



AVG Internet Security

Manual do Usuário

Revisão do documento AVG.07 (25/11/2016)

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



Conteúdo

1. Introdução	3
2. Requisitos de instalação do AVG	4
2.1 Sistemas operacionais com suporte	4
2.2 Requisitos mínimos e recomendados de hardware	4
3. Processo de instalação do AVG	5
3.1 Bem-vindo!	5
3.2 Insira seu número de licença	6
3.3 Personalize sua instalação	8
3.4 Instalação do AVG	9
3.5 Instalação concluída	10
4. Após a Instalação	11
4.1 Atualização do banco de dados de vírus	11
4.2 Registro do produto	11
4.3 Acesso à interface do usuário	11
4.4 Verificação de todo o computador	11
4.5 Teste Eicar	11
4.6 Configuração padrão do AVG	12
5. Interface de usuário do AVG	13
5.1 Linha superior de navegação	14
5.2 Informações sobre status de segurança	17
5.3 Visão geral dos componentes	18
5.4 Meus aplicativos	19
5.5 Verificar / Atualizar links rápidos	19
5.6 Ícone da bandeja do sistema	20
5.7 AVG Advisor	21
5.8 AVG Accelerator	21
6. Componentes do AVG	22
6.1 Proteção para o computador	22
6.2 Proteção de navegação da Web	26
6.3 Analisador de Software	27
6.4 Proteção de email	29
6.5 Firewall	30
6.6 PC Analyzer	33
7. Configurações avançadas do AVG	35
7.1 Aparência	35
7.2 Sons	37
7.3 Desativar temporariamente a proteção do AVG	38
7.4 Proteção para o computador	39



7.5 Verificador de Email	44
7.6 Proteção para a navegação web	60
7.7 Analisador de software	63
7.8 Verificações	64
7.9 Programações	70
7.10 Atualizar	78
7.11 Exceções	82
7.12 Quarentena de Vírus	84
7.13 Auto Proteção do AVG	85
7.14 Preferências de privacidade	85
7.15 Ignorar status de erro	87
7.16 Advisor – Redes conhecidas	88
8. Configurações de Firewall	89
8.1 Geral	89
8.2 Aplicativos	91
8.3 Compartilhamento de arquivos e impressora	92
8.4 Configurações avançadas	93
8.5 Redes definidas	94
8.6 Serviços de Sistema	95
8.7 Logs	96
9. Verificação do AVG	99
9.1 Verificações predefinidas	101
9.2 Verificando o Windows Explorer	110
9.3 Verificação de linha de comando	110
9.4 Programação de verificação	114
9.5 Resultados da verificação	122
9.6 Detalhes dos resultados da verificação	123
10. AVG File Shredder	124
11. Quarentena de Vírus	125
12. Histórico	126
12.1 Resultados da verificação	126
12.2 Resultado da Proteção Residente	127
12.3 Resultados do Identity Protection	130
12.4 Resultados da Proteção de Email	131
12.5 Resultado da Proteção Online	132
12.6 Histórico de Eventos	134
12.7 Log do firewall	135
13. Atualizações do AVG	137
14. Perguntas frequentes e Suporte técnico	138



1. Introdução

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

O **AVG Internet Security** fornece várias camadas de proteção para tudo o que você faz online. Isso significa que você não precisa se preocupar com roubos de identidade, vírus ou visitas a sites prejudiciais. Os recursos da AVG Protective Cloud Technology e AVG Community Protection Network estão incluídos, o que significa que obtemos as informações sobre as ameaças mais recentes e as compartilhamos com nossa comunidade para garantir que você receba a melhor proteção. Você pode fazer compras e usar serviços bancários com segurança, aproveitar as redes sociais ou navegar e pesquisar com a confiança de uma proteção em tempo real.

Você pode também usar outras fontes de informações:

- **Arquivo de ajuda:** Uma seção de *Solução de problemas* está disponível diretamente do arquivo de ajuda incluso no **AVG Internet Security** (para abrir o arquivo de ajuda, pressione a tecla F1 em qualquer diálogo do aplicativo). Essa seção fornece uma lista das situações mais frequentes que ocorrem quando um usuário deseja buscar ajuda profissional para um problema técnico. Selecione a situação que melhor descreve seu problema e clique nela para abrir instruções detalhadas que podem solucionar o problema.
- **Centro de suporte do website da AVG:** Outra opção é buscar a solução para seus problemas no site do AVG (<http://www.avg.com/>). Na seção **Suporte**, é possível encontrar uma visão geral de grupos temáticos que tratam de problemas técnicos e de venda, uma seção estruturada com perguntas frequentes e todos os contatos disponíveis.
- **AVG ThreatLabs:** Um website específico relacionado ao AVG (<http://www.avg.com/about-viruses>) dedicado a problemas de vírus que fornece uma visão geral estruturada de informações relacionadas a ameaças online. Você também pode encontrar instruções sobre a remoção de vírus, spyware e dicas sobre como permanecer protegido.
- **Fórum de discussões:** Você também pode usar o fórum de discussões de usuários do <http://community.avg.com/>.



2. Requisitos de instalação do AVG

2.1. Sistemas operacionais com suporte

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

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (todas as edições)
- Windows 7 (todas as edições)
- Windows 8 (todas as edições)
- Windows 10 (todas as edições)

(e possíveis service packs posteriores para sistemas operacionais específicos)

2.2. Requisitos mínimos e recomendados de hardware

Os requisitos mínimos de hardware para **AVG Internet Security**:

- Processador Intel Pentium 1,5 GHz ou mais veloz
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memória RAM
- 1,3 GB de espaço livre em disco rígido (*para fins de instalação*)

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

- Processador Intel Pentium 1,8 GHz ou mais veloz
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memória RAM
- 1,6 GB de espaço livre em disco rígido (*para fins de instalação*)



3. Processo de instalação do AVG

Para instalar o **AVG Internet Security** em seu computador, você precisa obter o arquivo de instalação mais recente. Para garantir que você esteja instalando a versão atualizada do **AVG Internet Security**, recomenda-se baixar o arquivo de instalação no site do AVG (<http://www.avg.com/>). A seção **Suporte** fornece uma visão geral estruturada dos arquivos de instalação para cada edição do AVG. Após baixar e salvar o arquivo de instalação no disco rígido, você poderá iniciar o processo de instalação. A instalação é uma sequência de caixas de diálogo simples e fáceis de entender. Cada caixa de diálogo oferece uma rápida descrição de como proceder em cada etapa do processo de instalação. Oferecemos uma explicação detalhada sobre cada janela de caixa de diálogo abaixo:

3.1. Bem-vindo!

O processo de instalação começa com a caixa de diálogo **Bem-vindo ao AVG Internet Security**.



Seleção de idioma

Nesse diálogo, você pode selecionar o idioma usado no processo de instalação. Clique na caixa de combinação ao lado da opção **Idioma** para rolar para baixo o menu de idioma. Selecione o idioma desejado e o processo de instalação continuará no idioma de sua escolha. Além disso, o aplicativo se comunicará no idioma selecionado, com a opção de trocar para inglês que sempre é instalado como padrão.

Contrato de Licença do Usuário Final e Política de Privacidade

Antes de continuar com o processo de instalação, recomendamos conhecer o **Contrato de Licença do Usuário Final** e a **Política de Privacidade**. Ambos os documentos podem ser acessados através dos links ativos na parte inferior da caixa de diálogo. Clique em qualquer um dos hyperlinks para abrir um novo diálogo / nova janela de navegador que fornece o texto integral do respectivo instrumento. Leia com atenção todos



esses documentos legalmente vinculativos. Ao clicar no botão **Prosseguir**, você confirma que concorda com os documentos.

Prossiga com a instalação

Para prosseguir com a instalação, é só clicar no botão **Prosseguir**. Você será solicitado a fornecer seu número de licença e o processo de instalação será executado então em modo totalmente automático. Para a maioria dos usuários, recomendamos usar essa opção padrão para instalar seu **AVG Internet Security** com todas as 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, sempre haverá a opção de fazer isso diretamente no aplicativo.

Como alternativa, há a opção de **Instalação personalizada** que está disponível na forma de um hyperlink localizado sob o botão **Prosseguir**. A instalação personalizada deve ser usada somente por usuários experientes que tenham um motivo válido para instalar o aplicativo com configurações diferentes do padrão, por exemplo, para atender aos requisitos específicos do sistema. Se decidir por essa instalação, após preencher seu número de licença, você será redirecionado à caixa de diálogo [Personalizar sua instalação](#), onde você pode especificar suas configurações.

3.2. Insira seu número de licença

Na caixa de diálogo **Insira seu número de licença** você é convidado a ativar sua licença digitando-a (ou usando o método "copiar e colar") no campo de texto fornecido:

AVG

← Insira seu número de licença

[Onde posso encontrá-lo?](#)

Não tem uma licença?
[Experimente o AVG Internet Security gratuitamente por 30 dias](#)

Continuar

Onde posso encontrar meu número de licença?

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



online. Digite o número exatamente como aparece. Se o formulário digital do número de licença estiver disponível (*no email*), é recomendável usar o método de copiar e colar para inseri-lo.

Como usar o método "copiar e colar".

O uso do método **copiar e colar** para inserir seu número de licença do **AVG Internet Security** no programa garante que o número seja inserido corretamente. Por favor, siga esse procedimento:

- Abra o email que contém o número de licença.
- Clique com o botão esquerdo do mouse no início do número de licença e mantenha o botão pressionando, arraste o mouse até o final do número e solte o botão. O número deverá estar realçado.
- Mantenha pressionada a tecla **Ctrl** enquanto pressiona **C**. Desse modo, o número é copiado.
- Aponte e clique na posição onde gostaria de colar o número copiado, ou seja, na caixa de texto da caixa de diálogo **Insira seu número de licença**.
- Mantenha pressionada a tecla **Ctrl** enquanto pressiona **V**. Desse modo, o número é colado no local selecionado.

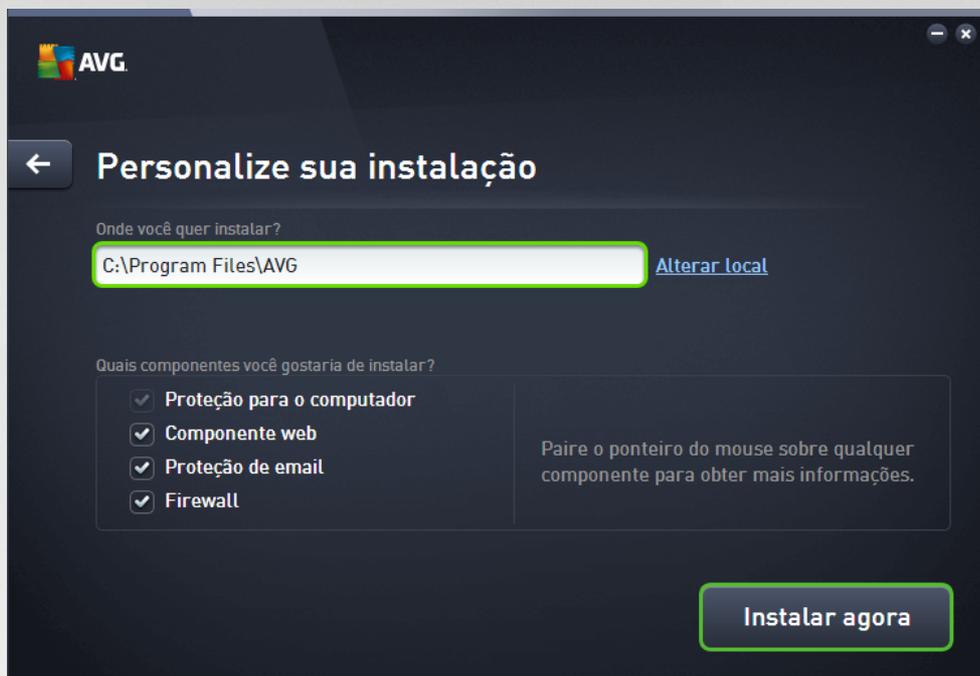
Prossiga com a instalação

Na parte inferior do diálogo você verá o botão **Instalar agora**. O botão é desativado após o número de licença ser inserido. Depois de ativado, basta clicar no botão e iniciar o processo de instalação. Caso não tenha um número de licença válido disponível, você pode escolher instalar o **AVG AntiVirus Free Edition** do aplicativo. Infelizmente, as versões gratuitas não comportam todos os recursos disponíveis na versão profissional completa. Assim, você deveria considerar acessar o website da AVG (<http://www.avg.com/>) para obter informações detalhadas sobre compras e atualizações da AVG.



3.3. Personalize sua instalação

A caixa de diálogo *Personalizar sua instalação* permite configurar parâmetros detalhados da instalação:



Onde você quer instalar?

Aqui, você pode especificar onde deseja instalar o aplicativo. O endereço no campo de texto mostra o local sugerido em sua pasta Arquivos de Programa. Se decidir usar outro local, clique no link **Alterar local** para abrir uma nova janela com a estrutura de árvore do seu disco. Depois, navegue para o local desejado e confirme.

Quais componentes você gostaria de instalar?

Essa seção exibe uma visão geral de todos os componentes que podem ser instalados. Se as configurações padrão não forem adequadas a você, será possível remover componentes específicos. Entretanto, você só pode selecionar os componentes incluídos na edição do AVG Internet Security! A única exceção é o componente **Proteção do computador**, que não pode ser excluída da instalação. Ao destacar algum item nessa seção, uma breve descrição do respectivo componente será exibida no lado direito. Para obter informações detalhadas sobre a funcionalidade de cada componente, consulte o capítulo 'Visão Geral de Componentes' dessa documentação.

Próxima com a instalação

Para prosseguir com a instalação, é só clicar no botão **Instalar agora**. Outra alternativa, caso precise alterar ou verificar suas configurações de idioma, é retroceder uma etapa da caixa de diálogo anterior usando o botão de seta  na parte superior dessa caixa de diálogo.



3.4. Instalação do AVG

Depois de confirmar o início da instalação na caixa de diálogo anterior, o processo de instalação é executado em modo totalmente automático e não exige nenhuma intervenção:

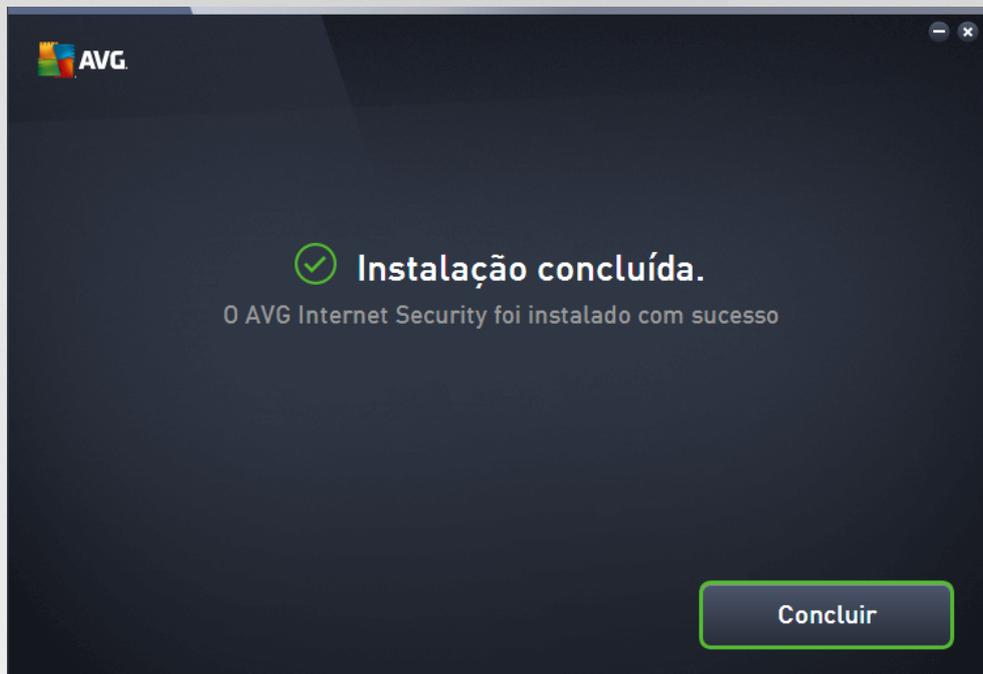


Após o término do processo de instalação, você será redirecionado automaticamente ao próximo diálogo.



3.5. Instalação concluída

A caixa de diálogo **Instalação concluída** confirma que o AVG Internet Security foi totalmente instalado e configurado:



Clique no botão **Finalizar** para finalizar o processo de instalação.



4. Após a Instalação

4.1. Atualização do banco de dados de vírus

Observe que, após a instalação (*após a reinicialização do computador, se for necessária*), o **AVG Internet Security** atualiza automaticamente seu banco de dados de vírus e todos os seus componentes, colocando-os em ordem de funcionamento total, o que pode levar alguns minutos. Enquanto o processo de atualização estiver em execução, você será notificado sobre o fato através das informações exibidas no diálogo principal. Espere um pouco para finalizar o processo de atualização e tenha seu **AVG Internet Security** completamente funcional e pronto para protegê-lo!

4.2. Registro do produto

Quando a instalação do **AVG Internet Security** for concluída, registre seu produto online no site do AVG (<http://www.avg.com/>). 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. A forma mais fácil de registrar o produto é diretamente pela interface de usuário do **AVG Internet Security**. Selecione o item [linha superior de navegação / Opções / Registrar-se agora](#). Você será direcionado à página de **Registro** no site do AVG (<http://www.avg.com/>). Siga as instruções fornecidas na página.

4.3. Acesso à interface do usuário

A [caixa de diálogo principal do AVG](#) pode ser acessada de várias maneiras:

- clique duas vezes no ícone da [bandeja do sistema](#) do AVG Internet Security
- clique duas vezes no ícone do AVG Protection na área de trabalho
- no menu *Iniciar / Todos os Programas / AVG / AVG Protection*

4.4. Verificação de todo o computador

Existe um risco potencial de um vírus de computador ter sido transmitido ao seu computador antes da instalação do **AVG Internet Security**. Por esse motivo, você deve executar uma [verificação de todo o computador](#) para assegurar que seu PC não esteja infectado. A primeira verificação levará algum tempo (*cerca de uma hora*), mas recomenda-se iniciá-la para garantir que seu computador não esteja comprometido com uma ameaça. Para ver as instruções sobre execução da [Verificação em todo o computador](#) consulte o capítulo [Verificação do AVG](#).

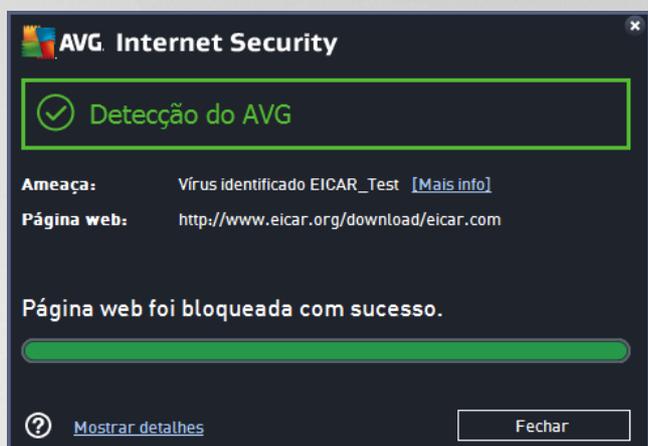
4.5. Teste Eicar

Para confirmar se o **AVG Internet Security** foi instalado corretamente, realize um teste EICAR.

O Teste Eicar é um método padrão e absolutamente seguro usado para testar o funcionamento do sistema antivírus. É seguro fazer o teste, porque não se trata de um vírus real e não inclui nenhum fragmento de código de vírus. A maioria dos produtos reage a ele como se fosse um vírus (*apesar de geralmente se referirem a ele por um nome óbvio: "EICAR-AV-Test"*). É possível baixar o vírus EICAR no site da EICAR, 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. Imediatamente, após confirmar o download do arquivo de teste, seu **AVG Internet Security** reagirá a ele com um aviso. Esse aviso demonstra que o AVG está instalado corretamente em seu computador.



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

4.6. Configuração padrão do AVG

A configuração padrão (*isto é, como o aplicativo é configurado logo após a instalação*) de **AVG Internet Security** 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.** Se desejar alterar a configuração do AVG de acordo com suas necessidades, vá para [Configurações Avançadas do AVG](#): selecione o item de menu do sistema *Opções/Configurações avançadas* e edite a configuração do AVG na nova caixa de diálogo aberta, a caixa de diálogo [Configurações avançadas do AVG](#).



5. Interface de usuário do AVG

AVG Internet Security abre a janela principal:



A janela principal é dividida em várias seções:

- **A linha superior de navegação** é composta por quatro links ativos alinhados na seção superior da janela principal (*Mais da AVG, Relatórios, Suporte, Opções*). [Detalhes >>](#)
- **Informações do Status de Segurança** fornece informações básicas sobre o status atual do seu AVG Internet Security. [Detalhes >>](#)
- A **visão geral dos componentes instalados** pode ser encontrada em uma faixa horizontal de blocos na seção central da janela principal. Os componentes são exibidos como blocos em verde claro, etiquetados com o ícone do respectivo componente, com as informações do status do componente. [Detalhes >>](#)
- **Meus Aplicativos** são representados graficamente na faixa central inferior da janela principal e oferecem uma visão geral dos aplicativos complementares ao **AVG Internet Security**, que já estão instalados em seu computador ou recomendados para instalação. [Detalhes >>](#)
- **Links rápidos de Verificação / Atualização** estão posicionados na linha inferior de blocos na janela principal. Esses botões permitem um acesso imediato às funções mais importantes e utilizadas mais frequentemente do AVG. [Detalhes >>](#)

Fora da janela principal do **AVG Internet Security**, há mais um elemento de controle que pode ser usado para acessar o aplicativo:

- O **ícone da bandeja do sistema** está localizado no canto inferior direito da tela (*na bandeja do sistema*), e indica o status atual do **AVG Internet Security**. [Detalhes >>](#)



5.1. Linha superior de navegação

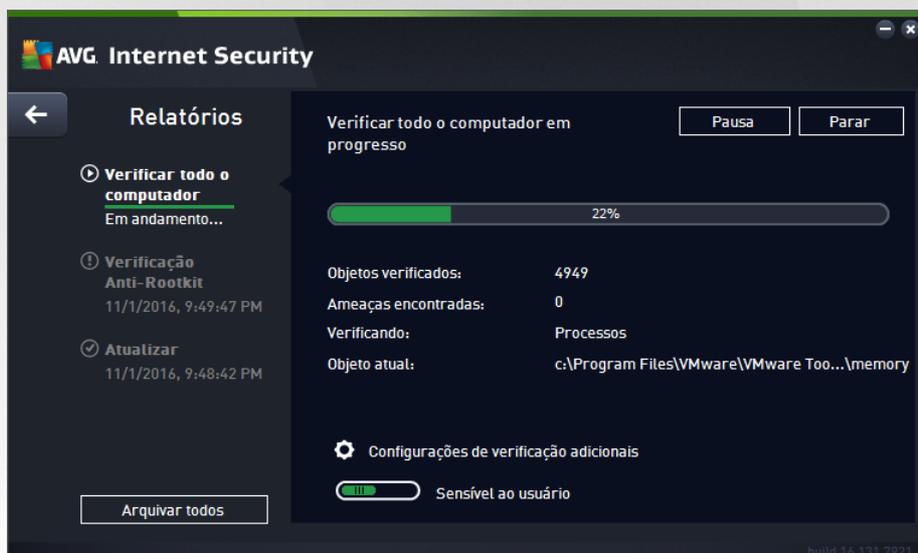
A **linha superior de navegação** abrange vários links ativos alinhados na seção superior da janela principal. A navegação contém os seguintes botões:

5.1.1. Mais da AVG

Clique uma vez no link para se conectar ao website da AVG para encontrar todas as informações sobre o AVG Protection e obter a máxima segurança na Internet.

5.1.2. Relatórios

Abre uma nova caixa de diálogo **Relatórios** com uma visão geral de todos os relatórios relevantes em processos de verificação e atualização anteriormente iniciados. Se a verificação ou atualização estiver sendo executada no momento, um círculo girando será exibido ao lado do texto **Relatórios** na navegação superior da [interface principal do usuário](#). Clique nesse círculo para obter o diálogo que descreve o progresso do processo em execução:





5.1.3. Suporte

Abre um novo diálogo estruturado em quatro guias onde é possível encontrar todas as informações relevantes sobre o **AVG Internet Security**:



- **Licença e suporte** – a guia fornece informações sobre o nome do produto, número de licença e data de expiração. Na parte inferior do diálogo é possível encontrar um resumo organizado claramente de todos os contatos disponíveis para o suporte ao cliente. Os links ativos e botões a seguir estão disponíveis na guia:
 - *(Re)ativar* – clique para abrir a nova caixa de diálogo **Ativar software AVG**. Insira seu número de licença no respectivo campo para substituir seu número de vendas (*que você usou durante a instalação do AVG Internet Security*) ou para substituir seu número de licença atual (*por exemplo, para fazer o upgrade para um produto AVG mais completo*).
 - *Copiar para área de transferência* – use esse link para copiar o número da licença e colá-lo onde for necessário. Desta forma você tem certeza que o número inserido está correto.
 - *Renovar agora* – recomendamos que você adquira a renovação da sua licença do **AVG Internet Security** com antecedência, pelo menos um mês antes da expiração da sua licença atual. Você será notificado sobre a aproximação da data de expiração. Clicar nesse link redireciona para o website da AVG (<http://www.avg.com/>), onde você encontra informações detalhadas sobre o status da sua licença, a data de expiração e a oferta de renovação/atualização.
- **Produto** – a guia fornece uma visão geral dos dados técnicos mais importantes do **AVG Internet Security** referentes às informações do produto antivírus, componentes instalados, proteção de email instalada e informações do sistema.
- **Programa** – nessa guia, você pode encontrar informações técnicas detalhadas sobre o **AVG Internet Security** instalado, como o número de versão do produto principal e a lista de números de versão de todos os produtos correspondentes (*p.ex., Zen, PC TuneUp, etc.*). Em seguida, essa guia fornece



uma visão geral de todos os componentes instalados e informações de seguranças específicas (números de versão do banco de dados de vírus, Link Scanner e Anti-Spam).

- **Contrato de licença** – a guia oferece o texto integral do contrato de licença entre você e a AVG Technologies.

5.1.4. Opções

A manutenção do **AVG Internet Security** é acessada através do item **Opções**. Clique na seta para abrir o menu de rolagem:

- [Verificar computador](#) inicia a verificação em todo o computador.
- [Verificar pasta selecionada...](#) – alterna para a interface de verificação do AVG e permite definir, na estrutura de árvore do computador, quais arquivos e pastas devem ser verificados.
- [Verificar arquivo...](#) – permite executar um teste sob demanda em um único arquivo específico. Clique nessa opção para abrir uma nova janela com a estrutura de árvore da sua unidade de disco. Selecione o arquivo desejado e confirme o início da verificação.
- [Atualizar](#) – inicia automaticamente o processo de atualização do **AVG Internet Security**.
- [Atualização a partir do diretório...](#) – executa o processo de atualização a partir dos arquivos de atualização localizados em uma pasta específica do disco local. No entanto, esta opção é recomendada somente em uma 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 o arquivo de atualização foi colocado anteriormente e inicialize o processo de atualização.
- [Quarentena de Vírus](#) – abre a interface para o espaço de quarentena, a Quarentena de Vírus, para onde o AVG remove todas as infecções detectadas. No espaço de quarentena, os arquivos infectados são isolados, a segurança do computador é preservada e, ao mesmo tempo, os arquivos infectados são armazenados para possível reparo futuro.
- [Histórico](#) – oferece mais opções de submenu específico:
 - [Resultados da verificação](#) – abre um diálogo fornecendo uma visão geral dos resultados da verificação.
 - [Resultados da Proteção Residente](#) – abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela Proteção Residente.
 - [Resultados do Analisador de Software](#) – abre uma caixa de diálogo com uma visão geral das ameaças detectadas pelo componente Analisador de Software.
 - [Resultados do Verificador de Email](#) – abre uma caixa de diálogo com uma visão geral dos anexos de email detectados como perigosos pelo componente Proteção de Email.
 - [Resultados da Proteção Online](#) – abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela Proteção Online.
 - [Log de histórico de eventos](#) – abre a interface de log de histórico com uma visão geral de todas as ações registradas do **AVG Internet Security**.



- [Log do firewall](#) – abre uma caixa de diálogo com uma visão geral detalhada de todas as ações do firewall.
- [Configurações avançadas...](#) – abre a caixa de diálogo Configurações avançadas do AVG, onde é possível editar a configuração do **AVG Internet Security**. Em geral, recomendamos manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.
- [Configurações de Firewall...](#) – abre uma caixa de diálogo independente para configuração avançada do componente Firewall.
- **Conteúdo da Ajuda** – abre os arquivos de ajuda do AVG.
- **Obter suporte** – abre o [diálogo de suporte](#) fornecendo todos os contatos e informações de suporte acessíveis.
- **Sua Web AVG** – abre o site do AVG (<http://www.avg.com/>).
- **Sobre vírus e ameaças** – abre a Enciclopédia de vírus online no website da AVG (<http://www.avg.com/>), onde é possível procurar informações sobre o vírus identificado.
- **(Re)ativar** – abre o diálogo de ativação com o número de licença fornecido durante o processo de instalação. Nessa caixa de diálogo é possível editar o número de licença para substituir o número de vendas (o número com o qual você instalou o AVG) ou para substituir o número antigo da licença (p.ex., durante a atualização de um novo produto da AVG). Se estiver utilizando a versão de teste do **AVG Internet Security**, os dois últimos itens aparecerão como **Comprar agora** e **Ativar**, permitindo comprar a versão completa do programa imediatamente. Para o **AVG Internet Security** instalado com um número de vendas, os itens são exibidos como **Registrar** e **Ativar**.
- **Registrar-se agora / MyAccount** – estabelece uma conexão com a página de registro do site da AVG (<http://www.avg.com/>). Informe seus dados de registro. Somente os clientes que registrarem seus produtos da AVG poderão receber suporte técnico gratuito.
- **Sobre o AVG** – abre um novo diálogo com quatro guias fornecendo dados sobre sua licença adquirida e informações de suporte, produto e programa, e o acordo de licença completo. (A mesma caixa de diálogo pode ser aberta através do link [Suporte](#) na navegação principal).

5.2. Informações sobre status de segurança

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



– o ícone verde indica que seu **AVG Internet Security está totalmente funcional**. Seu computador está totalmente protegido, atualizado e todos os componentes instalados estão funcionando corretamente.



– o ícone amarelo avisa que **um ou mais componentes estão configurados incorretamente** e é necessário verificar as propriedades e configurações. Não há problema crítico no **AVG Internet Security** e você provavelmente decidiu desativar um componente por algum motivo. Você continua protegido! Entretanto, preste atenção às configurações do componente com problema! O componente



configurado incorretamente será exibido com uma faixa de aviso laranja na [interface principal do usuário](#).

O ícone amarelo também aparecerá se, por algum motivo, você decidiu ignorar o status de erro de um componente. A opção **Ignorar status de erro** é acessada através da ramificação [Configurações avançadas / Ignorar status de erro](#). Você tem a opção para informar que você está ciente do estado de erro do componente, mas que, por alguma razão, deseja continuar com o **AVG Internet Security** e não quer ser avisado novamente sobre isso. Talvez seja necessário usar esta opção em uma situação específica, mas recomendamos desativar a opção **Ignorar status de erro** o mais rápido possível!

Como alternativa, o ícone amarelo será também exibido se o **AVG Internet Security** precisar reiniciar o computador (**reinicialização necessária**). Preste atenção a este aviso e reinicie seu PC.



– o ícone laranja indica que o **AVG Internet Security se encontra em estado crítico!** Um ou mais componentes não estão funcionando propriamente e o **AVG Internet Security** 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](#).

Caso o AVG Internet Security não tenha sido configurado para obter o melhor desempenho possível, um novo botão denominado Clique para corrigir (ou Clique para corrigir tudo, se o problema envolver mais de um componente) será exibido ao lado das informações sobre o status de segurança. Pressione o botão para iniciar um processo automático de verificação e configuração do programa. Essa é uma forma fácil de ajustar o AVG Internet Security para que ofereça o desempenho ideal e obtenha 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 Internet Security também podem ser obtidas a qualquer momento no [ícone da bandeja do sistema](#).

5.3. Visão geral dos componentes

A **visão geral dos componentes instalados** pode ser encontrada em uma faixa horizontal de blocos na seção central da [janela principal](#). Os componentes são exibidos como blocos em verde claro com o ícone do respectivo componente. Cada bloco fornece informações sobre o status atual da proteção. Se o componente for configurado corretamente e estiver completamente operacional, as informações são fornecidas em letras verdes. Se o componente estiver parado, com funcionamento limitado, ou o componente tem um estado de erro, você será notificado através de um texto de aviso exibido em um campo de texto laranja.

Recomendamos que você preste atenção às configurações dos respectivos componentes!

Mova o mouse sobre o componente para exibir um texto breve na parte inferior da [janela principal](#). O texto fornece uma introdução básica ao funcionamento do componente. Ele informa também sobre o status atual do componente e especifica quais serviços do componente não estão configurados corretamente.

Lista dos 'componentes instalados

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



- **Computador** - esses componentes abrangem dois serviços: **Proteção antivírus** que detecta vírus, spyware, worms, cavalos de Troia, arquivos executáveis indesejados ou bibliotecas no seu sistema, e protege contra adware mal intencionado; e o **Anti-Rootkit** que verifica se há rootkits perigosos ocultos em aplicativos, drivers ou bibliotecas. [Detalhes >>](#)
- **Navegação web** - protege contra ataques baseados na Web, enquanto você faz pesquisas ou navega na Internet. [Detalhes >>](#)
- **Software** - o componente executa o serviço **Analisador de Software** que protege constantemente seus ativos digitais contra ameaças novas e desconhecidas na Internet. [Detalhes >>](#)
- **Email** - verifica as mensagens de email recebidas em busca de SPAM, além de bloquear vírus, ataques de phishing ou outras ameaças. [Detalhes >>](#)
- **Firewall** - controla todas as comunicações em cada porta de rede, protegendo você contra ataques maliciosos e bloqueando todas as tentativas de invasão. [Detalhes >>](#)

Ações acessíveis

- **Mova o mouse sobre qualquer um dos ícones do componente** 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 uma vez no ícone do componente** para abrir a interface do componente com as informações sobre o seu status atual e acessar suas configurações e dados estatísticos.

5.4. Meus aplicativos

Na área **Meus aplicativos** (a linha de blocos verdes abaixo do conjunto de componentes) você pode encontrar uma visão geral de mais aplicativos do AVG que já estão instalados em seu computador, ou que são recomendados para instalação. Os blocos são exibidos condicionalmente, e podem representar um dos seguintes aplicativos:

- **Proteção móvel** é um aplicativo que protege seu celular contra vírus e malware. Ele também fornece a capacidade de rastrear seu smartphone remotamente se você se separar dele.
- O aplicativo **PC Tuneup** é uma ferramenta avançada para correção e análise detalhada do sistema, que tem o objetivo de aprimorar a velocidade e o desempenho geral de seu computador.

Para obter informações detalhadas sobre qualquer aplicativo dos **Meus Aplicativos**, clique no bloco correspondente. Você será direcionado à página web dedicada da AVG, onde também poderá baixar o componente imediatamente.

5.5. Verificar / Atualizar links rápidos

Links rápidos estão localizados na linha inferior de botões na [interface de usuário](#) do **AVG Internet Security**. Esses links permitem que você tenha acesso imediato aos recursos do aplicativo mais importantes e mais usados, como a verificação e a atualização. Os links rápidos podem ser acessados em todas as caixas de diálogo da interface do usuário:



- **Verificar agora** – esse botão divide-se graficamente em duas seções. Siga o link **Verificar agora** para iniciar a [Verificação de todo o computador](#) imediatamente e observe seu progresso e resultados na janela [Relatórios](#), que se abre automaticamente. O botão **Opções** abre o diálogo **Opções de verificação** onde é possível [gerenciar verificações programadas](#) e editar parâmetros da [Verificação de todo o computador / Verificar arquivos e pastas específicas](#). (Para obter detalhes, consulte o capítulo [Verificações do AVG](#))
- **Corrigir desempenho** – o botão leva para o serviço [PC Analyzer](#), uma ferramenta avançada para análise e correção detalhada do sistema, que mostra como a velocidade e desempenho geral do seu computador podem ser melhorados.
- **Atualizar agora** - pressione o botão para iniciar a atualização do produto imediatamente. Você será informado sobre os resultados da atualização no diálogo deslizante acima do ícone do AVG na bandeja do sistema. (Para obter detalhes, consulte o capítulo [Atualizações do AVG](#))

5.6. Ícone da bandeja do sistema

O **ícone da bandeja do sistema do AVG** (na barra de tarefas do Windows, no canto inferior direito da tela) indica o status atual do seu **AVG Internet Security**. Ele está sempre visível na bandeja do sistema, com a [interface de usuário](#) do seu **AVG Internet Security** aberta ou fechada:

Exibição do ícone da bandeja do sistema do AVG

-  Quando exibido colorido, sem elementos adicionais, o ícone indica que todos os componentes do **AVG Internet Security** estão ativos e totalmente funcionais. No entanto, o ícone também pode ser exibido dessa forma quando um dos componentes não está totalmente funcional, mas o usuário decidiu [ignorar o estado do componente](#). (Após confirmar a opção para ignorar o estado do componente, você está ciente do [estado de erro do componente](#), mas, por algum motivo, deseja mantê-lo, por isso não deseja ser informado sobre a situação).
-  O ícone com um ponto de exclamação indica que um componente (ou mais componentes) se encontra em [estado de erro](#). Preste sempre atenção nesses avisos e tente remover o problema de configuração de um componente que não foi configurado corretamente. Para alterar a configuração de um componente, clique duas vezes no ícone da bandeja do sistema para abrir a [interface de usuário do aplicativo](#). Para obter informações detalhadas sobre os componentes que se encontram em [estado de erro](#), consulte a seção de [informações sobre o status de segurança](#).
-  O ícone da bandeja do sistema também pode ser exibido em cores com um raio de luz que gira e pisca. Esta versão gráfica indica que há um processo de atualização em andamento.
-  A exibição em cores com uma seta indica que há uma verificação do **AVG Internet Security** em execução no momento.

