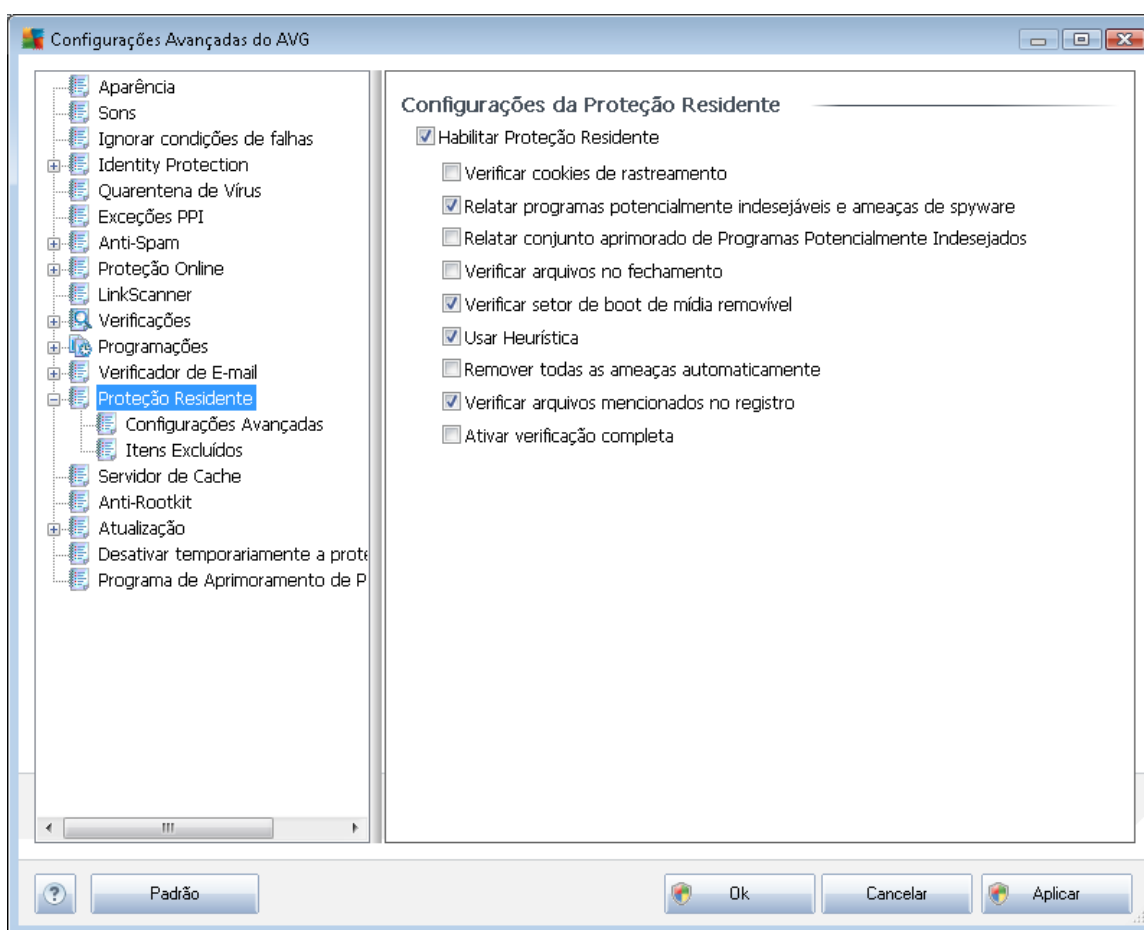
- **Nome do Servidor IMAP** - neste campo, é possível especificar o nome dos servidores recém-adicionados (*para adicionar um servidor IMAP, clique com o botão direito do mouse sobre o item IMAP do menu de navegação esquerdo*). Para o servidor "AutoIMAP" criado automaticamente, este campo fica desativado.
- **Tipo de login** - define o método para determinar o servidor de e-mail usado para e-mails enviados:
 - o **Automático** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail
 - o **Host fixo** - nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mails. Você pode usar um nome de domínio (*por exemplo, smtp.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de e-mail usar uma porta não padrão, você poderá digitar essa porta depois do nome do servidor usando dois pontos como delimitador (*por exemplo, imap.acme.com:8200*). A porta padrão para a

comunicação IMAP é 143.

- **Configurações adicionais** - especifica parâmetros mais detalhados:
 - o **Porta local** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação IMAP
 - o **Conexão** - no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso está disponível somente quando houver suporte no servidor de e-mail de destino.
- **Ativação do servidor IMAP do cliente de e-mail** - marque/desmarque este item para ativar ou desativar o servidor IMAP especificado acima

9.13. Proteção Residente

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



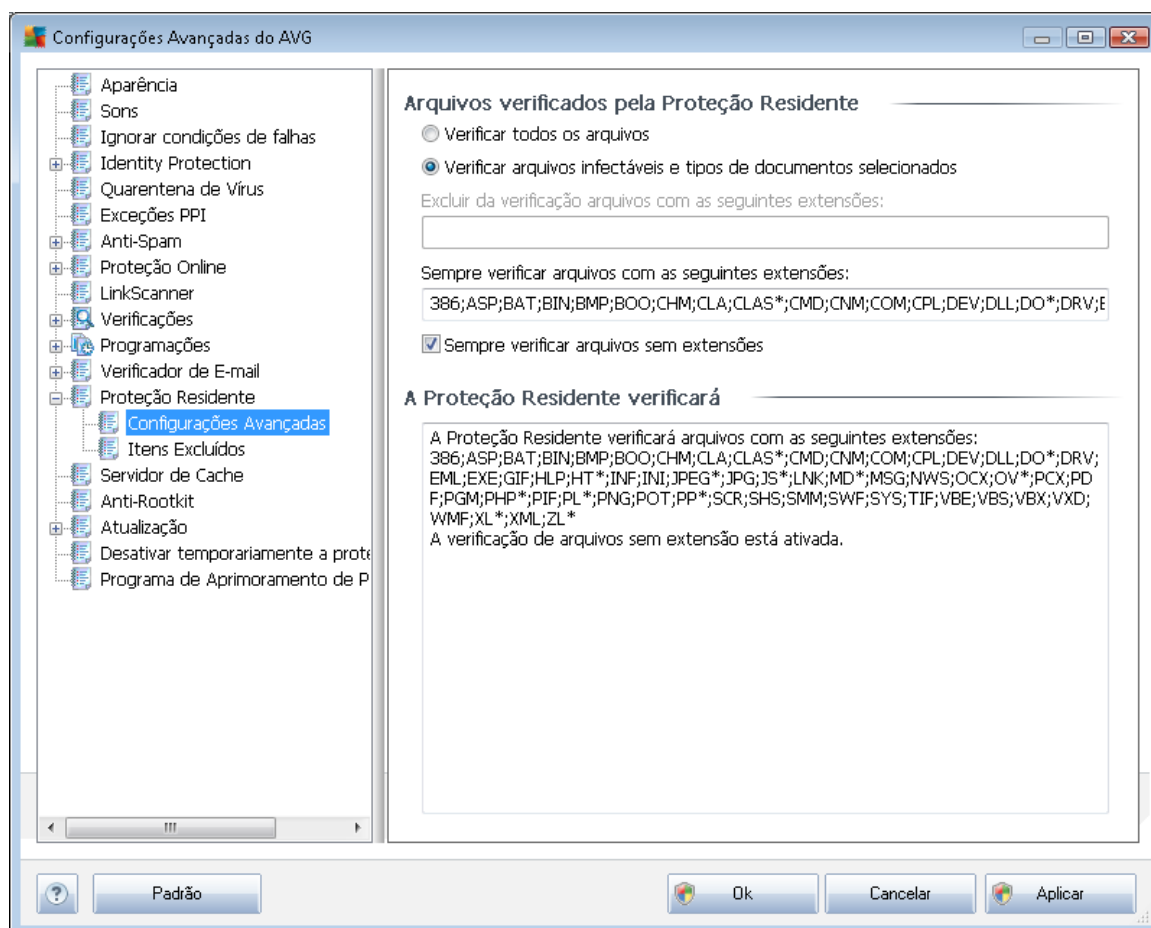


Na caixa de diálogo **Configurações da Proteção Residente**, é possível ativar ou desativar a **Proteção Residente** completamente marcando/desmarcando o item **Ativar Proteção Residente** (essa opção é ativada por padrão). Além disso, você pode selecionar quais recursos da **Proteção Residente** devem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

- **Verificar cookies de rastreamento** (desativada por padrão) - esse parâmetro define que os cookies devem ser detectados durante a verificação. (Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas)
- **Informar programas potencialmente indesejáveis e ameaças de spyware** – marque para ativar o mecanismo **Anti-Spyware** e **verificar spyware, bem como vírus**. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Informar conjunto avançado de programas potencialmente indesejáveis** (desativada por padrão) - marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.
- **Verificar arquivos no fechamento** (desativada por padrão) - 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** (ativada por padrão)
- **Usar Heurística** - (ativada por padrão) [a análise heurística](#) será usada para detecção (emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual)
- **Remover todas as ameaças automaticamente** (por padrão desativado) - se houver solução disponível, qualquer infecção detectada é reparada automaticamente, e todas as infecções que não puderem ser solucionadas serão removidas.
- **Verificar arquivos mencionados no registro** (ativada por padrão) - este parâmetro define que o AVG verificará todos os arquivos executáveis adicionados ao registro de inicialização para evitar que uma infecção conhecida seja executada na próxima inicialização do computador.
- **Ativar verificação completa** (desativada por padrão) - em situações específicas (em um estado de extrema emergência), você pode marcar esta opção para ativar os algoritmos mais completos que verificarão todos os objetos de ameaça possíveis minuciosamente. Entretanto, lembre-se de que esse método consome bastante tempo.

9.13.1. Configurações avançadas

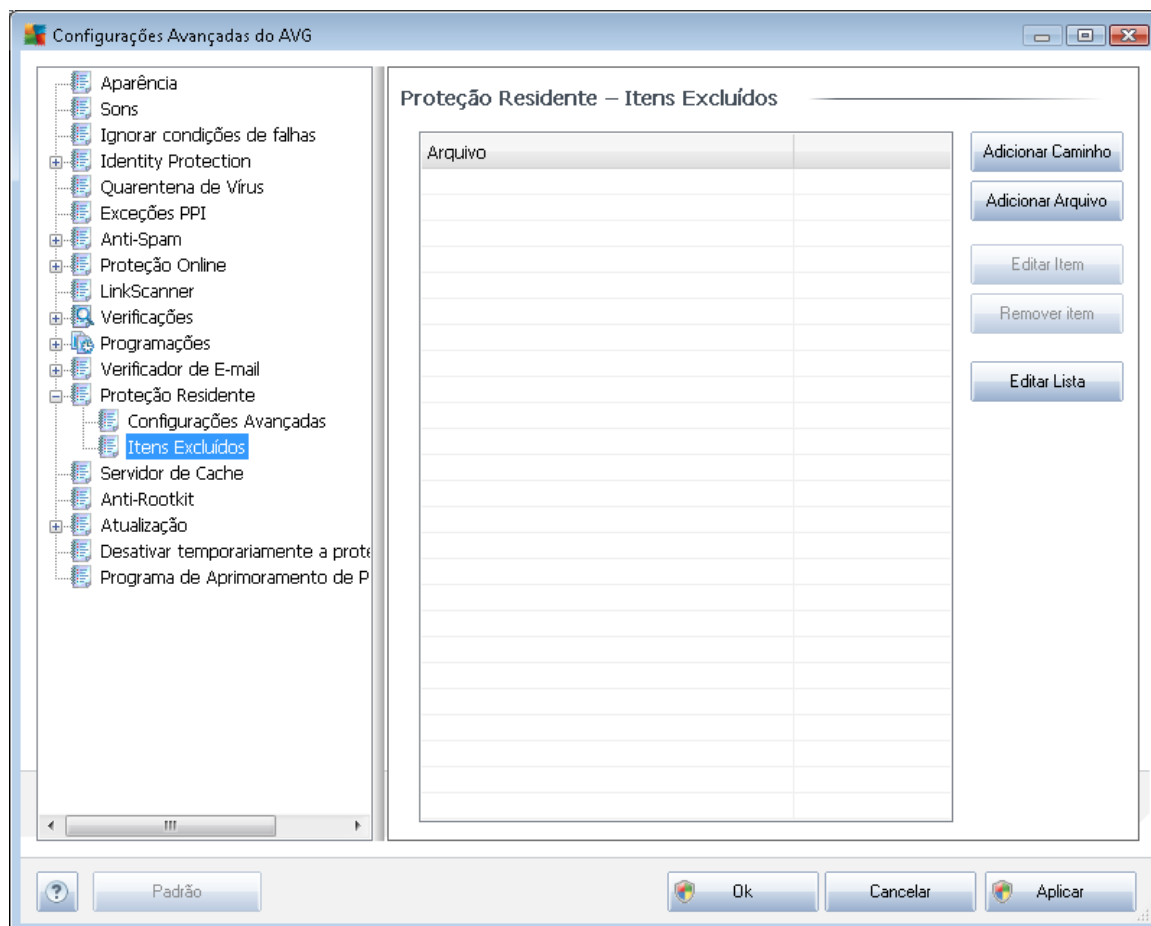
Na caixa de diálogo **Arquivos verificados pela Proteção Residente**, é possível configurar os arquivos que serão verificados (*por extensão específica*):



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.

A seção abaixo denominada **Proteção Residente vai verificar** sintetiza as configurações atuais, exibindo uma visão geral detalhada do que a **Proteção Residente** irá realmente verificar.

9.13.2. Itens excluídos



A caixa de diálogo **Proteção Residente - Itens Excluídos** oferece a possibilidade de definir as pastas e/ou arquivos que devem ser excluídos da verificação da **Proteção Residente**.

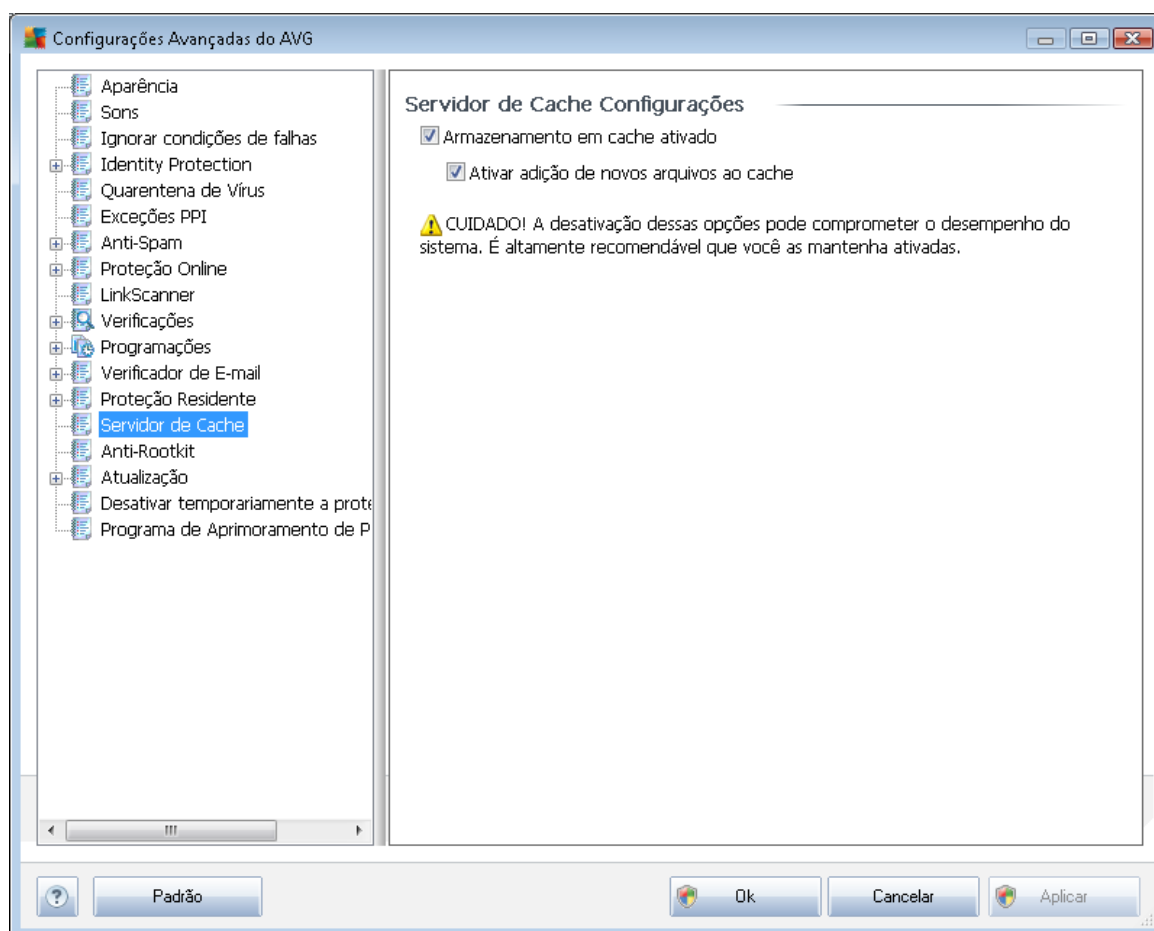
Se isso não for necessário, é altamente recomendável não excluir nenhum item.

Essa caixa de diálogo fornece os seguintes botões de controle:

- **Adicionar Caminho** – especifique um diretório (diretórios) a ser excluído da verificação, selecionando-o (um a um, no caso de haver mais de um) na árvore de navegação do disco local
- **Adicionar Arquivo** – especifique arquivos a serem excluídos da verificação, selecionando-os um a um na árvore de navegação do disco local
- **Editar Item** – permite editar o caminho especificado para um arquivo ou pasta selecionado
- **Remover Item** – permite excluir o caminho para um item selecionado da lista

9.14. Servidor de cache

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



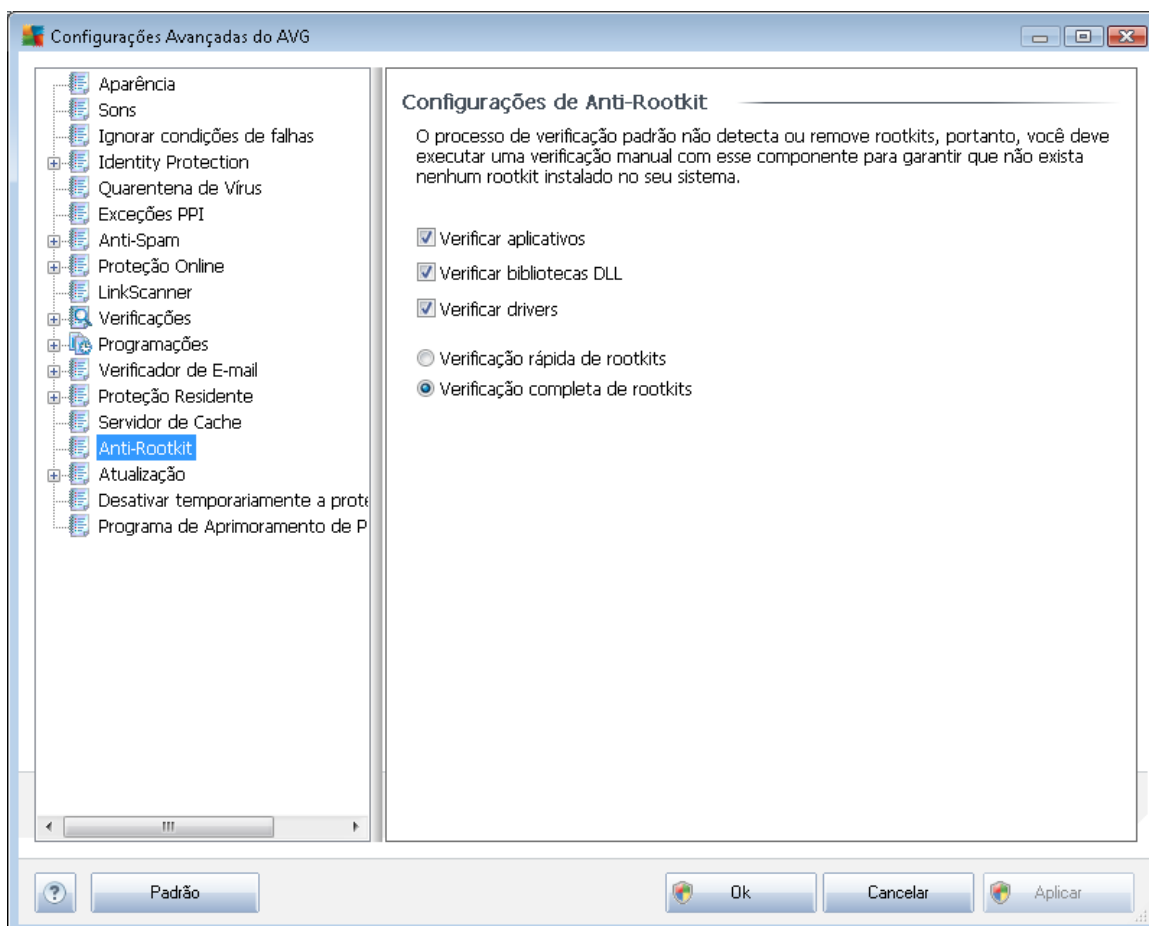
A caixa de diálogo configurações oferece duas opções:

- **Caching ativado** (*ativado por padrão*) - desmarque a caixa para desativar o **Servidor de Cache** e esvaziar a memória de cache. Observe que a verificação pode desacelerar, e o desempenho global de computador diminuir, conforme é feita a verificação de todos os arquivos únicos em uso procurando primeiro pela existência de vírus e spyware.
- **Ativar inclusão de novos arquivos em cache** (*ativado por padrão*) - desmarque a caixa para parar de adicionar mais arquivos na memória cache. Todos os arquivos já armazenados em cache serão mantidos e utilizados até que o cache seja desativado completamente, ou até a próxima atualização do banco de dados de vírus.