Informações do ícone da bandeja do sistema do AVG

O **ícone da bandeja do sistema AVG** também informa sobre as atividades atuais do seu **AVG Internet Security** e possíveis mudanças de status no programa (p.ex., *início automático de uma verificação ou atualização agendada, troca do perfil do Firewall, alteração do status de um componente, ocorrência de status de erro, etc.*) através de uma janela pop-up aberta pelo ícone na bandeja do sistema.



Ações que podem ser acessadas no ícone da bandeja do sistema do AVG

O **ícone da bandeja do sistema do AVG** também pode ser usado como um link rápido para acessar a [interface de usuário](#) do **AVG Internet Security**, clicando duas vezes no ícone. Ao clicar com o botão direito no ícone, você abre um breve menu de contexto que permite acessar alguns dos recursos mais importantes:

- **Abrir** – use este botão para abrir a [interface de usuário principal](#).
- **Verificar agora** – use este botão para iniciar imediatamente a função [Verificar todo o computador](#).
- **Proteção** (ativado  / desativado ) – use este botão para desligar os componentes do **AVG Internet Security** que fornecem proteção em tempo real. Então, será possível especificar por quanto tempo o **AVG Internet Security** permanecerá inativo. Você também pode decidir se o componente Firewall também deve ser desligado. Você pode reativar a proteção do **AVG Internet Security** a qualquer momento, basta clicar no botão novamente.

5.7. AVG Advisor

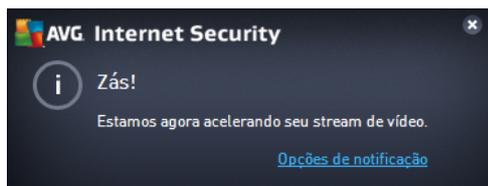
O **AVG Advisor** foi projetado para detectar problemas que possam colocar seu computador em risco e para recomendar uma ação para resolver essa situação. O **AVG Advisor** está visível na forma de um pop-up deslizante sobre a bandeja do sistema. O serviço detecta uma possível **rede desconhecida com um nome conhecido**. Isso geralmente se aplica a usuários que se conectam a várias redes, normalmente com computadores portáteis: Se uma rede nova e desconhecida tiver o mesmo nome de uma rede conhecida e frequentemente usada (*p.ex., Casa ou MeuWiFi*), pode ocorrer uma confusão e você se conectar acidentalmente em uma rede completamente desconhecida e potencialmente perigosa. O **AVG Advisor** pode evitar que isto ocorra, alertando de que o nome conhecido representa na verdade uma nova rede. Claro, se você decidir que a rede desconhecida é segura, você poderá salvá-la na lista de redes conhecidas do **AVG Advisor** para que ela não seja reportada novamente no futuro.

Navegadores web suportados

Este recurso funciona com os seguintes navegadores: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

O **AVG Accelerator** permite uma reprodução melhor de vídeos online e facilita downloads adicionais. Quando o processo de aceleração de vídeo estiver em andamento, você será notificado através de uma janela de pop-up na bandeja do sistema.





6. Componentes do AVG

6.1. Proteção para o computador

O componente **Computador** abrange dois serviços de segurança principais: **Antivírus** e **Cofre de Dados**.

- O **Antivírus** consiste em um mecanismo de verificação que protege todos os arquivos, áreas do sistema do computador e mídia removíveis (*pen drives, etc.*) e procura por vírus conhecidos. Todos os vírus detectados serão bloqueados para que não executem nenhuma ação e também serão apagados e colocados na [Quarentena de Vírus](#). Você nem notará o processo, já que essa proteção residente é executada "em segundo plano". O Antivírus utiliza também verificação heurística, na qual verifica-se se existem características típicas de vírus nos arquivos. Isso significa que o antivírus pode detectar um vírus novo e desconhecido se este contiver algumas características típicas dos vírus existentes. O **AVG Internet Security** é também capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL que podem ser potencialmente indesejáveis no sistema (*vários tipos de spyware, adware, etc.*). Além disso, o Antivírus verifica o registro do sistema em busca de entradas suspeitas, arquivos temporários da Internet e permite tratar todos os itens potencialmente indesejados da mesma maneira que qualquer outra infecção.
- O **Cofre de Dados** permite criar cofres virtuais seguros para armazenamento de dados valiosos ou sensíveis. O conteúdo de um Cofre de Dados é criptografado e protegido por uma senha de sua escolha, para que ninguém possa acessá-lo sem autorização.



Controles da caixa de diálogo

Para alternar entre as seções da caixa de diálogo, é só clicar em qualquer lugar do respectivo painel de serviço. O painel então fica destacado em um tom mais claro de azul. Em ambas as seções da caixa de diálogo, você pode encontrar os controles a seguir. Sua função é a mesma, não importando se ela pertence a um serviço de segurança ou ao outro (*Antivírus ou Cofres de Dados*):

 **Ativado / Desativado** – o botão se parece com um semáforo, tanto em aparência quanto em função. É só clicar para alternar entre as duas posições. A cor verde representa **Ativado**, o que



significa que o serviço de segurança AntiVirus está ativo e totalmente funcional. A cor vermelha representa o status de **Desativado**, ou seja, o serviço está desativado. Se não houver um bom motivo para desativar o serviço, recomendamos manter as configurações padrão de todas as configurações de segurança. As configurações padrão garantem o melhor desempenho do aplicativo e sua máxima segurança. Se por algum motivo você desejar desativar o serviço, você será avisado imediatamente sobre o possível risco através do sinal de **Aviso** vermelho e a informação de que você não está totalmente protegido no momento. **Tenha em mente que você deve ativar o serviço novamente assim que for possível!**

 **Configurações** – clique no botão para ser redirecionado para a interface de [configurações avançadas](#). Precisamente, a caixa de diálogo respectiva será exibida e você poderá configurar o serviço selecionado, ou seja, o [Antivírus](#). Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG Internet Security**, mas qualquer configuração só pode ser recomendada para usuários experientes!

 **Seta** – use a seta verde na parte superior esquerda da caixa de diálogo para voltar à [interface principal do usuário](#) com a visão geral dos 'componentes'.

Como criar seu cofre de dados

Na seção **Cofre de Dados** da caixa de diálogo **Proteção para o computador**, se encontra o botão **Criar seu cofre**. Clique no botão para abrir uma nova caixa de diálogo de mesmo nome, onde é possível especificar os parâmetros do seu cofre planejado. Preencha todas as informações necessárias e siga as instruções no aplicativo:



Primeiro, é necessário especificar o nome do seu cofre e criar uma senha forte:

- **Nome do cofre** – para criar um novo cofre de dados, é necessário primeiro escolher um nome de cofre adequado para reconhecê-lo. Se você compartilha o computador com outros membros da família, pode ser melhor incluir seu nome, além de uma indicação do conteúdo do cofre, por exemplo, *Emails do papai*.



- **Criar senha / Redigitar senha** – crie uma senha para seu cofre de dados e digite-a nos campos de texto respectivos. O indicador gráfico à direita informará se sua senha é fraca (*relativamente fácil de ser quebrada com uso de ferramentas de software especiais*) ou forte. Recomendamos escolher uma senha de pelo menos força média. É possível fortalecer sua senha incluindo letras maiúsculas, números e outros caracteres, como pontos, barras, etc. Se quiser ter certeza de que digitou a senha planejada, você pode marcar a caixa de seleção **Mostrar a senha** (*claro, ninguém mais deve estar olhando para sua tela*).
- **Dica de senha** – recomendamos criar também uma dica útil para a senha, que poderá lembrar qual é a sua senha, caso você se esqueça. Lembre-se de que o Cofre de Dados é projetado para manter seus arquivos seguros, permitindo acesso apenas com senha; não há como contornar isso e, caso você esqueça sua senha, não será mais possível acessar seu cofre de dados!

Depois de especificar todos os dados necessários nos campos de texto, clique no botão **Avançar** para prosseguir para a próxima etapa:



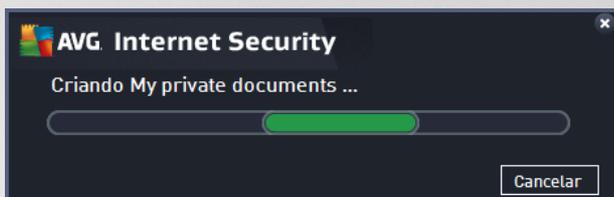
Essa caixa de diálogo fornece as seguintes opções de configuração:

- **Local** informa onde o cofre de dados será colocado fisicamente. Procure por um destino adequado em seu disco rígido ou mantenha o local predefinido, que é sua pasta *Documentos*. Observe que, após a criação de um cofre de dados, não será mais possível alterar seu local.
- **Tamanho** – é possível predefinir o tamanho do seu cofre de dados, o que alocará o espaço necessário no disco. O valor não deve ser nem tão pequeno (*insuficiente para suas necessidades*), nem tão grande (*deixando muito espaço em disco sem utilização*). Se você já sabe o que deseja colocar no cofre de dados, é possível colocar todos os arquivos em uma pasta e depois usar o link **Selecionar uma pasta** para calcular automaticamente o tamanho total. No entanto, o tamanho pode ser alterado mais tarde de acordo com as suas necessidades.
- **Acesso** – as caixas de seleção nessa seção permitem criar atalhos convenientes para seu cofre de dados.



Como usar seu cofre de dados

Quando estiver satisfeito com as configurações, clique no botão **Criar cofre**. Uma nova caixa de diálogo **Seu Cofre de Dados agora está pronto** será exibida anunciando que o cofre está disponível para armazenamento dos seus arquivos. Agora o cofre está aberto e você pode acessá-lo imediatamente. A cada tentativa de acessar o cofre, você será convidado a desbloquear o cofre com a senha definida:



Para usar seu novo cofre de dados, é necessário primeiro abri-lo – clique no botão **Abrir agora**. Ao ser aberto, o cofre de dados será exibido em seu computador como um novo disco virtual. Atribua a ele uma letra de sua escolha do menu suspenso (*you só terá a permissão de selecionar as unidades livres no momento*). Normalmente, você não terá permissão de escolher C (*geralmente atribuído ao seu disco rígido*), A (*unidade de disco flexível*), ou D (*unidade de DVD*). Observe que cada vez que você desbloquear um cofre de dados, será possível escolher uma letra de unidade disponível diferente.

Como desbloquear seu cofre de dados

Na sua próxima tentativa de acessar o cofre de dados, você será convidado a desbloquear o cofre com a senha definida:



No campo de texto, digite sua senha para se autorizar e clique no botão **Desbloquear**. Se precisar de ajuda para se lembrar da senha, clique em **Dica** para exibir a dica de senha que você definiu ao criar o cofre de dados. O novo cofre de dados será exibido como DESBLOQUEADO na visão geral dos seus cofres de dados e você poderá adicionar ou remover arquivos, conforme for necessário.



6.2. Proteção de navegação da Web

A **Proteção para a navegação web** consiste em dois serviços: **LinkScanner Surf-Shield** e **Proteção Online**:

- O **LinkScanner Surf-Shield** protege contra o crescente número de ameaças "fugazes" na web. Essas ameaças podem estar escondidas em qualquer tipo de site, de governamentais a grandes marcas bem conhecidas, até 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 de qualquer página da Web em exibição e garantindo que são seguras no único momento que isso importa: quando você está prestes a clicar nesse link. **O LinkScanner Surf-Shield não se destina à proteção de plataformas de servidores!**
- 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. Essa poderosa proteção bloqueará o conteúdo mal-intencionado de qualquer página da Web que você tente abrir e impedirá que ele seja baixado 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 páginas web mal-intencionadas podem afetar seu computador simplesmente através de uma visita ao site afetado. **A Proteção Online não se destina à proteção de plataformas de servidores!**



Controles da caixa de diálogo

Para alternar entre as seções da caixa de diálogo, é só clicar em qualquer lugar do respectivo painel de serviço. O painel então fica destacado em um tom mais claro de azul. Em ambas as seções da caixa de diálogo, você pode encontrar os controles a seguir. Sua funcionalidade é a mesma, não importando se ela pertence a um serviço de segurança ou ao outro (**LinkScanner Surf-Shield** ou **Proteção Online**):



 **Ativado / Desativado** – o botão se parece com um semáforo, tanto em aparência quanto em função. É só clicar para alternar entre as duas posições. A cor verde representa **Ativado**, o que significa que o serviço de segurança LinkScanner Surf-Shield / Proteção Online está ativo e totalmente funcional. A cor vermelha representa o status de **Desativado**, ou seja, o serviço está desativado. Se não houver um bom motivo para desativar o serviço, recomendamos manter as configurações padrão de todas as configurações de segurança. As configurações padrão garantem o melhor desempenho do aplicativo e sua máxima segurança. Se por algum motivo você desejar desativar o serviço, você será avisado imediatamente sobre o possível risco através do sinal de **Aviso** vermelho e a informação de que você não está totalmente protegido no momento. **Tenha em mente que você deve ativar o serviço novamente assim que for possível!**

 **Configurações** – clique no botão para ser redirecionado para a interface de [configurações avançadas](#). Precisamente, a caixa de diálogo respectiva será exibida e você poderá configurar o serviço selecionado, ou seja, [LinkScanner Surf-Shield](#) ou [Proteção Online](#). Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG Internet Security**, mas qualquer configuração só pode ser recomendada para usuários experientes!

 **Seta** – use a seta verde na parte superior esquerda da caixa de diálogo para voltar à [interface principal do usuário](#) com a visão geral dos componentes.

6.3. Analisador de Software

O componente **Analisador de Software** protege constantemente seus ativos digitais contra ameaças novas e desconhecidas na Internet:

- O **Analisador de Software** é um serviço antimalware que o protege contra todos os tipos de malwares (*spywares, robôs, roubo de identidade, etc.*) usando tecnologias comportamentais e fornece proteção imediata contra novos vírus. O foco do Identity Protection é evitar que ladrões de identidade roubem suas senhas, informações de conta bancária, números de cartões de crédito e outros dados pessoais digitais a partir de todos os tipos de software malicioso (*malware*) que visam ao seu PC. Ele verifica se todos os programas executados em seu PC ou em sua rede compartilhada estão operando corretamente. O Analisador de Software identifica e bloqueia comportamento suspeito permanentemente, além de proteger seu computador contra todos os novos malwares. O Analisador de Software fornece proteção em tempo real ao seu computador contra ameaças novas e, até mesmo, desconhecidas. Ele monitora todos os processos (*incluindo os ocultos*) e mais de 285 padrões de comportamentos diferentes, e pode determinar se algo prejudicial está ocorrendo em seu sistema. Assim, ele pode revelar ameaças ainda não descritas no banco de dados de vírus. Quando um código desconhecido chega ao seu computador, ele é monitorado para ver se exibe comportamento prejudicial e é rastreado. Se o arquivo for considerado prejudicial, o Analisador de Software removerá o código para a [Quarentena de vírus](#) e reverterá todas as alterações que foram feitas no sistema (*injeções de código, mudanças no registro, abertura de portas, etc.*). Não é preciso iniciar uma verificação para estar protegido. A tecnologia é muito proativa, raramente precisa ser atualizada e está sempre de prontidão.



Controles da caixa de diálogo

Na caixa de diálogo, você pode encontrar os controles a seguir:

 **Ativado / Desativado** – o botão se parece com um semáforo, tanto em aparência quanto em função. É só clicar para alternar entre as duas posições. A cor verde representa **Ativado**, o que significa que o serviço de segurança Analisador de Software está ativo e totalmente funcional. A cor vermelha representa o status de **Desativado**, ou seja, o serviço está desativado. Se não houver um bom motivo para desativar o serviço, recomendamos manter as configurações padrão de todas as configurações de segurança. As configurações padrão garantem o melhor desempenho do aplicativo e sua máxima segurança. Se por algum motivo você desejar desativar o serviço, você será avisado imediatamente sobre o possível risco através do sinal de **Aviso** vermelho e a informação de que você não está totalmente protegido no momento. **Tenha em mente que você deve ativar o serviço novamente assim que for possível!**

 **Configurações** – clique no botão para ser redirecionado para a interface de [configurações avançadas](#). Precisamente, a caixa de diálogo respectiva será exibida e você poderá configurar o serviço selecionado, ou seja, o [Analisador de Software](#). Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG Internet Security** mas qualquer configuração só pode ser recomendada para usuários experientes!

 **Seta** – use a seta verde na parte superior esquerda da caixa de diálogo para voltar à [interface principal do usuário](#) com a visão geral dos componentes.

Infelizmente, no **AVG Internet Security**, o serviço Identity Alert não está incluso. Se desejar utilizar esse tipo de proteção, siga o botão **Atualizar para ativar** para ser redirecionado à página da web dedicada onde é possível comprar a licença do Identity Alert.

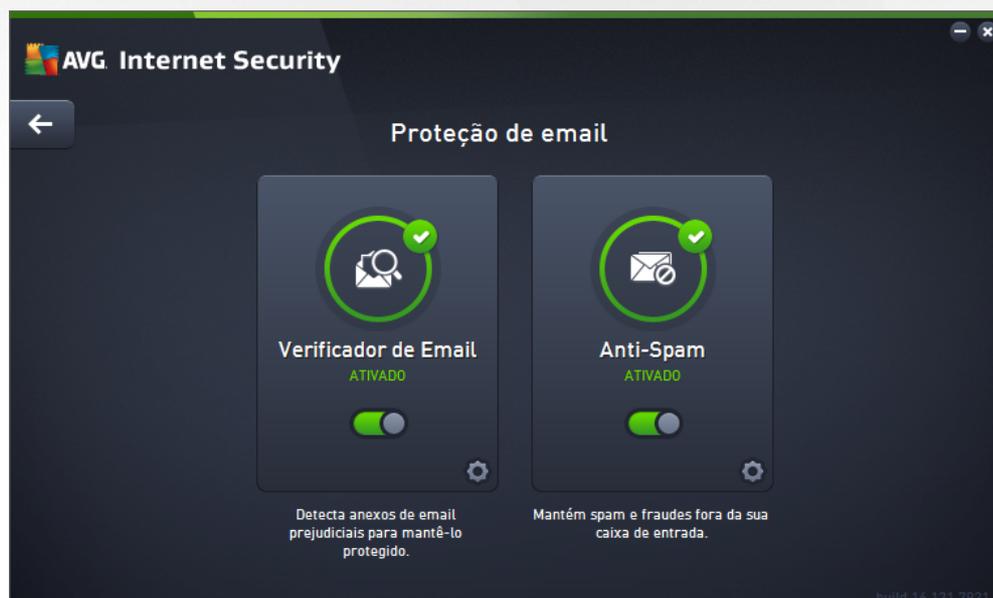
Saiba que mesmo com as edições AVG Premium Security, o serviço Identity Alert está disponível no momento apenas nas seguintes regiões: EUA, Reino Unido, Canadá e Irlanda.



6.4. Proteção de email

O componente **Proteção de Email** abrange os dois serviços de segurança a seguir: **Verificador de Email** e **Anti-Spam** (o serviço Anti-Spam está acessível apenas nas edições Internet / Premium Security).

- **Verificador de Email:** O email é uma das fontes mais comuns de vírus e cavalos de Troia. O phishing e o spam tornam o email uma fonte de riscos ainda maior. Contas gratuitas de email são as que têm maior probabilidade de receber mensagens de email mal-intencionadas (*já que raramente adotam tecnologias anti-spam*) e os usuários domésticos confiam demais nesse tipo de conta. Além dos usuários domésticos, sites desconhecidos e formulários de preenchimento on-line com dados pessoais (*como endereço de email*) aumentam a exposição a ataques via email. Em geral, as empresas usam contas de email corporativo e adotam filtros anti-spam, etc., para reduzir o risco. O componente Proteção de Email é responsável por verificar cada mensagem de email, enviada ou recebida. Quando um vírus é detectado em um email, ele é removido para a [Quarentena de vírus](#) imediatamente. O componente também pode filtrar determinados tipos de anexos de email e adicionar um texto de certificação a mensagens sem infecção. **O Verificador de Email não se destina a plataformas de servidores.**
- O **Anti-Spam** verifica todas as mensagens de email recebidas e marca as indesejadas como spam (*spam se refere a emails não solicitados, geralmente publicidade de produtos e serviços que são enviados em massa para um número enorme de emails ao mesmo tempo, enchendo as caixas de correio dos destinatários. Spam não se refere a email comercial válido, cujo envio conta com o consentimento por parte dos clientes*). O Anti-Spam pode modificar o assunto do email (*que foi identificado como spam*), adicionando uma string de texto especial. É então possível filtrar facilmente os seus emails no cliente de email. O componente Anti-Spam usa diversos métodos de análise para processar cada mensagem de email, oferecendo o máximo de proteção possível contra mensagens de email indesejáveis. O 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 email de "spammers conhecidos"*) e adicionar manualmente endereços de email à sua [Lista de exceções](#) (*nunca marcar como spam*) e à sua [Lista negra](#) (*sempre marcar como spam*).



Controles da caixa de diálogo



Para alternar entre as seções da caixa de diálogo, é só clicar em qualquer lugar do respectivo painel de serviço. O painel então fica destacado em um tom mais claro de azul. Em ambas as seções da caixa de diálogo, você pode encontrar os controles a seguir. Sua funcionalidade é a mesma, não importando se ela pertença a um serviço de segurança ou ao outro (*Verificador de email ou Anti-Spam*):

 **Ativado / Desativado** – o botão se parece com um semáforo, tanto em aparência quanto em função. É só clicar para alternar entre as duas posições. A cor verde representa **Ativado**, o que significa que o serviço de segurança está ativo e totalmente funcional. A cor vermelha representa o status de **Desativado**, ou seja, o serviço está desativado. Se não houver um bom motivo para desativar o serviço, recomendamos manter as configurações padrão de todas as configurações de segurança. As configurações padrão garantem o melhor desempenho do aplicativo e sua máxima segurança. Se por algum motivo você desejar desativar o serviço, você será avisado imediatamente sobre o possível risco através do sinal de **Aviso** vermelho e a informação de que você não está totalmente protegido no momento. **Tenha em mente que você deve ativar o serviço novamente assim que for possível!**

 **Configurações** – clique no botão para ser redirecionado para a interface de [configurações avançadas](#). Precisamente, a respectiva caixa de diálogo será exibida e você poderá configurar o serviço selecionado, ou seja, o [Verificador de email](#) ou [Anti-Spam](#). Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG Internet Security**, mas qualquer configuração só pode ser recomendada para usuários experientes!

 **Seta** – use a seta verde na parte superior esquerda da caixa de diálogo para voltar à [interface principal do usuário](#) com a visão geral dos componentes.

6.5. Firewall

Firewall é um sistema que aplica uma política de controle de acesso entre duas ou mais redes, bloqueando ou permitindo o tráfego. O Firewall contém um conjunto de regras que protege a rede interna de ataques com origem *externa (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, é permitida ou proibida. Se o Firewall reconhece qualquer 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*) através de portas definidas e para softwares aplicativos definidos. Por exemplo, o firewall pode ser configurado para permitir apenas o fluxo de entrada e saída de dados da Web usando o Microsoft Explorer. Qualquer tentativa de transmitir dados da Web por outro navegador seria bloqueada. Ele protege as informações identificadas como pessoais, impedindo que sejam enviadas do seu computador sem sua 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 computadores individuais contra ataques iniciados por usuários internos em outros computadores da rede.

No **AVG Internet Security**, o **Firewall** controla todo o tráfego em cada porta de rede de seu computador. Com base nas regras definidas, o Firewall avalia os aplicativos em execução no computador (*e que pretendem se conectar à rede local ou Internet*) ou aplicativos que abordam o computador externamente, tentando estabelecer conexão com o PC. Para cada um desses aplicativos, o Firewall irá permitir ou impedir a comunicação nas portas da rede. Como 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.

O Firewall AVG não se destina à proteção de plataformas de servidores!

Recomendação: *geralmente, não se recomenda usar mais de um firewall em um único computador. 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 usar somente um firewall no seu*



computador e desativar todos os outros, eliminando assim o risco de possível conflito e de problemas relacionados.



Observação: após a instalação do seu AVG Internet Security, o componente Firewall poderá exigir a reinicialização do computador. Nesse caso, a caixa de diálogo do componente é exibida informando que é necessário reinicializar. Diretamente na caixa de diálogo, você encontrará o botão **Reiniciar agora**. Até que seja reiniciado, o componente Firewall não estará ativado totalmente. Além disso, todas as opções de edição na caixa de diálogo serão desativadas. Preste atenção ao aviso e reinicie seu PC assim que for possível!

Modos de Firewall disponíveis

O firewall permite que você defina regras específicas de segurança baseando-se em se o seu computador está localizado em um domínio, ou se ele é um computador autônomo, ou até mesmo um notebook. Cada uma dessas opções requer um nível diferente de proteção e os níveis são abordados pelos respectivos modos. Resumindo, um modo do Firewall é uma configuração específica do componente Firewall e você pode usar várias dessas configurações predefinidas.

- **Automático** – nesse modo, o Firewall lida com todo o tráfego de rede automaticamente. Você não será solicitado a tomar decisões. O Firewall permitirá a conexão de todos os aplicativos conhecidos e, ao mesmo tempo, uma regra será criada para o aplicativo, especificando que ele sempre poderá se conectar no futuro. Para outros aplicativos, o Firewall decidirá se a conexão será permitida ou bloqueada, dependendo do comportamento do aplicativo. No entanto, em tal situação, a regra não será criada e o aplicativo será verificado novamente se tentar se conectar. O modo automático é discreto e recomendado para a maioria dos usuários.
- **Interativo** – este modo é útil se você quiser controlar completamente todo o tráfego de rede e de seu computador. O Firewall monitorará o tráfego para você e notificará cada tentativa de comunicação ou transferência de dados, possibilitando permitir ou bloquear a tentativa, à medida que achar necessário. Recomendado apenas para usuários avançados.



- **Bloquear acesso à Internet** – a conexão com a Internet é completamente bloqueada. Não é possível acessar a Internet e ninguém de fora pode acessar seu computador. Somente para uso especial ou por pouco tempo.
- **Desativar a proteção do Firewall (não recomendado)** – desativar o Firewall permitirá todo o tráfego de entrada e saída do seu computador. Conseqüentemente, isso o deixará vulnerável a ataques de hackers. Sempre tenha cuidado ao considerar esta opção.

Observe que um modo automático específico também está disponível no Firewall. Esse modo é ativado silenciosamente se o componente [Computador](#) ou [Analisador de Software](#) for desligado e seu computador estiver desta forma mais vulnerável. Em tais casos, o Firewall permitirá automaticamente apenas aplicativos conhecidos e perfeitamente seguros. Para todos os outros, será solicitada a sua decisão. Isso é feito para compensar os componentes de proteção desativados e manter seu computador seguro.

Nossa recomendação é não desligar nunca o Firewall! No entanto, se surgir uma necessidade e você realmente precisar desativar o componente de Firewall, será possível fazê-lo selecionando o modo de proteção Desabilitar o Firewall da lista acima de modos disponíveis de Firewall.

Controles da caixa de diálogo

A caixa de diálogo fornece uma visão geral das informações básicas do status do componente de Firewall:

- **Modo do Firewall** – fornece informações sobre o modo de Firewall selecionado no momento. Use o botão **Alterar**, localizado ao lado da informação fornecida, para ir para a interface [Configurações de Firewall](#), se desejar alterar o modo atual para outro (*para a descrição e recomendação sobre a utilização de perfis de Firewall, consulte o parágrafo anterior*).
- **Compartilhamento de arquivos e impressora** – informa se o compartilhamento de arquivos e impressora (*em ambos os sentidos*) é permitido no momento. O compartilhamento de arquivos e impressoras significa o compartilhamento de quaisquer arquivos e pastas que você marcar como "Compartilhado" no Windows, unidades de disco comuns, impressoras, scanners e todos os dispositivos similares. O compartilhamento desses itens só é desejável em redes que podem ser consideradas seguras (*por exemplo, em casa, no trabalho ou na escola*). No entanto, se estiver conectado a uma rede pública (*como um Wi-Fi de aeroporto ou um café com Internet*), não compartilhe nada.
- **Conectado ao** – fornece informações sobre o nome da rede em que você está conectado no momento. Com o Windows XP, o nome da rede responde ao nome escolhido para a rede específica quando você se conectou a ela pela primeira vez. Com o Windows Vista e superiores, o nome da rede é extraído automaticamente da Central de Redes e Compartilhamento.
- **Redefinir para o padrão** – pressione este botão para substituir a configuração de Firewall existente e reverter para a configuração padrão com base na detecção automática.

A caixa de diálogo contém os seguintes controles gráficos:



Configurações – clique no botão para abrir um menu pop-up que oferece duas opções:

- **Configurações avançadas** – essa opção redireciona você à interface de [Configurações do Firewall](#), onde é possível editar todas as configurações do Firewall. No entanto, lembre-se de que qualquer configuração deve ser executada somente por usuários experientes!



- **Remover proteção do Firewall** – ao selecionar essa opção, você está prestes a desinstalar o componente de Firewall, o que poderá enfraquecer sua proteção de segurança. Se você ainda quiser remover o componente de Firewall, confirme sua decisão e o componente será desinstalado completamente.

← **Seta** – use a seta verde na parte superior esquerda da caixa de diálogo para voltar à [interface principal do usuário](#) com a visão geral dos 'componentes.

6.6. PC Analyzer

O componente **PC Analyzer** é uma ferramenta avançada para análise detalhada e correção do sistema, sobre como a velocidade e o desempenho geral do seu computador pode ser aprimorado. Ele é aberto através do botão **Corrigir desempenho** localizado na [caixa de diálogo da interface de usuário principal](#) ou através da mesma opção listada no menu de contexto do [ícone do AVG na bandeja do sistema](#). Você poderá acompanhar o progresso da análise e os seus resultados diretamente no gráfico:



As seguintes categorias podem ser analisadas: erros de registro, arquivos indesejados, fragmentação e atalhos desfeitos:

- **Erros de registro** fornece o número do erro no Registro do Windows que pode ter causado a queda de velocidade do computador ou feito com que aparecessem mensagens de erro.
- **Arquivos indesejados** fornece o número dos arquivos que estão utilizando espaço em disco e que podem ser excluídos. 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, fazendo com que a maioria dos arquivos esteja espalhada por diferentes partes do disco físico.
- A opção **Atalhos corrompidos** encontrará atalhos que não funcionam mais e levam a locais não existentes, etc.



A visão geral de resultados apresenta o número de problemas de sistema detectados, 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

- **Parar análise** (*exibido durante a execução da análise*) – pressione este botão para interromper a análise do computador.
- **Corrigir agora** (*exibida assim que a análise é concluída*) – infelizmente, o recurso do PC Analyzer no **AVG Internet Security** está limitado à análise do status atual do seu PC. No entanto, a AVG fornece uma ferramenta avançada para análise detalhada e correção do sistema, sobre como a velocidade e o desempenho geral do seu computador pode ser aprimorado. Clique no botão para ser redirecionado ao website dedicado para obter mais informações.

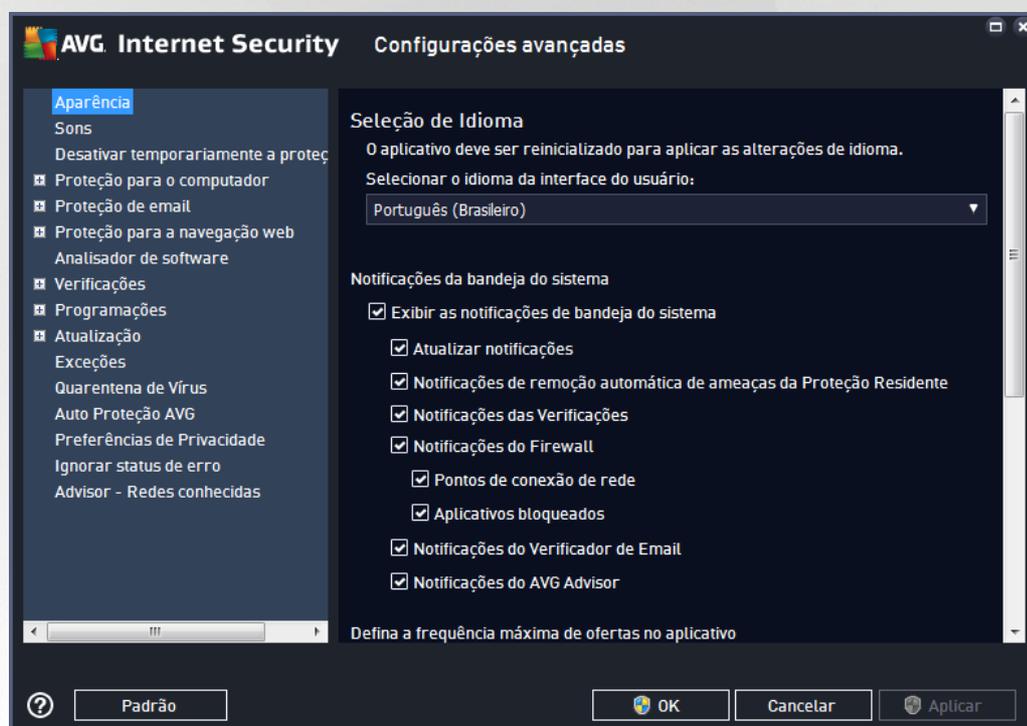


7. Configurações avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG Internet Security** 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 (*ou sua parte específica*) para abrir a caixa de edição na seção à direita da janela.

7.1. Aparência

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



Seleção de idioma

Na seção **Seleção de idioma**, você pode selecionar o idioma desejado no menu suspenso. O idioma selecionado será usado em toda a [interface de usuário](#) do **AVG Internet Security**. O menu suspenso oferece apenas os idiomas selecionados anteriormente para serem instalados durante o processo de instalação (*como padrão, inglês é sempre instalado automaticamente*). Para concluir a mudança de idioma do **AVG Internet Security**, é necessário reiniciar o aplicativo. Por favor, siga esse procedimento:

- No menu suspenso, selecione o idioma desejado para o aplicativo
- Confirme a seleção clicando no botão **Aplicar** (*canto inferior direito da caixa de diálogo*)
- Pressione o botão **OK** para confirmar



- Uma nova caixa de diálogo é exibida informando que, para mudar o idioma do aplicativo, é necessário reiniciar o **AVG Internet Security**
- Pressione o botão **Reiniciar o AVG agora** para concordar com o reinício do programa e aguarde um pouco até que a mudança de idioma seja efetuada:



Notificações da bandeja do sistema

Nesta seção, é possível ocultar as notificações na bandeja do sistema sobre o status do aplicativo **AVG Internet Security**. Como padrão, as notificações do sistema podem ser exibidas. Recomenda-se manter essa configuração! As notificações do sistema fornecem informações, por exemplo, sobre o início de processos de atualização ou verificação ou sobre a mudança de status de um componente do **AVG Internet Security**. É necessário prestar atenção a esses anúncios!

Entretanto, se, por alguma razão, você decidir que não deseja receber as informações dessa forma ou que gostaria de receber apenas algumas notificações (*relacionadas a um componente específico do AVG Internet Security*), é possível definir e especificar suas preferências marcando/desmarcando as seguintes opções:

- **Exibir as notificações de bandeja do sistema (ativada como padrão)** – todas as notificações são exibidas como padrão. Desmarque este item para desativar completamente a exibição de todas as notificações do sistema. Quanto ativado, é possível selecionar quais notificações específicas devem ser exibidas:
 - **Notificações de atualização (ativada como padrão)** – decide se as informações relacionadas ao início, andamento ou à finalização do processo de atualização do **AVG Internet Security** devem ser exibidas.
 - **Notificações de remoção automática de ameaças da Proteção Residente (ativada como padrão)** – decide se as informações relacionadas a salvar, copiar e abrir processos devem ser exibidas ou ocultadas (*esta configuração é exibida apenas se a opção de reparo automático da Proteção Residente está ativada*).
 - **Notificações de verificação (ativada como padrão)** – decide se devem ser exibidas as informações sobre o início automático da verificação agendada, seu andamento e resultados.
 - **Notificações de firewall (ativada como padrão)** – decide se serão exibidas informações relativas ao status e aos processos do Firewall, como avisos de ativação/desativação de componentes, possível bloqueio de tráfego, etc. Este item fornece mais duas opções específicas de seleção (*para obter explicações detalhadas de cada um, consulte o capítulo [Firewall](#) deste documento*):
 - **Pontos de conexão de rede (desativada como padrão)** – ao conectar-se em uma rede, o Firewall informa se ele conhece a rede e como o compartilhamento de arquivos e impressora será configurado.



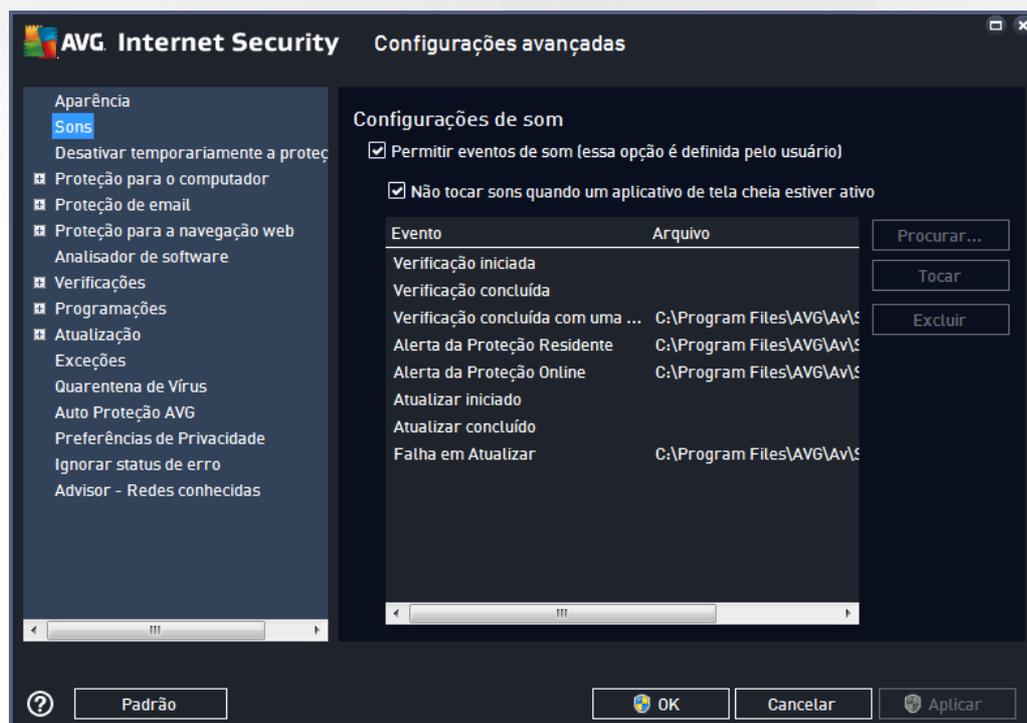
- **Aplicativos bloqueados** (ativada como padrão) – quando um aplicativo desconhecido ou suspeito tentar se conectar com uma rede, o Firewall bloqueia a tentativa e exibe uma notificação. Isso é útil para mantê-lo informado e, desta forma, recomendamos sempre manter o recurso ativado.
- o **Notificações do Verificador de Email** (ativada como padrão) – decide se as informações sobre a verificação de todas as mensagens de email de entrada e saída devem ser exibidas.
- o **Notificações de estatísticas** (ativada como padrão) – mantenha a opção selecionada para permitir que notificações regulares de análises estatísticas sejam exibidas na bandeja do sistema.
- o **Notificações do AVG Advisor** (ativado como padrão) – decide as informações sobre as atividades do [AVG Advisor](#) devem ser exibidas no painel deslizante da 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).

7.2. Sons

Na caixa de diálogo **Configurações de som**, é possível especificar se deseja receber informações sobre ações específicas do **AVG Internet Security** por meio de uma notificação sonora:





As configurações são válidas apenas para a conta de usuário atual. Isso significa que cada usuário no computador pode ter sua própria configuração de som. Para permitir a notificação sonora, mantenha a opção **Permitir eventos de som** marcada (a opção está ativada por padrão) para ativar a lista de todas as ações relevantes. Você também pode marcar a opção **Não tocar sons quando um aplicativo de tela cheia estiver ativo** para desativar a notificação sonora em situações em que ela pode ser disruptiva (consulte também a seção *Modo de jogo*, no capítulo [Configurações avançadas/Aparência](#) neste documento).

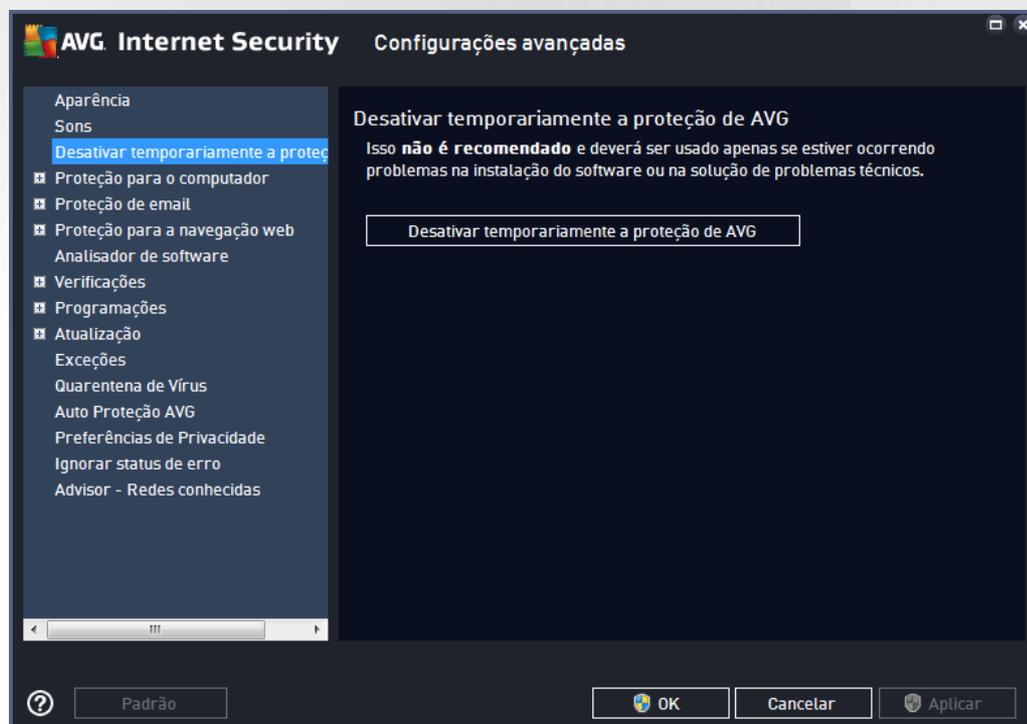
Botões de controle

- **Procurar...** – com o evento respectivo selecionado na lista, use o botão **Procurar** para localizar e atribuir o arquivo de som desejado no seu disco. (Somente sons no formato *.wav são suportados no momento!)
- **Tocar** – para ouvir o som selecionado, realce o evento na lista e pressione o botão **Tocar**.
- **Excluir** – use o botão **Excluir** para remover o som atribuído a um evento específico.

7.3. 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** de uma vez.

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



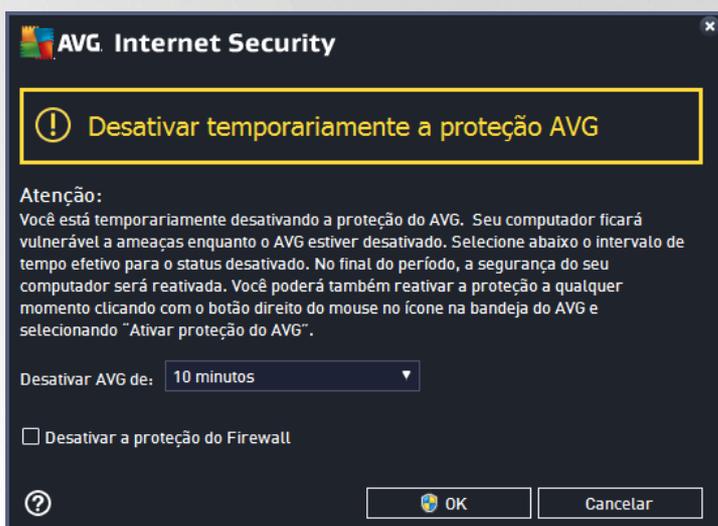
Na maioria dos casos, **não é necessário** desativar o **AVG Internet Security** antes de instalar novo software ou novos drivers, nem mesmo se o instalador ou assistente de software sugerir que programas e aplicativos em execução devem ser encerrados primeiro para garantir que não haja interrupções indesejadas durante o processo de instalação. Caso enfrente realmente problemas durante a instalação, experimente [desativar a](#)



[proteção residente](#) (no diálogo do link, desmarque o item **Ativar Proteção Residente**) primeiro. Se for necessário desativar temporariamente o **AVG Internet Security**, você deverá reativá-lo assim que concluir a tarefa que solicitou a desativação. Se estiver conectado à Internet ou a uma rede enquanto o software antivírus estiver desativado, o computador ficará vulnerável a ataques.

Como desativar a proteção do AVG

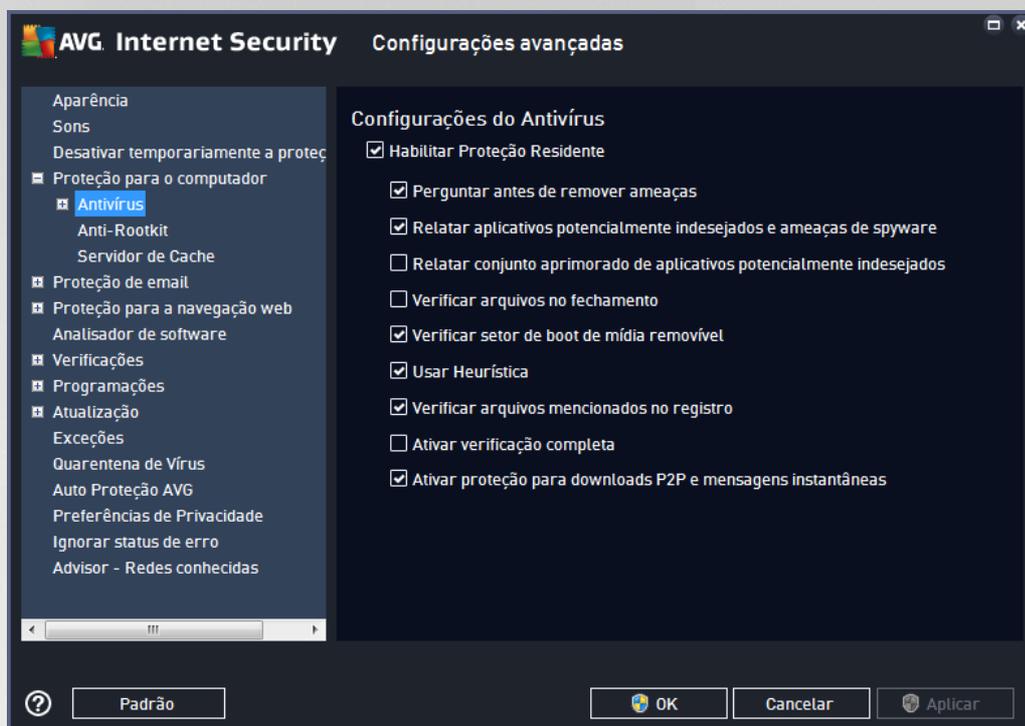
Marque a caixa de seleção **Desativar temporariamente a proteção AVG** e confirme sua opção, pressionando o botão **Aplicar**. Na caixa de diálogo recém-aberta, **Desativar temporariamente a proteção AVG**, especifique por quanto tempo você deseja manter o **AVG Internet Security** desativado. Como padrão, a proteção será desativada por 10 minutos, o que pode ser suficiente para qualquer tarefa comum, como instalar novo software, etc. Você pode decidir por um período maior de tempo, no entanto, essa opção não é recomendada, se não for absolutamente necessário. Depois, todos os componentes desativados serão ativados automaticamente. No máximo, é possível desativar a proteção do AVG até a próxima reinicialização do computador. Uma opção separada de desativação do componente de **Firewall** está presente no diálogo **Desativar temporariamente a proteção AVG**. Marque a caixa de seleção **Desativar a proteção do Firewall** para isso.



7.4. Proteção para o computador

7.4.1. AntiVirus

O **AntiVirus** junto com a **Proteção Residente** protegem seu computador permanentemente contra todos os tipos conhecidos de vírus, spyware e malware em geral (*incluindo os chamados malwares adormecidos e não ativos, ou seja, malwares que foram baixados, mas ainda não ativados*).



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 como padrão). Além disso, você pode selecionar os recursos da proteção residente que devem ser ativados:

- **Perguntar antes de remover ameaças** (ativado como padrão) – marque para certificar-se de que a Proteção Residente não executará nenhuma ação automaticamente; em vez disso, ela exibirá um diálogo descrevendo a ameaça detectada, permitindo que você decida o que fazer. Se você deixar esta caixa desmarcada, o **AVG Internet Security** irá recuperar automaticamente a infecção e, se isso não for possível, o objeto será movido para a [Quarentena de Vírus](#).
- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada como padrão) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois ele aumenta a segurança do seu computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (desativada como padrão) – marque para detectar os pacotes estendidos de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas que podem ser mal utilizados com más intenções posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador. No entanto, isso pode eventualmente bloquear programas lícitos e, portanto, é desativada como padrão.
- **Verificar arquivos no fechamento** (desativada como padrão) – a verificação durante o fechamento garante que o AVG examine objetos ativos (por exemplo, aplicativos, documentos etc.) quando forem abertos e também quando forem fechados. Este recurso ajuda a proteger o computador contra alguns tipos de vírus sofisticados.

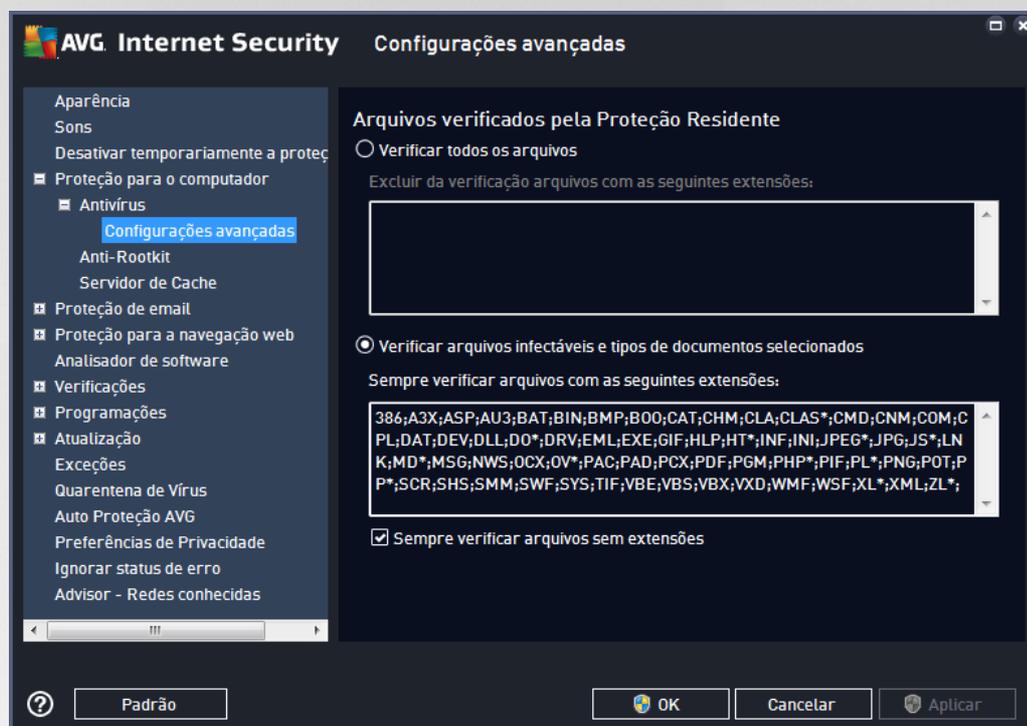


- **Verificar setor de inicialização de mídia removível** (ativado como padrão) – marque para verificar setores de inicialização de disquetes USB inseridos, unidades de disco externas e outra mídia removível quanto a ameaças.
- **Usar Heurística** (ativado por padrão) – a análise heurística será usada para detecção (emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual).
- **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** (desativado por padrão) – em situações específicas (como um estado de extrema emergência), você pode marcar esta opção para ativar os algoritmos mais completos, que examinarão todos os objetos de ameaça possíveis minuciosamente. Entretanto, lembre-se de que esse método é bastante demorado.
- **Ativar proteção para downloads P2P e mensagens instantâneas** (ativado por padrão) – marque este item se desejar verificar se a comunicação por mensagens instantâneas (p.ex. AIM, Yahoo!, ICQ, Skype, MSN Messenger, etc.) e os dados baixados em redes Peer-to-Peer (redes que permitem conexão direta entre clientes, sem um servidor, o que é potencialmente perigoso; geralmente utilizada para compartilhar arquivos de música) estão livres de vírus.

Obs.: se o AVG estiver instalado no Windows 10, um item adicional, chamado de **Ativar o Windows Antimalware Scan Interface (AMSI) para obter verificações minuciosas de software** estará presente na lista. Esse recurso melhora a proteção antivírus, pois permite que o Windows e a AVG colaborem mais intimamente para descobrir códigos malignos, tornando a proteção mais confiável e reduzindo o número de falsos positivos.



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

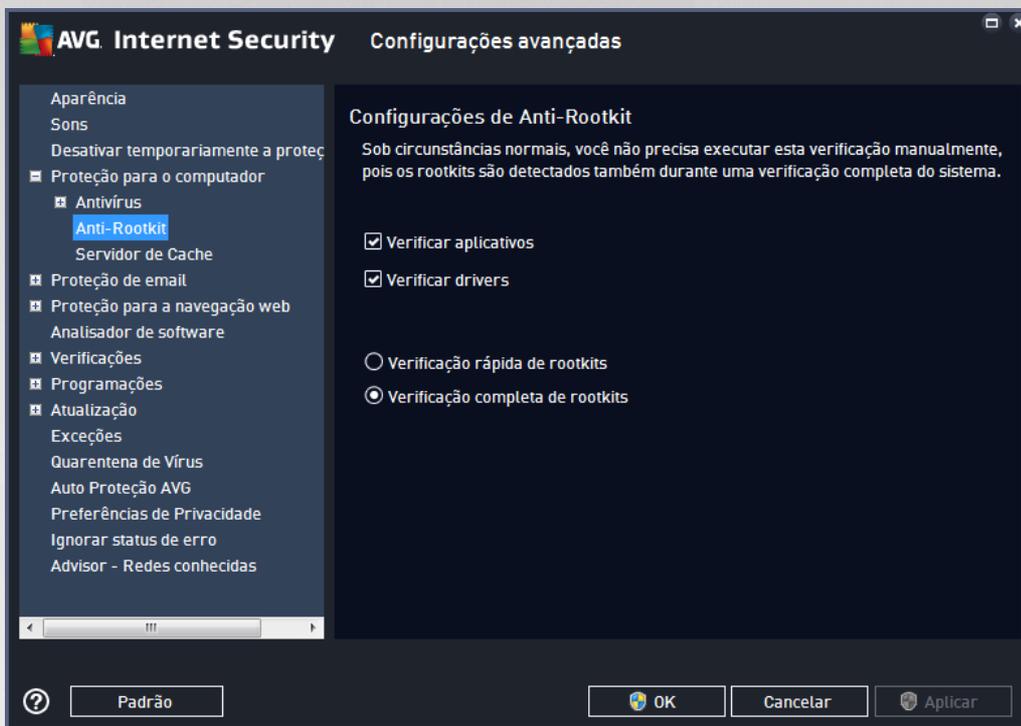


Marque a caixa de seleção respectiva para decidir se deseja **Verificar todos os arquivos** ou **Verificar arquivos infectáveis e tipos de documentos selecionados** somente. Para acelerar a verificação e fornecer o nível máximo de proteção, recomendamos manter as configurações padrão. Desta forma, apenas os arquivos que podem ser infectados serão verificados. Na seção respectiva da caixa de diálogo, você também pode encontrar uma lista de extensões editável que define os arquivos incluídos na verificação.

Marque **Sempre verificar arquivos sem extensões** (*ativado por padrão*) para garantir que até mesmo arquivos sem extensões e de formato desconhecido sejam verificados pela Proteção Residente. Recomendamos que este recurso seja mantido ativado, já que arquivos sem extensão são suspeitos.

7.4.2. Anti-Rootkit

No diálogo **Configurações anti-rootkit**, você pode editar as configurações do serviço **Anti-Rootkit** e parâmetros específicos da verificação anti-rootkit. A verificação anti-rootkit é um processo padrão incluso na [Verificação em todo o computador](#):



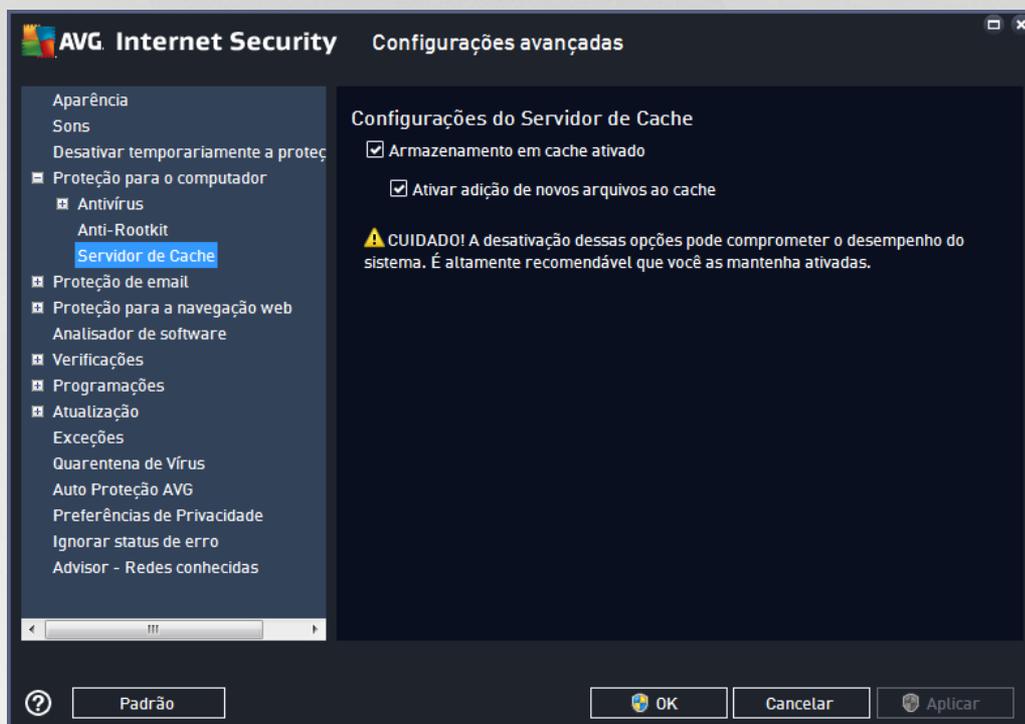
A **Verificação de aplicativos** e a **Verificação de drivers** permitem especificar em detalhes o que deve ser incluído na verificação Anti-Rootkit. Essas configurações são direcionadas a usuários avançados. Recomendamos manter todas as opções ativadas. Você também pode selecionar o modo de verificação de rootkits:

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



7.4.3. Servidor de cache

A caixa de diálogo **Configurações do servidor de cache** se refere ao processo do servidor de cache desenvolvido para agilizar todos os tipos de verificações do **AVG Internet Security**:



O servidor de cache coleta e mantém informações de arquivos confiáveis (*um arquivo é considerado confiável se tiver a assinatura digital de uma fonte confiável*). Esses arquivos são automaticamente considerados seguros e não precisam ser verificados novamente. Portanto, eles são ignorados durante a verificação.

A caixa de diálogo **Configurações do servidor de cache** oferece as seguintes opções de configuração:

- **Armazenamento em cache ativado** (*ativado como padrão*) - desmarque a caixa para desativar o **Servidor de Cache** e esvaziar a memória de cache. Observe que a verificação pode ficar lenta e o desempenho geral do seu computador pode diminuir, pois cada arquivo será verificado para detecção de vírus e spyware primeiramente.
- **Ativar adição de novos arquivos ao cache** (*ativado como 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.

A menos que você tenha um bom motivo para desativar o servidor de cache, recomendamos manter as configurações padrão e deixar as opções ativadas! Caso contrário, você poderá sentir uma redução significativa na velocidade e no desempenho de seu sistema.

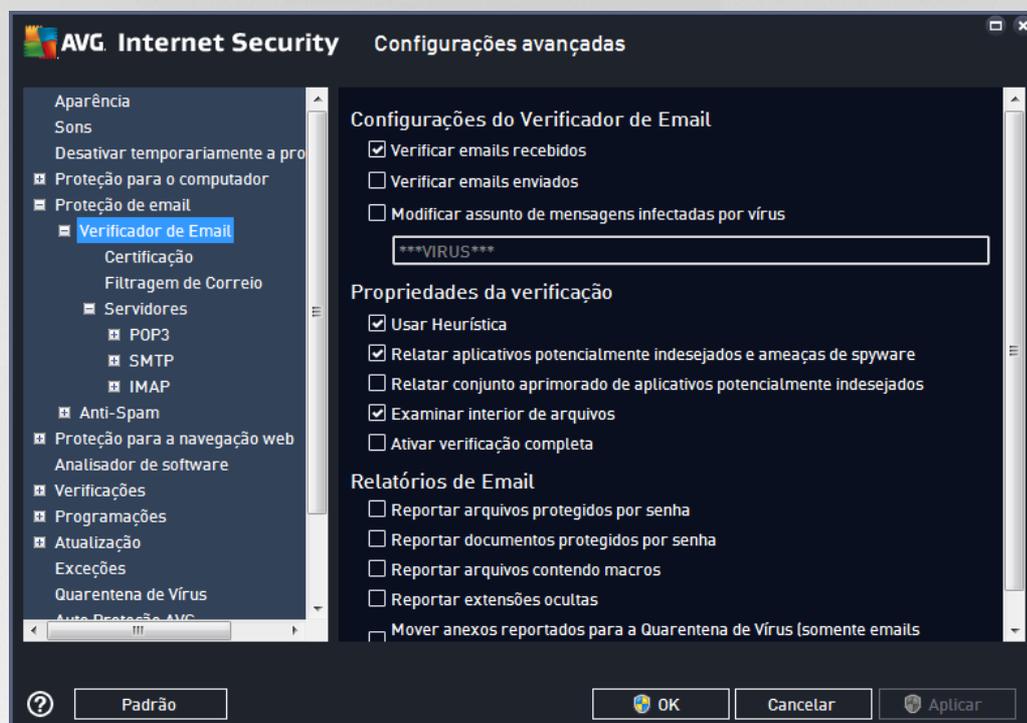
7.5. Verificador de Email

Nessa seção, é possível editar configurações detalhadas do [Verificador de Email](#) e do [Anti-Spam](#):



7.5.1. Verificador de Email

A caixa de diálogo *Verificador de Email* é dividida em três seções:



Verificação de email

Nesta seção, você pode definir as funções básicas a seguir para mensagens de email 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 infectada, marque este item e digite o texto desejado no campo de texto. Esse texto será adicionado ao campo "Assunto" para cada mensagem de email detectada para facilitar a identificação e filtragem. O valor padrão recomendável e que recomendamos manter é *****VIRUS*****.

Propriedades da verificação

Nesta seção, você pode especificar como as mensagens de email serão verificadas:

- **Usar heurística** (*ativada por padrão*) – marque para usar o método de detecção de heurística ao verificar mensagens de email. Quando essa opção está ativada, é possível filtrar anexos de email não



só por extensão, como também o conteúdo real do anexo será considerado. A filtragem pode ser definida na caixa de diálogo [Filtragem de email](#).

- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada por padrão) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (desativada por padrão) – marque para detectar os pacotes estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas que podem ser mal utilizados com más intenções posteriormente. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, ela pode bloquear programas lícitos; portanto, é desativada por padrão.
- **Verificar dentro de arquivos** (ativada por padrão) – marque para verificar os conteúdos de arquivos anexados às mensagens de email.
- **Ativar verificação completa** (desativada por padrão) – em situações específicas (por exemplo, suspeita de que seu computador foi infectado por vírus ou atacado), 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 é bastante demorado.

Relatório de anexos de email

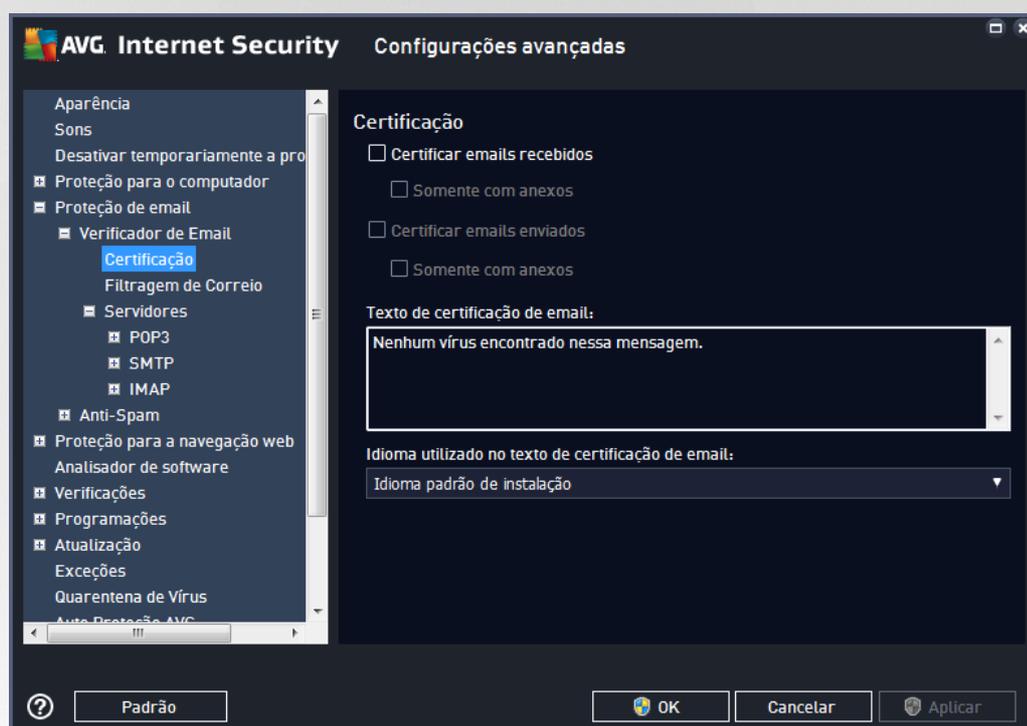
Nesta seção, você pode definir relatórios adicionais sobre arquivos potencialmente perigosos ou suspeitos. Observe que nenhuma caixa de diálogo de advertência será exibida, apenas um texto de certificação será adicionado ao final da mensagem de email e todos esses relatórios serão listados na caixa de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

- **Reportar arquivos protegidos por senha** – arquivos compactados (ZIP, RAR, etc.) que são 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 de MS Word são amplamente conhecidas). Como tal, uma macro pode conter instruções potencialmente perigosas e convém você marcar a caixa para garantir que os arquivos com macros sejam reportados como suspeitos.
- **Reportar extensões ocultas** – extensões ocultas podem tornar um arquivo executável suspeito, "algumacoisa.txt.exe", por exemplo, parecer-se com um arquivo de texto comum inofensivo "algumacoisa.txt". Marque a caixa de seleção para reportá-los como potencialmente perigosos.
- **Mover anexos de email relatados para a área de Quarentena** – especifique se você deseja ser notificado por email 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



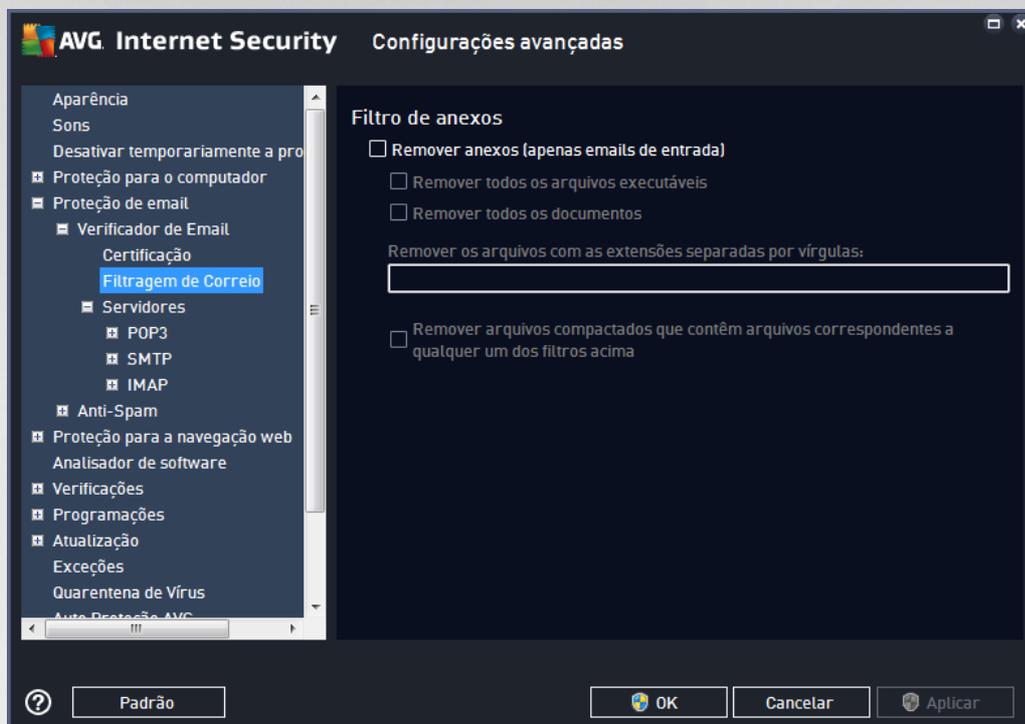
de email verificada. Se uma mensagem desse tipo for identificada durante a verificação, defina se o objeto infectado detectado deve ser movido para a [Quarentena de Vírus](#).

Na caixa de diálogo **Certificação**, você pode selecionar as caixas específicas para decidir se deseja certificar emails recebidos (**Certificar emails recebidos**) e/ou emails enviados (**Certificar emails enviados**). Para cada uma dessas opções, você pode especificar o parâmetro **Somente com anexos**, para que a certificação seja adicionada apenas às mensagens de email com anexos:



Como padrão, o texto de certificação consiste em informações básicas com o aviso *Nenhum vírus encontrado nessa mensagem*. No entanto, essas informações podem ser estendidas ou alteradas conforme suas necessidades: escreva o texto de certificação desejado no campo **Texto de certificação de email**. Na seção **Idioma utilizado no texto de certificação de email**, você pode definir melhor em que idioma deve ser exibida a parte da certificação que é gerada automaticamente (*Nenhum vírus encontrado nesta mensagem*).

Observação: tenha em mente que somente o texto padrão será exibido no idioma solicitado, e o texto personalizado não será traduzido automaticamente!