9.15. Anti-Rootkit

Nesta caixa de diálogo você pode editar a configuração do componente [Anti-Rootkit](#):



A edição de todas as funções do componente [Anti-Rootkit](#) conforme oferecido nesta caixa de diálogo também está acessível diretamente na [interface do componente Anti-Rootkit](#).

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

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

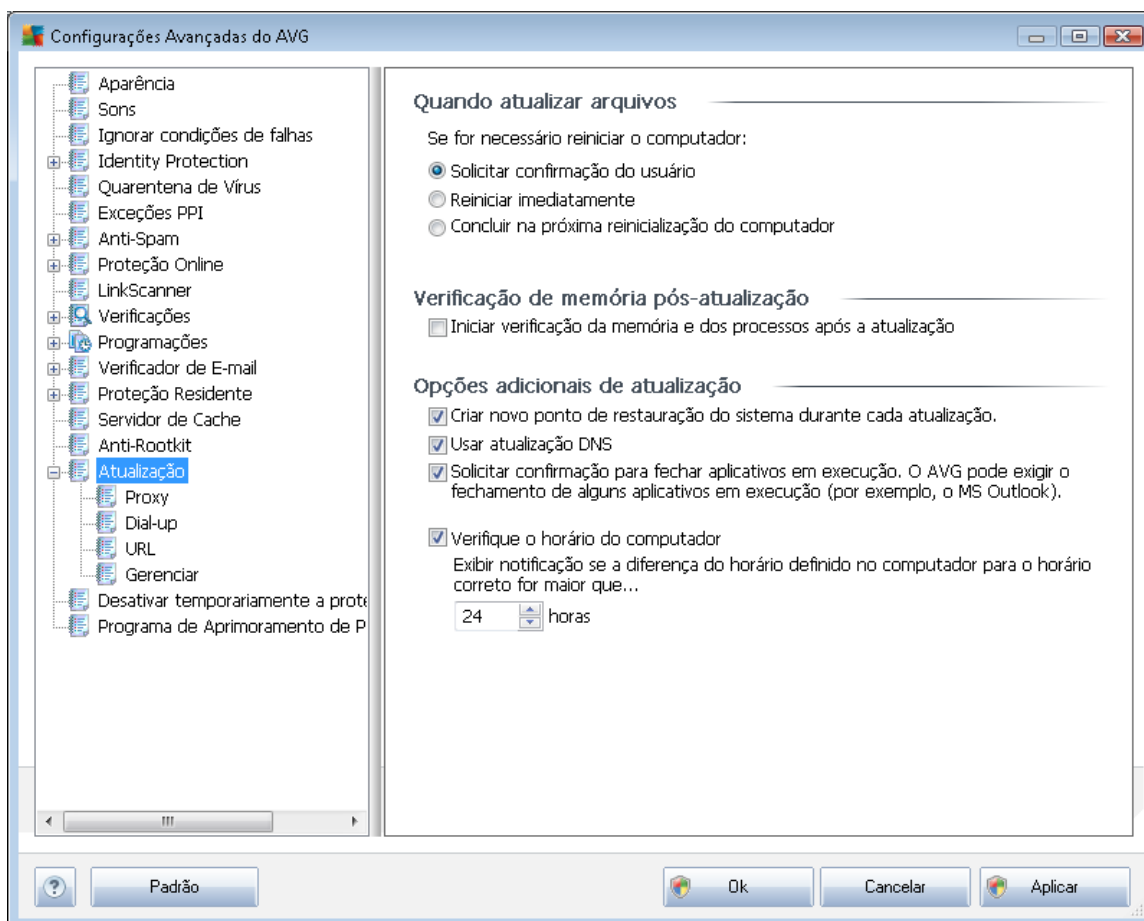
Em seguida, você pode selecionar o modo de verificação do rootkit:

- **Verificação rápida do rootkit** - verifica todos os processos em execução, unidades carregadas e pasta do sistema (*tipicamente c:\Windows*)
- **Verificação completa do rootkit** - verifica todos os processos em execução, unidades



carregadas, a pasta do sistema (*tipicamente c:\Windows*além de todos os discos locais (incluindo o disco flash, mas excluindo as unidades de CD/disquete)

9.16. Atualizar



O item de navegação **Atualizar** abre uma nova caixa de diálogo na qual é possível especificar parâmetros gerais relativos à [atualização do AVG](#):

Quando atualizar arquivos

{5389} Nesta seção você poderá escolher entre três opções alternativas caso o processo de atualização requeira a reinicialização do PC. A finalização da atualização pode ser agendada para a próxima reinicialização do PC, ou você pode reiniciar imediatamente:

- **Requer a confirmação do usuário (por padrão)**- será solicitado que você aprove 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.



- **Completar na próxima reinicialização do computador** - a finalização do [processo de atualização](#) será adiada até a próxima reinicialização do computador. Lembre que esta opção só é recomendada se você tiver certeza que o computador é reinicializado regularmente, pelo menos uma vez por dia!

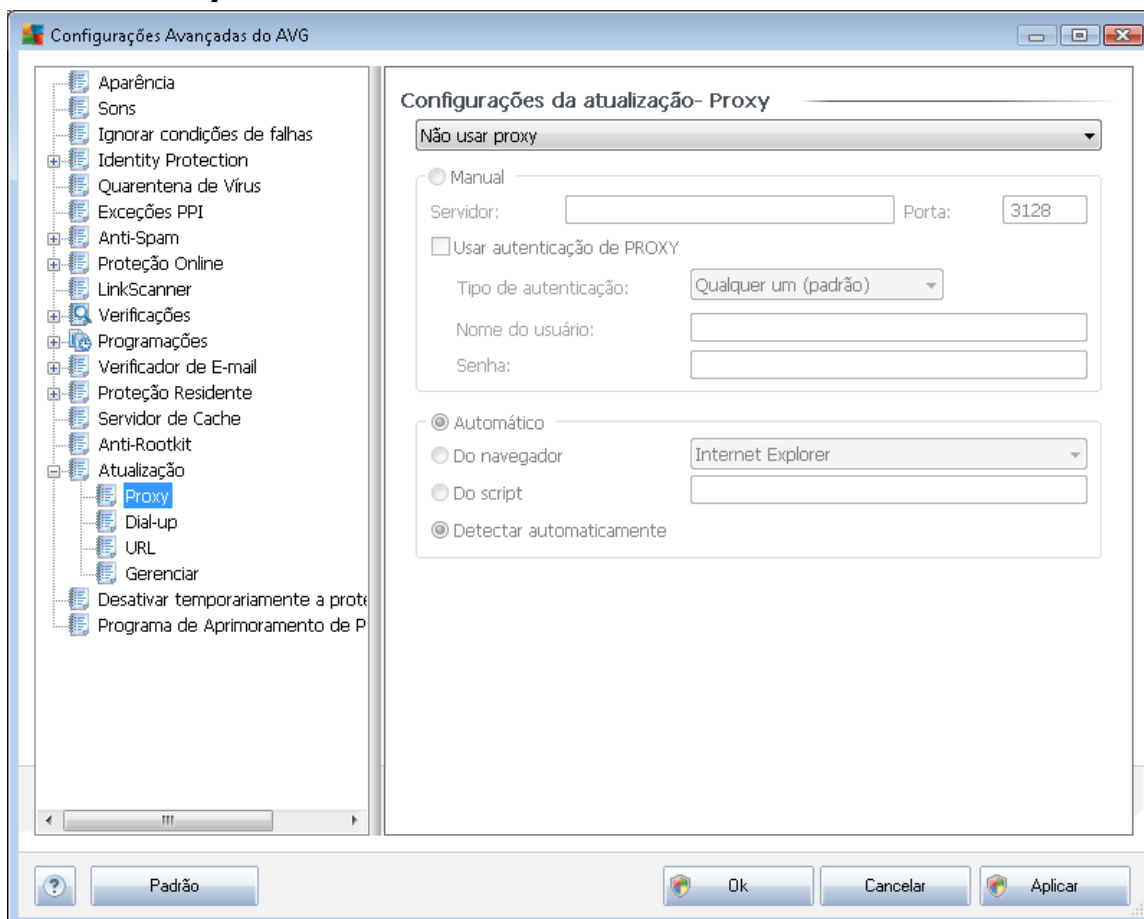
Verificação de memória pós-atualização

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 durante cada atualização do programa** - antes de 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** (ativada por padrão) - com este item marcado, depois que a atualização é iniciada, o **AVG Internet Security 2011** procura informações sobre a mais recente versão do banco de dados de vírus e sobre a versão mais recente do programa no servidor DNS. Então, somente os menores e mais indispensáveis arquivos de atualização são baixados e aplicados. Dessa forma, a quantidade total de dados baixados é reduzida e o processo de atualização é executado mais rapidamente.
- **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 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.

9.16.1. Proxy



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

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

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

Configuração manual

Se você selecionar a configuração manual (selecione a opção **Manual para ativar a seção**



apropriada da caixa de diálogo), terá que especificar os seguintes itens:

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

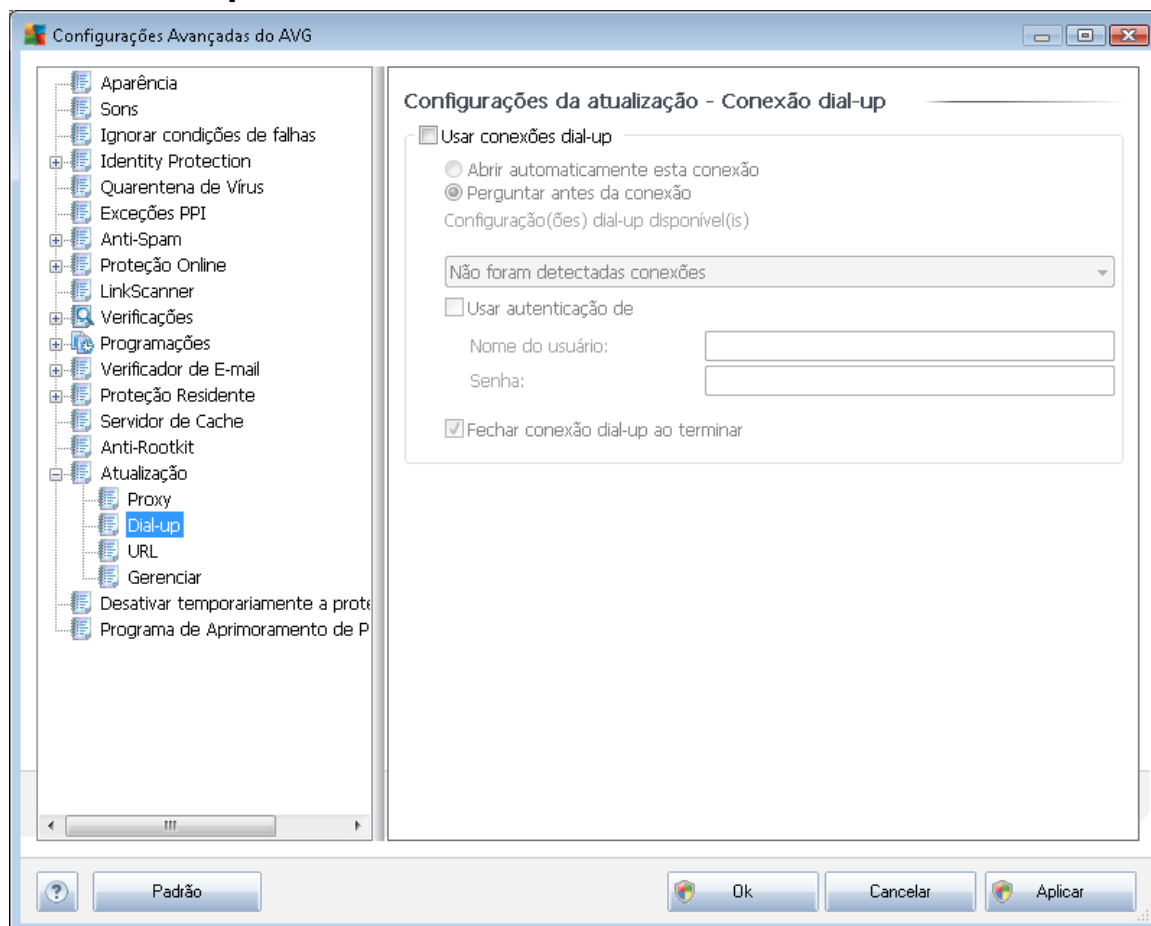
O servidor proxy também pode ter configurado regras específicas para cada usuário. Se o servidor proxy estiver configurado dessa forma, selecione a opção **Usar autenticação PROXY** para verificar se o nome de usuário e a senha são válidos para conexão à Internet por meio do servidor proxy.

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
- **Deteção automática** - a configuração será detectada de forma automática e direta do servidor proxy

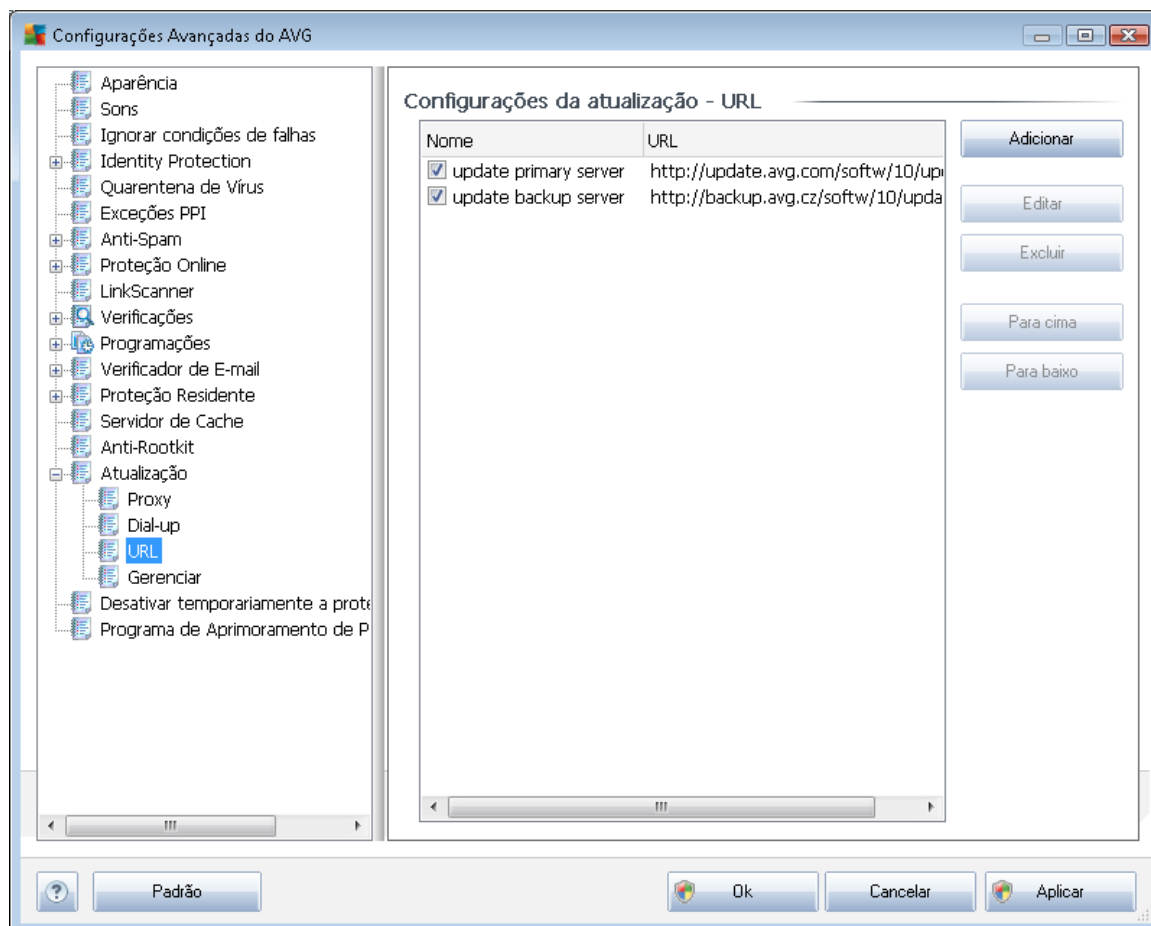
9.16.2. Dial-up



Todos os parâmetros definidos opcionalmente na caixa de diálogo **Atualizar configurações - Conexão dial-up** referem-se à conexão discada com a 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**).