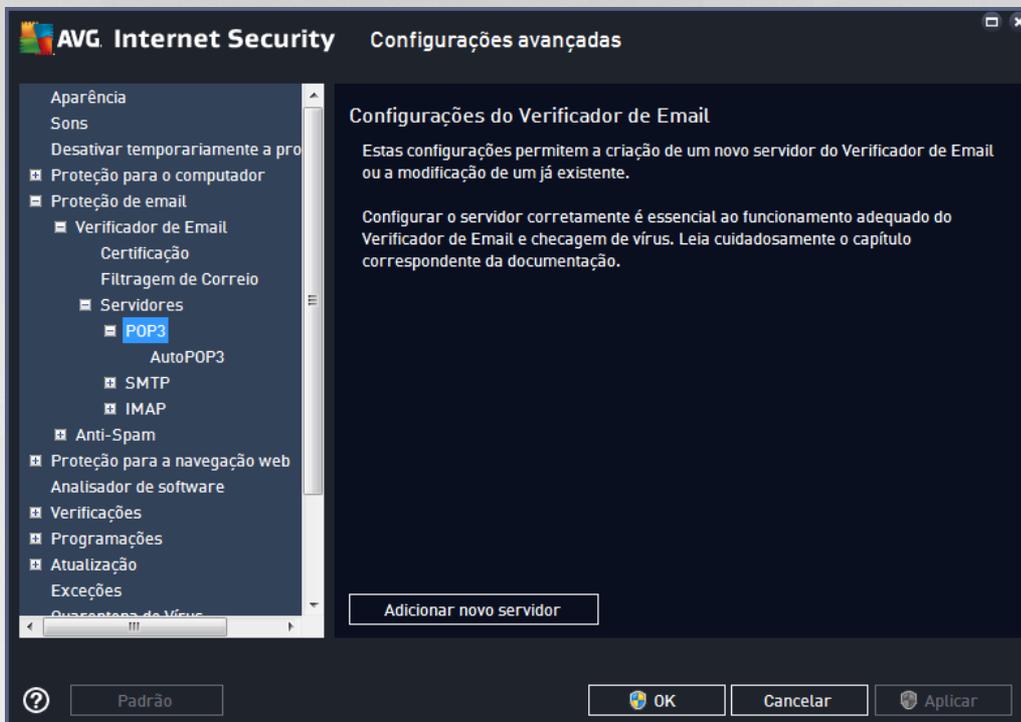
A caixa de diálogo **Filtro de anexos** permite definir os parâmetros da verificação dos anexos das mensagens de email. Como padrão, a opção **Remover anexos** é desativada. Se decidir ativá-la, todos os anexos de mensagem de email detectados como infectados ou potencialmente perigosos serão removidos automaticamente. Se 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

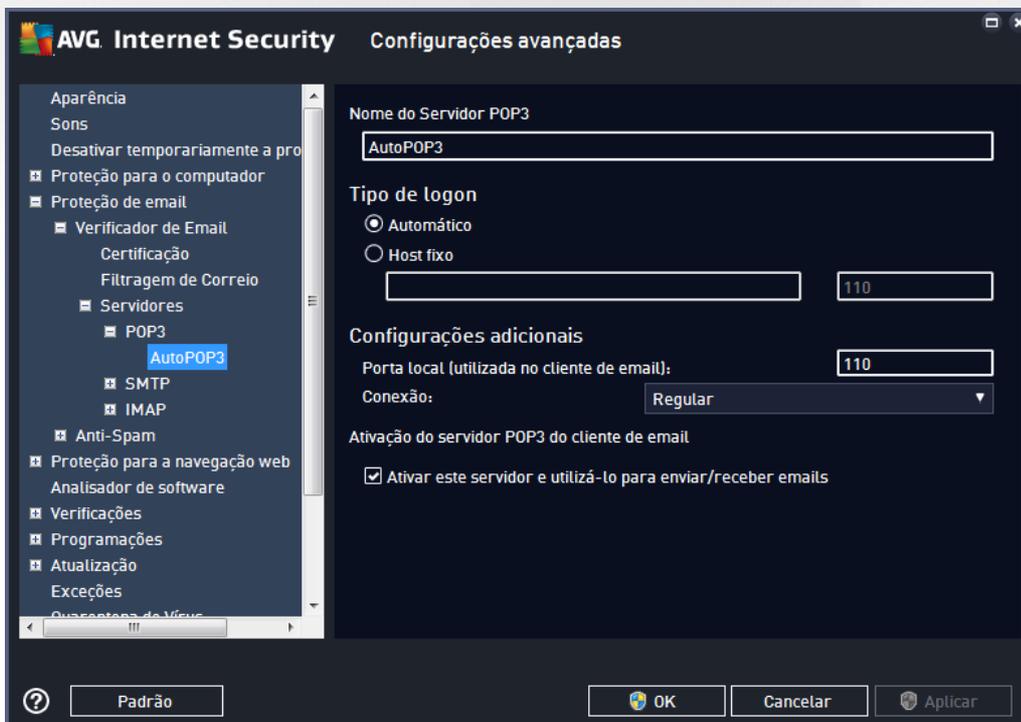
Na seção **Servidores**, você pode editar parâmetros dos servidores do [Verificador de Email](#):

- [Servidor POP3](#)
- [Servidor SMTP](#)
- [Servidor IMAP](#)

Você também pode definir novos servidores para emails de entrada e de saída usando o botão **Adicionar novo servidor**.

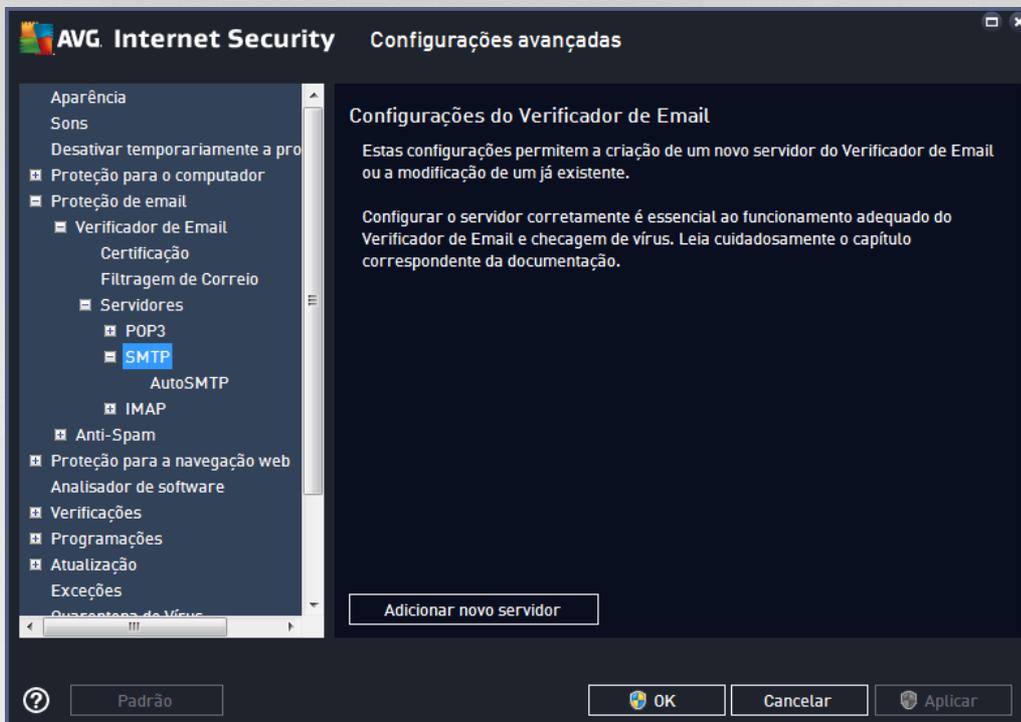


Nessa caixa de diálogo, você pode configurar um novo servidor do [Verificador de Email](#) usando o protocolo POP3 para emails recebidos:

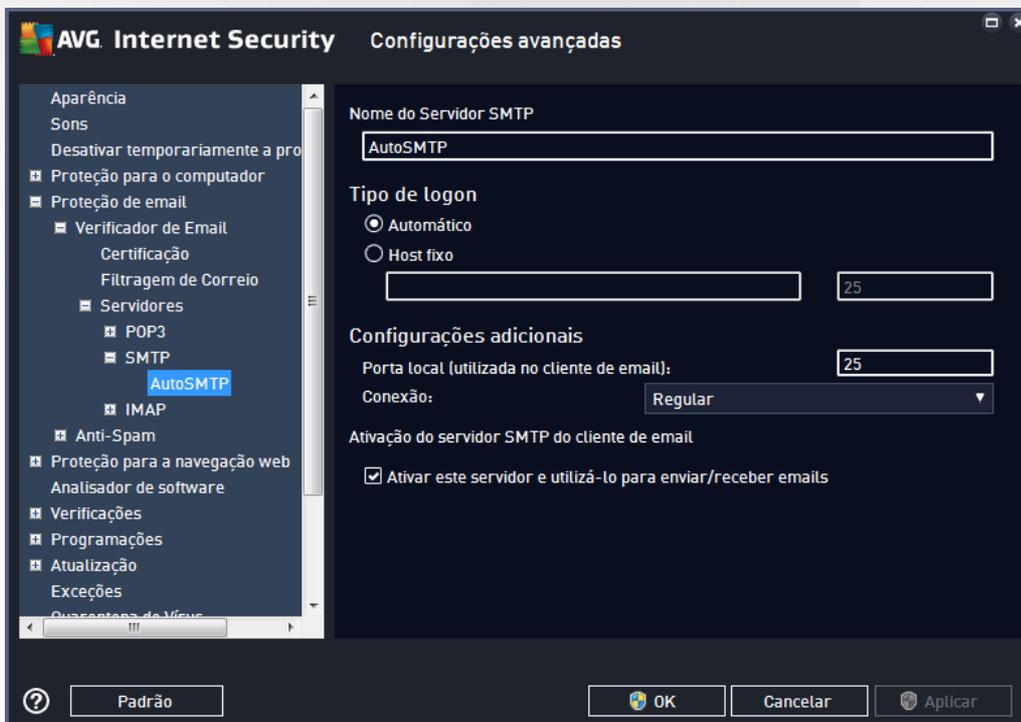




- **Nome do Servidor POP3** – neste campo, é possível especificar o nome dos servidores recém-adicionados (*para adicionar um servidor POP3, clique com o botão direito do mouse sobre o item POP3 do menu de navegação esquerdo*).
- **Tipo de logon** – define o método para determinar o servidor de email usado para emails recebidos:
 - **Automático** – o login será feito automaticamente, de acordo com as configurações do cliente de email.
 - **Host fixo** – nesse caso, o programa usará sempre o servidor especificado aqui. Especifique o endereço ou nome do servidor de emails. O nome de login permanece inalterado. Para o 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 email 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:
 - **Porta local** – especifica a porta em que a comunicação do seu aplicativo de email deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de email como a porta para comunicação POP3.
 - **Conexão** – no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso também só estará disponível quando houver suporte no servidor de email de destino.
- **Ativação do servidor POP3 do cliente de email** – marque/desmarque esse item para ativar ou desativar o servidor POP3 especificado

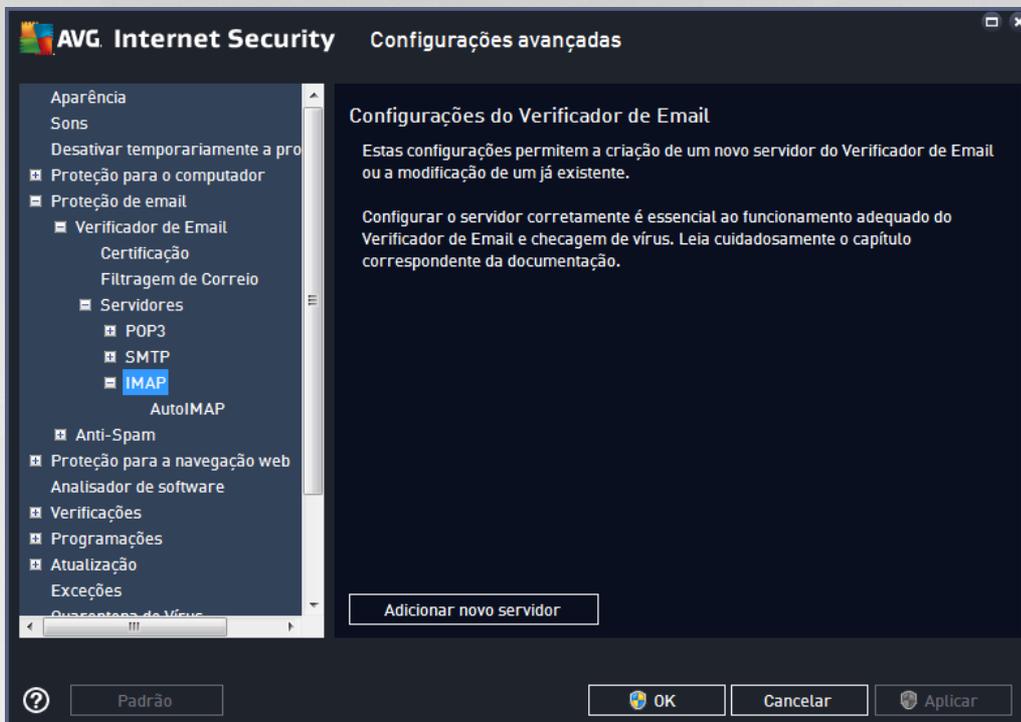


Nessa caixa de diálogo, você pode configurar um novo servidor do [Verificador de Email](#) usando o protocolo SMTP para mensagens enviadas:

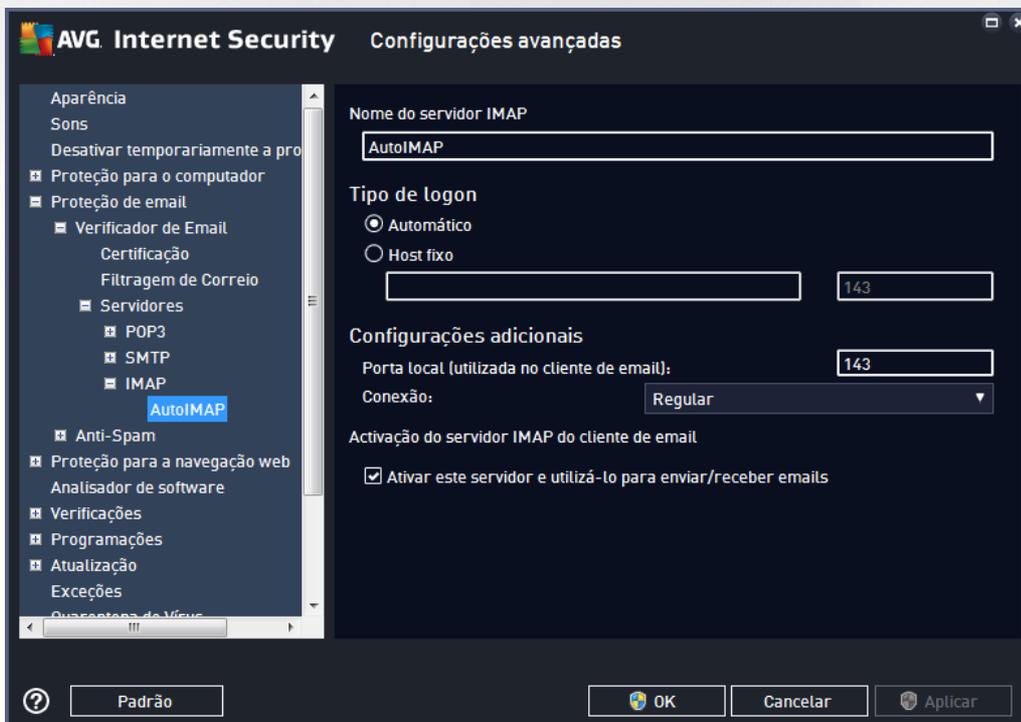




- **Nome do servidor SMTP** – neste campo, é possível especificar o nome dos servidores recém adicionados (*para adicionar um servidor SMTP, clique com o botão direito do mouse sobre o item SMTP do menu de navegação esquerdo*). Para o servidor "AutoSMTP" criado automaticamente, este campo fica desativado.
- **Tipo de login** – define o método para determinar o servidor de email usado para emails enviados:
 - **Automático** – o login será feito automaticamente, de acordo com as configurações do cliente de email
 - **Host fixo** – nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de emails. Você pode usar um nome de domínio (*por exemplo, smtp.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*) como nome. Se o servidor de email 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 é a 25.
- **Configurações adicionais** – especifica parâmetros mais detalhados:
 - **Porta local** – especifica a porta em que a comunicação do seu aplicativo de email deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de email como a porta para comunicação SMTP.
 - **Conexão** – nesse menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se 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 email de destino.
- **Ativação do servidor SMTP do cliente de email** – marque/desmarque esse item para ativar ou desativar o servidor SMTP especificado acima



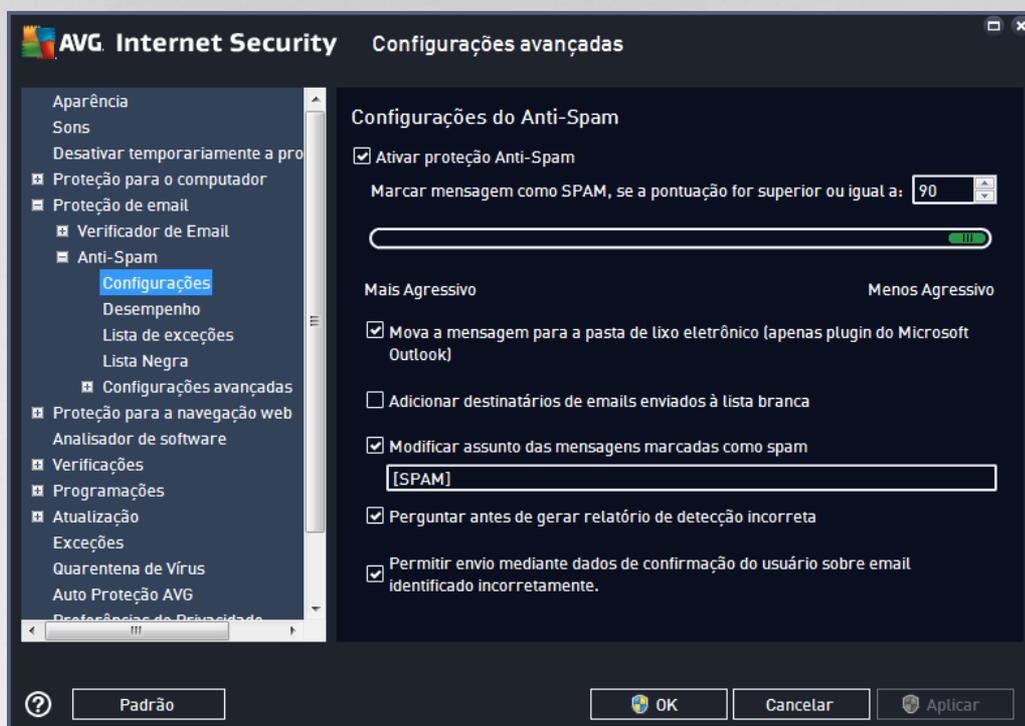
Nessa caixa de diálogo, você pode configurar um novo servidor do [Verificador de Email](#) usando o protocolo IMAP para mensagens enviadas:





- **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*).
- **Tipo de logon** – define o método para determinar o servidor de email usado para emails enviados:
 - **Automático** – o login será feito automaticamente, de acordo com as configurações do cliente de email
 - **Host fixo** – nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de emails. Você pode usar um nome de domínio (*por exemplo, smtp.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*) como nome. Se o servidor de email 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:
 - **Porta local (utilizada no cliente de email)** – especifica a porta em que a comunicação do seu aplicativo de email deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de email como a porta para comunicação IMAP
 - **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 serem rastreados ou monitorados por terceiros. Esse recurso está disponível somente quando houver suporte no servidor de email de destino.
- **Ativação do servidor IMAP do cliente de email** – marque/desmarque esse item para ativar ou desativar o servidor IMAP especificado acima

7.5.2. Anti-Spam



Na caixa de diálogo **Configurações do Anti-Spam**, é possível marcar/desmarcar a caixa de seleção **Ativar proteção Anti-Spam** para permitir/proibir a verificação anti-spam em comunicações por email. Essa opção está ativada como padrão e, como sempre, recomendamos 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 a pontuação for superior a** digitando o valor ou movendo o controle deslizante para a esquerda ou para a direita.

O intervalo de valores é limitado de 50 a 90. Veja uma análise geral do limite de pontuação:

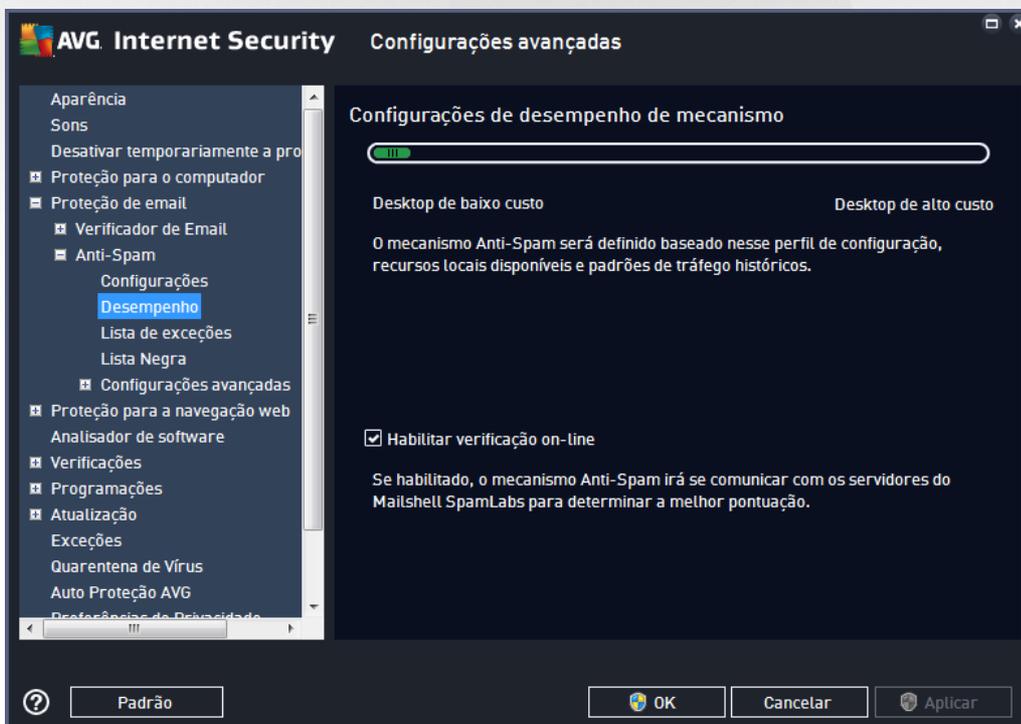
- **Valor entre 80 e 90** – as mensagens de email que parecem ser spam serão filtradas. Algumas mensagens que não são SPAM poderão ser bloqueadas incorretamente.
- **Valor entre 60 e 79** – uma configuração considerada bastante agressiva. As mensagens de email que provavelmente são spam serão filtradas. É provável que mensagens não SPAM também sejam bloqueadas.
- **Valor entre 50 e 59** – configuração muito agressiva. É provável que mensagens de email não spam sejam bloqueadas como se fosse spam verdadeiro. **Esse intervalo limite não é recomendado para uso normal.**

Na caixa de diálogo **Configurações do Anti-Spam**, você pode definir melhor como as mensagens de email de spam detectadas devem ser tratadas:



- **Mover mensagens para a pasta de lixo eletrônico** (apenas plugin do Microsoft Outlook) – marque esta caixa de seleção para especificar que cada mensagem de spam detectada será movida automaticamente para uma pasta de lixo específica em seu cliente de email MS Outlook. No momento, o recurso não é suportado em outros clientes de email.
- **Adicionar destinatários de emails enviados à sua lista branca** – marque essa caixa de seleção para confirmar que todos os destinatários de emails enviados são confiáveis e que todas as mensagens de email provenientes das contas desses destinatários podem ser entregues.
- **Modificar assunto das mensagens marcadas como spam** – 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 email. O texto desejado pode ser digitado no campo de texto ativado.
- **Perguntar antes de gerar relatório de detecção incorreta** – desde que, durante o processo de instalação, você tenha concordado em participar do projeto de [Preferências de Privacidade](#). Se for o caso, você autoriza a geração de relatório de ameaças detectadas para a AVG. O relatório é feito 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.

A caixa de diálogo **Configurações de desempenho do mecanismo** (que pode ser acessada por meio do link no 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 **Desktop de baixo custo/ Desktop de alto custo**.

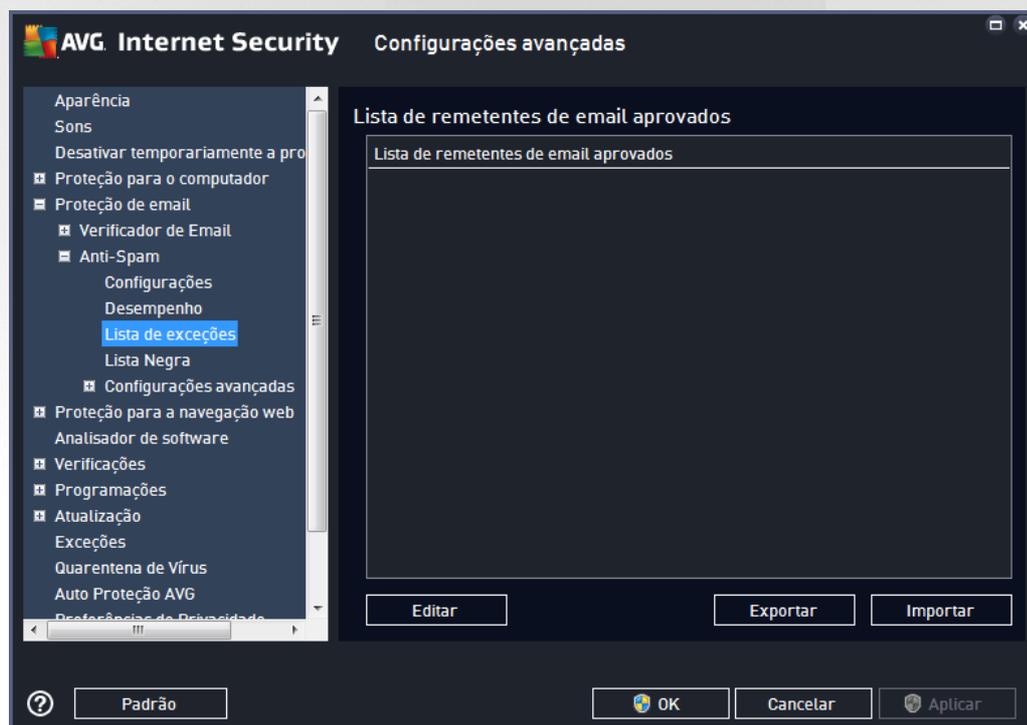


- **Desktop de baixo custo** – durante o processo de verificação para identificar spam, nenhuma regra será usada. Apenas os dados de treinamento serão usados para identificação. Esse modo não é recomendado para uso comum, a menos que o hardware do computador seja realmente fraco.
- **Desktop de alto custo** – esse modo consumirá uma grande quantidade de 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 como padrão. Isso 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!

O item **Lista de exceções** abre uma caixa de diálogo denominada **Lista de remetentes de email aprovados**, com uma lista global de endereços de email 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 com um dos métodos a seguir: digitando diretamente cada endereço de email ou importando toda a lista de endereços de uma vez.

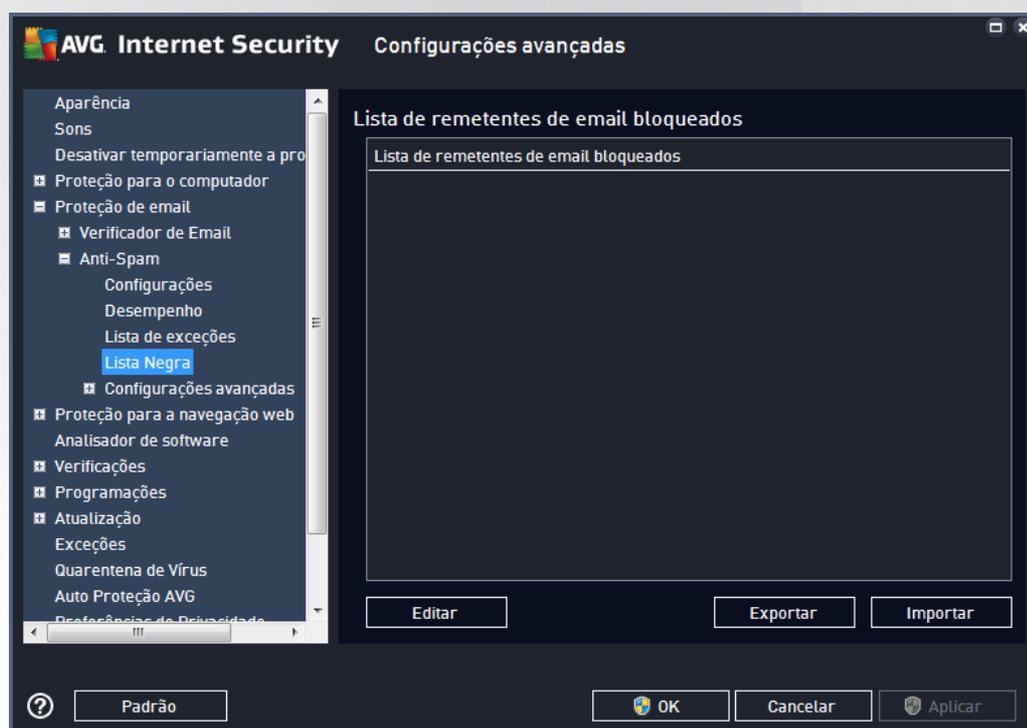
Botões de controle



Os seguintes botões estão disponíveis:

- **Editar** – pressione este botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (*you can use the copy/paste method*). Insira um item (*sender, domain name*) 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 email preparado, poderá simplesmente importá-lo selecionando este botão. O conteúdo do arquivo deve conter somente um item (*address, domain name*) por linha.

O item **Lista negra** abre uma caixa de diálogo com uma lista global de endereços de email 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 email/domínios listados serão identificados como spam. Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los com um dos métodos a seguir: digitando diretamente cada endereço de email ou importando toda a lista de endereços de uma vez.

Botões de controle

Os seguintes botões estão disponíveis:



- **Editar** - pressione este botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (*you can use the copy/paste method*). Insira um item (*sender, domain name*) 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 email preparado, poderá simplesmente importá-lo selecionando este botão.

A ramificação Configurações avançadas contém várias opções de configuração para o recurso Anti-Spam. Essas configurações se destinam exclusivamente a usuários experientes, principalmente administradores de rede, que precisam configurar a proteção anti-spam em detalhes para melhor proteger os servidores de email. 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 todas as configurações avançadas do Spamcatcher (MailShell Inc.). Qualquer alteração inapropriada poderá resultar em mau desempenho ou no funcionamento incorreto do componente.

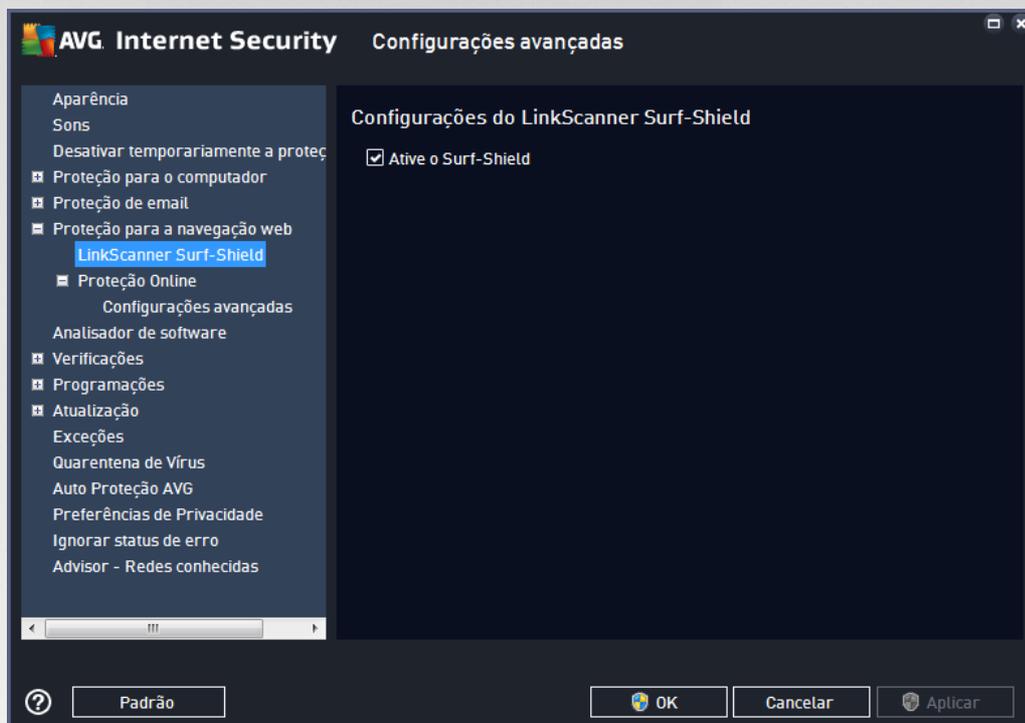
Se você ainda acredita que precisa alterar as configurações Anti-Spam no nível muito avançado, siga as instruções fornecidas diretamente na interface do usuário. Geralmente, em cada diálogo você encontrará um único recurso específico que pode ser editado. Sua descrição é sempre incluída no próprio diálogo. Você pode editar os seguintes parâmetros:

- **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



7.6. Proteção para a navegação web

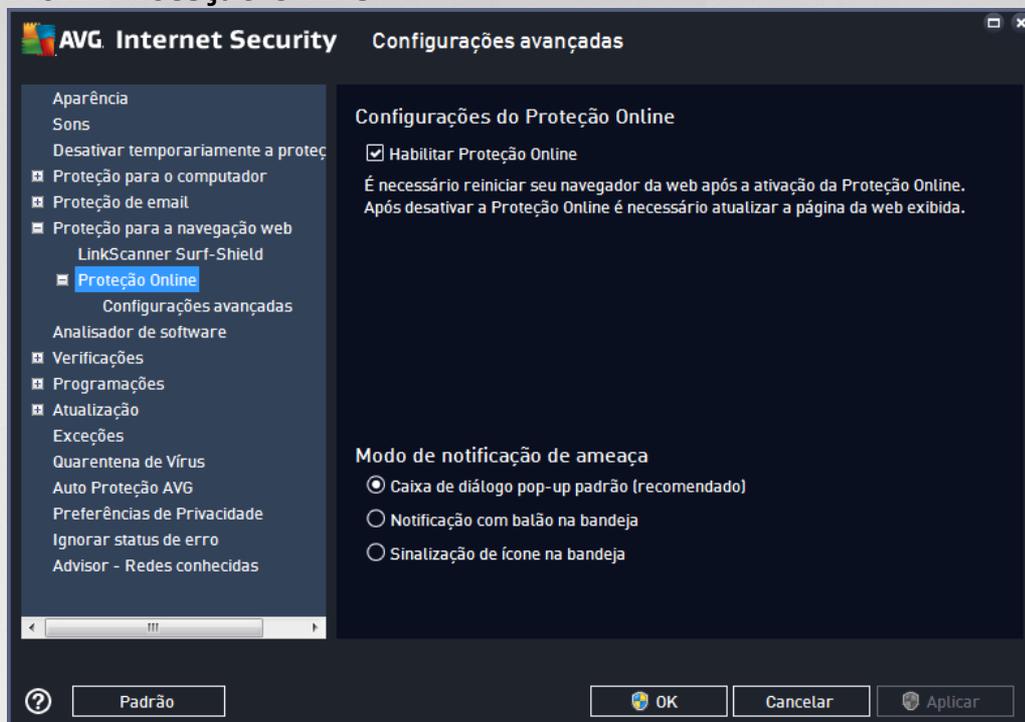
O diálogo de **configurações do LinkScanner** permite marcar/desmarcar os seguintes recursos:



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

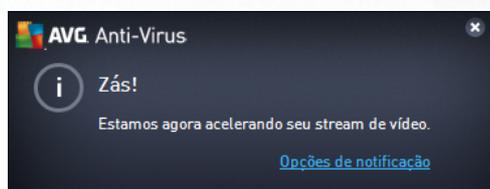


7.6.1. Proteção Online



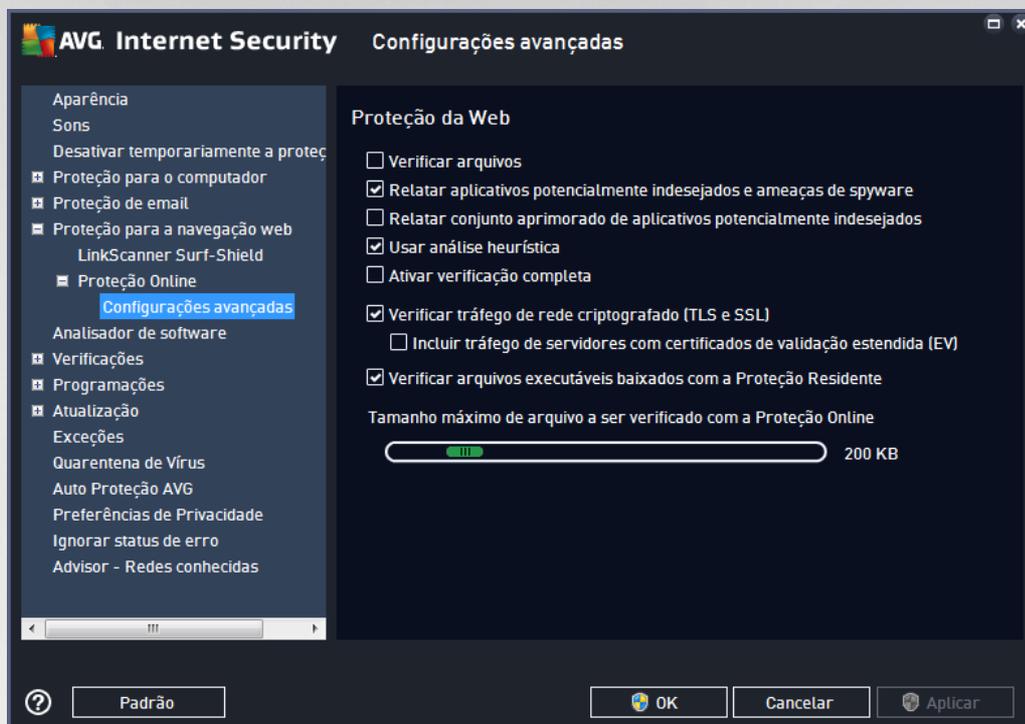
O diálogo **Proteção Online** oferece as seguintes opções:

- **Habilitar Proteção Online** (*ativado como padrão*) – ativa/desativa todo o serviço da **Proteção Online**. Para obter mais configurações avançadas da **Proteção Online**, siga para a caixa de diálogo seguinte: [Proteção da Web](#).
- **Habilitar AVG Accelerator** (*como padrão, ativado*) – ativa/desativa o serviço AVG Accelerator. O AVG Accelerator permite uma reprodução melhor de vídeos online e facilita downloads adicionais. Quando o processo de aceleração de vídeo estiver em andamento, você será notificado pela janela de pop-up na bandeja do sistema:



Modo de notificação de ameaça

Na parte inferior da caixa de diálogo, selecione o método desejado para ser informado sobre ameaças potenciais detectadas: por meio de uma caixa de diálogo pop-up, notificação de balão na bandeja ou nas informações de ícone na bandeja.



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:

- **Verificar arquivos** – (desativada como padrão): verifica o conteúdo dos arquivos possivelmente incluídos na página web a ser exibida.
- **Relatar programas potencialmente indesejáveis e ameaças de spyware** – (ativada como padrão): marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** – (ativada como padrão): marque para detectar os pacotes estendidos de spyware: programas que são saudáveis e inofensivos quando adquiridos diretamente do fabricante, mas que podem ser utilizados indevidamente para fins prejudiciais, posteriormente. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador. No entanto, como ela pode bloquear programas lícitos, ela se encontra desativada como padrão.
- **Usar heurística** – (ativada como padrão): verifica 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*).
- **Ativar verificação completa** – (desativada como padrão): em situações específicas, *suspeita de que seu computador foi infectado*, é possível marcar esta opção para ativar a maioria dos algoritmos de verificação 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 é bastante demorado.

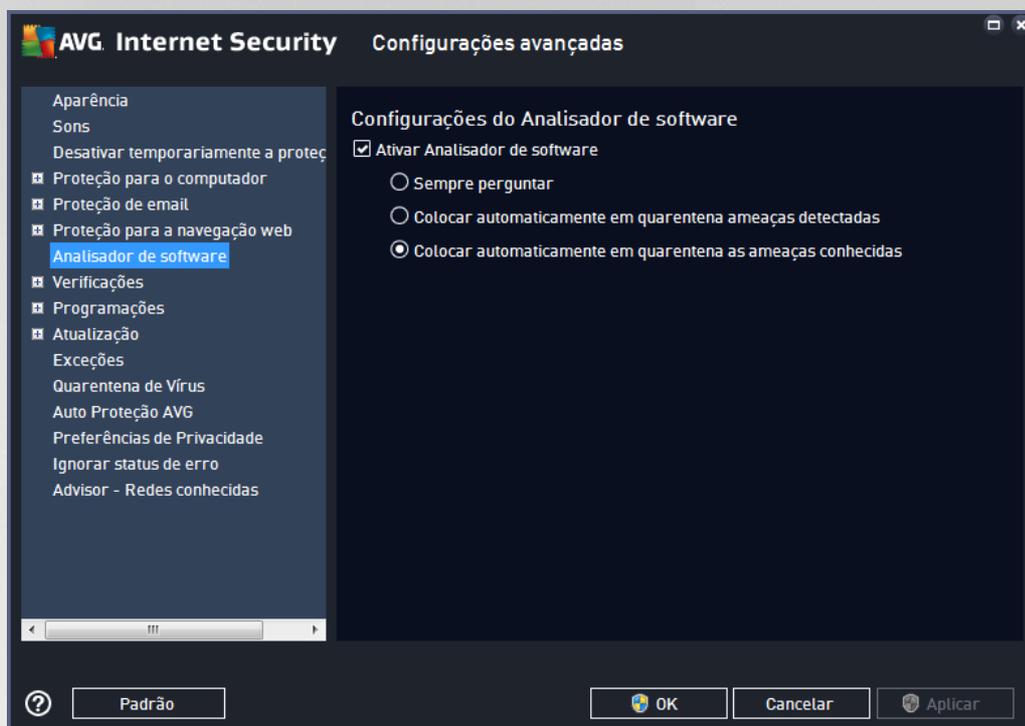
- **Verificar tráfego de rede criptografado (TLS e SSL)** – (ativado como padrão): deixe marcado para permitir que o AVG verifique também toda a comunicação de rede criptografada, ou seja, conexões através de protocolos de segurança (SSL e sua versão mais recente, TLS). Isso se aplica a websites utilizando HTTPS e conexões de cliente de email utilizando TLS/SSL. O tráfego protegido é descriptografado, verifica-se se existe malware e criptografado novamente para ser recebido com segurança ao seu computador. Nessa opção, é possível decidir **Incluir tráfego de servidores com certificados de validação estendida (EV)** e verificar também comunicação de rede criptografada de servidores certificados com Certificados de Validação Estendida. Emitir uma certificação EV exige validação extensiva pela autoridade de certificação e os websites que operam sob a certificação são, desta maneira, mais confiáveis (*menos propensos a distribuir malware*). Por esse motivo, não é necessário verificar o tráfego de servidores com certificação EV, o que tornará a comunicação criptografada moderadamente mais rápida.
- **Verificar arquivos executáveis baixados com a Proteção Residente** – (ativada como padrão): verifica arquivos executáveis (*normalmente arquivos com extensão exe, bat, com*) após terem sido baixados. A Proteção Residente verifica arquivos antes de baixá-los para garantir que nenhum arquivo prejudicial chegue ao seu computador. No entanto, essa verificação é limitada pelo **Tamanho máximo da parte do arquivo a ser verificado** – consulte o próximo item nessa caixa de diálogo. Dessa maneira, grandes arquivos são verificados por partes e isso é válido para a maioria dos arquivos executáveis. Os arquivos executáveis podem executar várias tarefas em seu computador e é vital que eles sejam 100% seguros. Isso pode ser garantido ao verificar o arquivo em partes antes de ele ser baixado e também logo após o término do download. Recomendamos manter essa opção marcada. Se você desativar essa opção, você ainda pode ficar tranquilo que o AVG encontrará qualquer código potencialmente perigoso. Normalmente, ele não poderá avaliar um arquivo executável como um complexo, então ele poderá produzir alguns falsos positivos.

A barra deslizante na caixa de diálogo permite definir o **tamanho máximo de um arquivo a ser verificado** – se os arquivos incluídos estiverem presentes na página exibida, será também possível verificar o conteúdo deles, mesmo antes que serem baixados para seu computador. Entretanto, a verificação de arquivos grandes pode levar tempo e o download da página da Web pode ficar significativamente mais lento. Use a barra deslizante para especificar o tamanho máximo de um arquivo que será verificado com a **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.

7.7. Analisador de software

O **Analisador de Software** é um componente antimalware que o protege contra todos os tipos de malwares (*spyware, robôs, roubo de identidade, etc.*) usando tecnologias comportamentais e que fornece proteção imediata contra novos vírus (*para obter uma descrição detalhada das funcionalidades dos componentes, consulte o capítulo [Analisador de Software](#)*).

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



Ativar o Analisador de Software (ativada como padrão) - desmarque para desativar o componente [Identidade](#). **É altamente recomendável não fazer isso a menos que você precise!** Quando o Analisador de Software está ativado, você pode especificar o que fazer quando uma ameaça é detectada:

- **Sempre perguntar** – 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 automaticamente em quarentena ameaças detectadas** – marque essa caixa para especificar que deseja mover todas as ameaças possivelmente detectadas para um espaço seguro da [Quarentena de Vírus](#) do 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 conhecidas** (ativado como padrão) – marque esse item se desejar que todos os aplicativos detectados como possíveis malware sejam movidos automaticamente e imediatamente para a [Quarentena de Vírus](#).

7.8. Verificações

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

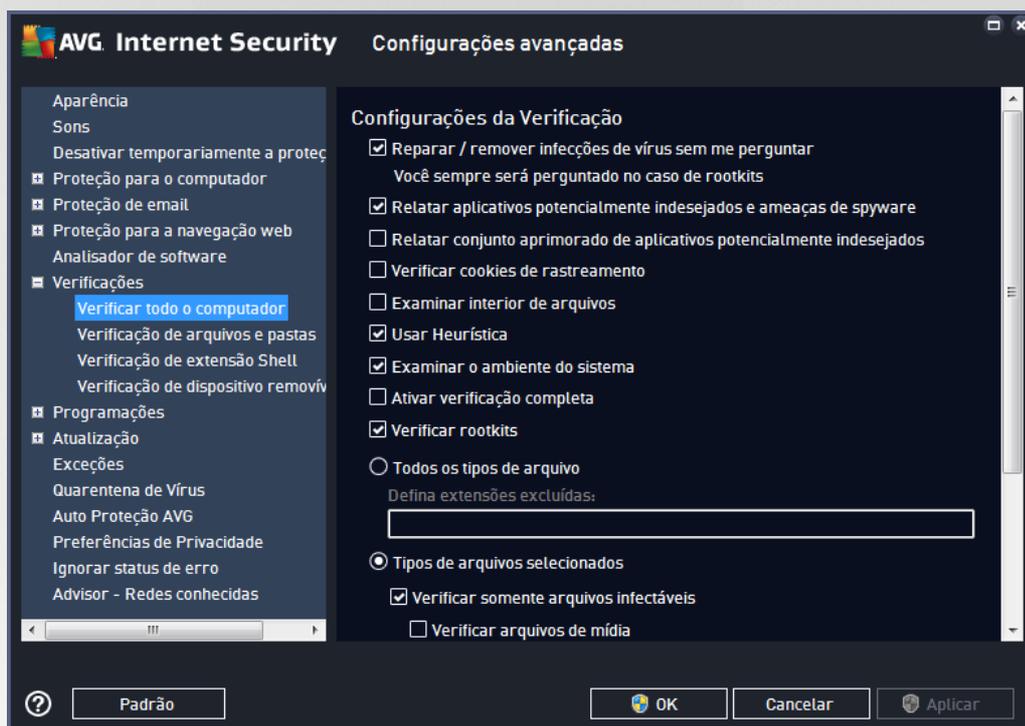
- [Verificar todo o computador](#) – verificação padrão predefinida de todo o computador
- [Verificação de arquivos e pastas](#) – verificação padrão predefinida de áreas selecionadas do computador
- [Verificação de extensão Shell](#) – verificação específica de um objeto selecionado diretamente do ambiente do Windows Explorer



- [Verificação de dispositivos removíveis](#) – verificação específica de dispositivos removíveis conectados ao computador

7.8.1. Verificar todo o computador

A opção **Verificar todo o computador** permite a edição de parâmetros de uma das verificações predefinidas pelo fornecedor do software, [Verificar todo o computador](#):



Configurações da verificação

A seção **Configurações da verificação** oferece uma lista de parâmetros de verificação que podem ser ativados ou desativados:

- **Reparar ou remover infecções vírus sem me consultar** (ativada como 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, ele será movido para a [Quarentena de Vírus](#).
- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada por padrão) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (desativada por padrão) – marque para detectar os pacotes estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas que podem ser mal utilizados com más



intenções posteriormente. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, ela pode bloquear programas lícitos; portanto, é desativada por padrão.

- **Verificar cookies de rastreamento** (desativada por padrão) – este parâmetro estipula 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).
- **Examinar interior de arquivos** (desativada por padrão) – esse parâmetro estipula 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.
- **Examinar o 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 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 é bastante demorado.
- **Verificar rootkits** (ativado como padrão) – a verificação [Anti-Rootkit](#) procura possíveis rootkits em seu PC, ou seja, programas e tecnologias que podem encobrir a atividade de malware em seu 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.

Você também deve decidir o que deseja verificar

- **Todos os tipos de arquivos** com a opção de definir exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (após serem salvas, as vírgulas mudam para ponto e vírgula) que não podem ser verificadas.
- **Tipos de arquivos selecionados** – você pode especificar que deseja verificar apenas os arquivos que podem ser infectados (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 pouco provável que sejam infectados por vírus). Novamente, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
- Opcionalmente, você pode optar por **Verificar arquivos sem extensões** – essa opção está ativada por padrão e recomendamos manter essa configuração, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são 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 os recursos do sistema utilizados serão bem maiores 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 os recursos do sistema utilizados ampliando a duração da verificação.

Defina relatórios de verificação adicionais...

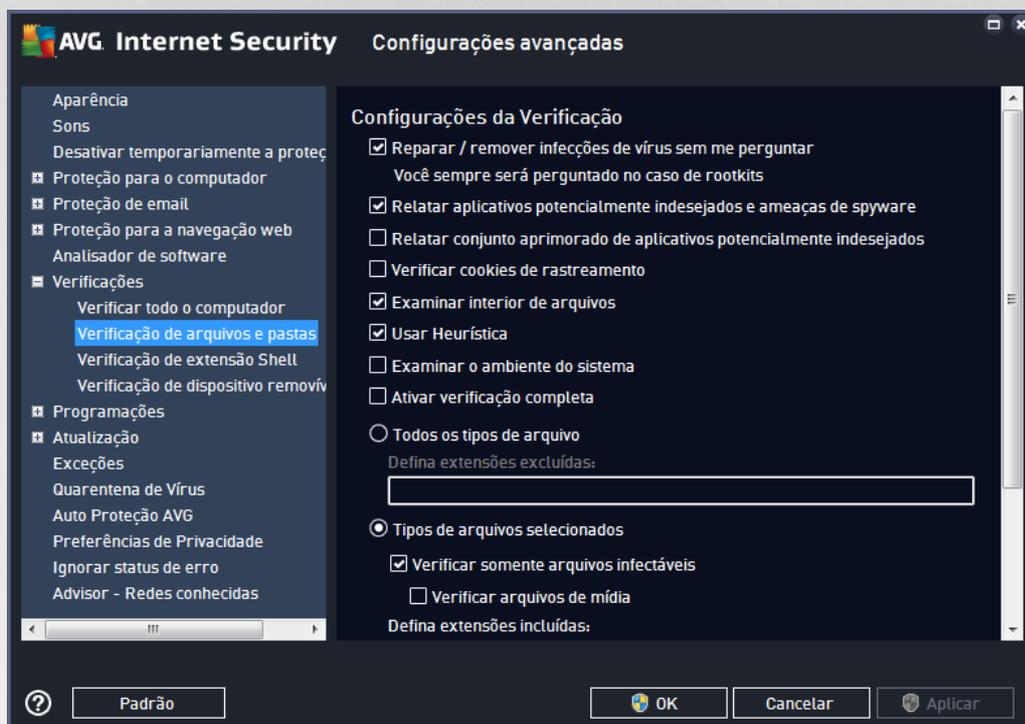
Clique no link **Relatórios de verificação adicionais...** para abrir uma janela independente da caixa de diálogo chamada **Verificar relatórios** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:





7.8.2. Verificação de arquivos e pastas

A interface de edição para **Verificar arquivos ou pastas** é quase idêntica ao diálogo de edição de [Verificar todo o computador](#), no entanto, as configurações padrão são mais rigorosas para [Verificar todo o computador](#):

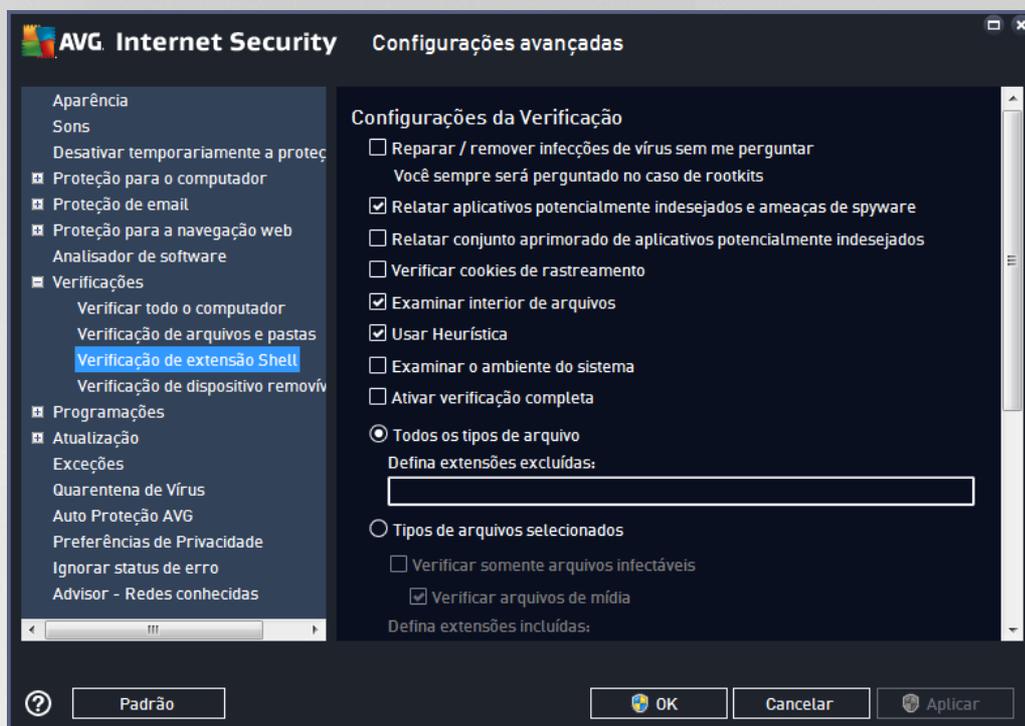


Todos os parâmetros definidos nesta caixa de diálogo de configuração aplicam-se apenas às áreas selecionadas para verificação com [Verificar arquivos ou pastas](#)!

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

7.8.3. Verificação da Extensão Shell

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



As opções de edição são quase idênticas das disponíveis em [Verificar todo o computador](#), no entanto, as configurações padrão diferem (por exemplo, *Verificar todo o computador*, por padrão, não verifica os arquivos compactados, mas verifica o ambiente do sistema; na *Verificação de extensão Shell* ocorre o contrário).

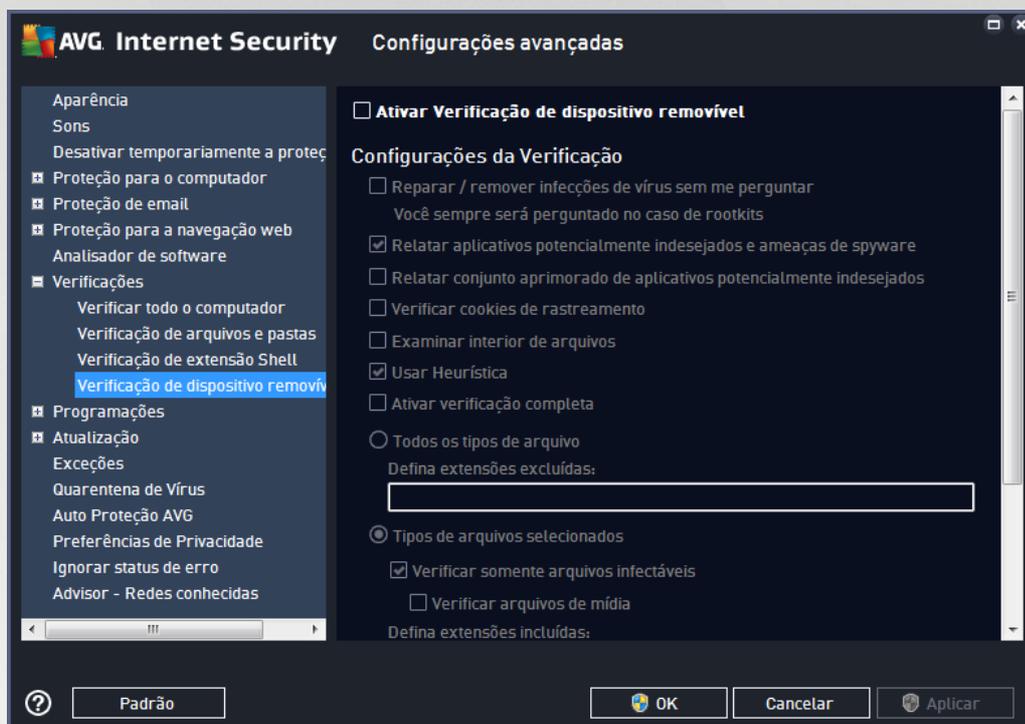
Obs.: para obter uma descrição dos parâmetros específicos, consulte o capítulo [Configurações avançadas do AVG/Verificações/Verificar todo o computador](#).

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



7.8.4. Verificação de Dispositivo Removível

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



A *Verificação de dispositivo removível* é ativada automaticamente ao conectar um dispositivo removível ao computador. Como 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**.

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

7.9. Programações

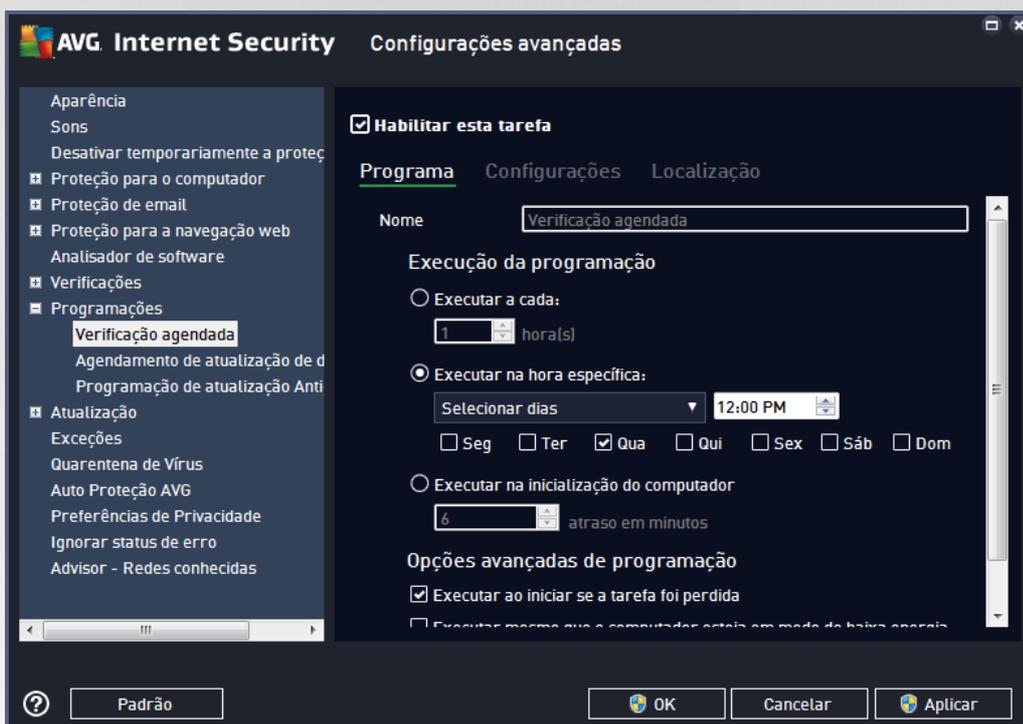
Na seção *Programações*, é possível editar as configurações padrão de:

- [Verificação agendada](#)
- [Agendamento de atualização de definições](#)
- Agendamento de atualização de programa
- [Agendamento de atualização do anti-spam](#)



7.9.1. Verificação agendada

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:



Depois, o campo de texto denominado **Nome** (*desativado para todas as programações padrão*) exibe 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 agendada** 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 facilitar seu reconhecimento, mais tarde.

Exemplo: não é bom 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 bom nome descritivo seria "Verificação da área do sistema", etc. Também não é necessário especificar no nome da verificação, se ela for uma verificação de todo o computador, ou apenas de arquivos ou pastas selecionados. Suas próprias verificações sempre serão uma versão específica da [verificação de arquivos ou pastas selecionadas](#).

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

Execução da programação

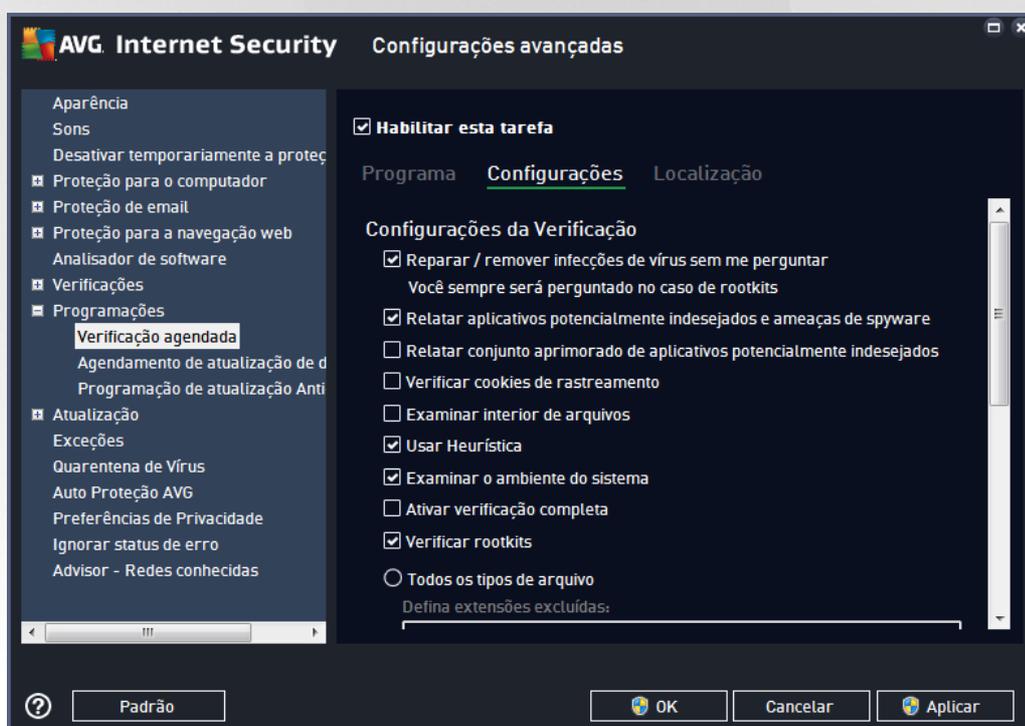
Aqui, você pode especificar intervalos de tempo para a ativação da verificação recém-programada. O tempo pode ser definido pela repetição da execução da verificação depois de um determinado período (**Executar a**



cada ...), pela definição de uma data e hora exatas (**Executar na hora específica**) ou talvez pela definição de um evento ao qual a ativação da verificação deve ser associada (**Executar na inicialização do computador**).

Opções avançadas de programação

- **Executar ao iniciar se a tarefa for perdida** – se você agendar a tarefa para ser executada em um momento específico, a opção irá garantir que a verificação seja realizada de maneira subsequente caso o computador seja desligado no momento agendado.
- **Executar mesmo que o computador esteja em modo de baixa energia** – a tarefa deve ser realizada mesmo que o computador esteja funcionando com energia da bateria no momento agendado.



Na guia **Configurações**, você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros está 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 / remover infecções de vírus sem me perguntar** (ativada 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, ele será movido para a [Quarentena de Vírus](#).
- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada por padrão): marque para ativar a verificação de spyware, além de vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses



programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (ativada por padrão): marque para detectar os pacotes estendidos de spyware: programas que são perfeitamente ok e inofensivos quando adquiridos diretamente do fabricante, mas que podem ser utilizados indevidamente para fins prejudiciais, posteriormente. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, ela pode bloquear programas lícitos; portanto, é desativada por padrão.
- **Verificar cookies de rastreamento** (desativada por padrão): este parâmetro especifica 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 especifica 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 raramente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método é bastante demorado.
- **Verificar rootkits** (ativada como padrão): a verificação Anti-Rootkit procura possíveis rootkits em seu computador, ou seja, programas e tecnologias que podem encobrir a atividade de malware em seu 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.

Você também deve decidir o que deseja verificar

- **Todos os tipos de arquivos** com a opção de definir exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (após serem salvas, as vírgulas mudam para ponto e vírgula) que não podem ser verificadas.
- **Tipos de arquivos selecionados** – você pode especificar se deseja verificar apenas os arquivos que podem ser infectados (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 pouco provável que sejam infectados por vírus). Novamente, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.



- Opcionalmente, você pode optar por **Verificar arquivos sem extensões** – essa opção está ativada por padrão e recomendamos manter essa configuração, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção Verificar prioridade do processo, você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas os recursos do sistema utilizados serão bem maiores 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 os recursos do sistema utilizados ampliando a duração da verificação.

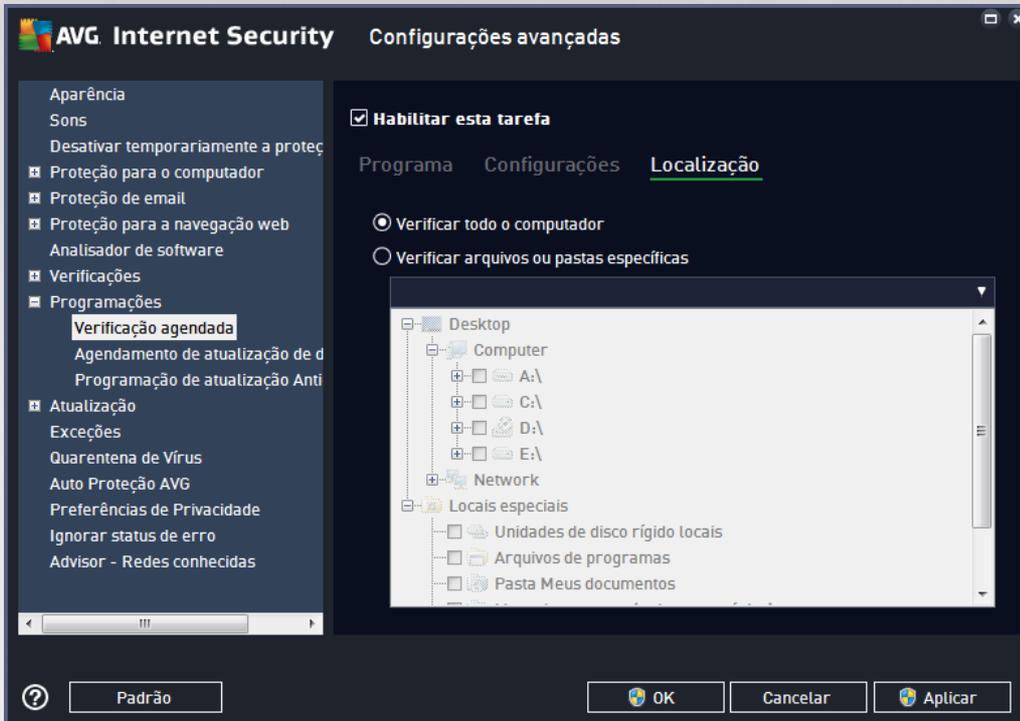
Defina relatórios de verificação adicionais

Clique no link **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:



Opções de desligamento do computador

Na seção **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**).

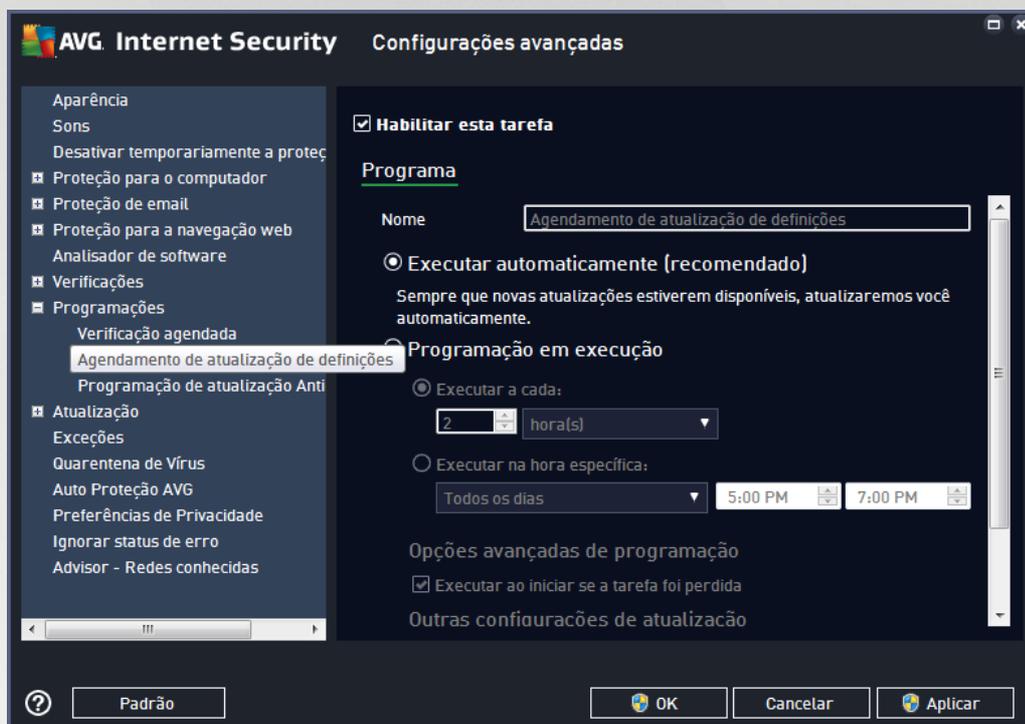


Na guia **Localização**, você pode definir se deseja programar a [verificação de todo o computador](#) ou a [verificação de arquivos e pastas](#). Se você selecionar a verificação de arquivos e pastas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação.



7.9.2. Agendamento de atualização de definições

Se for *realmente necessário*, você pode desmarcar o item **Habilitar esta tarefa** para desativar temporariamente a atualização de definições programada e ativá-la novamente mais tarde:



Nessa caixa de diálogo, você pode configurar alguns parâmetros detalhados do programa de atualização de definições. O campo de texto denominado **Nome** (*desativado para todas as programações padrão*) exibe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Como padrão, a tarefa é iniciada automaticamente (**Executar automaticamente**) assim que uma nova atualização de definição de vírus está disponível. Recomendamos manter essa configuração a menos que tenha um bom motivo para alterá-la! Depois, é possível configurar manualmente o início da tarefa e especificar os intervalos de tempo para o início das atualizações de definições recém-programadas. A hora pode ser definida através do início repetido da atualização após um certo período de tempo (**Executar a cada...**) ou definindo uma data e hora exata (**Executar na hora específica**).

Opções avançadas de programação

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

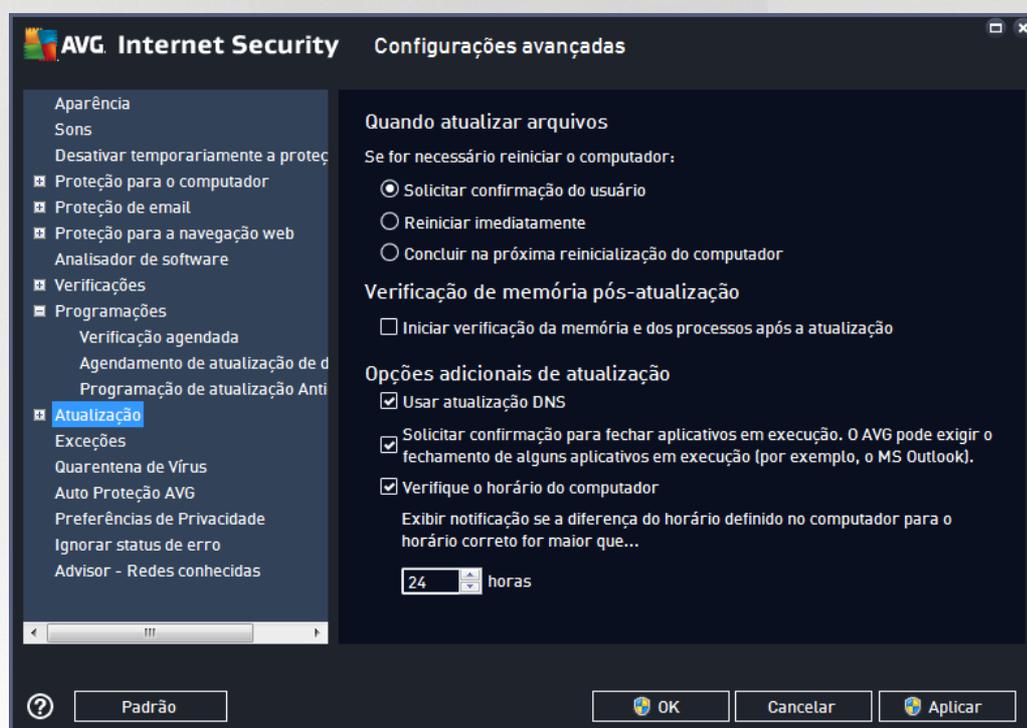
Outras configurações de atualização



Por fim, marque a opção **Executar novamente a atualização após a conexão de Internet estar disponível**, para ter certeza de que, se a conexão com a Internet for interrompida 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 do AVG na bandeja do sistema](#) (caso você tenha mantido a configuração padrão da caixa de diálogo [Configurações avançadas/Aparência](#)).