9.16.3. URL

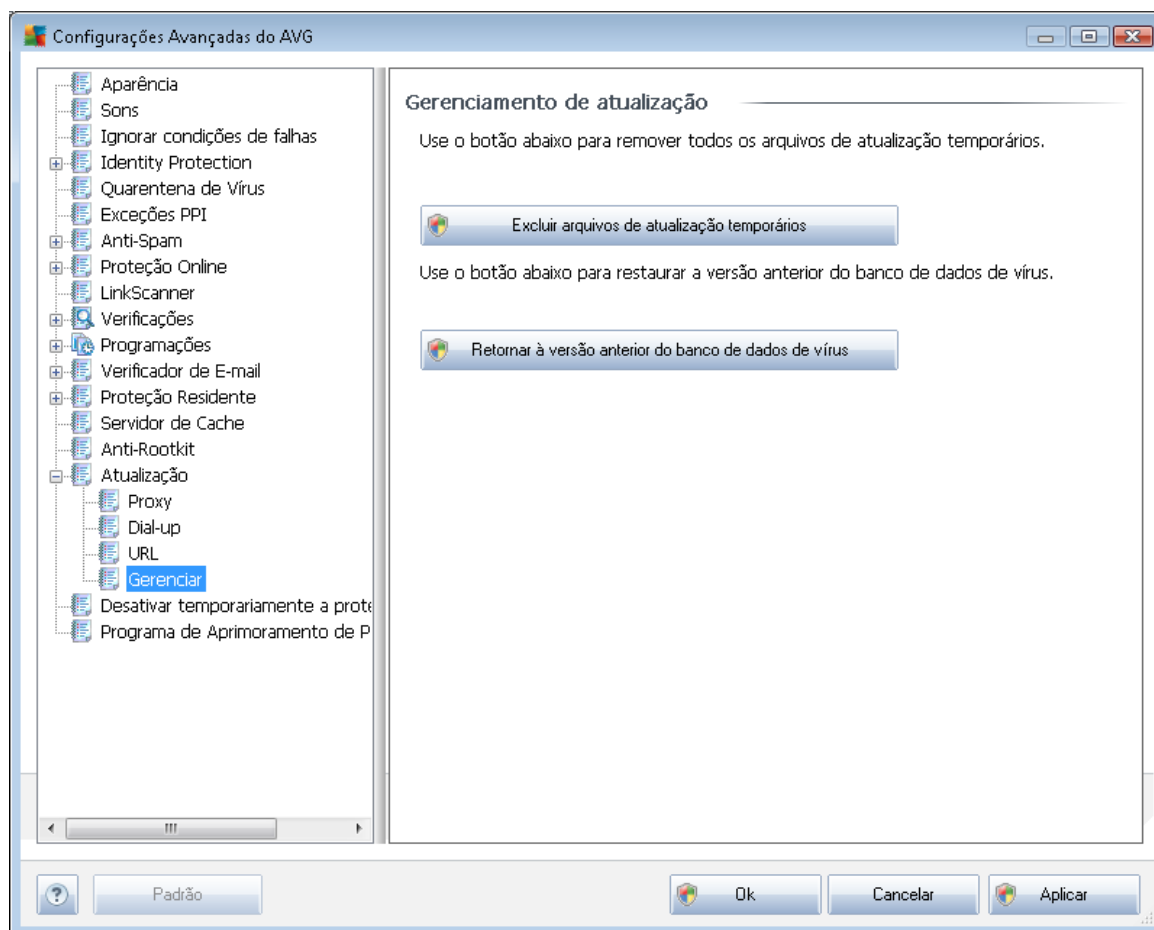


A caixa de diálogo **URL** oferece uma lista de endereços da Internet, a partir da qual você poderá baixar os arquivos de atualização. A lista e os itens podem ser modificados por meio dos seguintes botões de controle:

- **Adicionar**- abre uma caixa de diálogo na qual você especificará a nova URL a ser adicionada à lista
- **Editar** – abre uma caixa de diálogo na qual 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.

9.16.4. Gerenciar

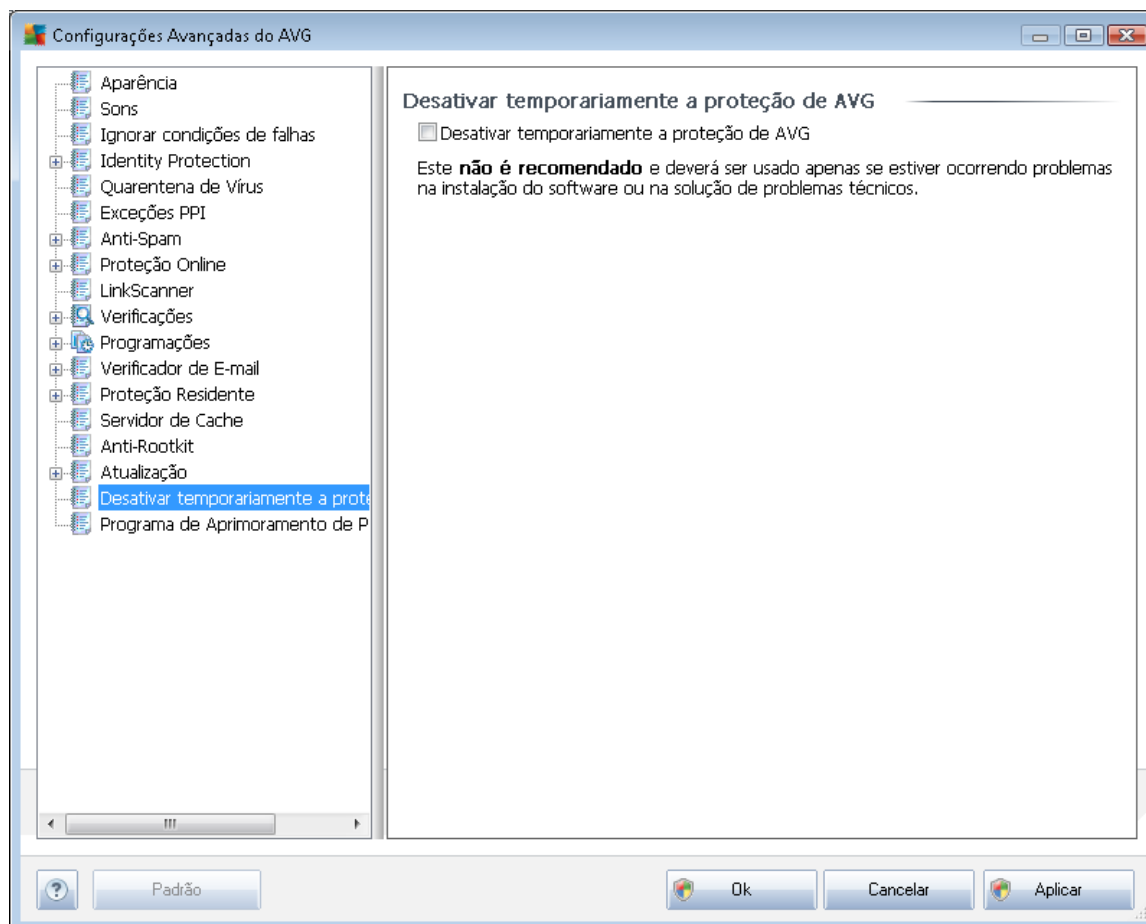
A caixa de diálogo **Gerenciar** oferece duas opções acessíveis via dois botões:



- **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*)



9.17. Desativar temporariamente a proteção do AVG



Na caixa de diálogo **Desativar temporariamente a proteção do AVG**, você tem a opção de desativar toda a proteção oferecida pelo **AVG Internet Security 2011** de uma vez.

Lembre-se de que você não deve usar essa opção, a menos que ela seja absolutamente necessária!

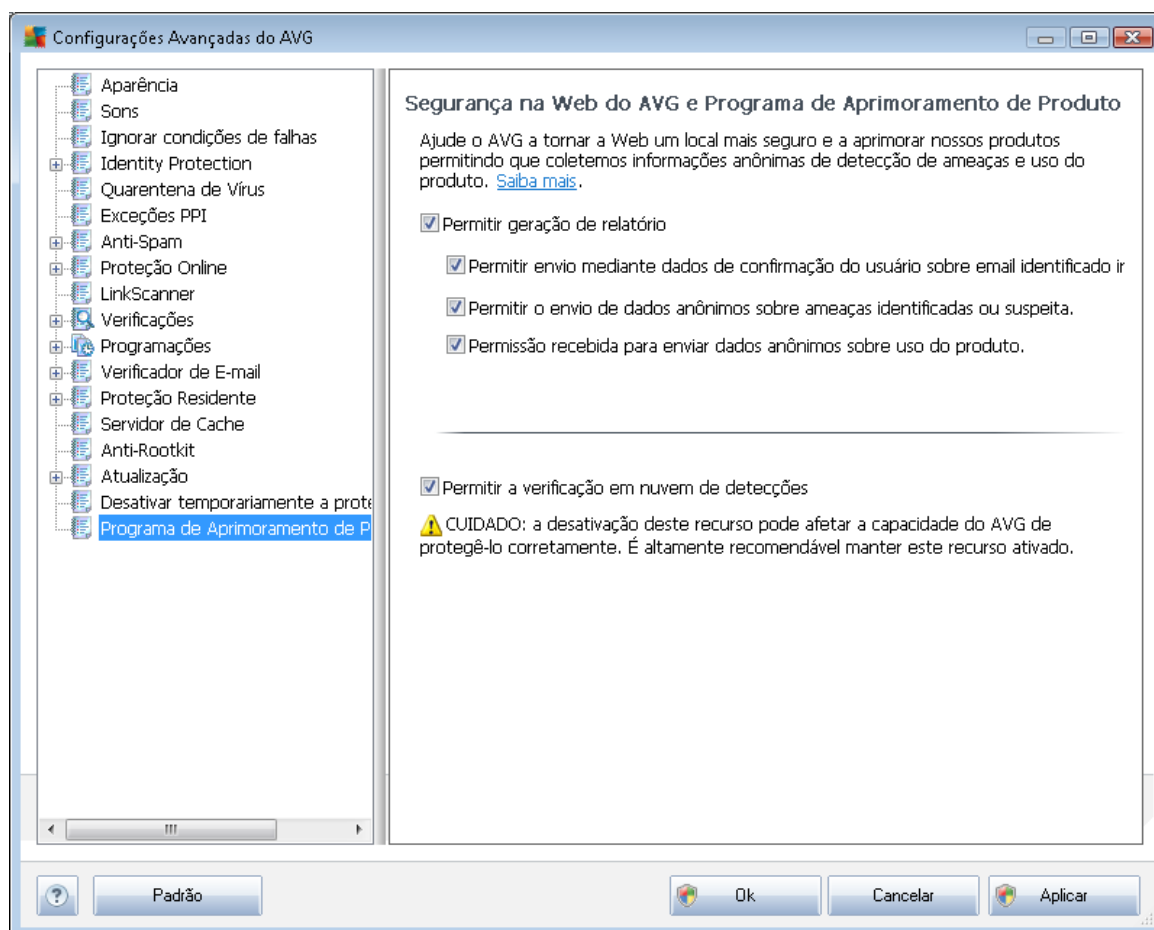
Na maioria dos casos, não **é necessário** desativar o AVG antes de instalar novo software ou novos drivers, nem mesmo se o instalador ou assistente de software sugerir que programas e aplicativos em execução devem ser encerrados primeiro para garantir que não haja interrupções indesejadas durante o processo de instalação. Caso você tenha algum problema durante a instalação, tente desativar o componente **Proteção Residente** primeiro. Se precisar desativar temporariamente o AVG, você deverá reativá-lo assim que concluir a sua tarefa que solicitou a desativação. Se você estiver conectado à Internet ou a uma rede durante o período em que o software antivírus está desativado, o computador ficará vulnerável a ataques.



9.18. Programa de Aprimoramento de Produto

A caixa de diálogo **Segurança na Web e Programa de Aprimoramento de Produto** convida você a participar do aperfeiçoamento de produto AVG e nos ajudar a aumentar o nível de segurança geral na Internet. Marque a opção **Permitir relatórios** a fim de permitir a geração de relatórios de ameaças detectadas para o AVG. Isso nos ajuda a coletar informações atualizadas sobre as ameaças mais recentes dos participantes do mundo todo e, em retorno, podemos melhorar a proteção para todos.

O relatório é feito automaticamente, portanto, não causa nenhum inconveniente a você e nenhum dado pessoal é incluído nos relatórios. É opcional registrar ameaças detectadas; no entanto, solicitamos que ative esse recurso porque ele nos ajuda a melhorar a proteção de navegação online tanto para você quanto outros usuários do AVG.



Hoje em dia, existem muito mais ameaças do que apenas vírus comuns. Os criadores de códigos maliciosos e sites perigosos são muito inovadores, e novos tipos de ameaças surgem frequentemente, a vasta maioria na Internet. Estas são algumas das mais comuns:

- ***Um vírus é um código mal-intencionado que se copia e se espalha, muitas vezes não percebido até que o estrago seja feito.*** Alguns vírus são uma ameaça séria, excluindo ou alterando deliberadamente arquivos no seu caminho, enquanto alguns vírus podem fazer



algo aparentemente inofensivo, como reproduzir o trecho de uma música. No entanto, todos os vírus são perigosos devido à capacidade básica de se multiplicarem – mesmo um vírus simples pode ocupar toda a memória do computador em um instante e causar uma falha.

- ***Uma subcategoria de vírus é um worm*** que, diferentemente do vírus, não precisa de um objeto "transportador" ao qual se anexar; ele se envia a outros computadores dentro de si mesmo, normalmente por e-mail e, como resultado, muitas vezes sobrecarrega servidores de e-mail e sistemas de rede.
- ***O spyware normalmente é definido como uma categoria de malware (malware = qualquer software mal intencionado, incluindo vírus) que abrange programas – tipicamente Cavalos de Tróia – com o objetivo de roubar informações pessoais, senhas, números de cartão de crédito ou para se infiltrar em um computador e permitir que o atacante controle-o remotamente; é claro que tudo isso sem o conhecimento ou consentimento do dono do computador.***
- ***Programas potencialmente indesejados*** são um tipo de spyware que pode ser, mas não necessariamente precisa ser, perigoso ao computador. Um exemplo específico de um PPI é o adware, software projetado para distribuir propaganda, normalmente exibindo pop-ups de anúncio; é irritante, mas não diretamente prejudicial.
- Os ***cookies de rastreamento*** podem também ser contados como um tipo de spyware, uma vez que esses pequenos arquivos, armazenados no navegador da Web e enviados automaticamente ao site "pai" quando você visitá-lo novamente, podem conter dados como seu histórico de navegação e outras informações similares.
- ***Vulnerabilidade*** é um código mal intencionado que se aproveita de uma falha ou vulnerabilidade em um sistema operacional, navegador da Internet ou outro programa essencial.
- ***Phishing*** é uma tentativa de adquirir dados pessoais confidenciais simulando uma organização confiável e bem conhecida. Normalmente, as possíveis vítimas são contatadas por um e-mail em massa solicitando que elas, por exemplo, atualizem os detalhes da sua conta bancária. Para fazer isso, elas são convidadas a seguir o link fornecido que leva a um site falso do banco.
- ***Hoax é um e-mail em massa contendo informações perigosas, alarmantes ou apenas irritantes e inúteis.*** Muitas das ameaças acima usam o e-mail hoax para se espalharem.
- ***Sites mal-intencionados*** são aqueles que deliberadamente instalam software mal-intencionado no seu computador, e sites invadidos fazem o mesmo, a única diferença é que esses sites são legítimos, foram invadidos e infectam os visitantes.

Para protegê-lo de todos esses tipos diferentes de ameaças, o AVG inclui estes componentes especializados:

- ***[Anti-Vírus](#)*** para proteger seu computador de vírus,
- ***[Anti-Spyware](#)*** para proteger seu computador de spyware,



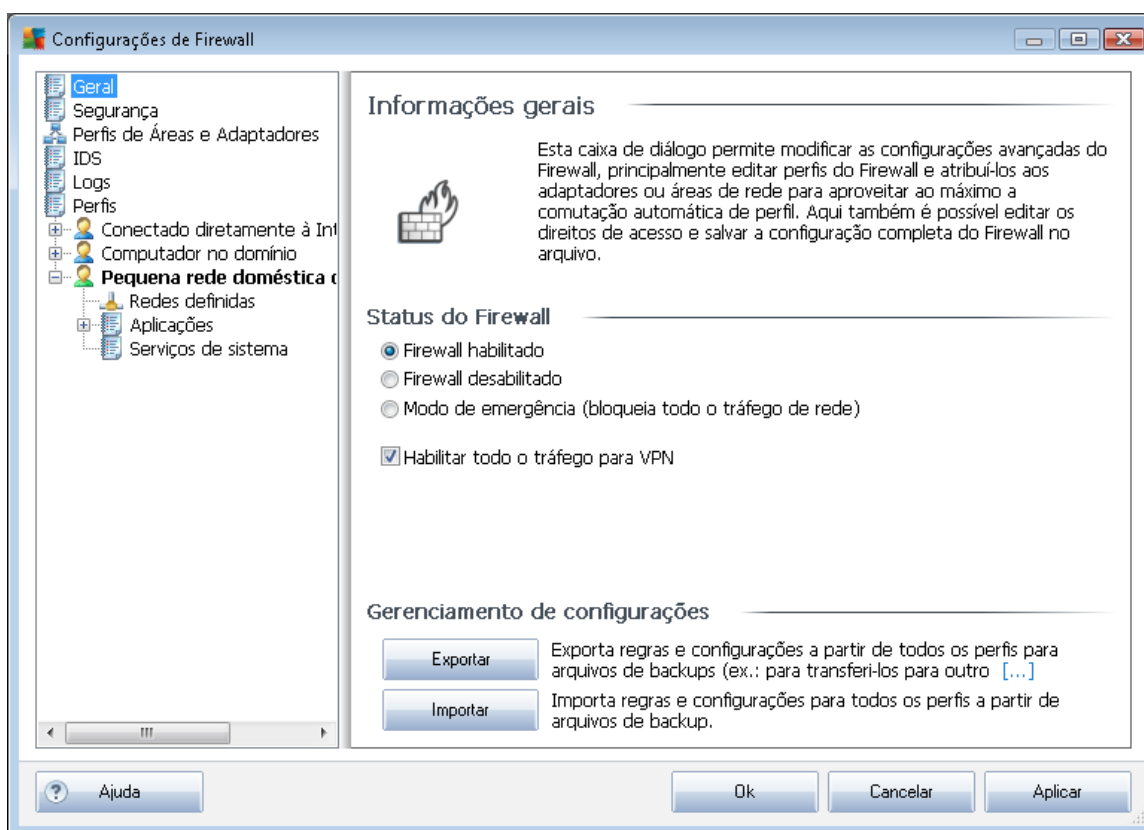
- [Proteção Online](#) para protegê-lo de vírus e spyware ao navegar pela Internet,
- [LinkScanner](#) para protegê-lo contra outras ameaças online mencionadas neste capítulo.

10. Configurações de Firewall

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

10.1. Geral

A caixa de diálogo **Informações gerais** está dividida em duas seções:



Status do Firewall

Na seção **Status do firewall**, você pode trocar o status do **Firewall** de acordo com a necessidade:

- **Firewall ativado** - selecione esta opção para permitir a comunicação nesses aplicativos considerados 'permitidos' no conjunto de regras definidas no perfil de **Firewall selecionado**
- **Firewall desativado** - esta opção desativa totalmente o **Firewall**, todo o tráfego da rede é permitido mas não verificado!
- **Modo de emergência (bloquear todo o tráfego de Internet)** - selecione esta opção para bloquear todo o tráfego em toda porta de rede; o **Firewall** ainda está em execução, mas todo o tráfego da rede é interrompido

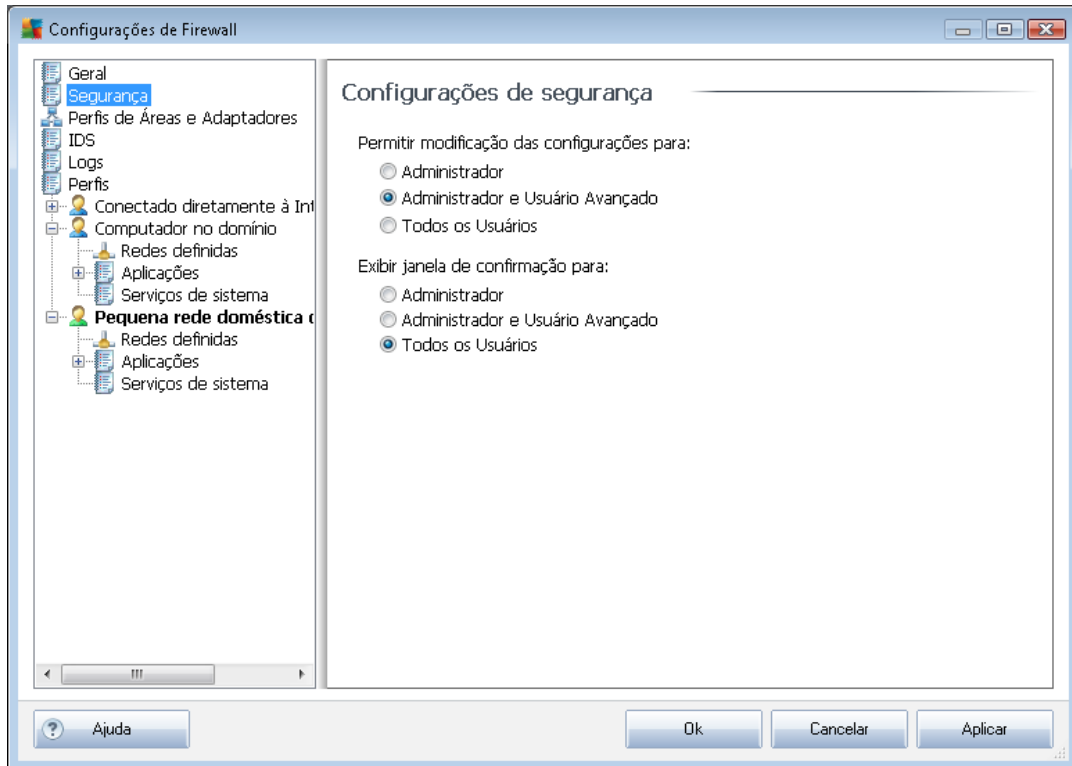
- **Permitir que todo o tráfego VPN** - se você usa uma conexão VPN (*Rede Privada Virtual*), por exemplo, para se conectar de casa com o seu escritório, recomendamos que marque a caixa. **O AVG Firewall** irá procurar automaticamente através de adaptadores de rede, encontrar aqueles usados para a conexão VPN, e permitir que todos os aplicativos se conectem à rede de destino (*aplica-se somente a aplicativos com nenhuma regra de firewall específica atribuída*). Em um sistema padrão com adaptadores de rede comum, essa etapa simples deve evitar que você tenha que configurar uma regra detalhada em cada aplicação que você tenha que usar solução VPN.