7.9.3. Agendamento de atualização do anti-spam

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



Nessa caixa de diálogo, você pode configurar parâmetros detalhados do programa de atualização. O campo de texto denominado **Nome** (*desativado para todas as programações padrão*) exibe 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 execução da atualização do Anti-Spam depois de um determinado período (**Executar a cada...**), pela definição de uma data e hora exatas (**Executar na hora específica**) ou pela definição de um evento ao qual a execução da atualização deve ser associada (**Executar na inicialização do computador**).

Opções avançadas de programação



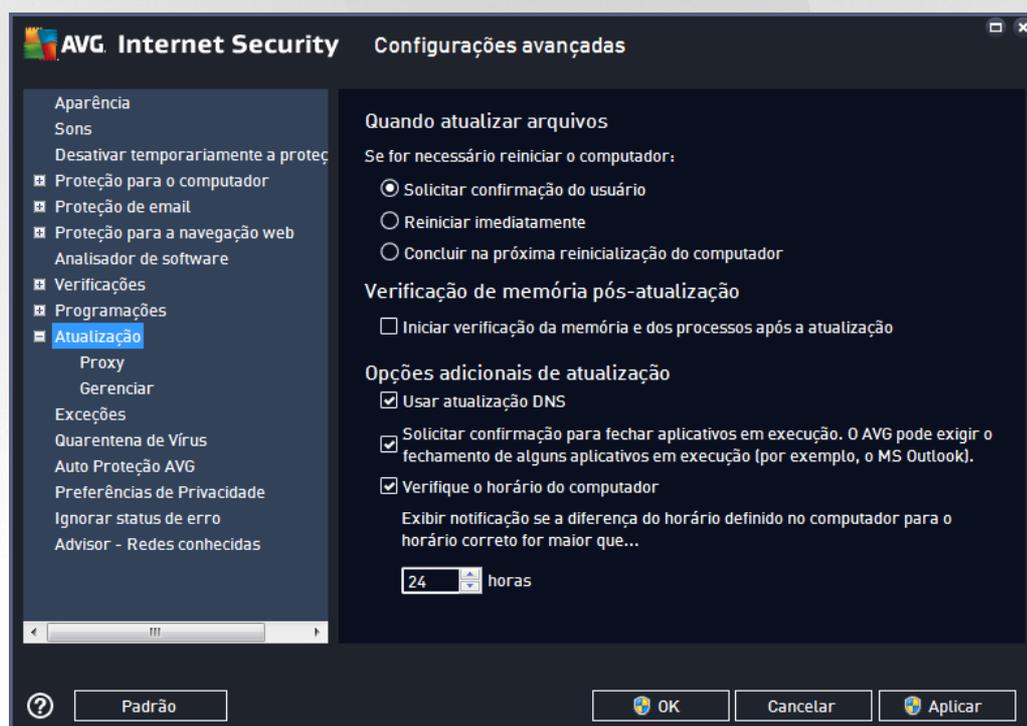
Esta seção permite definir sob quais condições a atualização do Anti-Spam deverá ou não ser executada se o computador estiver no modo de pouca energia ou completamente desligado.

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

7.10. 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

Nesta seção você poderá escolher três opções alternativas caso o processo de atualização exija a reinicialização do PC. A finalização da atualização pode ser programada para a próxima reinicialização do PC, ou você pode reiniciar imediatamente:

- **Solicitar confirmação do usuário** (como padrão) – será solicitada a sua aprovação da reinicialização do PC necessária para finalizar o processo de [atualização](#)



- **Reiniciar imediatamente** – o computador será reiniciado automaticamente após a conclusão do processo de [atualização](#) e sua aprovação não será necessária.
- **Concluir na próxima reinicialização do computador** – a finalização do processo de [atualização](#) será adiada até a próxima reinicialização do computador. Lembre-se de que esta opção só é recomendada se você tiver certeza que o computador será reinicializado regularmente, pelo menos uma vez por dia!

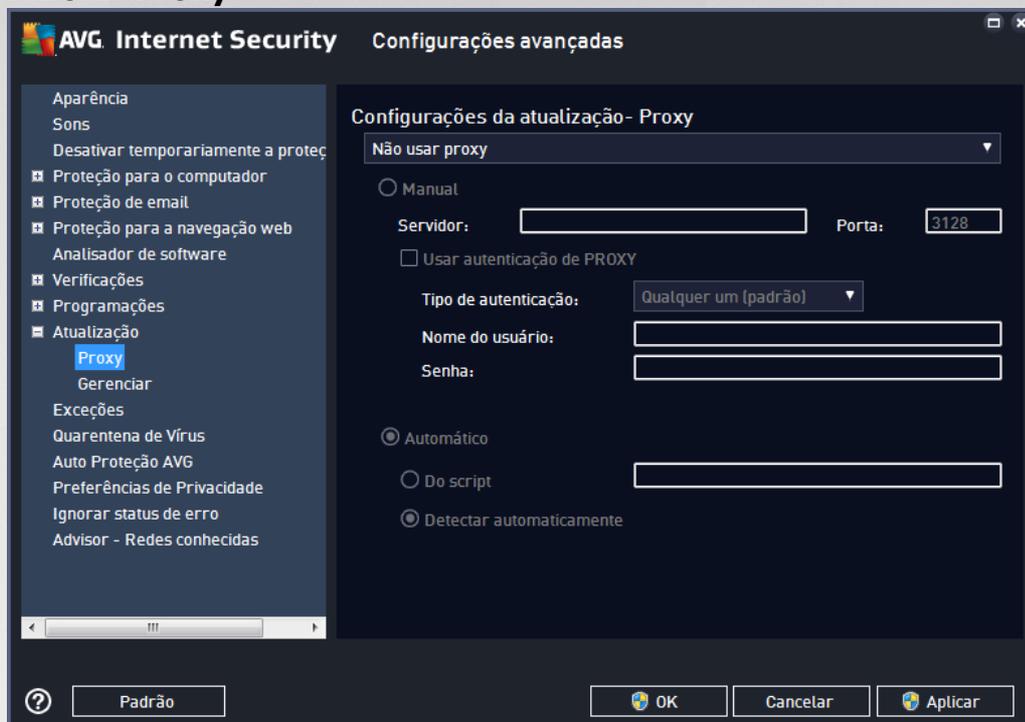
Verificação de memória pós-atualização

Marque essa caixa de seleção para estipular 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** (*ativado como padrão*) – após cada ativação da atualização do programa AVG, um ponto de restauração do sistema é criado. No caso de falha no processo de atualização e do sistema operacional, você poderá restaurar seu SO para a configuração original a partir 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** (*ativado como padrão*) – com este item marcado, depois que a atualização é iniciada, o **AVG Internet Security** 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.
- **Solicitar confirmação para fechar aplicativos em execução** (*ativado como padrão*) – ajuda a garantir que nenhum aplicativo em execução no momento será fechado sem sua permissão, se isso for necessário para a conclusão do processo de atualização.
- **Verifique o horário do computador** (*ativado como padrão*) – marque esta opção para declarar que você deseja que sejam exibidas notificações, caso o horário do computador seja diferente do horário correto em um número de horas maior que o especificado.

7.10.1. 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. Ambas as possibilidades também podem ser permitidas ao mesmo tempo. Em seguida, no primeiro item da caixa de diálogo **Configurações da atualização - Proxy**, você deverá selecionar no menu da caixa, se desejar:

- **Não usar proxy** – configurações padrão
- **Usar proxy**
- **Usar proxy; se falhar, se conecte diretamente**

Se você selecionar uma opção usando um 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 (*como padrão, esse número está definido como 3128, mas pode ser definido de forma diferente. Em caso de dúvida, 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.

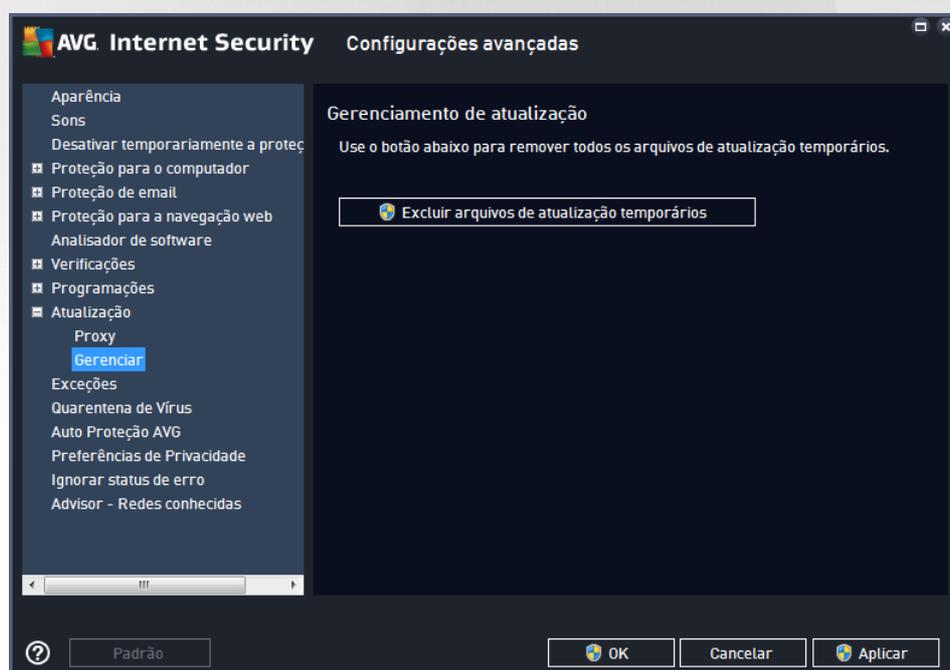
Configuração automática

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

- **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
- **Detectar automaticamente** – a configuração será detectada de forma automática e direta do servidor proxy

7.10.2. Gerenciar

A caixa de diálogo **Gerenciamento de atualização** oferece duas opções que podem ser acessadas por meio de dois botões:



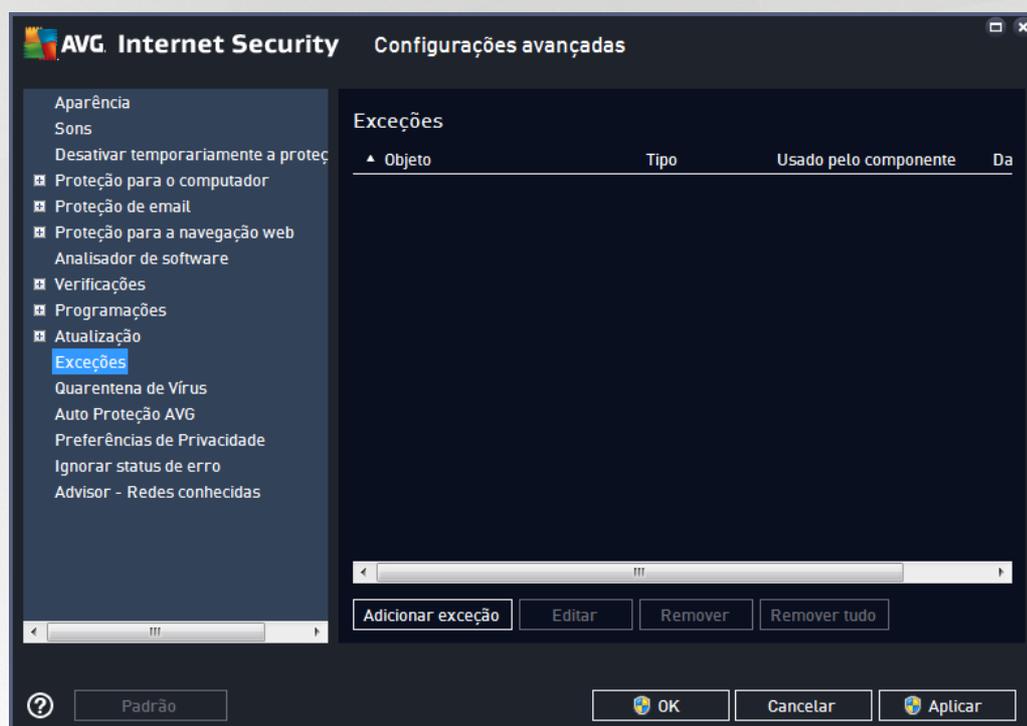
- **Excluir arquivos de atualização temporários** – pressione este botão para excluir todos os arquivos de atualização redundantes do seu disco rígido (*como padrão, eles são armazenados por 30 dias*)
- **Retornar à versão anterior do banco de dados de vírus** – pressione este botão para excluir a versão 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*)



7.11. Exceções

No diálogo **Exceções**, é possível definir exceções, ou seja, itens que o **AVG Internet Security** irá ignorar. Normalmente, você precisará definir uma exceção se o AVG continuar detectando um programa ou arquivo como uma ameaça ou bloqueando um website seguro como sendo perigoso. Adicione este arquivo ou website a esta lista de exceções, e o AVG não irá reportar ou bloqueá-lo mais.

Certifique-se sempre de que o arquivo, programa ou website em questão realmente está absolutamente seguro!



A carta do diálogo exibe uma lista de exceções, se qualquer uma já tiver sido definida. Cada item tem uma caixa de seleção próxima dele. Se a caixa de seleção está marcada, então a exceção está em efeito; se não, a exceção é apenas definida, mas não utilizada no momento. Clicando no cabeçalho de uma coluna, é possível classificar os itens permitidos de acordo com os respectivos critérios.

Botões de controle

- **Adicionar exceção** – clique para abrir um novo diálogo onde é possível especificar o item que deveria ser excluído da verificação do AVG.

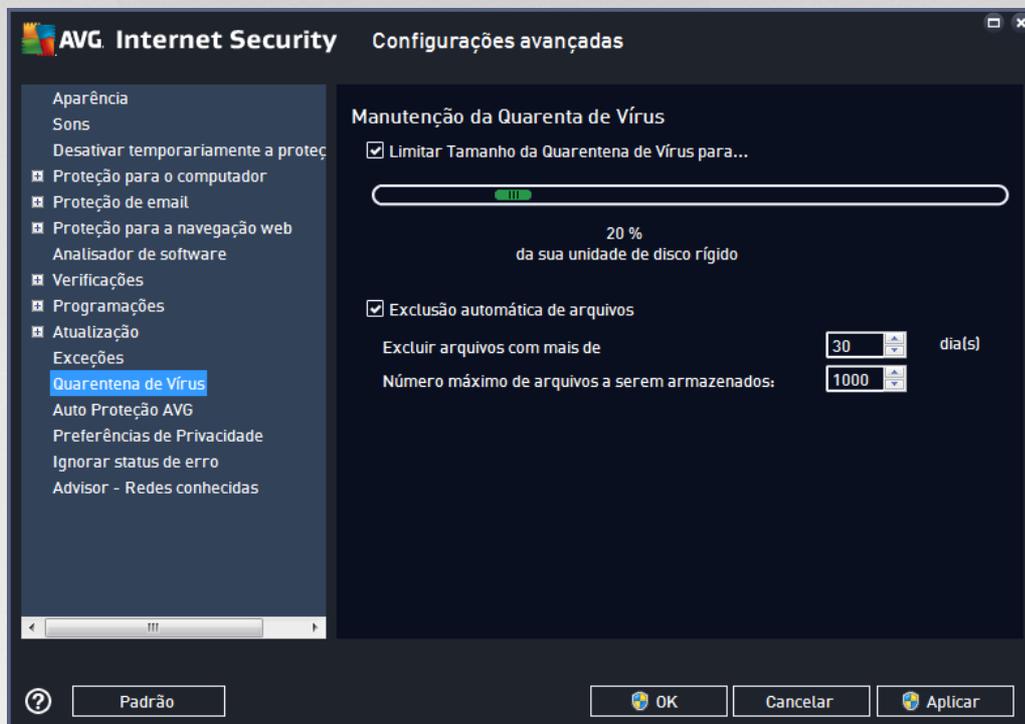


Primeiro, você será convidado a definir o tipo do objeto, ou seja, se é um aplicativo ou arquivo, uma pasta, URL ou um certificado. Depois você terá que procurar no seu disco o caminho do respectivo objeto, ou digitar o URL. Por fim, você pode selecionar quais recursos do AVG devem ignorar o objeto selecionado (*Proteção Residente, Verificação Manual e Agendada, Analisador de Software, Proteção Online e Interface de Verificação Antimalware do Windows*).

- **Editar** – esse botão está ativo somente se algumas exceções já tiverem sido definidas, e estão listadas no gráfico. Depois, é possível usar o botão para abrir o diálogo de edição sobre uma exceção selecionada e configurar os parâmetros da exceção.
- **Remover** – use este botão para cancelar uma exceção previamente definida. Você pode removê-las uma a uma, ou destacar um bloco de exceções na lista e cancelar as exceções definidas. Ao cancelar a exceção, o respectivo arquivo, pasta ou URL será verificado novamente pelo AVG. Observe que apenas a exceção será removida, não o arquivo ou a pasta!
- **Remover tudo** – Use esse botão para excluir todas as exceções definidas na lista.



7.12. Quarentena de Vírus

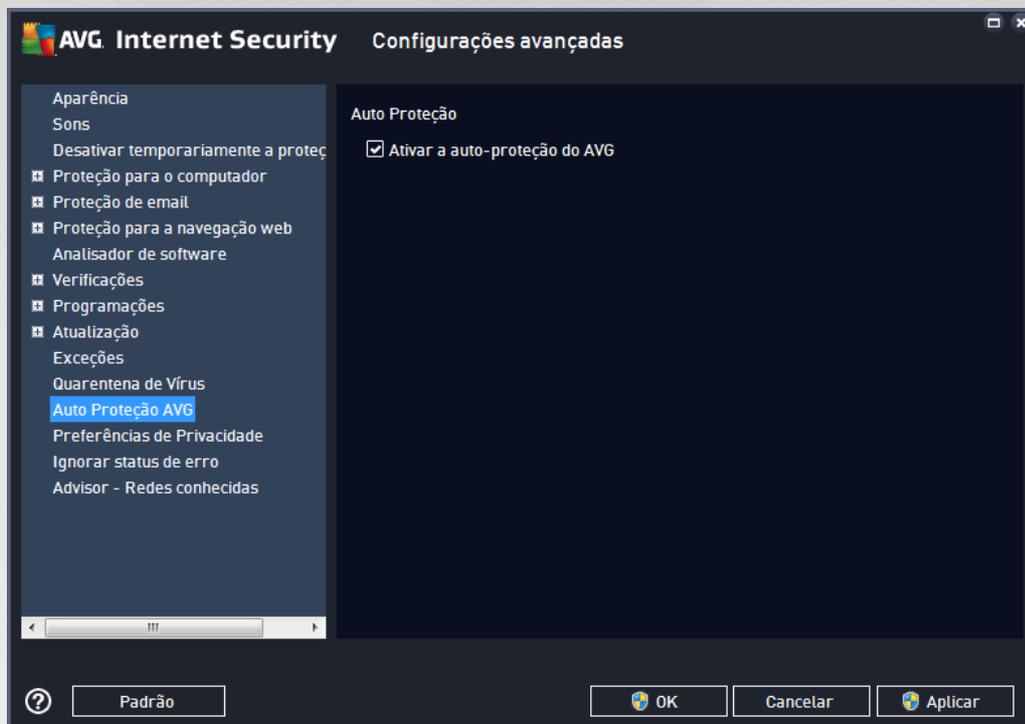


A caixa de diálogo **Manutenção da quarentena** permite definir vários parâmetros relativos à administração de objetos armazenados na [Quarentena](#):

- **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 arquivos** – nesta seção, defina a duração máxima de armazenamento dos objetos na [Quarentena de Vírus](#) (**Excluir arquivos mais antigos que... dias**) e o número máximo de arquivos a serem armazenados na [Quarentena de Vírus](#) (**Número máximo de arquivos a serem armazenados**).



7.13. Auto Proteção do AVG

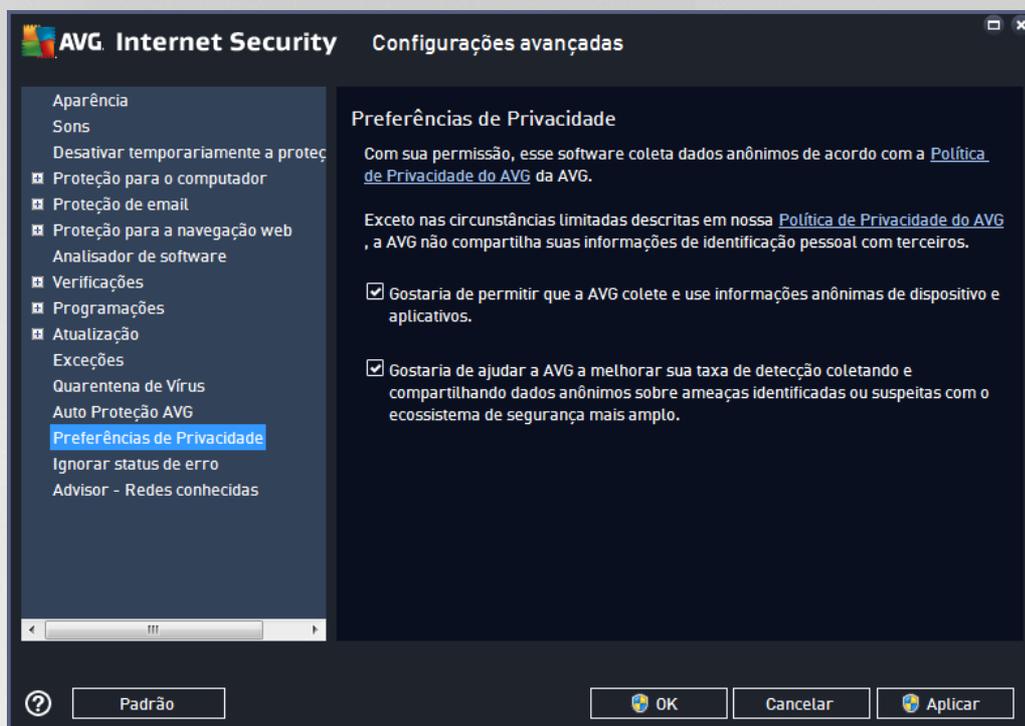


A **Auto Proteção AVG** possibilita que o **AVG Internet Security** proteja seus próprios processos, arquivos, chaves de registro e drivers contra alteração e desativação. O principal motivo para este tipo de proteção é que algumas ameaças sofisticadas tentam desarmar a proteção antivírus e depois livremente causam danos a seu computador.

Nós recomendamos manter esse recurso ativado!

7.14. Preferências de privacidade

A caixa de diálogo **Preferências de Privacidade** o convida a participar do programa de aprimoramento de produto AVG e nos ajuda a aumentar o nível de segurança geral na Internet. Seu relatório 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 de modo automático e assim não causa nenhuma inconveniência a você. Nenhum dado pessoal é incluído nos relatórios. A geração de relatórios de ameaças detectadas é opcional. No entanto, solicitamos que você mantenha essa opção ativada. Ela nos ajuda a melhorar a proteção para você e para os usuários do AVG.



Dentro do diálogo, as seguintes opções de configuração estão disponíveis:

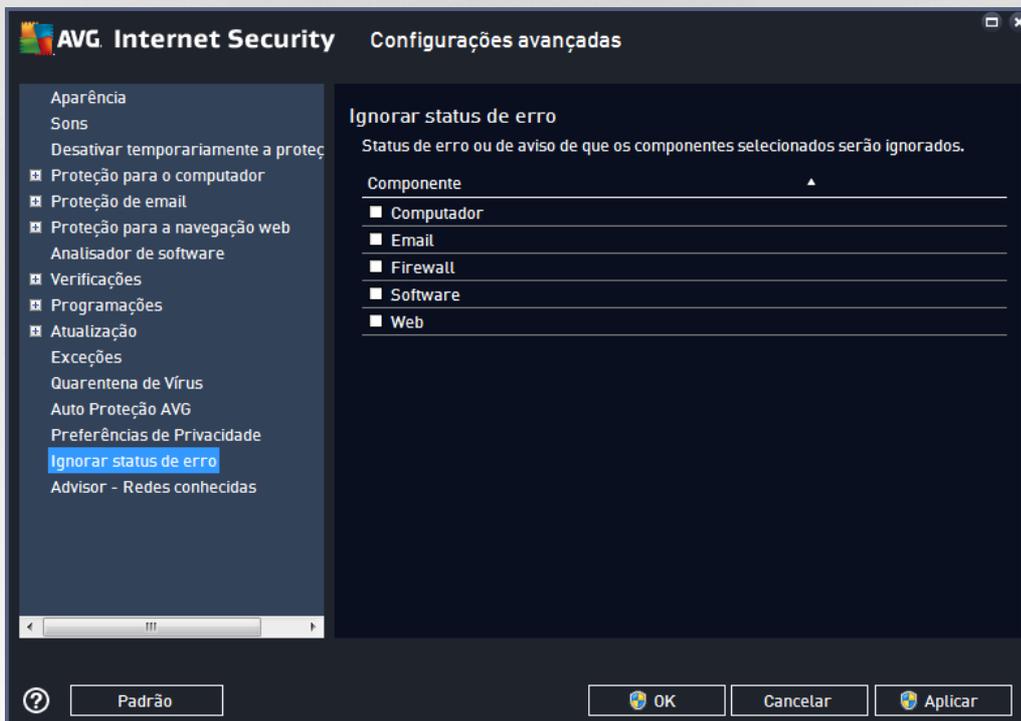
- **Gostaria de ajudar a AVG a aprimorar seus produtos através da participação no Programa de Aprimoramento de Produtos da AVG (ativado como padrão)** – se desejar nos ajudar a aprimorar ainda mais o **AVG Internet Security**, mantenha a caixa de seleção marcada. Isso permitirá que todas as ameaças encontradas sejam relatadas à AVG, para que possamos coletar informações atualizadas sobre as ameaças mais recentes dos participantes do mundo todo e, em retorno, 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.
 - **Permitir envio mediante dados de confirmação do usuário sobre email identificado incorretamente (ativada como padrão)** – envie informações sobre mensagens de email identificadas incorretamente como spam, ou sobre mensagens de spam que não foram detectadas pelo serviço Anti-Spam. Ao enviar este tipo de informação, será solicitada a sua confirmação.
 - **Permitir o envio de dados anônimos sobre ameaças identificadas ou suspeita (ativada como padrão)** – envie informações sobre qualquer código ou padrão de comportamento perigoso ou positivamente perigoso (*pode ser um vírus, spyware ou página web mal intencionada que você está tentando acessar*) detectado em seu computador.
 - **Permitir o envio de dados anônimos sobre uso do produto (ativada como padrão)** – envie estatísticas básicas sobre o uso do aplicativo, como número de detecções, verificações executadas, atualizações com ou sem sucesso, etc.
- **Permitir a verificação de detecções na nuvem (ativada como padrão)** – verifica se as ameaças detectadas são realmente infecções, para identificar falsos positivos.



- **Gostaria que a AVG personalize a minha experiência ativando o AVG Personalization** (como padrão, desativado) – esse recurso analisa anonimamente o comportamento de programas e aplicativos instalados em seu PC. Com base nessa análise, a AVG pode oferecer serviços direcionados às suas necessidades, para protegê-lo com segurança máxima.

7.15. Ignorar status de erro

Na caixa de diálogo **Ignorar status de erro** você pode selecionar os componentes dos quais não deseja receber informações:



Como padrão, não há componentes selecionados nesta lista. Isso significa que, caso qualquer componente forneça um status de erro, você será informado imediatamente por meio de:

- [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 haver uma situação na qual, por algum motivo, seja necessário desativar um componente temporariamente. **Isso não é recomendado, você deve tentar manter todos os componentes permanentemente ligados e na configuração padrão**, mas isso 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.

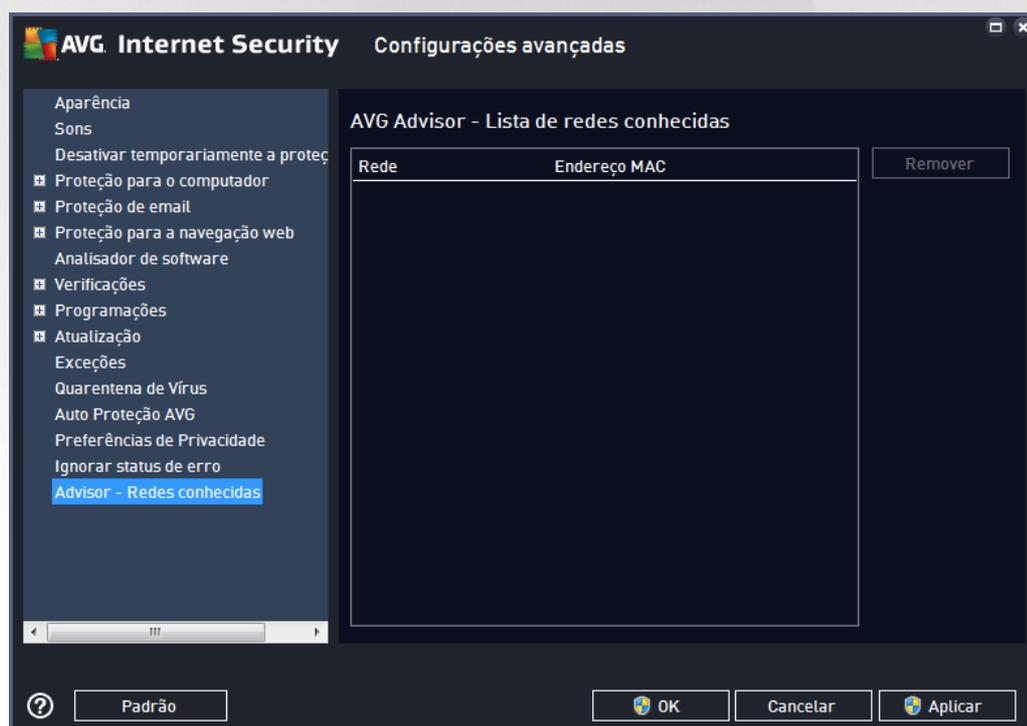


Neste caso, na caixa de diálogo **Ignorar status de erro**, é possível selecionar componentes que podem estar em estado de erro (ou desligado) e você não deseja receber informações sobre isso. Pressione o botão **OK para confirmar**.

7.16. Advisor – Redes conhecidas

O [AVG Advisor](#) contém um recurso que monitora as redes nas quais você se conecta e, se uma nova rede for encontrada (com um nome de rede já utilizado, que pode causar confusão), ele notificará e recomendará que você verifique a segurança da rede. Se decidir que a rede é segura para conexão, é possível salvá-la nessa lista (através do link fornecido da notificação na bandeja do AVG Advisor que desliza sobre a bandeja do sistema assim que uma rede desconhecida é detectada. Para obter detalhes, consulte o capítulo sobre o [AVG Advisor](#)). Assim, o [AVG Advisor](#) recordará dos atributos exclusivos da rede (especificamente o endereço MAC), e não exibirá a notificação novamente. Cada rede em que você se conectar será automaticamente considerada como rede conhecida e adicionada à lista. Você pode excluir entradas individuais pressionando o botão **Remover**. A respectiva rede será então considerada novamente desconhecida e potencialmente insegura.

Na janela da caixa de diálogo, é possível verificar quais redes são consideradas conhecidas:



Obs.: o recurso de redes conhecidas no AVG Advisor não é compatível com o Windows XP 64-bit.



8. 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. A configuração do Firewall abre uma nova janela onde é possível editar os parâmetros avançados do componente em várias caixas de diálogo de configuração. A configuração pode ser exibida, como alternativa, no modo básico ou avançado. Ao entrar pela primeira vez na janela de configuração, ela abre a versão básica fornecendo a edição dos parâmetros a seguir:

- [Geral](#)
- [Aplicativos](#)
- [Compartilhamento de arquivos e impressora](#)

Na parte inferior do diálogo, encontra-se o botão **Modo avançado**. Pressione o botão para exibir mais itens no diálogo de navegação para configuração avançada de Firewall:

- [Configurações avançadas](#)
- [Redes definidas](#)
- [Serviços do sistema](#)
- [Logs](#)

8.1. Geral

O diálogo **Informações gerais** fornece uma visão geral de todos os modos disponíveis de Firewall. A seleção atual do modo de Firewall pode ser alterada simplesmente através da seleção de outro modo do menu.

No entanto, o fornecedor do software configurou todos os componentes do AVG Internet Security para proporcionar um desempenho ideal. A menos que você tenha um motivo real para isso, não altere as configurações padrão. Alterações nas configurações devem ser realizadas somente por um usuário experiente!



O firewall permite que você defina regras específicas de segurança baseando-se em se o seu computador está localizado em um domínio, ou se ele é um computador autônomo, ou até mesmo um notebook. Cada uma dessas opções requer um nível diferente de proteção e os níveis são abordados pelos respectivos modos. Em suma, um modo do Firewall é uma configuração específica do componente Firewall e você pode usar várias dessas configurações predefinidas:

- **Automático** – nesse modo, o Firewall lida com todo o tráfego de rede automaticamente. Você não será solicitado a tomar decisões. O Firewall permitirá a conexão de todos os aplicativos conhecidos e, ao mesmo tempo, uma regra será criada para o aplicativo, especificando que ele sempre poderá se conectar no futuro. Para outros aplicativos, o Firewall decidirá se a conexão será permitida ou bloqueada, dependendo do comportamento do aplicativo. No entanto, em tal situação, a regra não será criada e o aplicativo será verificado novamente se tentar se conectar. **O modo automático é discreto e recomendado para a maioria dos usuários.**
- **Interativo** – este modo é útil se você quiser controlar completamente todo o tráfego de rede e de seu computador. O Firewall monitorará o tráfego para você e notificará cada tentativa de comunicação ou transferência de dados, possibilitando permitir ou bloquear a tentativa, à medida que achar necessário. Recomendado apenas para usuários avançados.
- **Bloquear acesso à Internet** – a conexão com a Internet é completamente bloqueada; não é possível acessar a Internet e ninguém de fora pode acessar seu computador. Somente para uso especial ou por pouco tempo.
- **Desativar a proteção do Firewall** – desativar o Firewall permitirá todo o tráfego de entrada e saída do seu computador. Consequentemente, isso o deixará vulnerável a ataques de hackers. Sempre tenha cuidado ao considerar esta opção.

Observe que um modo automático específico também está disponível no Firewall. Esse modo é ativado silenciosamente se o componente [Computador](#) ou [Analisador de Software](#) for desligado e seu computador estiver desta forma mais vulnerável. Em tais casos, o Firewall permitirá automaticamente apenas aplicativos



conhecidos e perfeitamente seguros. Para todos os outros, será solicitada a sua decisão. Isso é feito para compensar os componentes de proteção desativados e manter seu computador seguro.

8.2. Aplicativos

O diálogo **Aplicativo** lista todos os aplicativos que tentaram se comunicar na rede até o momento e os ícones para a ação atribuída:



Os aplicativos na **Lista de aplicativos** são aqueles detectados em seu computador (e que recebem as respectivas ações). Os seguintes tipos de ação podem ser usados:

-  - permitir comunicação para todas as redes
-  - bloquear comunicação
-  - Configurações avançadas definidas

Observe que apenas os aplicativos já instalados puderam ser detectados. Como padrão, quando um novo aplicativo tenta se conectar através da rede pela primeira vez, o Firewall cria uma regra para ele automaticamente, de acordo com o [banco de dados confiável](#), ou pergunta se deseja permitir ou bloquear a comunicação. Neste último caso, você será capaz de salvar sua resposta como uma regra permanente (que será listada nesta caixa de diálogo).

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

Além dos aplicativos, a lista também contém dois itens especiais. **Regras prioritárias do aplicativo** (na parte superior da lista) são preferenciais e são aplicadas sempre antes das regras de qualquer aplicativo individual. **Outras regras de aplicativos** (na parte inferior da lista) são usadas como uma "última instância", quando não é aplicada nenhuma regra específica. Por exemplo, para um aplicativo desconhecido e não definido. Selecione



a ação que deve ser acionada quando um aplicativo tentar se comunicar pela rede: Bloquear (*a comunicação será sempre bloqueada*), Permitir (*a comunicação será permitida através de qualquer rede*), Perguntar (*you will need to decide if the communication should be permitted or blocked*). **Esses itens têm diferentes opções de configuração em relação aos aplicativos comuns e são destinados somente a usuários experientes. Recomendamos que você não modifique as configurações!**

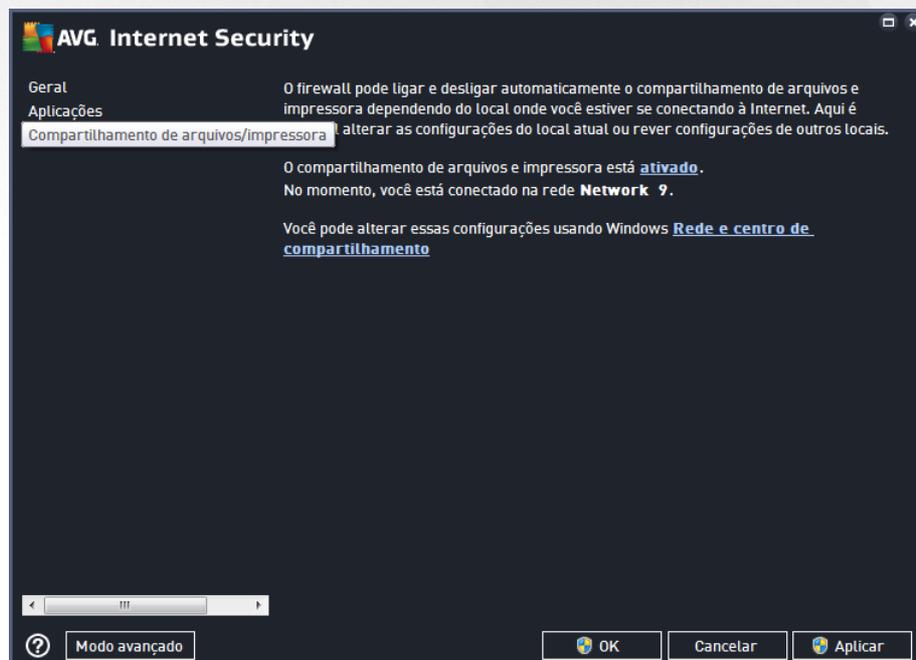
Botões de controle

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

- **Adicionar** - abre uma caixa de diálogo vazia Ações da página para definir novas regras de aplicativo.
- **Editar** - abre a mesma caixa de diálogo para edição de um conjunto de regras de um aplicativo existente.
- **Excluir** - remove o aplicativo selecionado da lista.

8.3. Compartilhamento de arquivos e impressora

O compartilhamento de arquivos e impressoras significa o compartilhamento de quaisquer arquivos e pastas que você marcar como "Compartilhado" no Windows, unidades de disco comuns, impressoras, scanners e todos os dispositivos similares. O compartilhamento desses itens só é desejável em redes que podem ser consideradas seguras (*por exemplo, em casa, no trabalho ou na escola*). No entanto, se estiver conectado a uma rede pública (*como um Wi-Fi de aeroporto ou um café com Internet*), não compartilhe nada. O Firewall do AVG pode bloquear ou permitir facilmente o compartilhamento e possibilita salvar sua opção de redes que já foram visitadas.



No diálogo **Compartilhamento de arquivos e impressora**, você pode editar a configuração de compartilhamento de arquivos e impressora e as redes conectadas no momento. Com o Windows XP, o nome da rede responde ao nome escolhido para a rede específica quando você se conectou a ela pela primeira vez.



Com o Windows Vista e superiores, o nome da rede é extraído automaticamente da Central de Redes e Compartilhamento.

8.4. Configurações avançadas

Todas as edições no diálogo de configurações avançadas são APENAS PARA USUÁRIOS EXPERIENTES!



A caixa de diálogo das **Configurações avançadas** permite que você opte por aceitar ou não os seguintes parâmetros de Firewall:

- **Possibilite qualquer tráfego de/para máquinas virtuais suportadas por Firewall** - suporte para conexão de rede em máquinas virtuais como VMware.
- **Possibilite que qualquer tráfego para redes privadas virtuais (VPN)** - suporte para conexões com a VPN (usadas para conectar com computadores remotos).
- **Registrar tráfego de entrada/saída desconhecido** - todas as tentativas de comunicação (entrada/saída) por aplicativos desconhecidos serão registradas no [log do Firewall](#).
- **Desativar verificação de regra de todas as regras de aplicativo** - o firewall monitora continuamente todos os arquivos cobertos por cada regra de aplicativo. Quando uma modificação do arquivo binário ocorrer, o Firewall tentará confirmar mais uma vez a credibilidade do aplicativo através de meios padrão, ou seja, verificando seu certificado, consultando o [banco de dados de aplicativos confiáveis](#), etc. Se o aplicativo não pode ser considerado seguro, o Firewall ainda tratará o aplicativo baseando-se no [modo selecionado](#):
 - caso o firewall seja executado no **modo Automático**, o aplicativo, como padrão, será permitido;

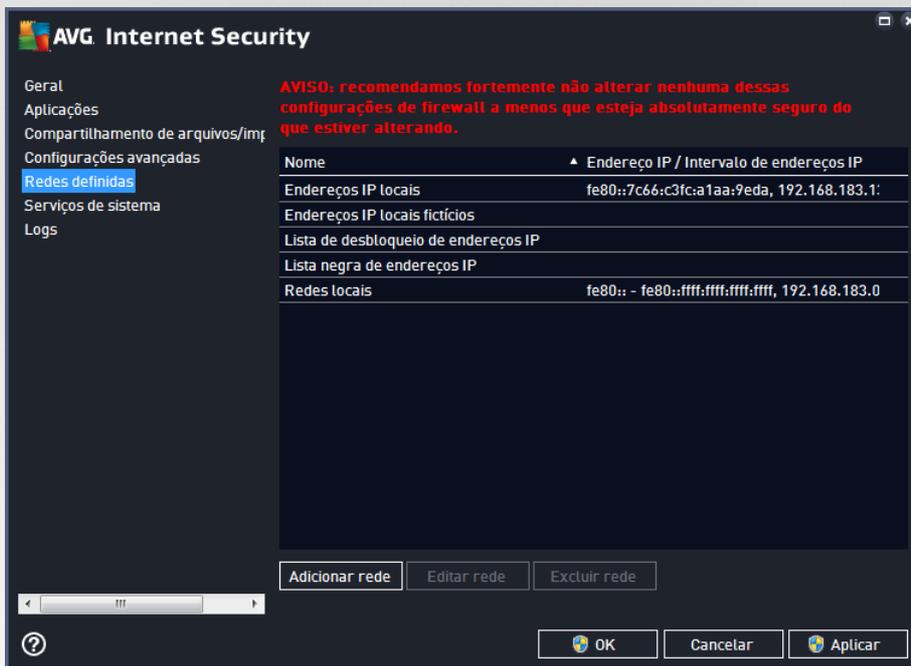


- o caso o firewall seja executado no **modo Interativo**, o aplicativo será bloqueado e será exibido uma caixa de diálogo solicitando que o usuário decida como o aplicativo deve ser tratado.

O procedimento desejado para o tratamento de um aplicativo específico pode ser definido para cada aplicativo separadamente na caixa de diálogo [Aplicativos](#).

8.5. Redes definidas

Todas as edições no diálogo de redes definidas são APENAS PARA USUÁRIOS EXPERIENTES!

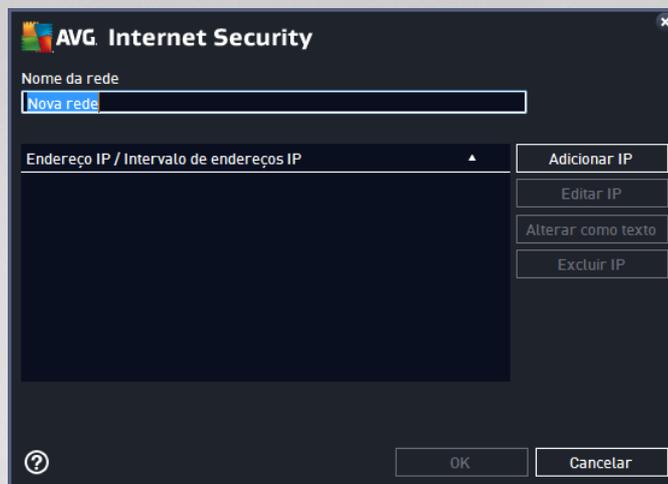


A caixa de diálogo **Redes definidas** oferece uma lista de todas as redes às quais seu computador está conectado. A lista fornece as seguintes informações sobre cada rede detectada:

- **Redes** – fornece uma lista de nomes de todas as redes às quais o computador está conectado.
- **Intervalo de endereços IP** – cada rede será detectada automaticamente e especificada na forma de intervalos de endereços IP.

Botões de controle

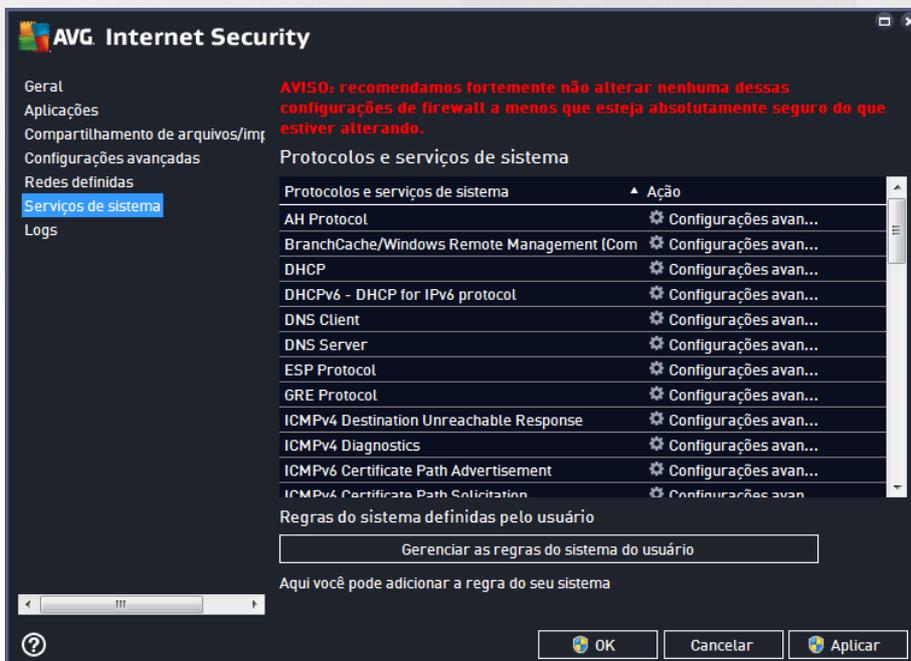
- **Adicionar rede** – abre uma nova janela de diálogo onde é possível editar parâmetros para as redes recém definidas, ou seja, fornecer o **Nome da rede** e especificar o **intervalo de endereços IP**.



- **Editar rede** – abre a caixa de diálogo **Propriedades da rede** (consulte acima), na qual é possível editar parâmetros de uma rede já definida (a caixa de diálogo é idêntica à caixa de diálogo de inclusão de novas redes; consulte a descrição no parágrafo anterior).
- **Excluir rede** – remove a referência de uma rede selecionada da lista de redes.

8.6. Serviços de Sistema

As edições na caixa de diálogo **Protocolos e serviços do sistema** **SÓ DEVEM SER FEITAS POR USUÁRIOS EXPERIENTES**.



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

- **Protocolos e serviços do sistema** – esta coluna mostra o nome do respectivo serviço do sistema.

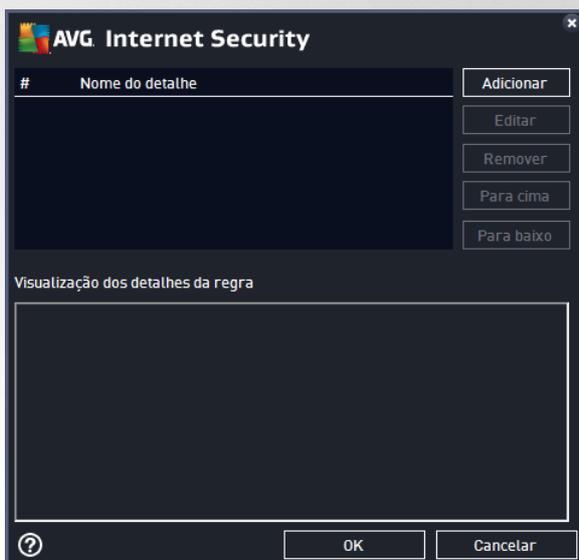


- **Ação** – esta coluna exibe um ícone para a ação atribuída:
 - Permitir comunicação para todas as redes
 - Bloquear comunicação

Para editar as configurações de qualquer item na lista (*incluindo as ações atribuídas*), dê um clique com o botão direito no item e selecione **Editar**. **Entretanto, uma edição das regras do sistema deve ser feita apenas por usuários avançados, e é altamente recomendado não editar as regras de sistema!**

Regras do sistema definidas pelo usuário

Para abrir uma nova caixa de diálogo para definir sua própria regra de serviço do sistema, veja a figura abaixo e pressione o botão **Gerenciar as regras do sistema do usuário**. O mesmo diálogo é aberto se você decidir editar as configurações de qualquer dos itens existentes nos serviços do sistema e lista de protocolos. A seção superior desta caixa de diálogo exibe uma visão geral de todos os detalhes da regra do sistema atualmente editada; a seção inferior exibe o detalhe selecionado. Os detalhes de regra podem ser editados, adicionados ou excluídos pelo respectivo botão:



Observe que estas configurações dos detalhes da regra são avançadas e destinadas principalmente a administradores de rede que necessitam de controle total sobre a configuração de Firewall. Se você não estiver familiarizado com os tipos de protocolos de comunicação, números de porta de rede, definições de endereço IP, etc., não modifique estas definições! Se você realmente precisa alterar a configuração, consulte os arquivos de ajuda da caixa de diálogo respectiva para detalhes específicos.

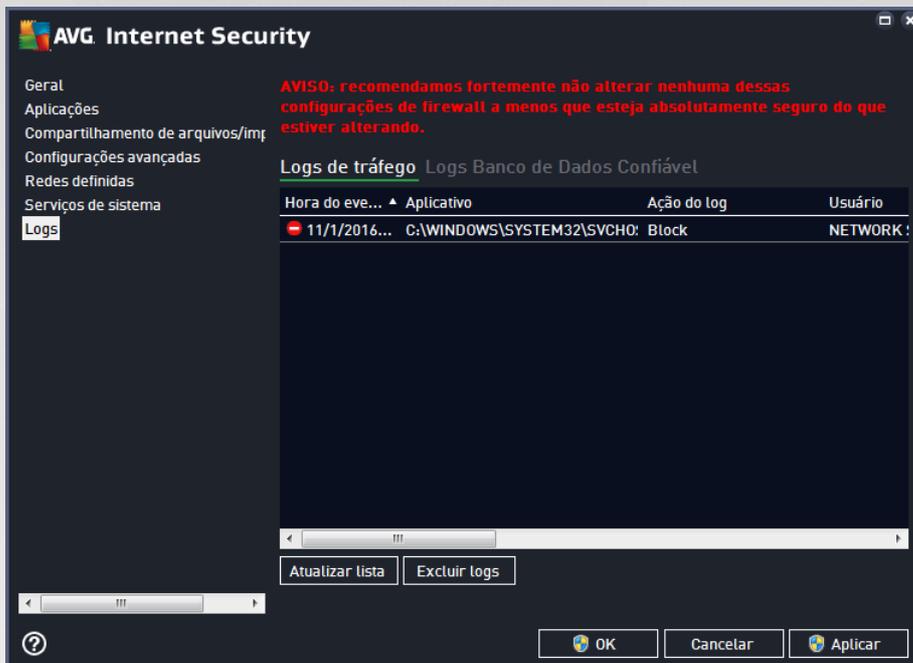
8.7. Logs

Todas as edições no diálogo de logs são APENAS PARA USUÁRIOS EXPERIENTES!

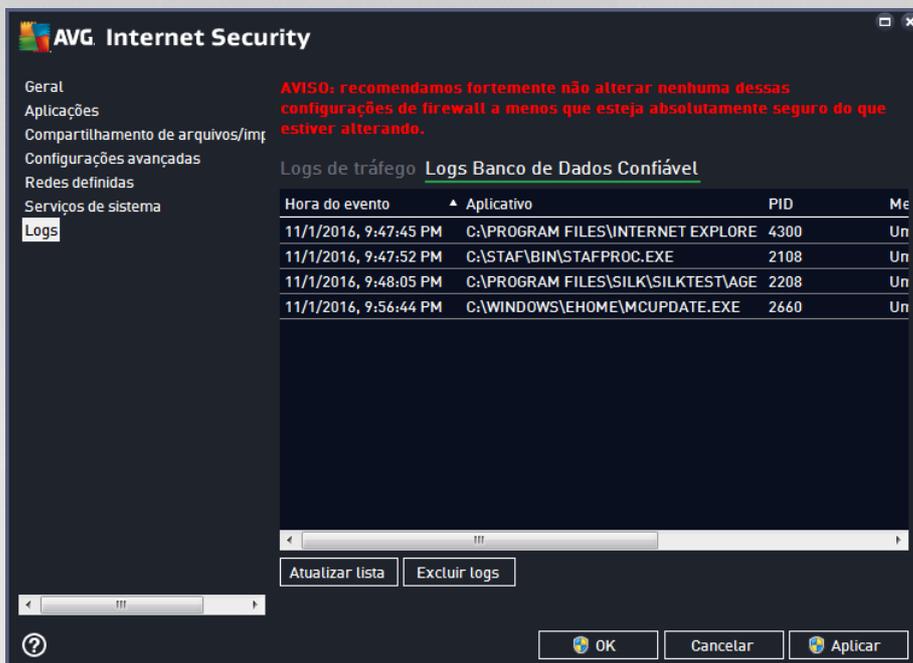
A caixa de diálogo **Logs** permite rever a lista de todas as ações e eventos registrados do Firewall com uma descrição detalhada de parâmetros relevantes exibida em duas guias:



- **Logs de tráfego** – essa guia oferece informações sobre atividades de todos os aplicativos que tentaram se conectar à rede. Para cada item, você encontrará informações sobre o horário do evento, nome do aplicativo, ação de log respectiva, nome do usuário, PID, direção do tráfego, tipo de protocolo, números das portas remotas e locais, e informações sobre o endereço IP local e remoto.



- **Logs do banco de dados confiável** – O banco de dados 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. Na 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 dados confiável e, se o aplicativo estiver listado, ele receberá acesso automático à rede. Somente depois disso, desde que não haja informações sobre o aplicativo disponíveis no banco de dados, você será solicitado a especificar em uma caixa de diálogo à parte se deseja permitir que esse aplicativo acesse a rede.



Botões de controle

- **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.
- **Excluir logs** – pressione esta opção para excluir todas as entradas exibidas.



9. Verificação do AVG

Como padrão, o **AVG Internet Security** não executa verificações, já que, após a verificação inicial (*que você será solicitado a iniciar*), você deverá estar totalmente protegido pelos componentes residentes do **AVG Internet Security**, que estão sempre prontos e não permitem que códigos mal intencionados entrem em seu computador. No entanto, você pode [agendar uma verificação](#) para que seja executada em intervalos regulares ou iniciar uma verificação manual, de acordo com suas necessidades, a qualquer momento.

A interface de verificação do AVG está acessível na [interface principal do usuário](#) através do botão

graficamente dividido em duas seções: 

- **Verificar agora** – pressione o botão para iniciar a opção [Verificar todo o computador](#) imediatamente e observe seu progresso e resultados na janela [Relatórios](#):



- **Opções** – selecione esse botão (*graficamente exibido como três linhas horizontais em um campo verde*) para abrir a caixa de diálogo **Opções de verificação** onde é possível [gerenciar as verificações programadas](#) e editar os parâmetros para [Verificar todo o computador](#) / [Verificar arquivos e pastas](#).



Na caixa de diálogo **Opções de verificação**, é possível ver três seções principais de configuração de verificação:

- **Verificações agendadas** – clique nessa opção para abrir um novo [diálogo com uma visão geral de todas as verificações agendadas](#). Antes de definir suas próprias verificações, você só poderá ver uma verificação agendada predefinida pelo fornecedor do software listada. A verificação está desativada, como padrão. Para ativá-la, clique com o botão direito e selecione a opção *Habilitar tarefa* no menu de contexto. Assim que a verificação agendada for ativada, você poderá [editar sua configuração](#) através do botão *Editar verificação agendada*. Também é possível clicar em *Adicionar verificação agendada* para criar uma nova programação própria.
- **Verificar todo o computador – Configurações** – o botão é dividido em duas seções. Clique na opção *Verificar todo o computador* para iniciar imediatamente a verificação de todo o seu computador (*para obter detalhes sobre a verificação de todo o computador, consulte o capítulo respectivo chamado [Verificações predefinidas / Verificar todo o computador](#)*). Clicar na seção inferior *Configurações* leva ao [diálogo de configuração Verificar todo o computador](#).
- **Verificar arquivos e pastas / Configurações** – novamente, o botão é dividido em duas seções. Clique na opção *Verificar arquivos ou pastas* para iniciar imediatamente a verificação de áreas selecionadas do seu computador (*para obter detalhes sobre a verificação de arquivos ou pastas selecionados, consulte o capítulo respectivo chamado [Verificações predefinidas / Verificar arquivos ou pastas](#)*). Clicar na seção inferior *Configurações* leva ao [diálogo de configuração Verificar arquivos ou pastas](#).
- **Verificar se há rootkits no computador / Configurações** – a seção esquerda do botão chamado *Verificar se há rootkits no computador* inicia a verificação imediata anti-rootkit (*para obter detalhes sobre a verificação de rootkit, consulte o capítulo correspondente chamado [Verificações predefinidas / Verificar se há rootkits no computador](#)*). Clicar na seção *Configurações* leva ao [diálogo de configuração de verificação de rootkit](#).



9.1. Verificações predefinidas

Um dos recursos principais do **AVG Internet Security** é a verificação sob demanda. Testes sob demanda são desenvolvidos para verificar várias partes do seu computador, sempre que surgir a suspeita sobre uma possível infecção por vírus. De qualquer forma, é altamente recomendável realizar esses testes regularmente, mesmo que você pense que nenhum vírus poderá ser encontrado em seu computador.

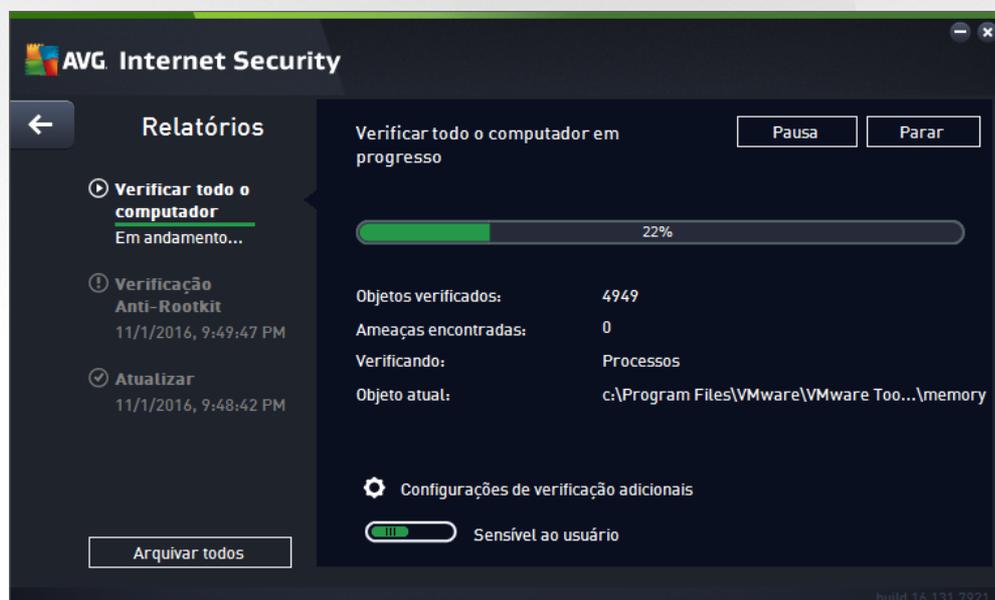
No **AVG Internet Security**, você encontrará os seguintes tipos de verificação predefinidas pelo fornecedor do software:

9.1.1. Verificar todo o computador

Verificar todo o computador verifica todo seu computador em busca de possíveis infecções e/ou aplicativos potencialmente indesejados. 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 seu computador pelo menos uma vez por semana.

Iniciar verificação

A **verificação de todo o computador** pode ser iniciada diretamente a partir da [interface principal do usuário](#) clicando no botão **Verificar agora**. Nenhuma outra configuração precisa ser definida para esse tipo de verificação; a verificação iniciará automaticamente. Na caixa de diálogo **Verificar todo o computador em andamento** (veja [captura de tela](#)), você pode observar o andamento e resultados. A verificação pode ser interrompida temporariamente (**Pausar**) ou cancelada (**Parar**), se necessário.



Edição da configuração da verificação

Você pode editar a configuração da **Verificação de todo o computador** na caixa de diálogo **Verificar todo o computador – Configurações** (o diálogo é acessado através do link [Configurações da verificação de todo o computador](#) na caixa de diálogo [Opções de verificação](#)). **É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.**

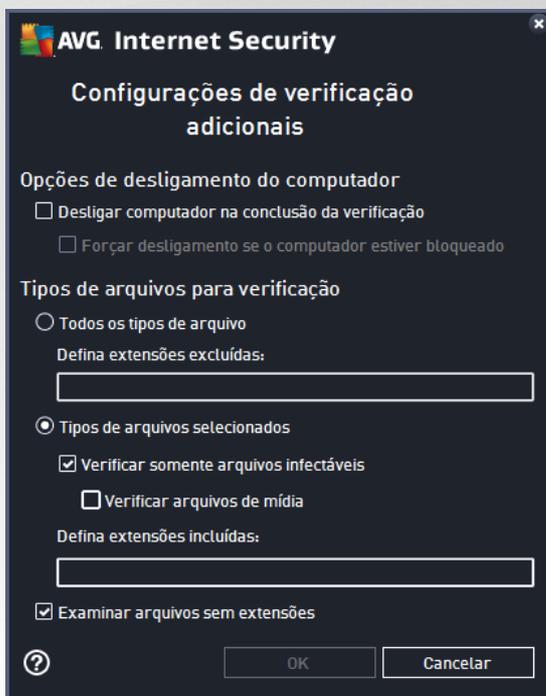


Na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades.

- **Reparar ou remover infecções vírus sem me consultar** (ativada como 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, ele será movido para a [Quarentena de Vírus](#).
- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada como padrão) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (desativada como padrão) – marque para detectar os pacotes estendidos de spyware: programas saudáveis e inofensivos quando adquiridos do fabricante diretamente, mas que podem ser utilizados indevidamente para fins prejudiciais mais tarde. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador. No entanto, como ela pode bloquear programas lícitos, ela se encontra desativada como padrão.
- **Verificar cookies de rastreamento** (desativada como padrão) – este parâmetro estipula 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 interior de arquivos** (desativada como padrão) – esse parâmetro especifica que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR, etc.
- **Usar Heurística** (ativada como 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.



- **Examinar o ambiente do sistema** (ativada como padrão) – a verificação também atuará nas áreas do sistema do seu computador.
- **Ativar verificação completa** (desativada como padrão) – em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação, que verificará até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método é bastante demorado.
- **Verificar rootkits** (ativado como padrão): inclui verificação anti-rootkits na verificação de todo o computador. A [verificação anti-rootkits](#) pode também ser iniciada separadamente.
- **Configurações de verificação adicionais** – o link abre uma nova caixa de diálogo Configurações de verificação adicionais, na qual é possível especificar os seguintes parâmetros:



- **Opções de desligamento do computador** – decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (**Desligar o computador quando o processo de verificação for concluído**), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (**Forçar desligamento do computador se estiver bloqueado**).
- **Tipos de arquivo para verificação** – você também deve decidir se deseja verificar:
 - **Todos os tipos de arquivos** com a opção de definir 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 que podem ser infectados (*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 pouco provável que sejam infectados por vírus). Novamente, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

- Opcionalmente, você pode optar por **Examinar arquivos sem extensões** – essa opção está ativada como padrão e convém mantê-la assim, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são 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. Como padrão, esse valor de 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 do sistema (*por exemplo, quando o computador fica ocioso temporariamente*).
- **Defina 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.

9.1.2. Verificar arquivos ou pastas específicas

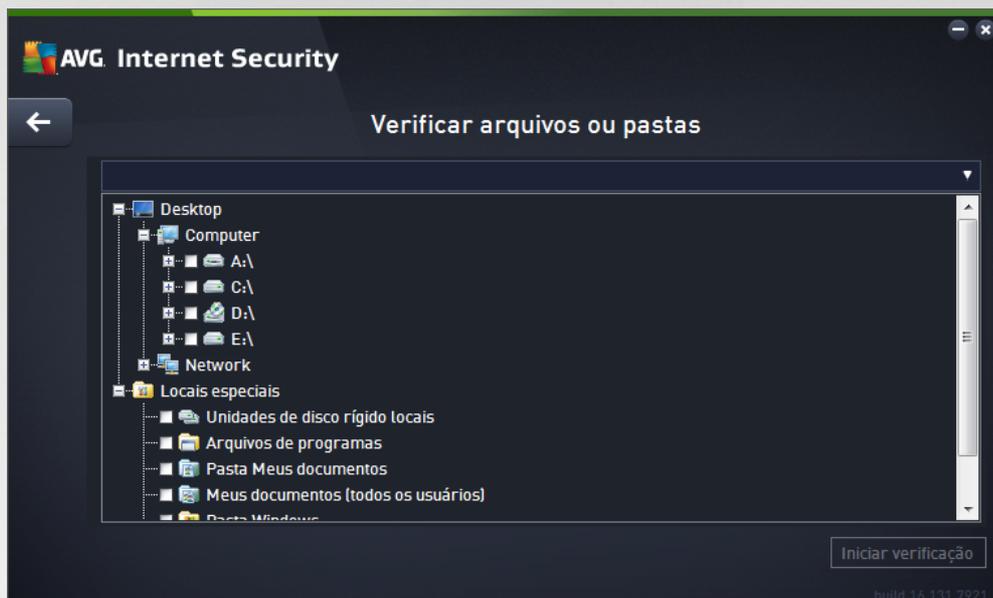
Verificar arquivos ou pastas específicas – verifica somente as áreas do computador selecionadas para verificação (*pastas selecionadas, discos rígidos, unidades de disquete, CDs, etc.*). O andamento da verificação em caso de detecção e tratamento de vírus é o mesmo da verificação de todo o computador: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

Iniciar verificação

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

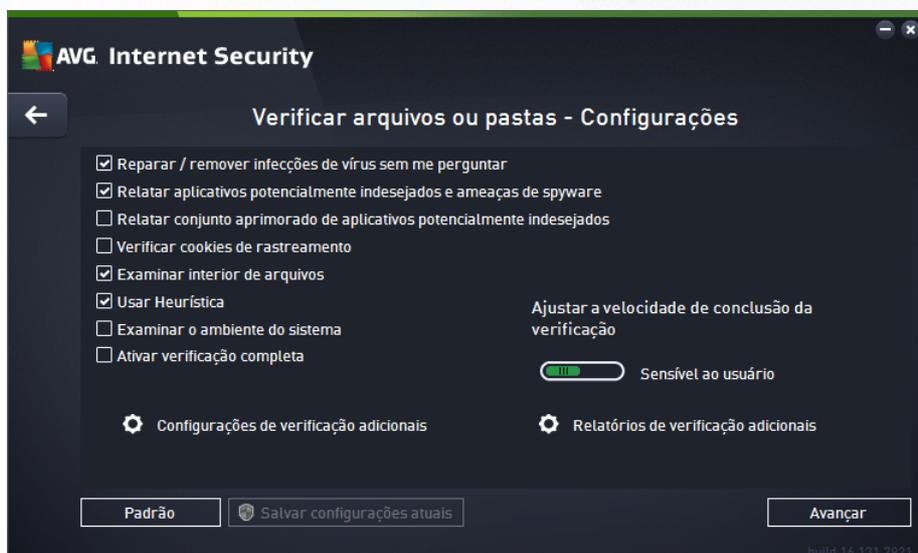


arquivos ou pastas específicos para verificação será aberta. Na estrutura de árvores do computador, selecione as pastas que deseja verificar. O caminho para cada pasta selecionada será gerado automaticamente e exibido na caixa de texto na parte superior dessa caixa de diálogo. Existe também a opção de verificar uma pasta específica 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 a pasta inteira da verificação, 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](#).



Edição da configuração da verificação

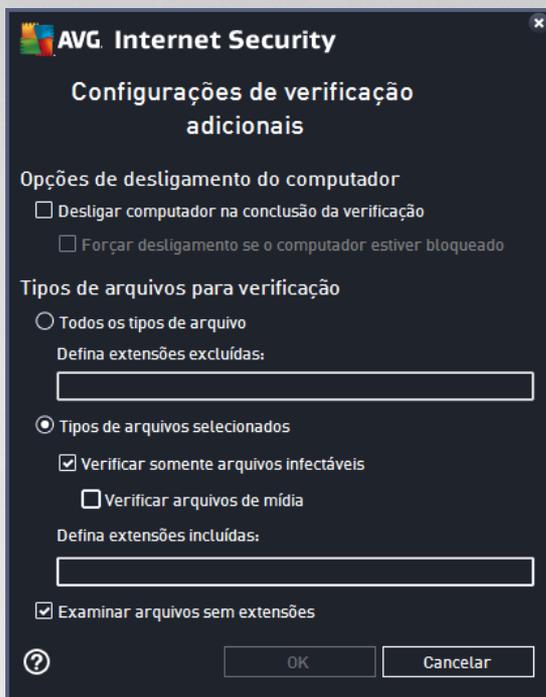
É possível editar a configuração da opção **Verificar arquivos ou pastas** na caixa de diálogo **Verificar arquivos ou pastas – Configurações** (o diálogo pode ser acessado através do link *Configurações de Verificar arquivos ou pastas* no diálogo *Opções de verificação*). **É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.**





Na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades.

- **Reparar / remover infecções de vírus sem me perguntar** (ativada como 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, ele será movido para a [Quarentena de Vírus](#).
- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada como padrão): marque para ativar a verificação de spyware, além de vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (ativada como padrão): marque para detectar os pacotes estendidos de spyware: programas que são perfeitamente ok e inofensivos quando adquiridos diretamente do fabricante, mas que podem ser utilizados indevidamente para fins prejudiciais, posteriormente. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador. No entanto, como ela pode bloquear programas lícitos, ela se encontra desativada como padrão.
- **Verificar cookies de rastreamento** (desativada como padrão): este parâmetro estipula que os cookies devem ser detectados (*cookies HTTP são usados para autenticar, rastrear e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*).
- **Verificar dentro dos arquivos** (ativado como padrão): esse parâmetro define se a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR, etc.
- **Usar Heurística** (ativada como 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.
- **Examinar o ambiente do sistema** (desativada como padrão): a verificação também examinará as áreas do sistema do seu computador.
- **Ativar verificação completa** (desativada como padrão): em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação que examinarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método é bastante demorado.
- **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 **Tipos de arquivo para verificação** – você também deve decidir se deseja verificar:
 - **Todos os tipos de arquivos** com a opção de definir 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 que podem ser infectados (*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 pouco provável que sejam infectados por vírus*). Novamente, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
 - Opcionalmente, você pode optar por **Examinar arquivos sem extensões** – essa opção está ativada como padrão e convém mantê-la assim, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são 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. Como padrão, esse valor de opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Como alternativa, 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 do sistema (*por exemplo, quando o computador fica ocioso temporariamente*).

- **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:



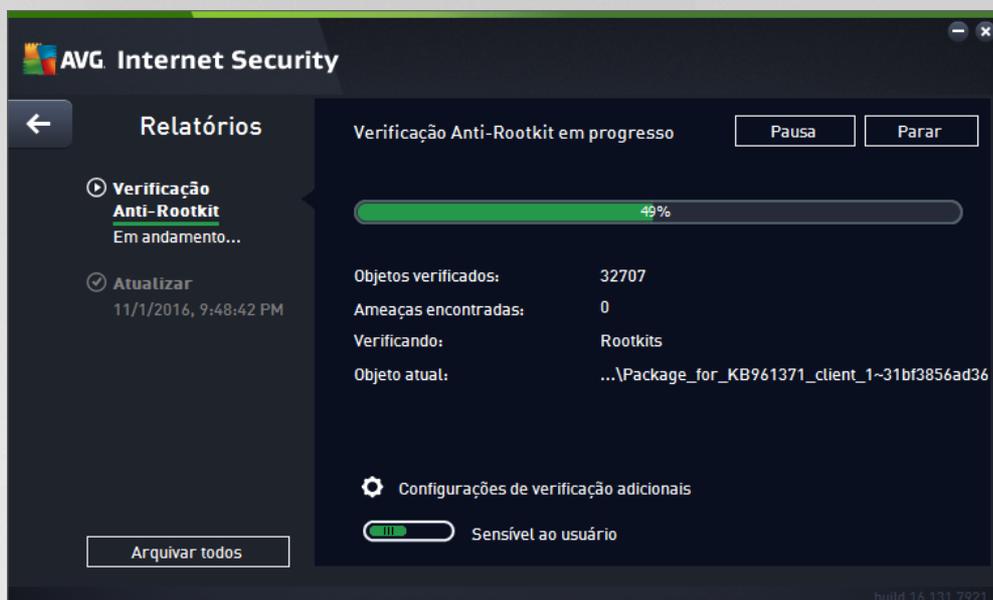
Aviso: essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo [Verificação do AVG/Programação da verificação/Como verificar](#). Se você decidir alterar as configurações padrão de **Verificar arquivos ou pastas específicas**, 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](#)).