Nota: Para habilitar uma conexão VPN, é necessário permitir comunicação com os seguintes protocolos de sistema: GRE, ESP, L2TP, PPTP. Pode-se fazer isso na caixa de diálogo *Serviços do sistema*.

Gerenciamento de configurações

Na seção **Gerenciamento de configuração**, você pode **Exportar/Importar** a configuração do **Firewall**; ou seja, exportar as regras e as configurações de **Firewall** definidas para arquivos de backup ou, por outro lado, importar o arquivo de backup inteiro.

10.2. Segurança



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

- **Permitir modificação de configurações** - especifique quem tem permissão para alterar a

configuração do [Firewall](#)

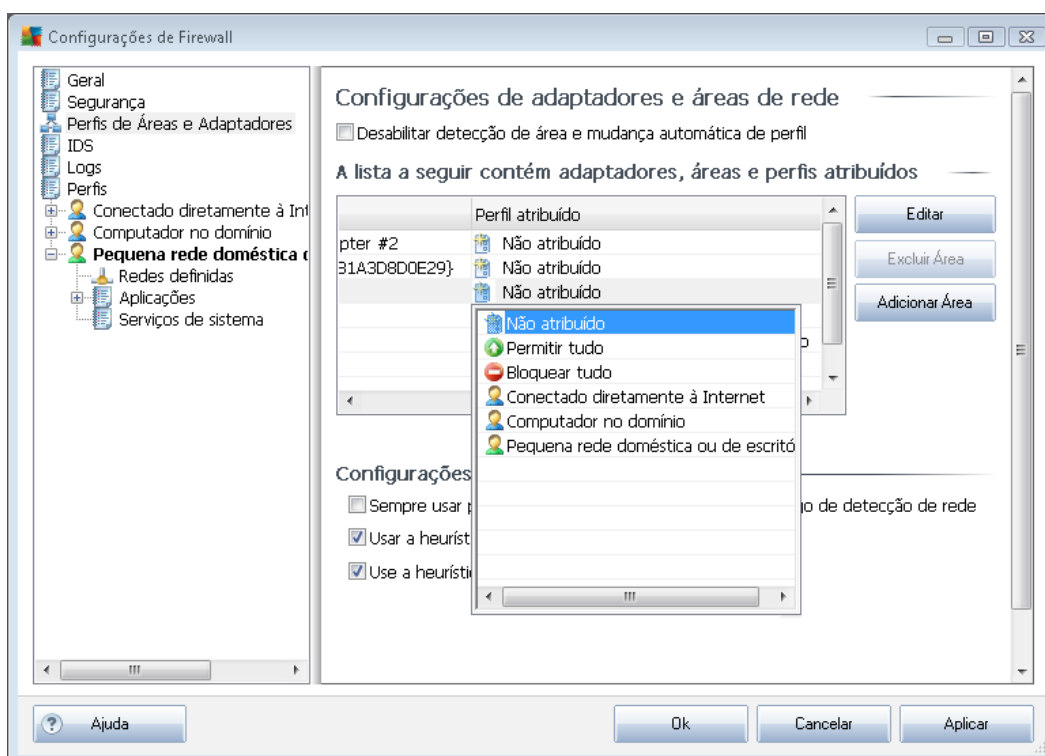
- **Mostrar a caixa de diálogo de confirmação** - especifique para quem as caixas de diálogo de confirmação (caixas de diálogo que solicitam uma decisão em situações não cobertas por uma regra definida do [Firewall](#)) devem ser exibidas

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

- **Administrador** - controla totalmente o computador e tem o direito de atribuir cada usuário a grupos com permissões definidas especificamente
- **Administradores e Usuários Avançados** - o administrador pode atribuir qualquer usuário a um grupo específico (*Usuários Avançados*) e definir permissões dos membros do grupo.
- **Todos os Usuários** - outros usuários não atribuídos a nenhum grupo específico.

10.3. Perfis de áreas e adaptadores

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



- **Desativar detecção de área e troca automática de perfil** - um dos perfis definidos pode ser atribuído a cada tipo de interface de rede, a cada área respectivamente. Se você não



quiser definir perfis específicos, será usado um perfil comum. Entretanto, se você optar por especificar perfis e atribuí-los a determinados adaptadores e áreas e posteriormente, por algum motivo, quiser trocar esse esquema temporariamente, marque a opção **Desativar detecção de área e perfil automático**.

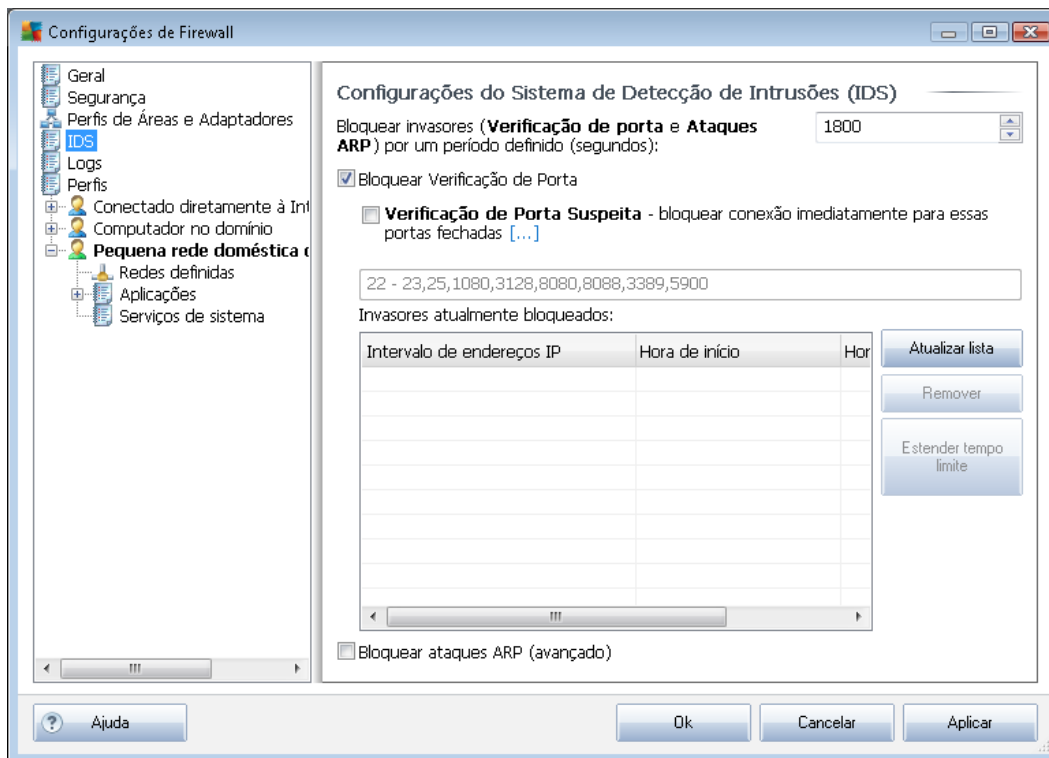
- **Lista de adaptadores, áreas e perfis atribuídos** - nesta lista, é possível encontrar uma visão geral de áreas e adaptadores detectados. Para cada um deles, é possível atribuir um perfil específico para o menu de perfis definidos. Para abrir esse menu, clique no respectivo item na lista de adaptadores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

Configurações avançadas

- o **Sempre usar perfil padrão e não exibir nova caixa de diálogo de detecção de rede** - quando seu computador se conectar a uma nova rede, o [Firewall](#) alertará você e exibirá uma caixa de diálogo solicitando que você selecione um tipo de conexão de rede, e atribua a ele um [perfil de Firewall](#). Se você não quiser que a caixa de diálogo seja exibida, marque esta caixa.
- o **Usar a heurística do AVG para a detecção de novas redes** - permite a obtenção de informações sobre uma rede recém-detectada com o mecanismo próprio do AVG (no entanto, esta opção só está disponível no sistema operacional Windows Vista, e mais recentes).
- o **Usar a heurística da Microsoft para detecção de novas redes** - permite a obtenção de informações sobre uma rede recém-detectada do serviço Windows (esta opção só está disponível no Windows Vista e mais recentes).

10.4. IDS

O **Intrusion Detection System (sistema de detecção de intrusão)** é um recurso de análise comportamento especial para identificar e bloquear tentativas de comunicação suspeitas em portas específicas de seu computador. É possível configurar os parâmetros de IDS na seguinte interface:



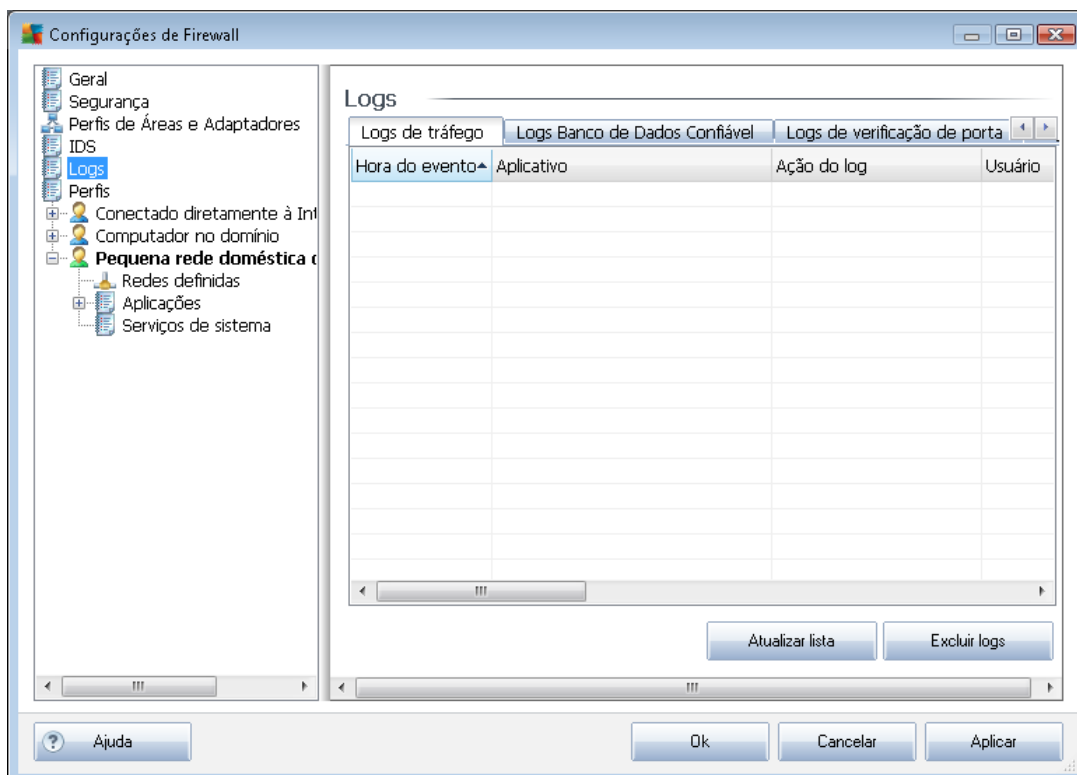
A caixa de diálogo **Configurações do Sistema de Detecção de Intrusões (IDS)** oferece estas opções de configuração:

- **Bloquear invasores por um período definido** - você pode especificar aqui por quantos segundos uma porta fica bloqueada, quando uma tentativa de comunicação suspeita é detectada nela. Por padrão, o intervalo de tempo é definido como 1800 segundos (30 minutos).
- **Bloquear verificação de porta** – marque a caixa para bloquear tentativas de comunicação em todas as portas TCP e UDP enviadas de fora para o computador. Para tal conexão, cinco tentativas são permitidas, e a sexta é bloqueada.
 - o **Bloquear verificação de porta** – marque a caixa para bloquear imediatamente qualquer tentativa de comunicação nas portas especificadas no campo de texto abaixo. Portas individuais ou intervalos de portas devem ser divididos por vírgulas. Há uma lista predefinida de portas recomendadas caso você queira usar este recurso.
 - o **Invasores atualmente bloqueados** - esta seção lista qualquer tentativa de comunicação que esteja sendo bloqueada no momento pelo **Firewall**. Um histórico completo de tentativas bloqueadas pode ser exibido na caixa de diálogo **Logs** (guia **Logs de verificação de porta**).
- **Bloquear ataques ARP** ativa o bloqueio de tipos especiais de tentativas de comunicação em uma rede local detectada pelo **IDS** como potencialmente perigosa. O tempo definido em **Bloquear invasores por um período definido aplica-se**. Recomendamos que apenas usuários avançados, familiarizados com o tipo e nível de risco de sua rede local, usem esse recurso.

Botões de controle

- **Atualizar lista** - pressione o botão para atualizar a lista *(para incluir todas as tentativas bloqueadas mais recentes)*
- **Remover** - pressione para cancelar um bloqueio selecionado
- **Estender tempo limite** - pressione para prolongar o período de bloqueio de uma tentativa selecionada. Uma nova caixa de diálogo aparecerá, permitindo que você defina a hora e a data específicas ou uma duração específica.

10.5. Logs



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

- **Logs de tráfego** - oferece informações sobre atividades de todos os aplicativos que tentaram se conectar à rede.
- **Logs do banco de dado confiável** - O banco de dado confiável é um banco de dados interno do AVG que coleta informações sobre aplicativos certificados e confiáveis que sempre têm permissão para se comunicarem on-line. Da primeira vez que um novo



aplicativo tentar se conectar à rede (ou seja, quando ainda não houver uma regra de firewall especificada para esse aplicativo), será necessário descobrir se a comunicação de rede deve ser permitida para o respectivo aplicativo. Em primeiro lugar, o AVG pesquisa o *Banco de dado confiável* e, se o aplicativo estiver listado, ele receberá acesso automático à rede. Somente depois disso, desde que não haja informações sobre o aplicativo disponíveis no banco de dados, você será solicitado a especificar em uma caixa de diálogo à parte se deseja permitir que esse aplicativo acesse a rede.

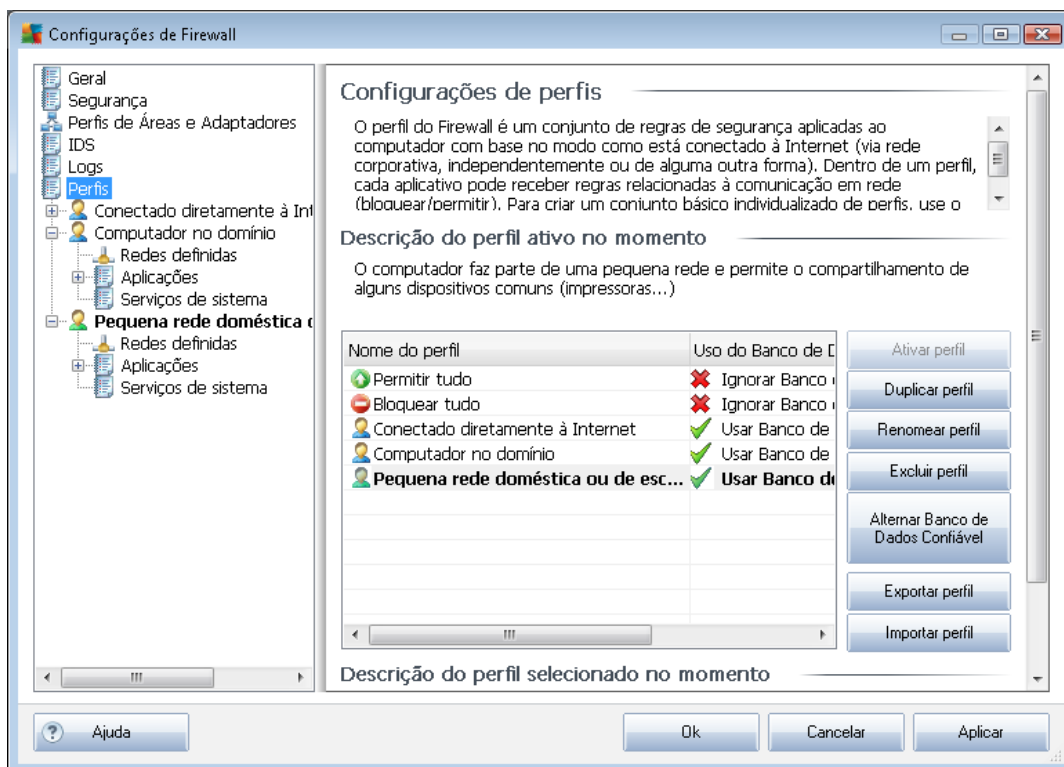
- **Logs de verificação de porta** - fornece toda de todas as atividades do [Sistema de Detecção de Intrusões](#).
- **Logs de ARP** - informações de log ativa sobre o bloqueio de tipos especiais de tentativas de comunicação em uma rede local (opção [Bloquear ataques ARP](#)) detectados pelo [Sistema de Detecção de Intrusões](#) como potencialmente perigosos.

Botões de controle

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

10.6. Perfis

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



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

- **Ativar perfil** - este botão define o perfil selecionado como ativo, o que significa que a configuração do perfil selecionado será usada pelo [Firewall](#) para controlar o tráfego da rede
- **Perfil duplicado** - cria uma cópia idêntica do perfil selecionado; posteriormente, você poderá editar e renomear a cópia para criar um novo perfil baseado na cópia original duplicada
- **Renomear perfil** - permite definir um novo nome para um perfil selecionado
- **Excluir perfil** - exclui o perfil selecionado da lista
- **Alternar banco de dados confiável** - para o perfil selecionado, você pode optar por usar as informações do Banco de dados confiável (o banco de dados confiável é um banco de dados interno do AVG que coleta dados sobre aplicativos confiáveis e certificados que sempre têm permissão de comunicação on-line.)
- **Exportar perfil** - registra a configuração do perfil selecionado em um arquivo que será salvo para possível uso futuro



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

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

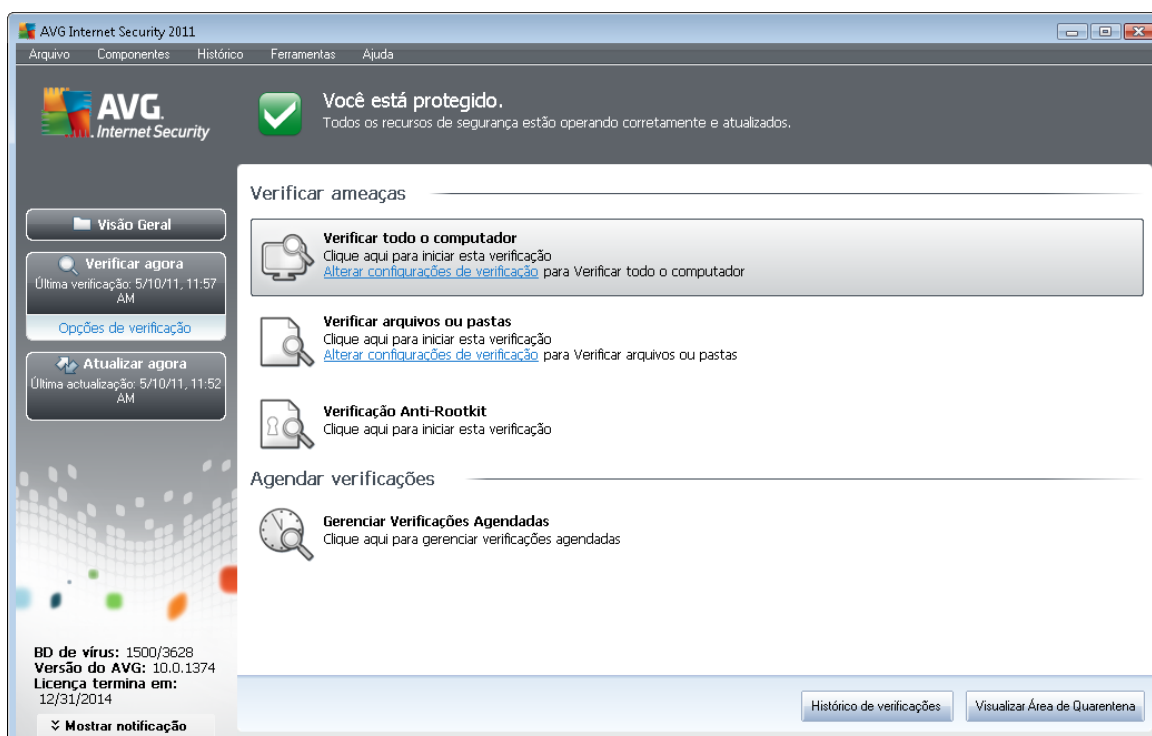
Com base no número de perfis definidos mencionados na lista da caixa de diálogo **Perfil**, a estrutura do menu de navegação à esquerda também muda. Cada perfil definido cria uma ramificação específica no item **Perfil**. Os perfis específicos podem ser editados nas seguintes caixas de diálogo, *que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



11. Verificação do AVG

A verificação é uma parte crucial da funcionalidade **AVG Internet Security 2011**. 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](#) **Opções de verificação**. 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:
 - o [Verificação de todo o computador](#)
 - o [Verificar arquivos ou pastas específicas](#)
 - o [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 principais recursos do **AVG Internet Security 2011** 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 em seu computador.

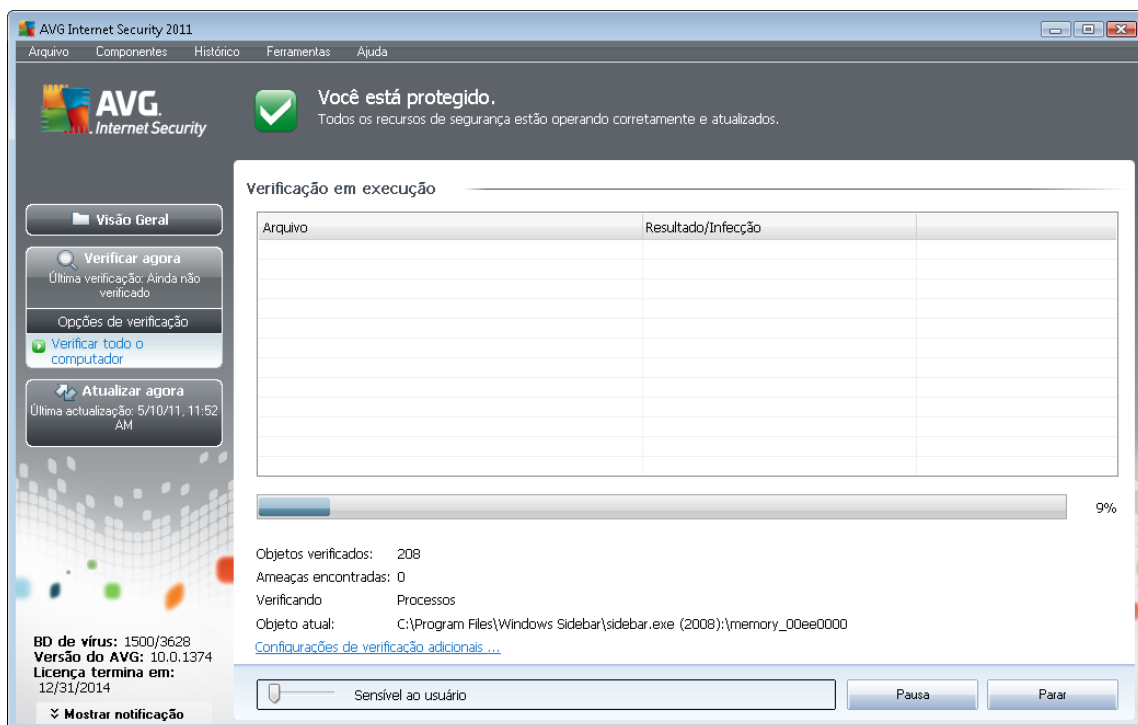
No **AVG Internet Security 2011** você encontrará os seguintes tipos de verificação predefinidos pelo fornecedor do software:

11.2.1. Verificação de todo o computador

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

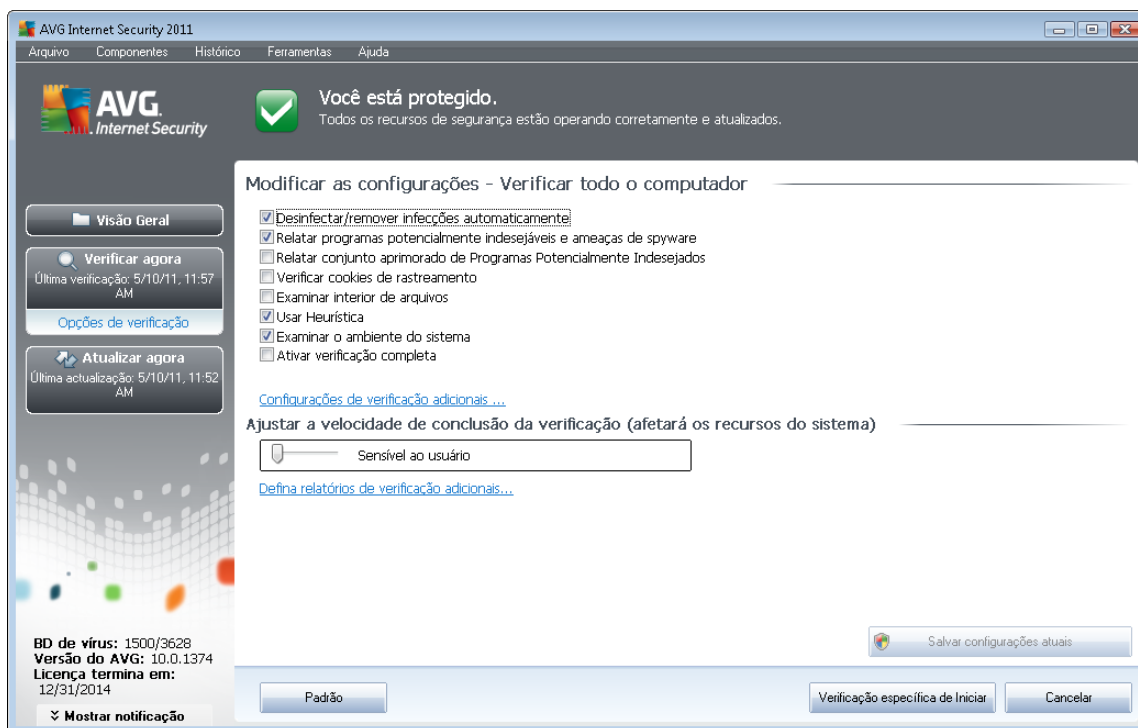
Iniciar verificação

Verificar todo o computador pode ser iniciado 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

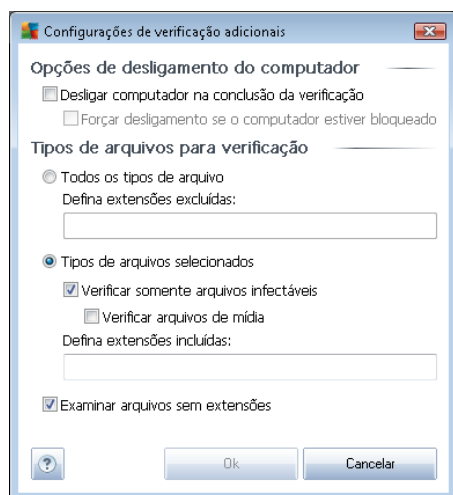
Você tem a opção de editar as configurações padrão predefinidas de **Verificar todo o computador**. Clique no link **Alterar as configurações de verificação** para acessar a caixa de diálogo **Alterar configurações de verificação de Verificar todo o computador** (acessível pela [interface de verificação](#) por meio do link **Alterar as configurações de verificação para 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:
 - o **Reparar ou remover infecção automaticamente** (ativada por padrão) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a [Quarentena de Vírus](#).
 - o **Informar programas potencialmente indesejáveis e ameaças de spyware** (ativada por padrão) - marque para ativar o mecanismo [Anti-Spyware](#) e verificar se há spyware e vírus. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
 - o **Informar conjunto avançado de programas potencialmente indesejáveis** (desativada por padrão) - marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.
 - o **Verificar cookies de rastreamento** (desativada por padrão) - este 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 de sites ou conteúdo de carrinhos de compras

eletrônicas).

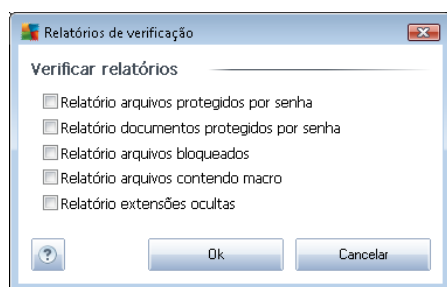
- o **Verificar dentro dos arquivos** (desativada por padrão) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.
- o **Usar Heurística** (ativada por padrão) - a análise heurística (emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual) será um dos métodos usados para detecção de vírus durante a verificação
- o **Verificar ambiente do sistema** (ativada por padrão) - a verificação também atuará nas áreas do sistema do seu computador.
- o **Ativar verificação completa** (desativada por padrão) - em situações específicas (suspeita de que seu computador foi infectado), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.
- **Configurações de verificação adicionais** - o link abre uma nova caixa de diálogo **Configurações de verificação adicionais**, na qual é possível especificar os seguintes parâmetros:



- o **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 que ele esteja bloqueado (**Forçar desligamento do computador se estiver bloqueado**).
- o **Definir tipos de arquivo para verificação** - além disso, você deve decidir se deseja verificar os seguintes itens:
 - **Todos os tipos de arquivos** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por

vírgula que não devem ser verificadas;

- **Tipos de arquivos selecionados** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
- Opcionalmente, você pode optar por **Verificar arquivos sem extensão** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.
- **Ajustar a velocidade de conclusão da verificação** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade 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 específicos - verifica somente as áreas do computador que você tenha selecionado para verificação (*pastas selecionadas, discos rígidos, 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



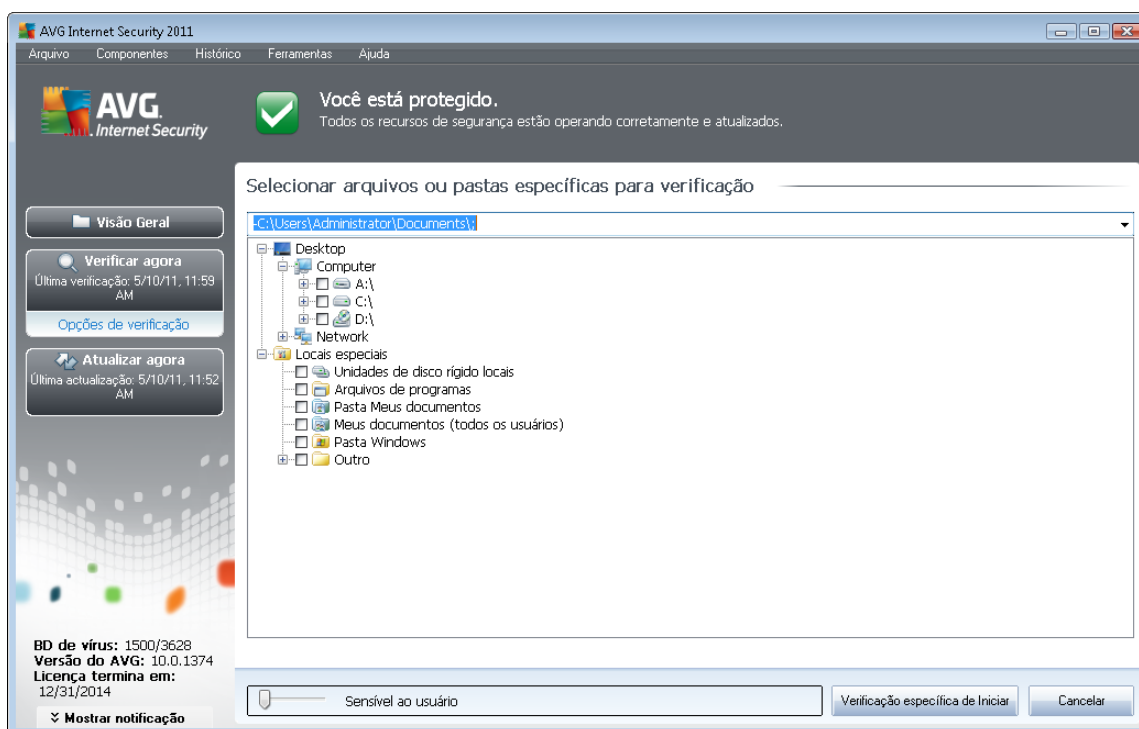
Quarentena de vírus. A verificação de arquivos ou pastas específicos pode ser usada para configurar seus próprios testes e sua programação com base nas necessidades.

Iniciar verificação

A opção **Verificar arquivos ou pastas específicos** pode ser iniciada diretamente na [interface de verificação](#) clicando no ícone de verificação. Uma nova caixa de diálogo chamada **Selecionar arquivos ou pastas específicos 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.

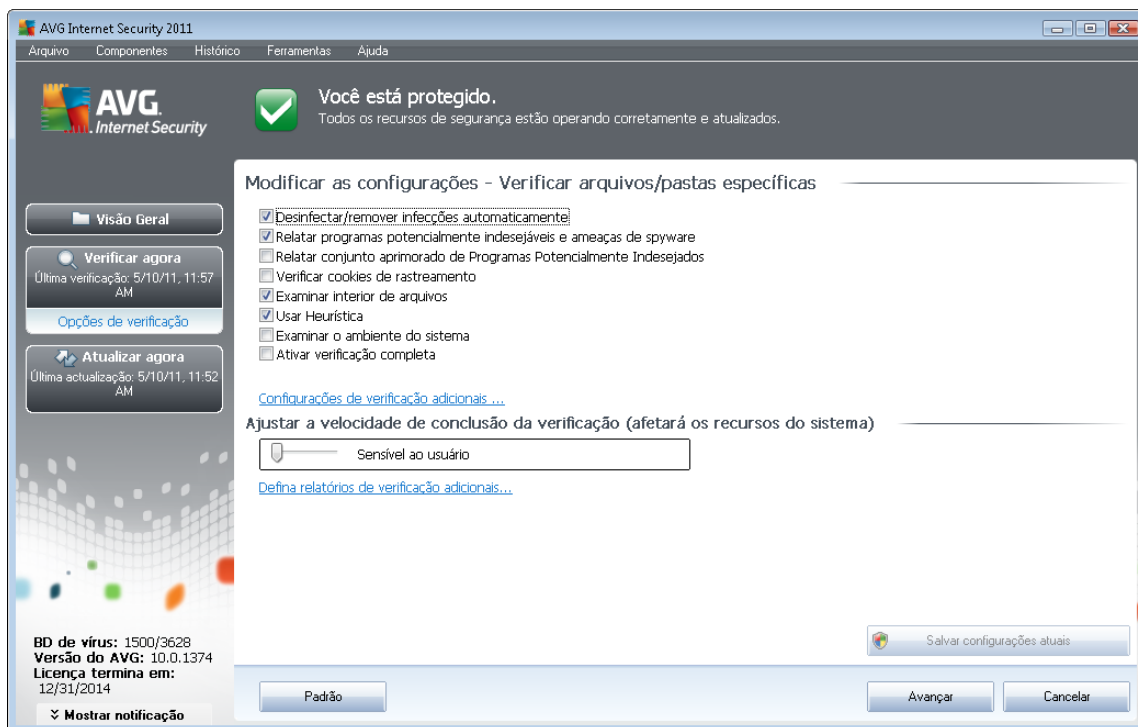
Também existe a possibilidade de fazer a verificação em uma determinada pasta enquanto suas subpastas são excluídas da verificação; para isso, insira um sinal de menos "-" na frente do caminho gerado automaticamente (veja a imagem). Para excluir da verificação a pasta inteira, use o parâmetro "!" .

Finalmente, para iniciar a verificação, pressione o botão **Iniciar verificação**; o processo de verificação será basicamente idêntico a [Verificar todo o computador](#).



Verificar edições de configuração

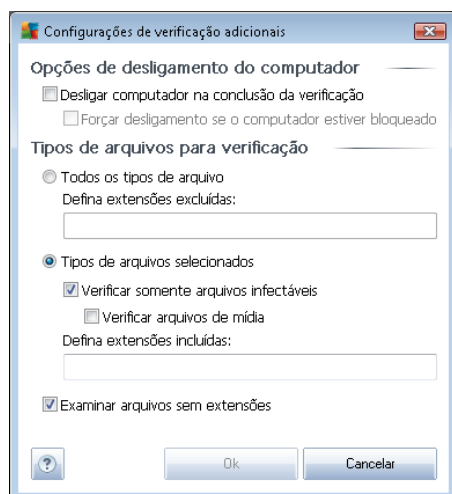
Você tem a opção de editar as configurações padrão predefinidas de **Verificar arquivos ou pastas específicos**. Acesse o link **Alterar as configurações de verificação** para abrir a caixa de diálogo **Alterar configurações de verificação de Verificar arquivos ou pastas específicos**. É recomendável 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:
 - o **Reparar ou remover infecção automaticamente** (ativada por padrão) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a [Quarentena de Vírus](#).
 - o **Informar programas potencialmente indesejáveis e ameaças de spyware** (ativada por padrão) - marque para ativar o mecanismo [Anti-Spyware](#) e verificar se há spyware e vírus. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente.](#) Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
 - o **Informar conjunto avançado de programas potencialmente indesejáveis** (desativada por padrão) - marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.
 - o **Verificar cookies de rastreamento** (desativada por padrão) - este 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 de sites ou conteúdo de carrinhos de compras eletrônicas).

- o **Verificar dentro dos arquivos** (ativada por padrão) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.
- o **Usar heurística** (desativada 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.
- o **Verificar ambiente do sistema** (desativada por padrão) - a verificação também atuará nas áreas do sistema do seu computador.
- o **Ativar verificação completa** (desativada por padrão) - em situações específicas (suspeita de que seu computador foi infectado), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.
- **Configurações de verificação adicionais** - o link abre uma nova caixa de diálogo **Configurações de verificação adicionais**, na qual é possível especificar os seguintes parâmetros:

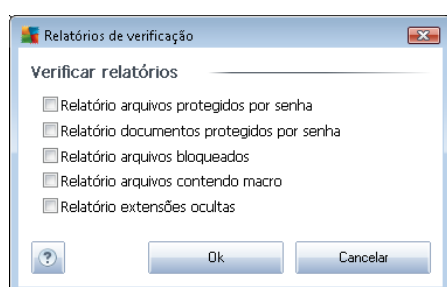


- o **Opções de desligamento do computador** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (**Desligar o computador quando o processo de verificação for concluído**), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (**Forçar desligamento do computador se estiver bloqueado**).
- o **Definir tipos de arquivo para verificação** - além disso, você deve decidir se deseja verificar os seguintes itens:

➤ **Todos os tipos de arquivos** com a possibilidade de definirem exceções a partir

da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

- **Tipos de arquivos selecionados** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
- Opcionalmente, você pode optar por **Verificar arquivos sem extensão** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.
- **Prioridade do processo de verificação** - você pode usar esse controle para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade 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 tipos de possíveis localizações 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 arquivos ou pastas específicas**, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de arquivos ou pastas específicas. Além disso, essa configuração será usada como modelo para todas as novas verificações programadas ([todas as verificações personalizadas são baseadas na configuração atual de Verificação de arquivos ou pastas selecionados](#)).

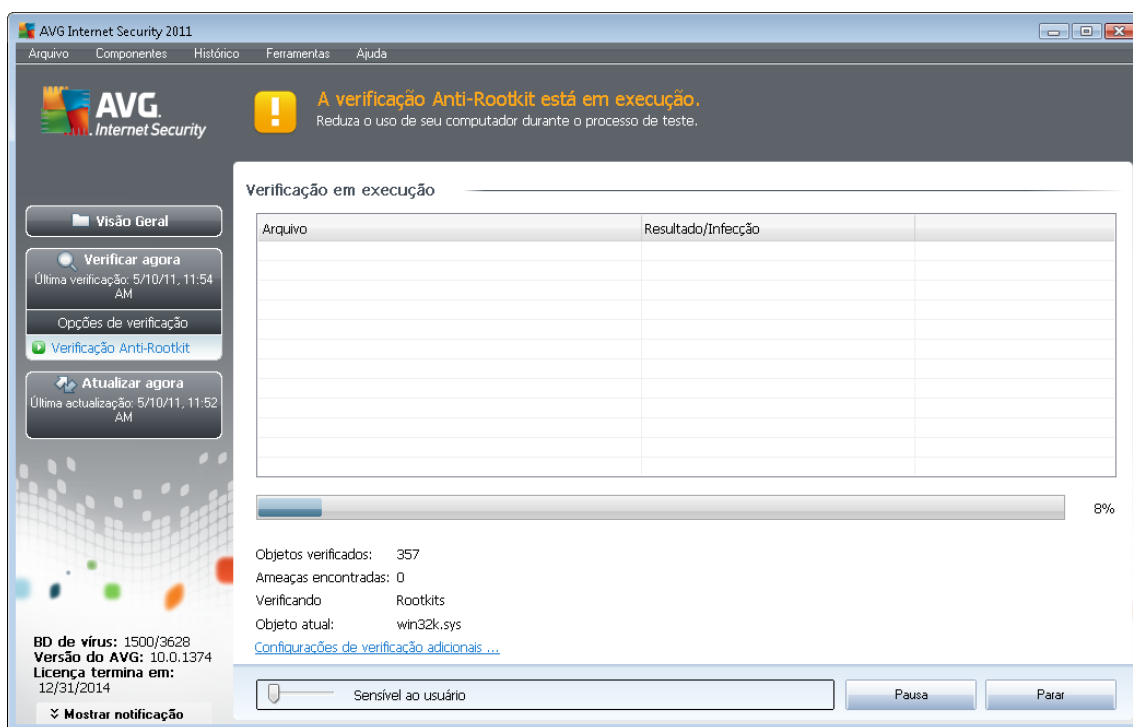


11.2.3. Verificação Anti-Rootkit

A **Verificação Anti-Rootkit** verifica seu computador em busca de possíveis rootkits (*programas e tecnologias que possam ocultar atividades de malware no computador*). Se um rootkit for detectado, isso não quer dizer necessariamente que o computador está infectado. Em alguns casos, drivers específicos ou seções de aplicativos comuns podem ser detectados por engano como rootkits.

Iniciar verificação

A **Verificação Anti-Rootkit** pode ser iniciada diretamente na [interface de verificação](#) clicando no ícone de verificação. Se nenhuma outra configuração específica for definida para esse tipo de verificação, ela será iniciada imediatamente na caixa de diálogo **Verificação em andamento** (veja a [imagem](#)). A verificação pode ser interrompida temporariamente (**Pausar**) ou cancelada (**Parar**), se necessário.



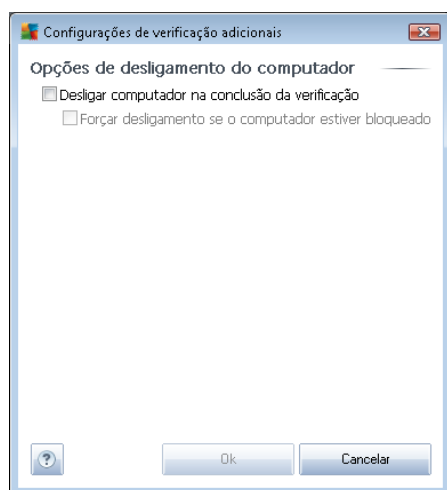
Verificar edições de configuração

A **Verificação Anti-Rootkit** é sempre iniciada nas configurações padrão, e a edição dos parâmetros de verificação só pode ser acessada na caixa de diálogo [Configurações avançadas do AVG/Anti-Rootkit](#). Na interface de verificação, a seguinte configuração está disponível, mas apenas enquanto a verificação está em execução:

- **Verificação automática** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de

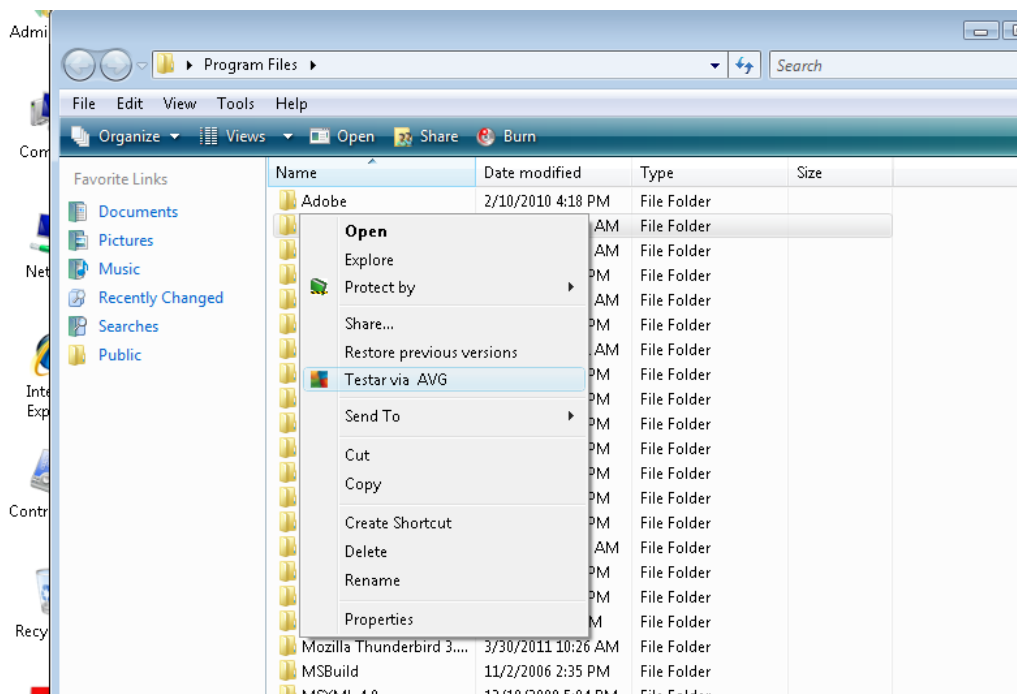
verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- **Configurações de verificação adicionais** - este link abre uma nova caixa de diálogo **Configurações de verificação adicionais**, na qual você pode definir possíveis condições de desligamento do computador relacionadas à **Verificação Anti-Rootkit (Desligar o computador após a conclusão da verificação e possivelmente Forçar encerramento se o computador estiver travado)**:



11.3. Verificando o Windows Explorer

Além das verificações predefinidas iniciadas em todo o computador ou em áreas selecionadas, o **AVG Internet Security 2011** 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, destaque 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

No **AVG Internet Security 2011** 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 em que 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 caractere de barra
- se o parâmetro exigir um valor específico a ser fornecido (por exemplo, o parâmetro **/scan** requer informações sobre quais são as áreas selecionadas do seu computador a serem verificadas, e você precisa informar o caminho exato da seção selecionada), os valores serão divididos por ponto e vírgula, como por exemplo: **avgscanx /scan=C:\;D:**

Parâmetros de verificação

Para exibir uma visão completa dos parâmetros disponíveis, digite o respectivo comando junto com o parâmetro **/?** ou **/HELP** (por ex., **avgscanx /?**). O único parâmetro obrigatório é **/SCAN**, que especifica que áreas do computador que devem ser verificadas. Para obter uma explicação mais detalhada 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, também é 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 está acessível apenas 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 estas extensões/por exemplo, EXT=EXE,DLL
- **/NOEXT** Não verificar estas 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
- **/PRIORITY** Definir prioridade de verificação/Baixa, Automática, Alta (veja [Configurações avançadas/Verificações](#))
- **/SHUTDOWN** Desligar o computador na conclusão da verificação
- **/FORCESHUTDOWN** Forçar o computador a ser desligado na conclusão da verificação
- **/ADS** Verificar fluxos de dados alternativos (apenas NTFS)
- **/ARCBOMBSW** Informar arquivos compactados novamente

11.5. Programação de verificação

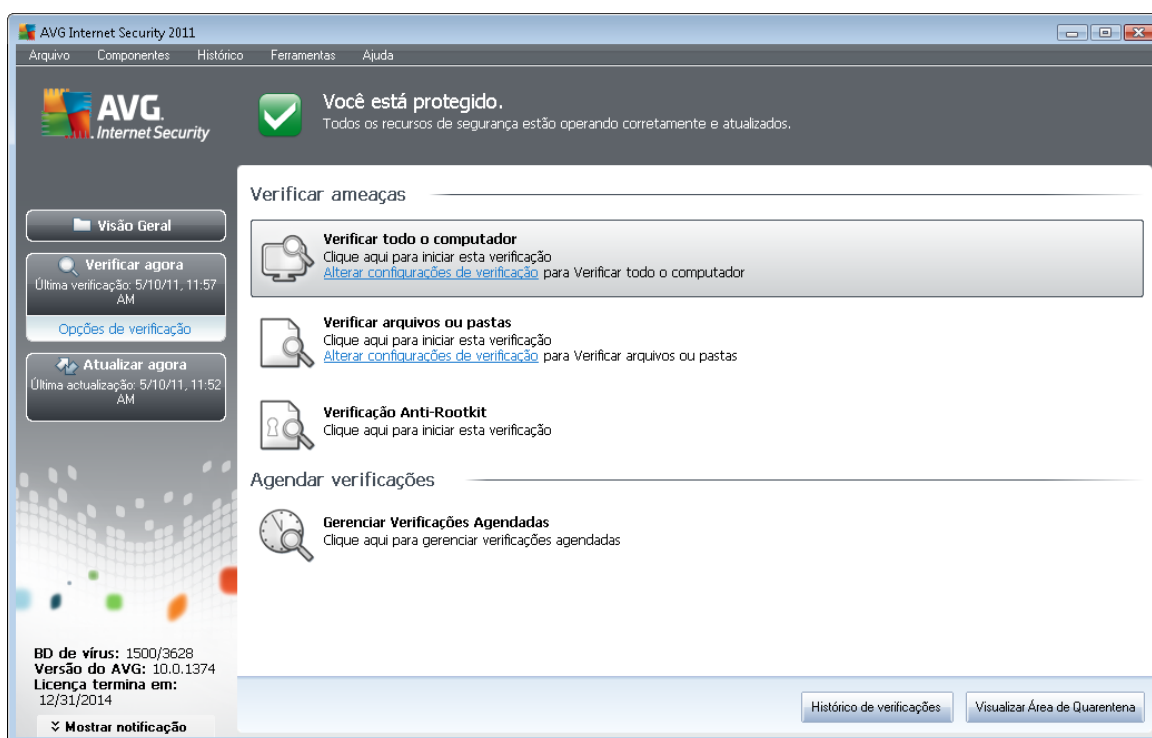
Com o **AVG Internet Security 2011**, é possível executar uma verificação sob demanda (por exemplo, quando você suspeitar de uma infecção no seu computador) ou com base em um plano programado. É altamente recomendável executar verificações com base em uma programação. Dessa forma, você pode assegurar que seu computador esteja protegido contra a possibilidade de



infecção e não precisará se preocupar com a inicialização da verificação.

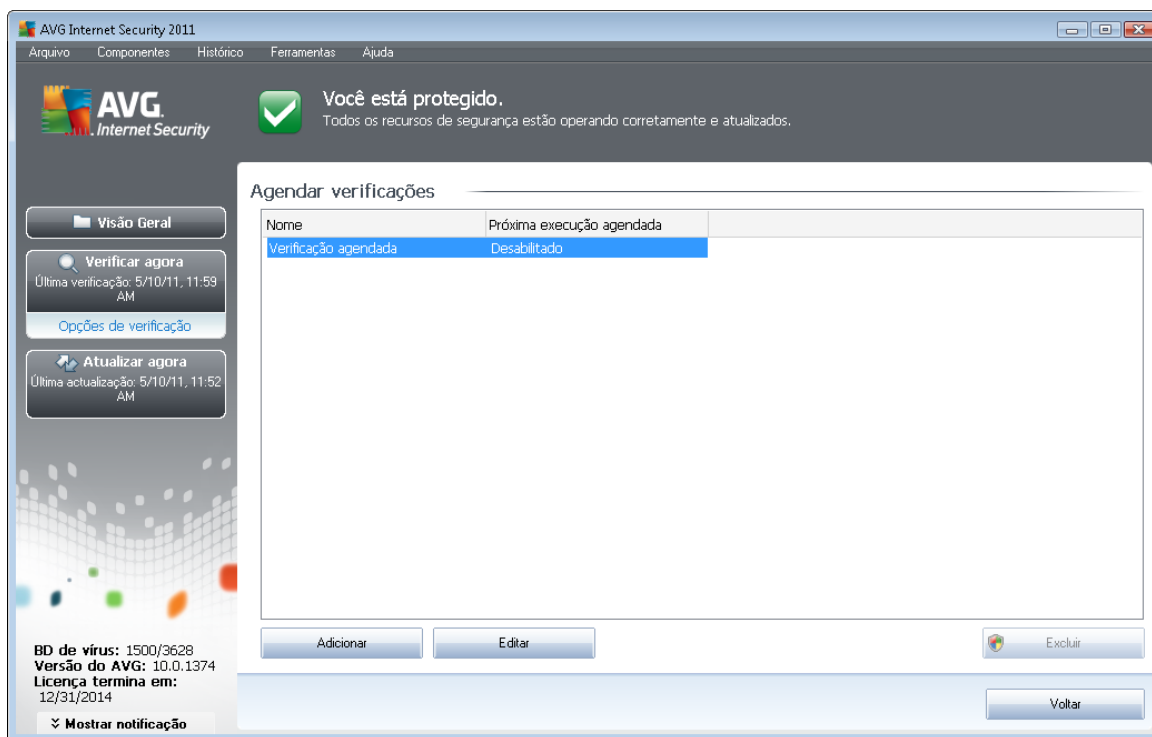
Você deve [Verificar todo o computador](#) regularmente, pelo menos uma vez por semana. Mas, se possível, inicie a verificação de todo o computador diariamente, conforme definido na configuração padrão da programação da verificação. Se o computador estiver "sempre ligado", você poderá programar verificações 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:

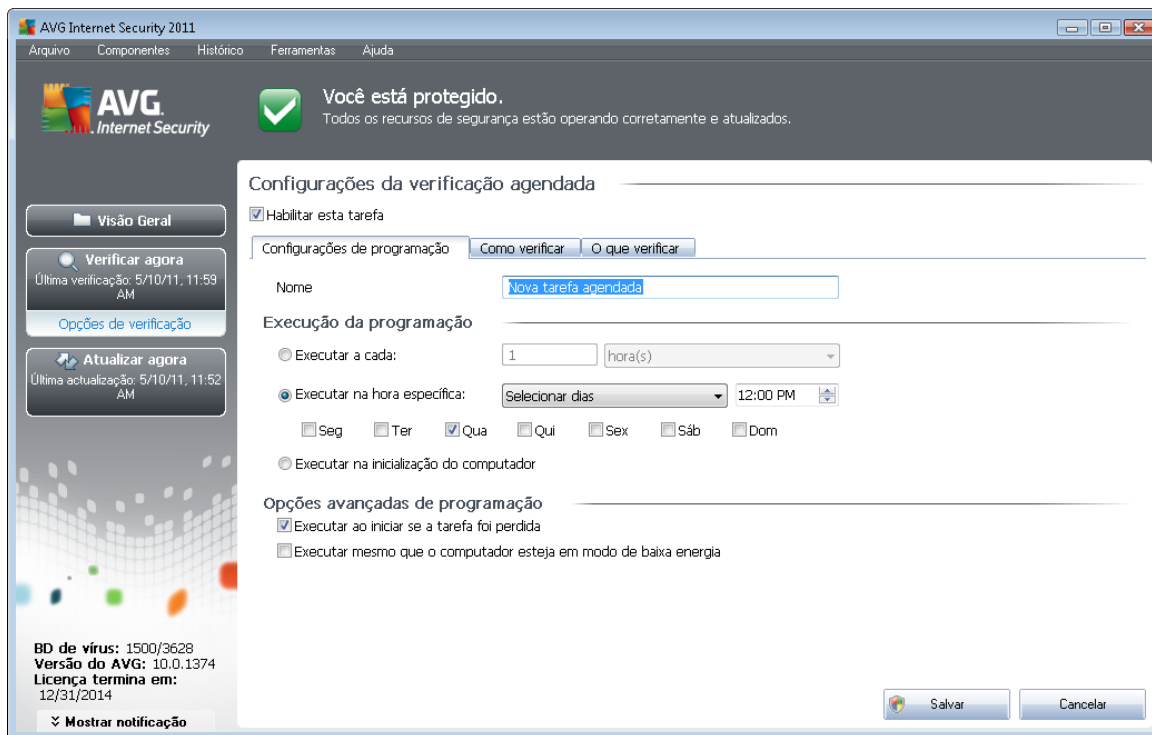


É possível editar/adicionar verificações usando os seguintes botões de controle:

- **Adicionar programação de verificação** - o botão abre a caixa de diálogo **Configurações da verificação programada**, guia [Configurações de programação](#). Nessa caixa de diálogo, você pode especificar os parâmetros do teste definido recentemente.
- **Editar programação de 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 programação](#). Os parâmetros do teste selecionado já estão especificados e poderão ser editados aqui.
- **Excluir programação de 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 **Programação 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 programação

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



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

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

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

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

- **Execução do programa** - especifica os intervalos de tempo para a inicialização de novas verificações programadas. O tempo pode ser definido pela repetição da inicialização da verificação depois de um determinado período (**Executar a cada ...**) pela definição de uma data e hora exatas (**Executar em uma hora específica...**), ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (**Ação baseada na inicialização do computador**).
- **Opções de programa avançadas** - essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

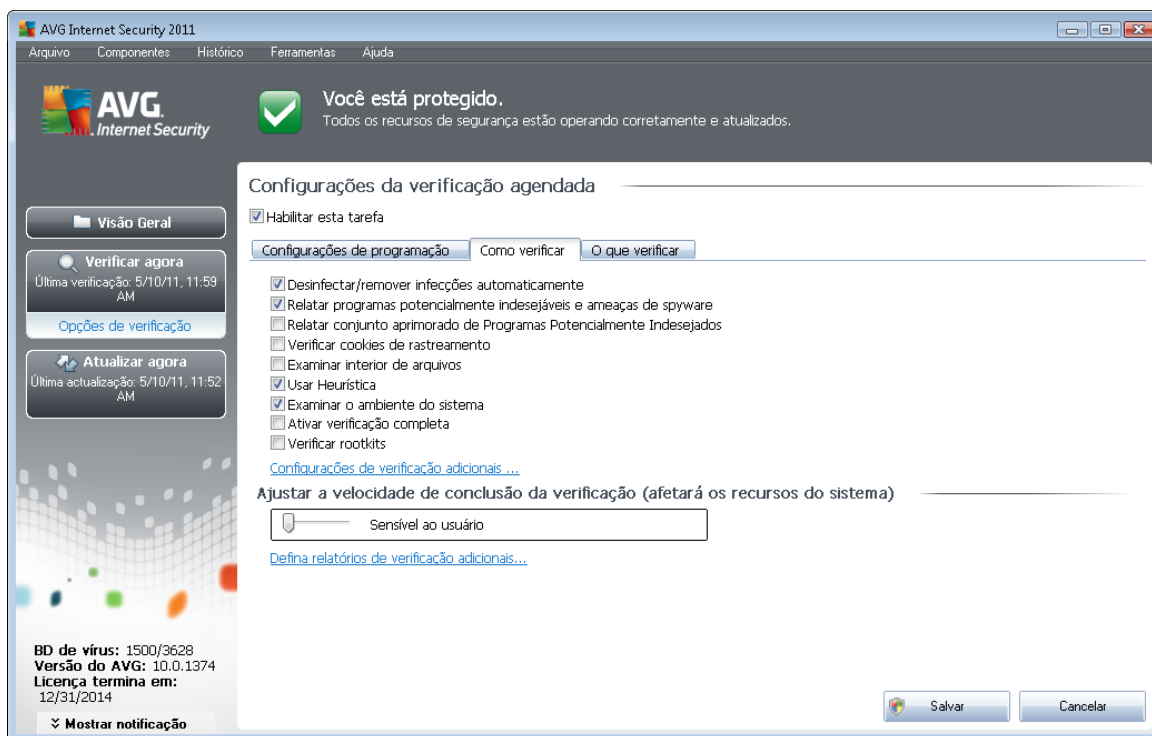


Botões de controle da caixa de diálogo Configurações para verificação programada

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

- **Salvar** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a [caixa de diálogo padrão da interface de verificação do AVG](#). Portanto, se você deseja 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:

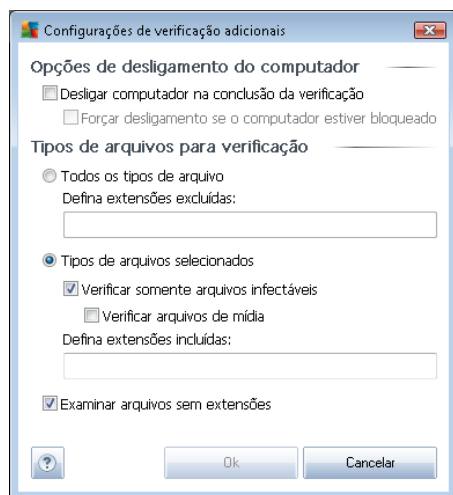
- **Reparar ou remover vírus automaticamente** (ativada por padrão): se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Caso não seja possível reparar o arquivo infectado automaticamente ou se você decidir desativar essa opção, você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

o arquivo infectado para a [Quarentena de vírus](#).

- **Informar programas potencialmente indesejáveis e ameaças de spyware** – marque para ativar o mecanismo [Anti-Spyware](#) e **verificar spyware, bem como vírus**. [Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente](#). Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Informar conjunto avançado de programas potencialmente indesejáveis** (desativada por padrão): marque para detectar o pacote estendido de [spyware](#): programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.
- **Verificar cookies de rastreamento** (desativada por padrão): este 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 carrinhos de compras eletrônicas).
- **Verificar interior dos arquivos** (desativada 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** (ativada 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** (ativada por padrão): a verificação também atuará nas áreas do sistema do seu computador.
- **Ativar verificação completa** (desativada por padrão) - em situações específicas (suspeita de que seu computador foi infectado), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

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

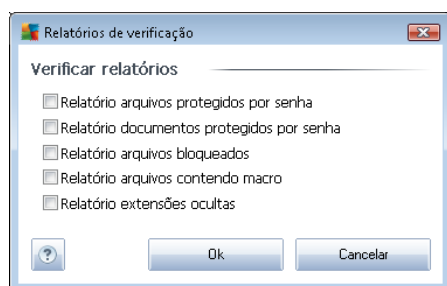
- **Configurações de verificação adicionais** - o link abre uma nova caixa de diálogo **Configurações de verificação adicionais**, na qual é possível especificar os seguintes parâmetros:



- o **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 que ele esteja bloqueado (**Forçar desligamento do computador se estiver bloqueado**).
- o **Definir tipos de arquivo para verificação** - além disso, você deve decidir se deseja verificar os seguintes itens:
 - **Todos os tipos de arquivos** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;
 - **Tipos de arquivos selecionados** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
 - Opcionalmente, você pode optar por **Verificar arquivos sem extensão** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.
- **Ajustar a velocidade de conclusão da verificação** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará*

para fazer a verificação), ou mais rápido, com maior necessidade 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:



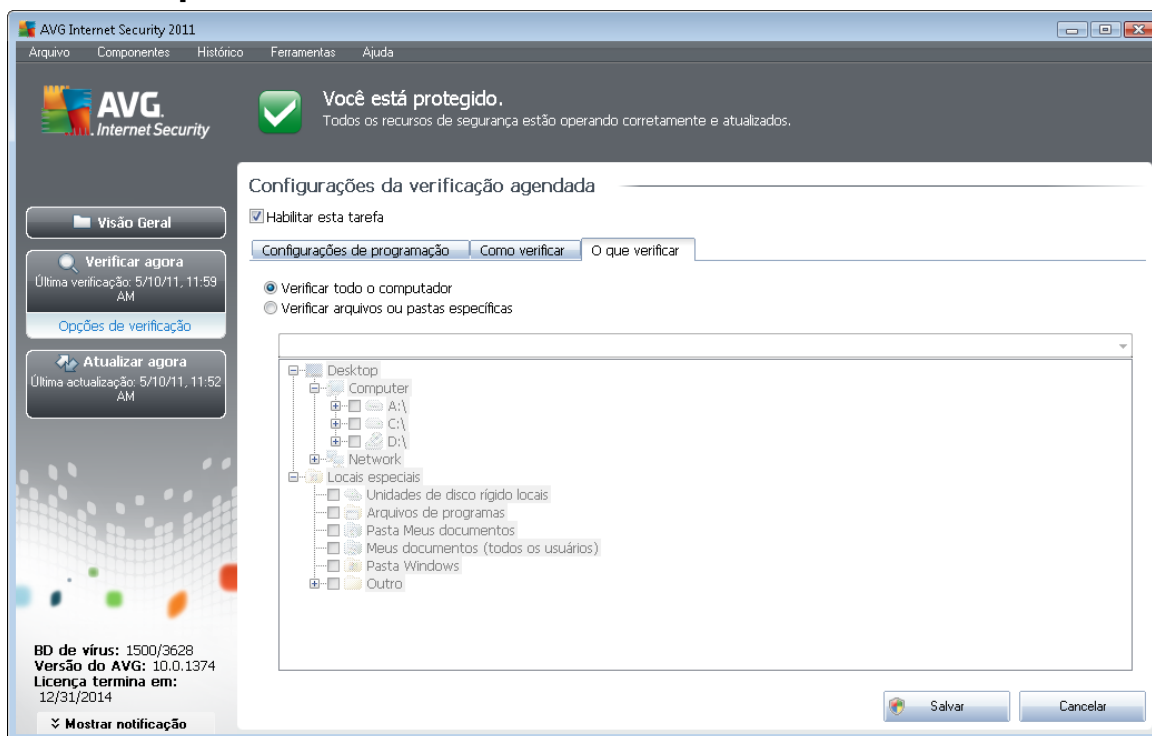
Observação: por padrão, a configuração da verificação é definida para desempenho ideal. A menos que você tenha um motivo válido para alterar essas configurações, é altamente recomendável manter a configuração predefinida. As alterações de configuração devem ser realizadas somente por usuários experientes. 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 (expanda os itens clicando no nó de mais até encontrar a pasta que deseja verificar). Você pode selecionar várias pastas marcando as respectivas caixas. As pastas selecionadas aparecerão no campo de texto na parte superior da caixa de diálogo e o menu suspenso manterá o histórico das verificações selecionadas para um uso posterior. *Ou você pode inserir o caminho inteiro para a pasta desejada manualmente (se inserir vários caminhos, será necessário separar com pontos-e-vírgulas sem espaços extras).*

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

- **Discos rígidos locais** - todos os discos rígidos de seu computador
- **Arquivos de programas**
 - o C:\Arquivos de Programas\
 - o na versão de 64 bits C:\Arquivos de Programas (x86)
- **Pasta Meus documentos**



o para Windows XP: C:\Documents and Settings\Usuário padrão\Meus documentos\

o para Windows Vista/7: C:\Usuários\usuário\Documentos\

- **Meus documentos (todos os usuários)**

o para Windows XP: C:\Documents and Settings\Todos os usuários\Documentos\

o para Windows Vista/7: C:\Usuários\Público\Documentos\

- **Pasta do Windows** - C:\Windows\

- **Outro**

o Drive de sistema – o disco rígido no qual o sistema operacional está instalado (normalmente C:)

o Pasta do sistema - C:\Windows\System32\

o Pasta Arquivos Temporários - C:\Documents and Settings\Usuário\Local\ (Windows XP); ou C:\Usuários\usuário\AppData\Local\Temp\ (Windows Vista/7)

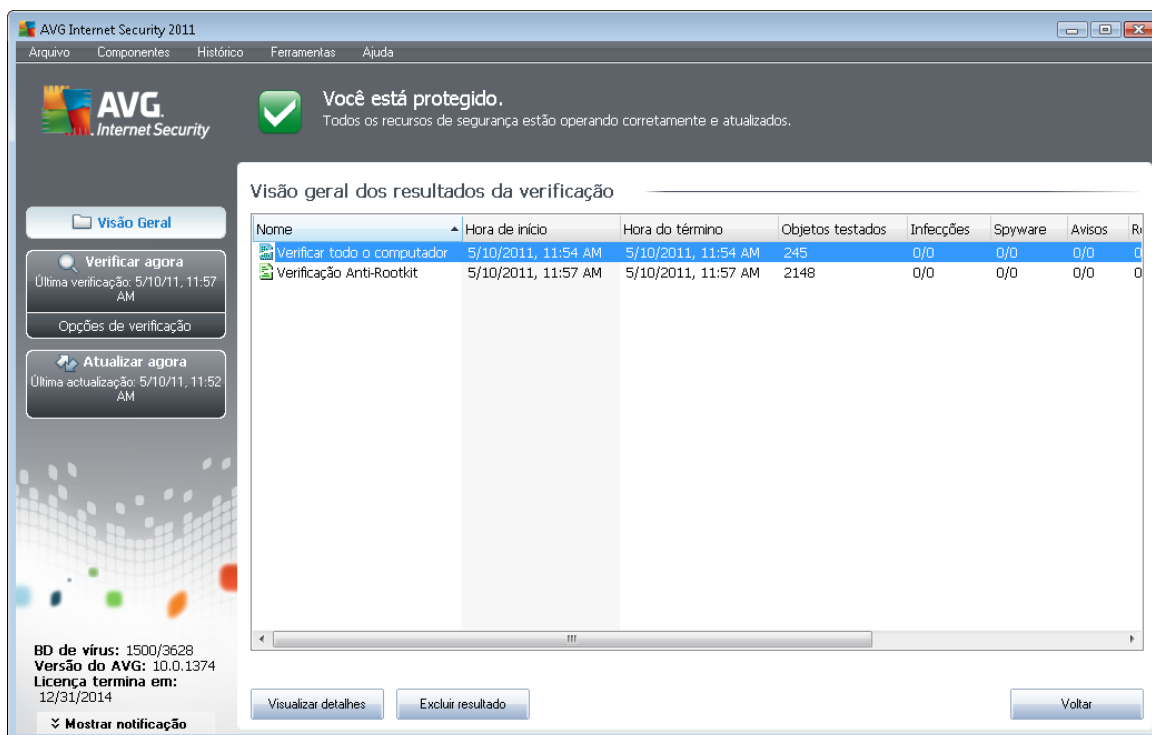
o Arquivos Temporários de Internet - C:\Documents and Settings\Usuário\Configurações locais\Arquivos temporários de Internet\ (Windows XP); ou C:\Usuários\usuário\AppData\Local\Microsoft\Windows\Arquivos Temporários de Internet (Windows Vista/7)

Botões de controle da caixa de diálogo Configurações para verificação programada

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

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

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
- **Infeções** - número de [infeções por vírus](#) detectadas/removidas
- **Spyware** - número de [spyware](#) detectados/removidos
- **Aviso** - número de [objetos suspeitos detectados](#)
- **Rootkits** - número de rootkits detectados [rootkits](#)
- **Informações do log de verificação** - informações relacionadas ao processo e o resultado da verificação (geralmente em sua finalização ou interrupção)

Botões de controle

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

- **Exibir detalhes** - pressione-o para ativar a caixa de diálogo [Resultados da verificação](#) para exibir dados detalhados na verificação selecionada
- **Excluir resultado** - pressione-o para remover o item selecionado a partir da visão geral dos resultados da verificação
- **Voltar** - volta para a caixa de diálogo padrão da [interface de verificação do AVG](#)

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.

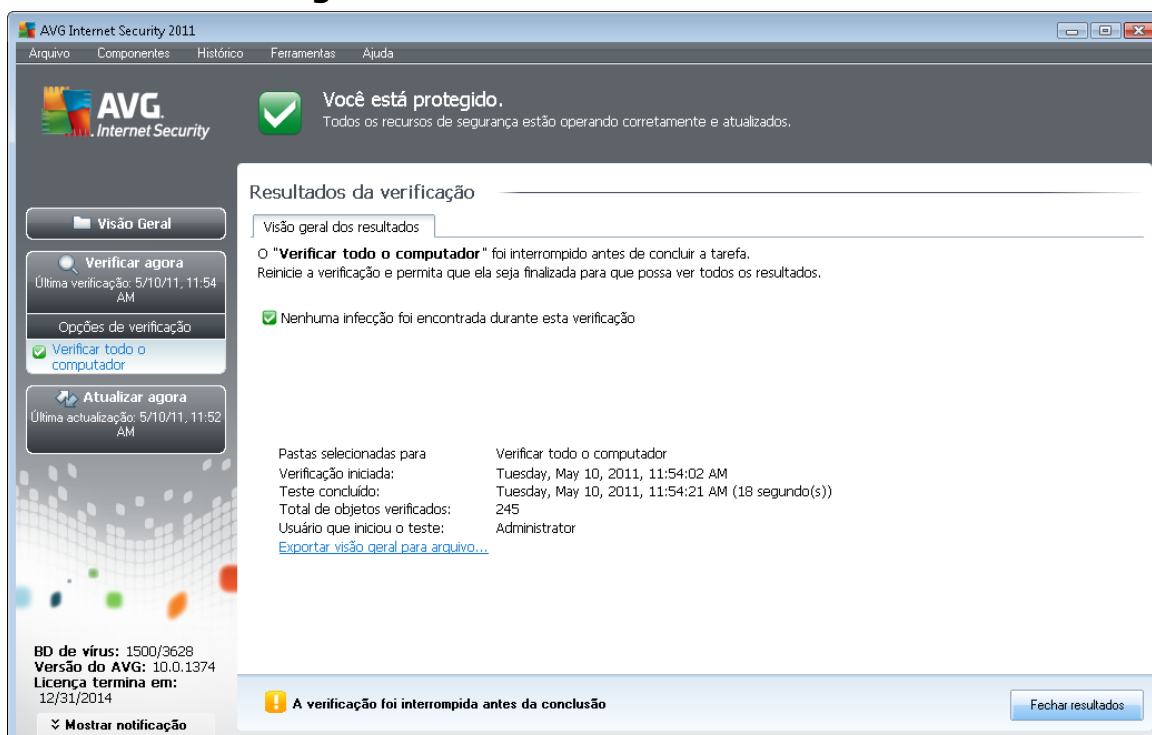
A caixa de diálogo divide-se em várias guias:

- [Visão Geral dos Resultados](#) - essa guia é exibida sempre e fornece dados estatísticos descrevendo o processo de verificação.
- [Infeções](#) - essa guia é exibida somente se uma [infeção por vírus](#) tiver sido detectada durante a verificação
- [Spyware](#) - essa guia é exibida somente se um [spyware](#) tiver sido detectado durante a verificação
- [Aviso](#) - essa guia é exibida somente se cookies forem detectados durante a verificação
- [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. Além disso, você vai encontrar aqui informações sobre objetos que não podem ser verificados (por exemplo, arquivos protegidos por senha).

11.7.1. Guia Visão geral dos resultados



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

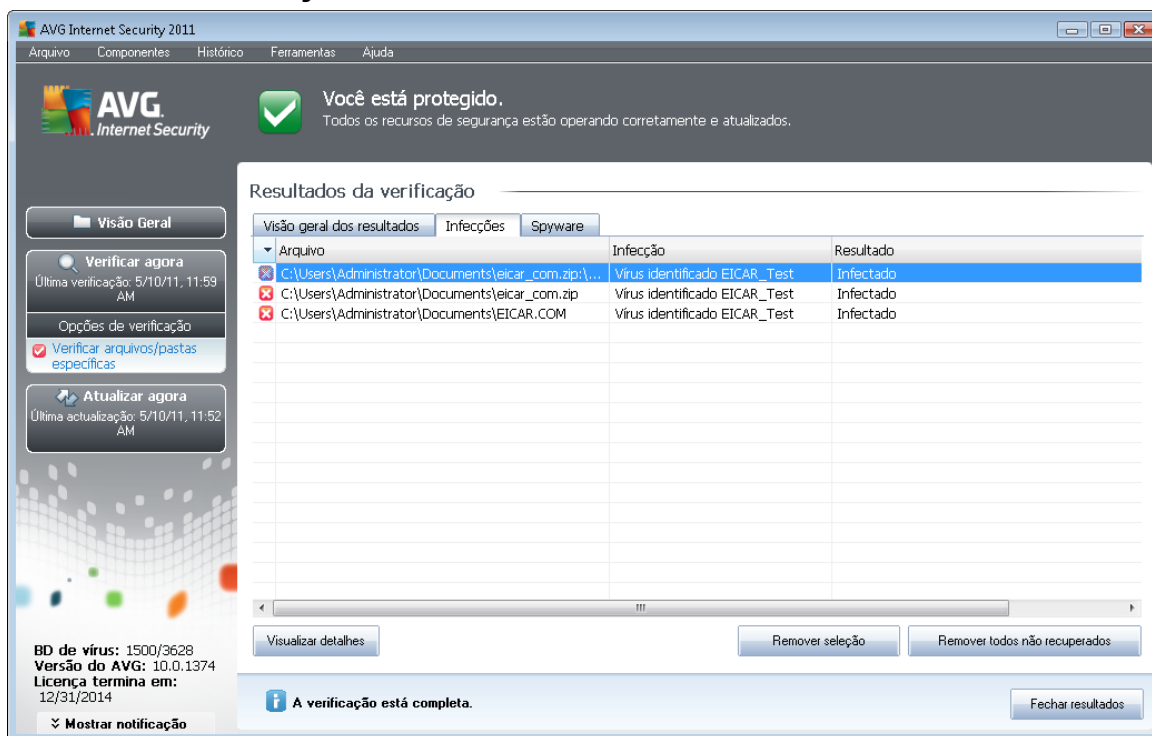
- infecções por [vírus/spyware detectadas](#)
- infecções [por vírus/spyware removidas](#)
- o número de [infecções por vírus/spyware](#) que não puderam ser removidas ou reparadas

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 será exibida na caixa de diálogo **Resultados da verificação** 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.
 - o **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).
 - o **Reparado** - o objeto infectado foi reparado automaticamente e mantido no local original
 - o **Movido para Quarentena de Vírus** - o objeto infectado foi movido para a [Quarentena de vírus](#).
 - o **Excluído** - o objeto infectado foi excluído.
 - o **Adicionado às exceções PPI** - a detecção foi avaliada como exceção e adicionada à lista de exceções PPI (configurada na caixa de diálogo [Exceções PPI](#) das

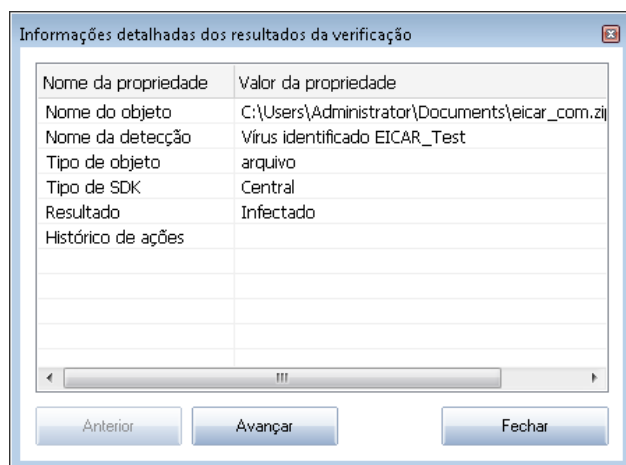
configurações avançadas)

- o **Arquivo bloqueado - não testado** - o objeto é bloqueado e o AVG não pode verificá-lo.
- o **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 como aviso.
- o **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:

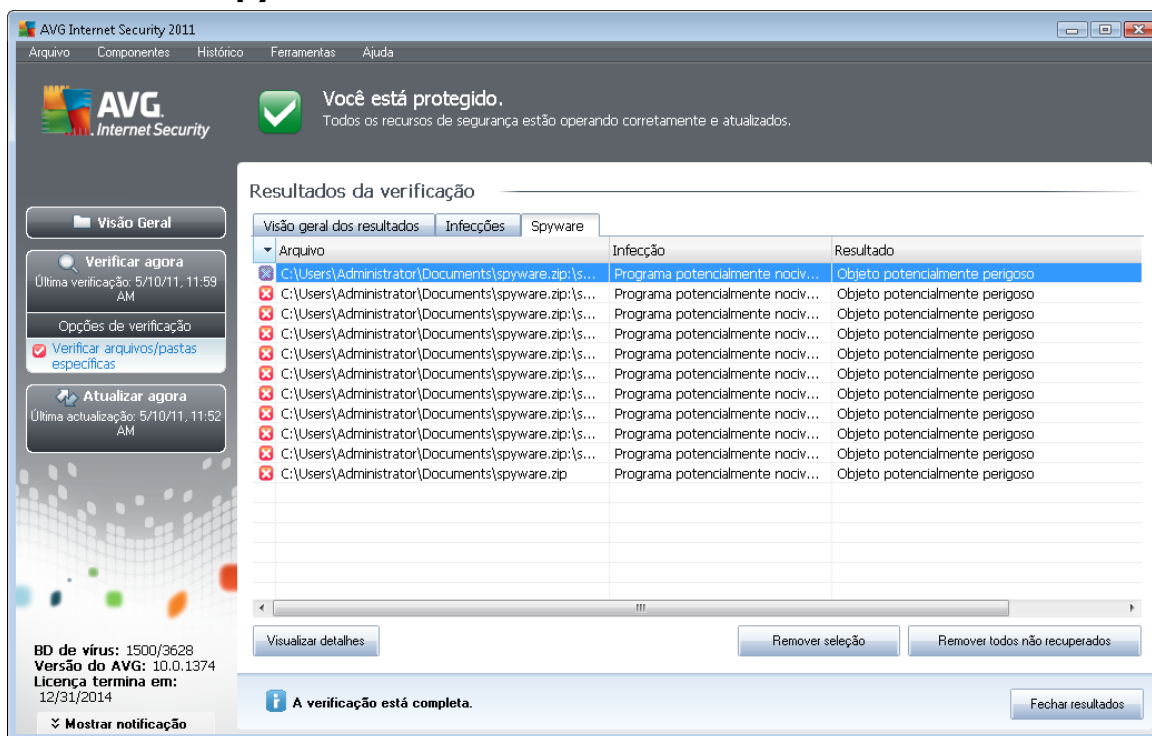
- **Exibir detalhes** - o botão abre uma nova janela de diálogo denominada **Informações detalhadas do objeto**:



Nesta caixa de diálogo, você pode encontrar informações detalhadas sobre o objeto infeccioso selecionado (*por exemplo, nome e local do objeto infeccioso, tipo de objeto, tipo de SDK, resultado da detecção e histórico de ações relacionado ao objeto detectado*). Usando os botões **Voltar/Avançar**, você pode ver informações sobre descobertas específicas. Use o botão **Fechar** para fechar a caixa de diálogo.

- **Remover selecionadas** - use o botão para mover a descoberta selecionada para a [Quarentena](#)
- **Remover todas as 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:

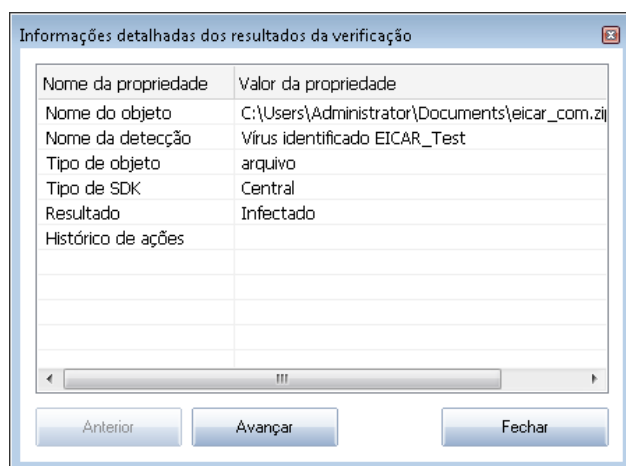
- **Arquivo** - caminho completo para o local original do objeto infectado
- **Infecções** - nome do **spyware** detectado (*para obter detalhes sobre os vírus específicos, consulte a [Enciclopédia de Vírus](#) online*)
- **Resultado** - define o status atual do objeto detectado durante a verificação.
 - o **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).
 - o **Reparado** - o objeto infectado foi reparado automaticamente e mantido no local original
 - o **Movido para Quarentena de vírus** - o objeto infectado foi movido para a [Quarentena de vírus](#).
 - o **Excluído** - o objeto infectado foi excluído.
 - o **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*)

- o **Arquivo bloqueado - não testado** - o objeto é bloqueado e o AVG não pode verificá-lo.
- o **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.
- o **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 **Informações detalhadas do objeto**:



Nesta caixa de diálogo, você pode encontrar informações detalhadas sobre o objeto infeccioso selecionado (*por exemplo, nome e local do objeto infeccioso, tipo de objeto, tipo de SDK, resultado da detecção e histórico de ações relacionado ao objeto detectado*). Usando os botões **Voltar/Avançar**, você pode ver informações sobre descobertas específicas. Use o botão **Fechar** para sair da caixa de diálogo.

- **Remover selecionadas** - use o botão para mover a descoberta selecionada para a [Quarentena](#)
- **Remover todas as 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 Rootkits

A guia **Rootkits** exibe informações sobre rootkits detectados durante a verificação caso você tenha iniciado a [Verificação Anti-Rootkit](#).

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

A estrutura dessa guia é basicamente a mesma que a da [guia Infecções](#) ou da [guia Spyware](#).

11.7.6. Guia Informações

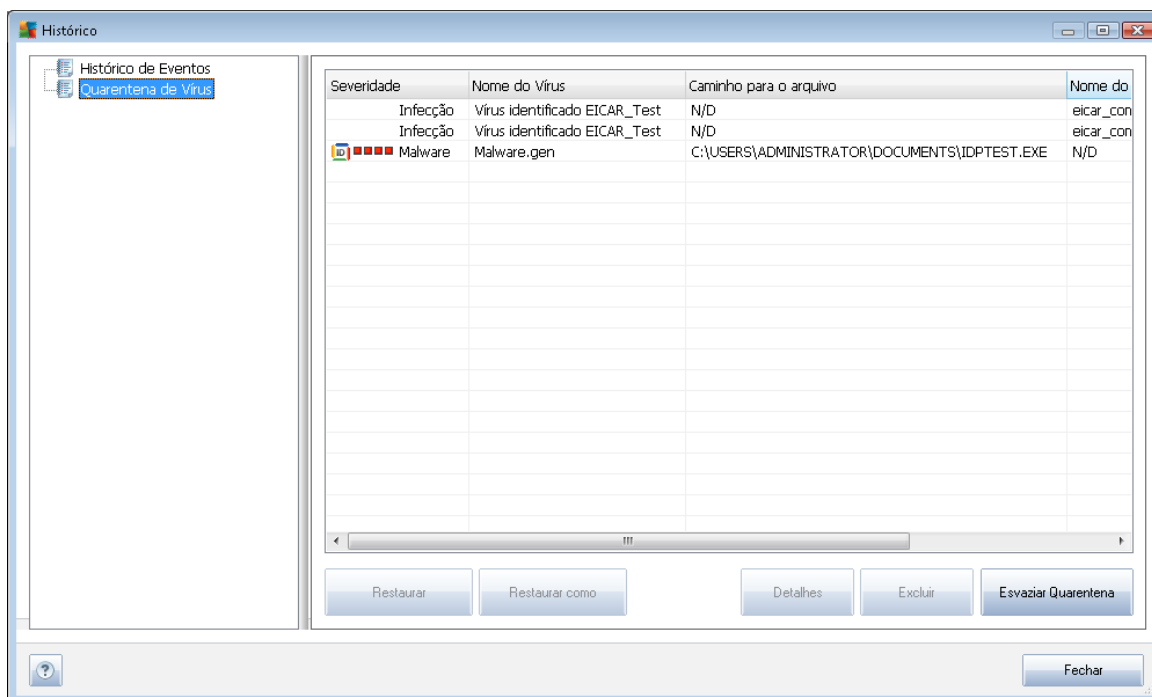
A guia **Informações** contém dados como "descobertas" que não podem ser categorizadas como infecções, spyware etc. Elas também não podem ser rotuladas positivamente como perigosas, mas merecem a sua atenção. A verificação do AVG pode detectar arquivos que talvez não estejam infectados, mas que são suspeitos.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

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



- **Compactado em tempo de execução** - o arquivo foi compactado com um dos compactadores menos comuns, o que pode indicar uma tentativa de impedir a verificação desse arquivo. Entretanto, nem todos os relatórios de tal arquivo indica um vírus.
- **Compactado em tempo de execução com recorrência** - semelhante ao problema acima, mas menos freqüente entre os softwares comuns. Esses arquivos são suspeitos e convém considerar sua remoção ou envio para análise.
- **Arquivamento ou documento protegido por senha** - arquivos protegidos por senha não podem ser verificados pelo AVG (ou em geral por qualquer outro programa anti-malware).
- **Documento com macros** - o documento relatado contém macros, que podem ser mal-intencionadas.
- **Extensão oculta** - arquivos com extensão oculta podem parecer ser, por exemplo, imagens, quando na verdade são arquivos executáveis (por exemplo, *imagem.jpg.exe*). A segunda extensão não está visível no Windows por padrão, e o AVG relata esses arquivos para evitar a abertura acidental.
- **Caminho de arquivo impróprio** - se algum arquivo do sistema importante estiver em execução a partir de um caminho diferente do padrão (por exemplo, *winlogon.exe* em execução a partir de um caminho diferente da pasta *Windows*), o AVG irá relatar essa discrepância. Em alguns casos, vírus usam nomes de processos padrão do sistema para tornar sua presença menos aparente no sistema.
- **Arquivo bloqueado** - o arquivo relatado está bloqueado, e por isso não pode ser verificado pelo AVG. Isso normalmente significa que algum arquivo é constantemente utilizado pelo sistema (por exemplo, *arquivo swap*).

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. O principal objetivo da Quarentena de Vírus é conservar qualquer arquivo excluído por um certo período de tempo para que você tenha certeza de que não precisa mais dele em seu local original. Se você descobrir que a ausência de arquivos causa problemas, pode enviar o arquivo em questão para análise ou restaurá-lo para o local original.

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

- **Severidade** caso você decida instalar o componente [Identity Protection](#) no seu **AVG Internet Security 2011**, uma identificação gráfica da respectiva severidade da descoberta, em uma escala de quatro níveis que varia desde incensurável (■□□□) até muito perigosa (■■■■) será fornecida nesta seção; e as informações sobre o tipo de infecção (com base em seu nível de infecção - todos os objetos listados podem estar positivamente ou potencialmente infectados).
- **Nome do vírus** - especifica o nome da infecção detectada de acordo com a [Enciclopédia de vírus](#) (online)
- **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



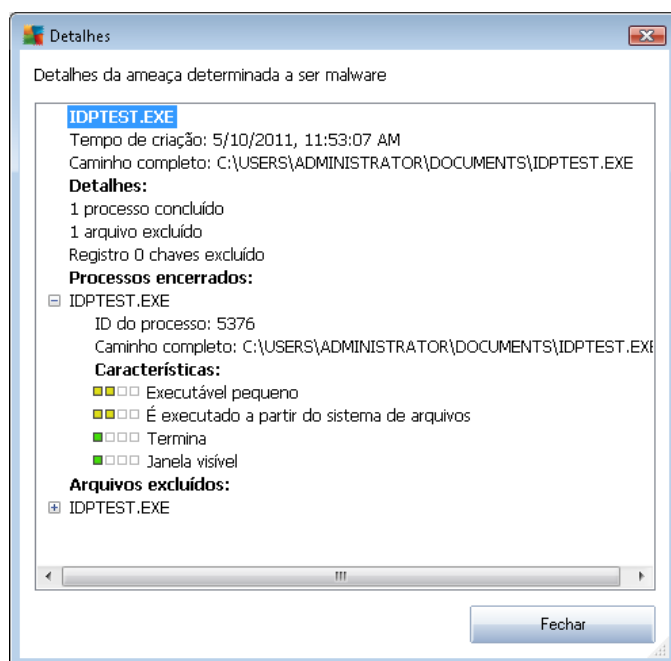
com o nome padrão dado pelo AVG durante o processo de verificação. No caso de o objeto ter tido um nome original que é conhecido (*por ex., o nome de um anexo de e-mail que não corresponda ao conteúdo real do anexo*), ele será fornecido nesta coluna.

- **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** – move o arquivo infectado para a pasta selecionada
- **Detalhes** – esse botão aplica-se apenas às ameaças detectadas pelo [Identity Protection](#). Ao clicar, exibe uma visão geral sinótica dos detalhes da ameaça (quais arquivos/processos foram afetados, características do processo, etc.). Observe que para todos os outros itens que não sejam detectados pelo IDP, esse botão fica esmaecido e inativo!



- **Excluir** - remove de maneira completa e irreversível o arquivo infectado da **Quarentena**
- **Esvaziar a Quarentena** - remove completamente todo o conteúdo da **Quarentena de Vírus**. Removendo os arquivos da **Quarentena**, esses arquivos serão removidos de modo irreversível do disco (*e não para a Lixeira*).



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 ou com frequência ainda maior. Somente dessa forma você pode ter a certeza de que o seu **AVG Internet Security 2011** é mantido atualizado também durante o dia.

12.1. Níveis de atualização

O AVG oferece dois níveis de atualização à sua escolha:

- **A atualização de definições** contém as alterações necessárias para a proteção antivírus confiável. Em geral, não inclui nenhuma alteração no código e atualiza apenas o banco de dados de definições. Essa atualização deverá ser aplicada assim que estiver disponível.
- **A atualização do programa** contém várias alterações, correções e aperfeiçoamentos para o programa.

Ao [programar uma atualização](#), é possível selecionar o nível de prioridade a ser baixado e aplicado.

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

12.2. Tipos de atualização

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 diretamente da Internet ou do diretório da 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](#).

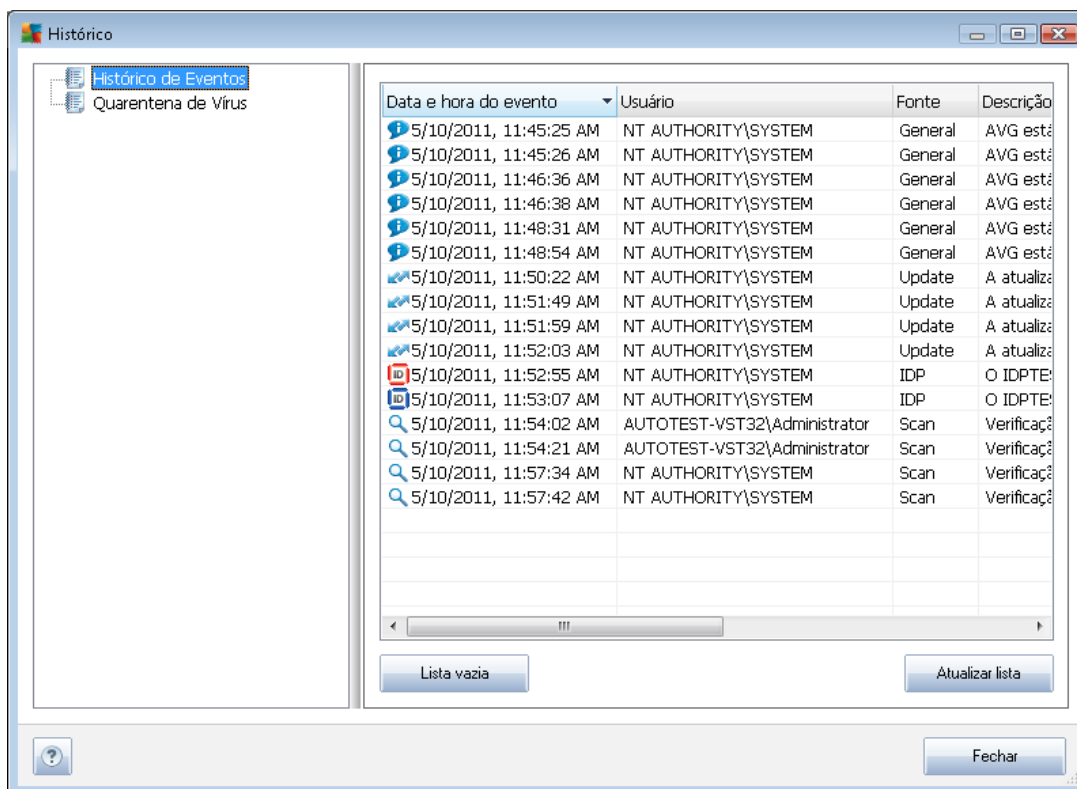
Quando você inicia a atualização, o AVG primeiro verifica se há novos arquivos de atualização disponíveis. Se houver, o AVG inicia o download e inicializa o processo de atualização propriamente



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*. Recomendável apenas para usuários experientes!

13. Histórico de eventos



A caixa de diálogo **Histórico** 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 Internet Security 2011. **Histórico** 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 [verificação](#)*), incluindo o local de ocorrência
- Outros eventos importantes

Para cada evento, as seguintes informações são listadas:

- **Data e hora do evento** fornece a data e a hora exata em que o evento ocorreu
- **Usuário** declara quem iniciou o evento
- **Origem** fornece o componente de origem ou a outra parte do sistema AVG que disparou o evento



- ***Descrição do evento*** fornece um breve resumo do que realmente aconteceu

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 Frequentes e Suporte Técnico

Se você tiver algum problema com o seu AVG, seja comercial ou técnico, consulte a seção [Perguntas frequentes](http://www.avg.com/) 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**.