9.1.3. Verificar se há rootkits no computador

Verificar se há rootkits no computador é eficaz em detectar e remover efetivamente rootkits perigosos, ou seja, programas e tecnologias que podem camuflar a presença de software malicioso no seu computador. Um rootkit é criado para assumir o controle fundamental de um sistema de computador, sem autorização dos proprietários do sistema e gerentes legítimos. A verificação é capaz de detectar rootkits com base em um conjunto de regras predefinidas. Se um rootkit for encontrado, isso não quer dizer necessariamente que ele está infectado. Algumas vezes os rootkits são usados como drivers ou fazem parte de aplicativos corretos.

Iniciar verificação

Verificar se há rootkits no computador pode ser iniciado diretamente na caixa de diálogo [Opções de verificação](#) clicando no botão **Verificar se há rootkits no computador**. Uma nova caixa de diálogo chamada **Verificação anti-rootkit em andamento** é exibida mostrando o progresso da verificação iniciada:



Edição da configuração da verificação

É possível editar a configuração de verificação na caixa de diálogo **Configurações Anti-Rootkit** (o diálogo é acessível através do link [Configurações da verificação do computador para rootkits](#) na caixa de diálogo [Opções de verificação](#)). **É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.**



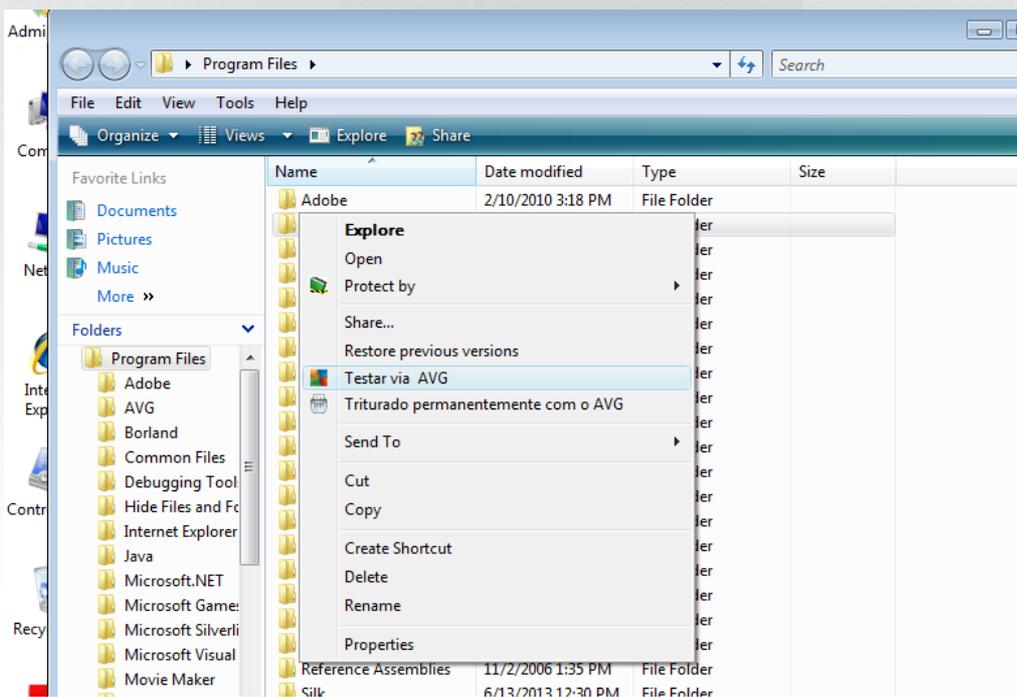


Verificar aplicativos e **Verificar drivers** permitem que você especifique em detalhes o que deve ser incluído na verificação Anti-Rootkit. Essas configurações são direcionadas a usuários avançados; recomendamos que você mantenha todas as opções ativadas. Você também pode selecionar o modo de verificação do rootkit:

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

9.2. Verificando o Windows Explorer

Além das verificações predefinidas iniciadas em todo o computador ou em áreas selecionadas, o **AVG Internet Security** ainda oferece a opção de uma verificação rápida de um objeto específico diretamente no ambiente do Windows Explorer. Se você desejar abrir um arquivo desconhecido e não tiver certeza sobre o seu conteúdo, poderá verificá-lo sob demanda. Siga estas etapas:



- No Windows Explorer, realce o arquivo (*ou a 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 Internet Security**

9.3. Verificação de linha de comando

Dentro do **AVG Internet Security**, 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 na 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

9.3.1. 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 um 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 precisar informar o caminho exato da seção selecionada), os valores serão divididos por ponto e vírgula, como por exemplo: **avgscanx /scan=C:\;D:**

9.3.2. Parâmetros de verificação

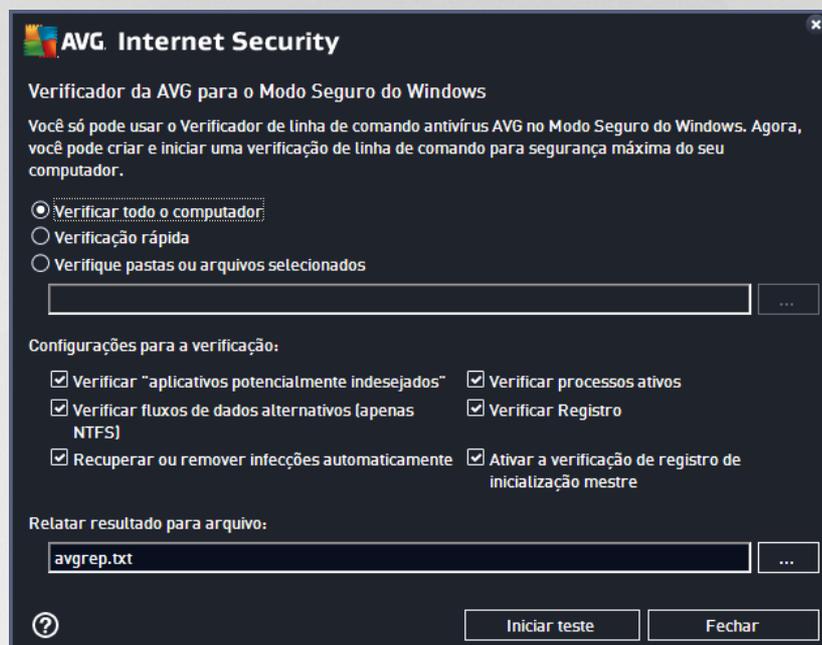
Para exibir uma visão completa dos parâmetros disponíveis, digite o respectivo comando junto com o parâmetro **/?** ou **/HELP** (p.ex., **avgscanx /?**). O único parâmetro obrigatório é **/SCAN**, que especifica que áreas do computador que devem ser verificadas. Para obter uma explicação mais detalhada 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**.



9.3.3. Verificação CMD iniciada pela interface gráfica

Quando você executa seu computador no Modo de segurança do Windows, também existe a opção de iniciar a verificação das linhas de comando pela interface gráfica do usuário:



No Modo de Segurança, a verificação será iniciada a partir da linha de comando. Essa caixa de diálogo permite apenas especificar parâmetros de verificação na interface gráfica confortável.

Primeiro, selecione as áreas do seu computador que você deseja verificar. Você pode escolher entre as opções [Verificar todo o computador](#) ou [Verificar pastas ou arquivos selecionados](#). A terceira opção, a **Verificação rápida**, inicia uma verificação específica projetada para uso no Modo de Segurança que inspeciona todas as áreas importantes do seu computador que são necessárias na inicialização.

As configurações de verificação na seção a seguir permitem que você especifique parâmetros de verificação detalhados. Todos estão marcados como padrão e recomendamos manter assim e cancelar a seleção de um deles apenas se houver um motivo específico para fazê-lo:

- **Verificar "aplicativos potencialmente indesejados"** - verifica se há spyware, além de vírus
- **Verificar fluxos de dados alternativos (apenas NTFS)** - verificação dos fluxos de dados alternativos de NTFS, ou seja, um recurso do Windows que pode ser usado indevidamente por hackers para ocultar dados, especialmente código maligno
- **Recuperar ou remover infecções automaticamente** - todas as detecções possíveis serão tratadas e recuperadas ou removidas do seu computador automaticamente
- **Verificar processos ativos** - verificação de processos e aplicativos carregados na memória do seu computador
- **Verificar registro** - verificação do registro do Windows



- **Ativar a verificação de registro de inicialização mestre** - verificação da tabela de partição e o setor de inicialização

Finalmente, na parte inferior desse diálogo, você pode especificar o nome do arquivo e tipo para o relatório de verificação.

9.3.4. Parâmetros da verificação CMD

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

- /? Exibir ajuda neste tópico
- /@ Arquivo de comando/nome de arquivo/
- /ADS Verifica fluxos de dados alternativos (*apenas NTFS*)
- /ARC Verifica arquivos
- /ARCBOMBSW Informa arquivos compactados novamente
- /ARCBOMBSW Relatar bombas de arquivos (*arquivos compactados repetidamente*)
- /BOOT Ativa verificação de MBR/BOOT
- /BOOTPATH Inicia a verificação rápida
- /CLEAN Limpa automaticamente
- /CLOUDCHECK Verifica a existência de falsos positivos
- /COMP [Verifica todo o computador](#)
- /COO Verificar cookies
- /EXCLUDE Exclui caminho ou arquivo da verificação
- /EXT Verifica estas extensões (*por exemplo EXT=EXE,DLL*)
- /FORCESHUTDOWN Forçar o computador a ser desligado na conclusão da verificação
- /HELP Exibe ajuda neste tópico
- /HEUR Usa análise heurística
- /HIDDEN Relata arquivos com extensão oculta
- /IGNLOCKED Ignora arquivos bloqueados
- /INFECTABLEONLY Verificar apenas os arquivos com extensões infectáveis
- /LOG Gera um arquivo de resultado de verificação
- /MACROW Relata macros

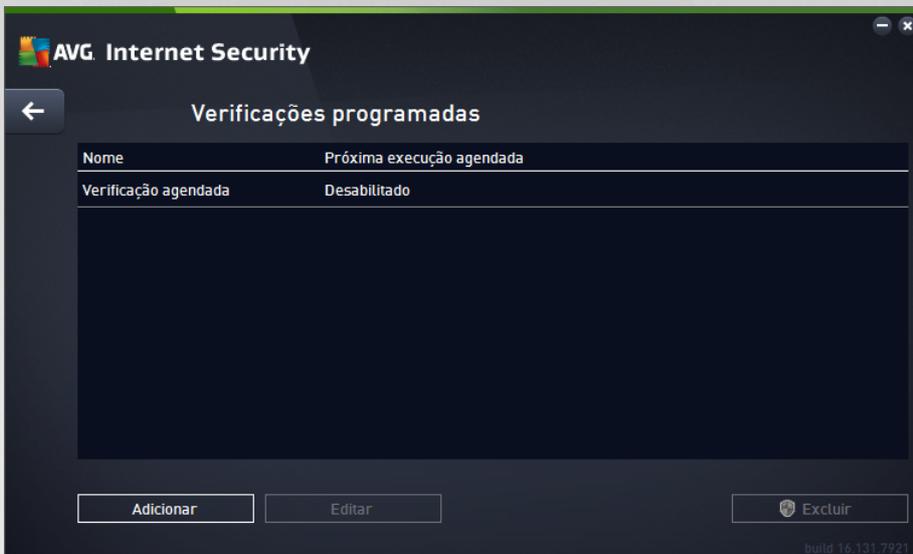


- /NOBREAK Não permite abortar com CTRL-BREAK
- /NOEXT Não verifica estas extensões (*por exemplo, NOEXT=JPG/*
- /PRIORITY Defina a prioridade da verificação (*Baixa, Automática, Alta. Consulte [Configurações avançadas/Verificações](#)*)
- /PROC Verifica processos ativos
- /PUP Relatar aplicativos potencialmente indesejados
- /PUPEXT Relatar conjunto avançado de aplicativos potencialmente indesejados
- /PWDW Relata arquivos protegidos por senha
- /QT Teste rápido
- /REG Verifica registro
- /REPAPPEND Acrescenta ao arquivo de relatório
- /REPOK Relata arquivos não infectados como OK
- /REPORT Relata para arquivo (*nome de arquivo*)
- /SCAN [Verificar arquivos ou pastas específicos](#) (SCAN=caminho;caminho (e.x. /SCAN=C:\;D:\))
- /SHUTDOWN Desliga o computador na conclusão da verificação
- /THOROUGHSCAN Ativar verificação completa
- /TRASH Move arquivos infectados para a [Quarentena de vírus](#)

9.4. Programação de verificação

Com o **AVG Internet Security**, 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 programadas. 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 iniciar [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 [inicialização do computador quando a tarefa tiver sido executada](#).

A programação de verificação pode ser criada / editada na caixa de diálogo **Verificações programadas**, acessada através do botão **Gerenciar verificações agendadas** na caixa de diálogo [Opções de verificação](#). Na nova caixa de diálogo **Verificações agendadas**, você pode ver uma visão geral completa de todas as verificações programadas:

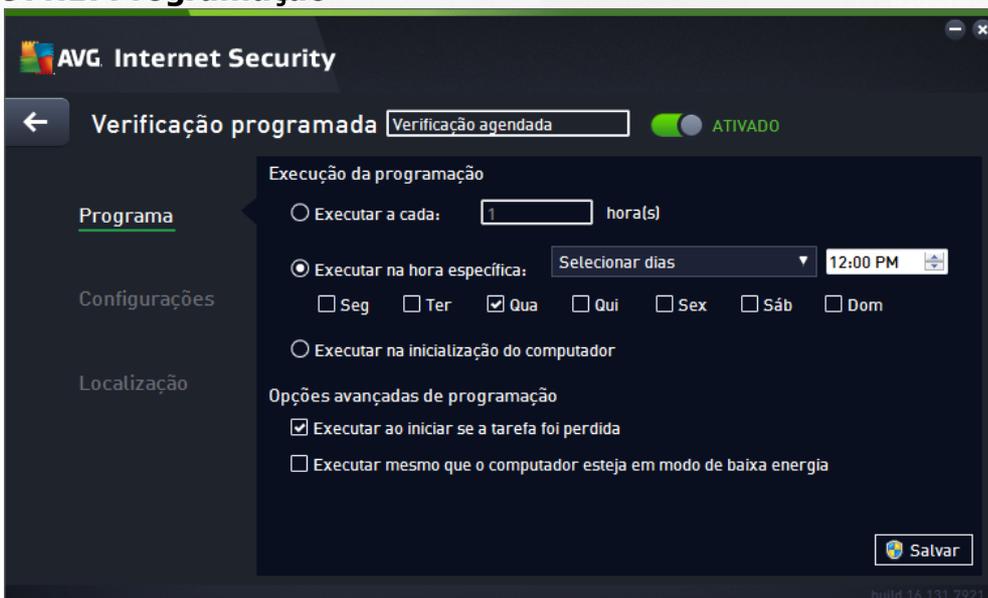


Na caixa de diálogo, é possível especificar suas próprias verificações. Também é possível clicar em **Adicionar verificação agendada** para criar uma nova programação própria. Os parâmetros da verificação agendada podem ser editados (ou uma nova configuração de agenda) em três guias.

- [Programa](#)
- [Configurações](#)
- [Localização](#)

Em cada guia, você pode simplesmente desativar o botão de "semáforo"  para desativar o teste programado temporariamente e ativá-lo novamente quando surgir a necessidade.

9.4.1. Programação





Na parte superior da guia **Verificação agendada**, você pode encontrar o campo de texto onde é possível especificar o nome da programação de verificação sendo definida no momento. Tente sempre usar nomes curtos, descritivos e apropriados para a verificação para facilitar seu reconhecimento, mais tarde. Exemplo: não é bom 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.

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

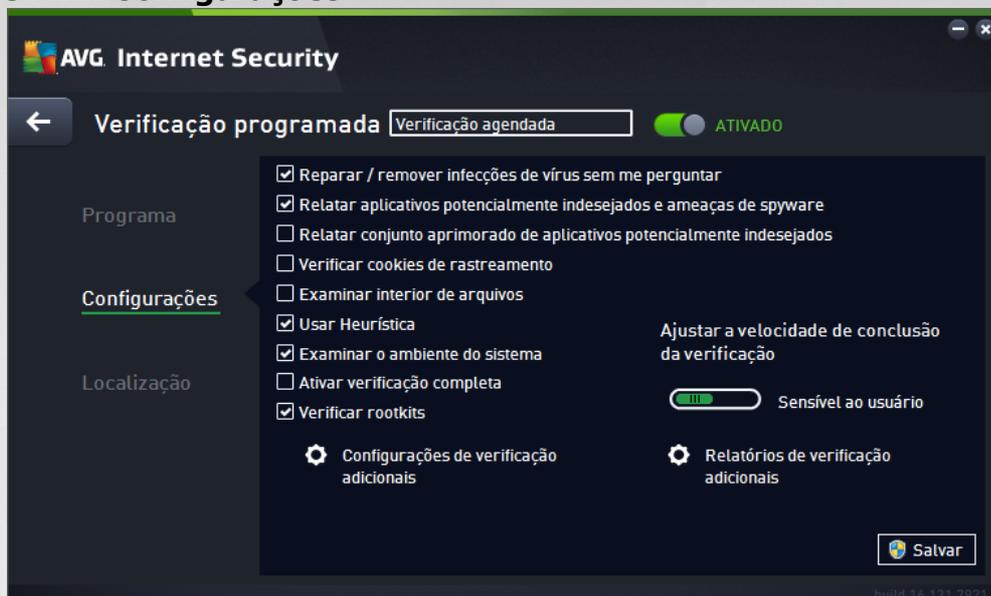
- **Execução da programação** – aqui, você pode especificar intervalos de tempo para a ativação da verificação recém-programada. O tempo pode ser definido pela repetição da execução da verificação depois de um determinado período (*Executar a cada...*), pela definição de uma data e hora exatas (*Executar na hora específica...*), ou talvez pela definição de um evento ao qual a ativação da verificação deve ser associada (*Executar 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 da bandeja do sistema da AVG](#). Um novo [ícone da bandeja do sistema da AVG](#) 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.

Controles no diálogo

- **Salvar** – salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a visão geral das [Verificações agendadas](#). 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.
-  – use a seta verde na parte superior esquerda da caixa de diálogo para voltar para a visão geral das [Verificações programadas](#).



9.4.2. Configurações



Na parte superior da guia **Configurações**, você pode encontrar o campo de texto onde é possível especificar o nome da programação de verificação sendo definida no momento. Tente sempre usar nomes curtos, descritivos e apropriados para a verificação para facilitar seu reconhecimento, mais tarde. Exemplo: não é bom 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.

Na guia **Configurações**, você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. **A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida:**

- **Reparar / remover infecções de vírus sem me perguntar** (ativada 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, ele será movido para a [Quarentena de Vírus](#).
- **Relatar aplicativos potencialmente indesejados e ameaças de spyware** (ativada por padrão): marque para ativar a verificação de spyware, além de vírus. Spyware representa uma categoria de malware questionável: embora geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
- **Relatar conjunto aprimorado de aplicativos potencialmente indesejados** (ativada por padrão): marque para detectar os pacotes estendidos de spyware: programas que são perfeitamente ok e inofensivos quando adquiridos diretamente do fabricante, mas que podem ser utilizados indevidamente para fins prejudiciais, posteriormente. Essa é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, ela pode bloquear programas lícitos; portanto, é desativada por padrão.
- **Verificar cookies de rastreamento** (desativada por padrão): este parâmetro especifica que os cookies devem ser detectados durante a verificação; (cookies HTTP são usados para autenticar,

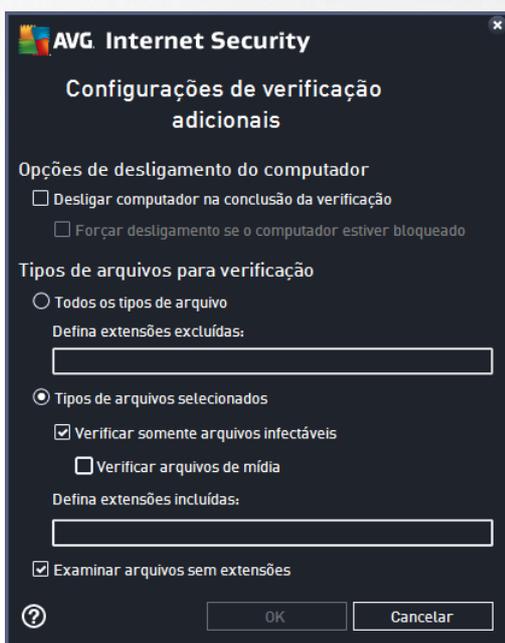


controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas).

- **Verificar interior dos arquivos** (desativada por padrão): este parâmetro especifica 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 raramente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método é bastante demorado.
- **Verificar rootkits** (ativada como padrão): a verificação Anti-Rootkit procura possíveis rootkits em seu computador, ou seja, programas e tecnologias que podem encobrir a atividade de malware em seu 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.

Configurações de verificação adicionais

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





- **Opções de desligamento do computador** – decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (*Desligar o computador quando o processo de verificação for concluído*), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (*Forçar desligamento do computador se estiver bloqueado*).
- **Tipos de arquivo para verificação** – você também deve decidir se deseja verificar:
 - **Todos os tipos de arquivos** com a opção de definir 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 que podem ser infectados (*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 pouco provável que sejam infectados por vírus*). Novamente, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
 - Opcionalmente, você pode optar por **Verificar arquivos sem extensões** – essa opção está ativada por padrão e recomendamos manter essa configuração, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção Verificar prioridade do processo, você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas os recursos do sistema utilizados serão bem maiores 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 os recursos do sistema utilizados ampliando a duração da verificação.

Defina relatórios de verificação adicionais

Clique no link **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:



Controles no diálogo

- **Salvar** – salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a visão geral das [Verificações agendadas](#). 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.
-  – use a seta verde na parte superior esquerda da caixa de diálogo para voltar para a visão geral das [Verificações programadas](#).

9.4.3. Localização

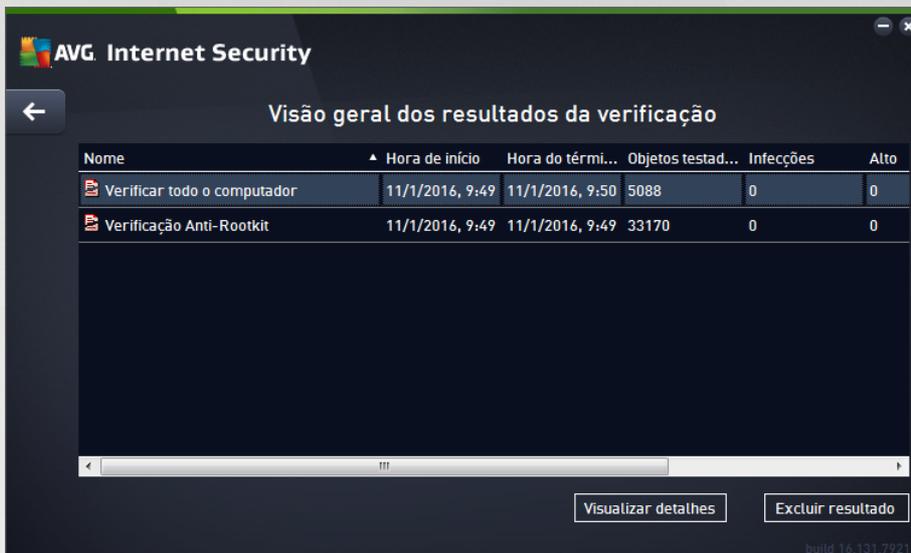


Na guia **Localização**, você pode definir se deseja programar a [verificação de todo o computador](#) ou a [verificação de arquivos e pastas](#). Se você selecionar a verificação de arquivos e pastas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação (expandir 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



- – use a seta verde na parte superior esquerda da caixa de diálogo para voltar para a visão geral das [Verificações programadas](#).

9.5. Resultados da verificação



A caixa de diálogo **Resumo dos resultados de verificação** fornece uma lista dos resultados de todas as verificações executadas até o momento. A lista fornece as seguintes informações sobre cada resultado de verificação:

- **Ícone** – a primeira coluna exibe um ícone de informações descrevendo o status da verificação:
 - Nenhuma infecção encontrada. Verificação concluída
 - Nenhuma infecção encontrada. A verificação foi interrompida antes da conclusão
 - Infecções foram encontradas, mas não recuperadas. Verificação concluída
 - Infecções foram encontradas, mas não recuperadas. A verificação foi interrompida antes da conclusão
 - Infecções foram encontradas e recuperadas ou removidas. Verificação concluída
 - Infecções foram encontradas e recuperadas ou removidas. A verificação foi interrompida antes da conclusão
- **Nome** – a coluna fornece o nome da respectiva verificação. Seja uma das duas [verificações predefinidas](#), ou sua própria [verificação agendada](#).
- **Hora de início** – a data e a hora exatas em que a verificação foi inicializada.
- **Hora do término** – a data e a hora exatas em que a verificação foi finalizada, pausada ou interrompida.



- **Objetos testados** – fornece o número total de todos os objetos que foram verificados.
- **Infecções** – fornece o número de infecções removidas/total encontradas.
- **Alto / Médio / Baixo** – as três colunas subsequentes fornece o número de infecções de alta, média e baixa gravidade encontradas, respectivamente.
- **Rootkits** – número total de [rootkits](#) encontrados durante a verificação.

Controles da caixa de diálogo

Visualizar detalhes – clique no botão para ver [informações detalhadas sobre uma verificação selecionada](#) (destacada na lista acima).

Excluir resultados – clique no botão para remover uma informação de resultado de verificação selecionada na lista.

← – Use a seta verde na parte superior esquerda da caixa de diálogo para voltar à [interface principal do usuário](#) com a 'visão geral dos componentes.

9.6. Detalhes dos resultados da verificação

Para abrir uma visão geral das informações detalhadas sobre um resultado de verificação selecionado, clique no botão **Exibir detalhes**, acessado através da caixa de diálogo [Visão geral dos resultados da verificação](#). Você será redirecionado para a mesma interface de diálogo que descreve em detalhes as informações sobre um respectivo resultado de verificação. As informações são divididas em três guias:

- **Sumário** – a guia fornece informações básicas sobre a verificação: se ela foi concluída com sucesso, se qualquer ameaça foi encontrada e o que aconteceu com elas.
- **Detalhes** – a guia exibe todas as informações sobre a verificação, incluindo detalhes sobre quaisquer ameaças detectadas. Visão geral da exportação para o arquivo possibilita que você o salve como um arquivo .csv.
- **Deteções** – essa guia só será exibida se forem detectadas ameaças durante a verificação, e fornece informações detalhadas sobre as ameaças:

● **Gravidade de informações:** informações ou avisos, não ameaças verdadeiras. Normalmente documentos que contêm macros, documentos ou arquivos protegidos por uma senha, arquivos bloqueados, etc.

●● **Gravidade média:** normalmente aplicativos potencialmente indesejados (como *adware*) ou cookies de rastreamento.

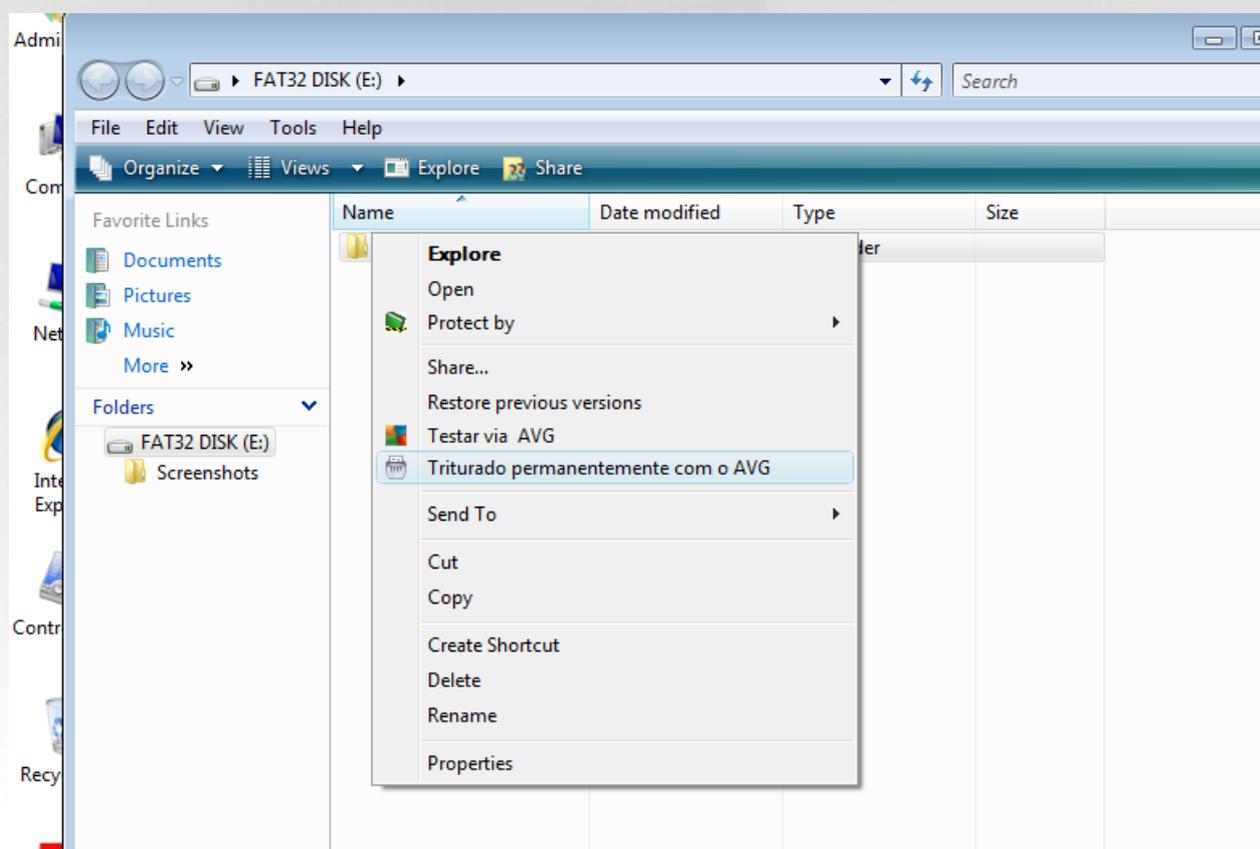
●●● **Gravidade alta:** ameaças sérias como vírus, cavalos de Troia, exploits, etc. Também objetos detectados pelo método de detecção heurística, ou seja, ameaças ainda não descritas no banco de dados de vírus.



10. AVG File Shredder

O **AVG File Shredder** foi projetado para excluir arquivos de forma absolutamente segura, ou seja, sem nenhuma chance de serem recuperados, mesmo por ferramentas de software avançadas que tenham essa finalidade.

Para destruir um arquivo ou pasta, clique com o botão direito no gerenciador de arquivos (*Windows Explorer, Total Commander, etc.*) e selecione **Triturar permanentemente com o AVG** no menu de contexto. Os arquivos na lixeira também podem ser destruídos. Se um arquivo específico em um local específico (p.ex., CD-ROM) não puder ser destruído confiavelmente, você será notificado ou a opção no menu de contexto não estará disponível.



Sempre tenha em mente: Assim que excluir um arquivo com o Shredder, ele não poderá mais ser recuperado.



11. 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 os arquivos excluídos por um certo período de tempo para que você tenha certeza de que não precisa mais deles em seu local original. Se você descobrir que a ausência dos arquivos causa problemas, é possível enviar os arquivos 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:

- **Data de adição** – fornece a data e hora em que o arquivo suspeito foi detectado e armazenado na Quarentena.
- **Ameaça** – caso decida instalar o componente [Analisador de Software](#) em seu **AVG Internet Security**, uma identificação gráfica da gravidade da descoberta será fornecida nessa seção: desde inquestionável (*três pontos verdes*) até muito perigoso (*três pontos vermelhos*). Além disso, você encontrará informações sobre o tipo de infecção e seu local original. O link *Mais informações* acessa uma página que fornece informações detalhadas sobre a ameaça detectada na [enciclopédia de vírus online](#).
- **Origem** – especifica qual componente do **AVG Internet Security** detectou a respectiva ameaça.
- **Notificações** – em uma situação muito rara, algumas observações podem ocorrer nesta coluna, fornecendo comentários detalhados sobre a detecção da respectiva ameaça.

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.
- **Enviar para análise** – o botão está ativo apenas ao destacar um objeto na lista de detecções acima. Em tal caso, você tem a opção de enviar a detecção selecionada ao laboratório de vírus da AVG para obter uma análise mais detalhada. Observe que a finalidade principal desse recurso é enviar arquivos de falsos positivos, ou seja, arquivos que foram detectados pelo AVG como infectados ou suspeitos, mas que você acredita serem inofensivos.
- **Detalhes** – para obter informações detalhadas sobre ameaças específicas na **Quarentena de Vírus**, destaque o item na lista e clique no botão **Detalhes** para abrir uma nova caixa de diálogo com uma descrição da ameaça detectada.
- **Excluir** – remove de maneira completa e irreversível o arquivo infectado da **Quarentena de Vírus**.
- **Esvaziar Quarentena** – remove o conteúdo da **Quarentena de Vírus** completamente. Remover os arquivos da **Quarentena de Vírus** faz com que eles sejam removidos de modo irreversível do disco (*não para a Lixeira*).

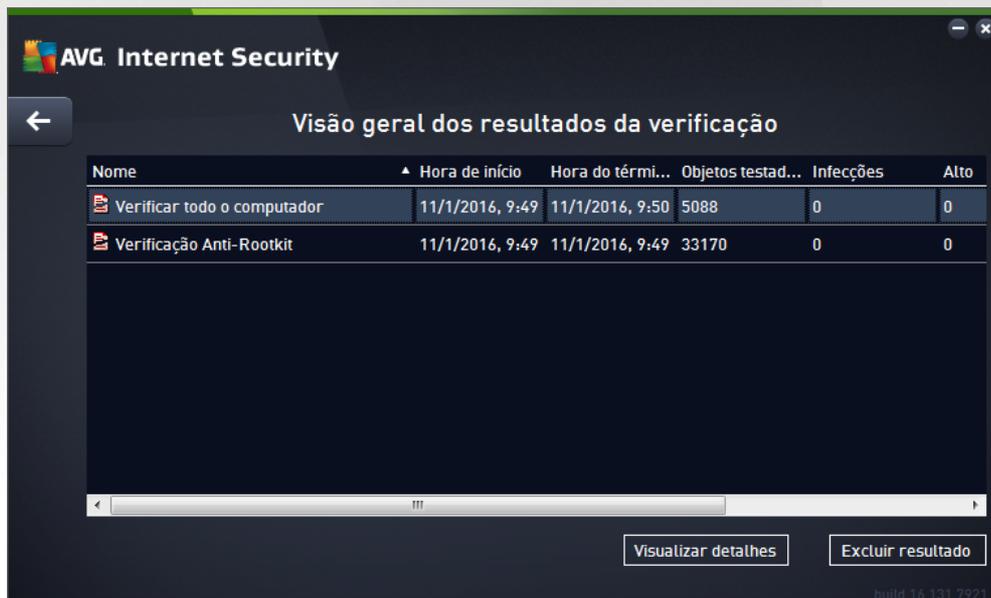


12. Histórico

A seção **Histórico** contém informações sobre todos os eventos anteriores (como atualizações, verificações, detecções, etc.) e relatórios sobre esses eventos. A seção pode ser acessada através da [interface principal do usuário](#), através do item **Opções / Histórico**. Além disso, o histórico de todos os eventos registrados está dividido nas seguintes partes:

- [Resultados da verificação](#)
- [Resultados da Proteção Residente](#)
- [Resultados da Proteção de Email](#)
- [Resultados da Proteção Online](#)
- [Histórico de Eventos](#)
- [Log do Firewall](#)

12.1. Resultados da verificação



O diálogo **Visão geral dos resultados da verificação** é acessado através do item de menu **Opções / Histórico / Resultados da verificação** na linha superior de navegação da janela principal do **AVG Internet Security**. 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.

Obs.: 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).

- **Hora de início** – a data e a hora em que a verificação foi inicializada
- **Hora do término** – a data e a hora em que a verificação foi encerrada
- **Objetos testados** – número de objetos que foram verificados
- **Infecções** – número de infecções por vírus detectadas/removidas
- **Alto / Médio** – essas colunas fornecem o número de infecções, removidas e total, encontradas de gravidade alta e média, respectivamente
- **Info** – informações relacionadas ao processo e o resultado da verificação (*geralmente em sua finalização ou interrupção*)
- **Rootkits** – número de [rootkits](#) detectados

Botões de controle

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

- **Visualizar 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
-  – para voltar ao [diálogo principal AVG padrão](#) (*visão geral dos componentes*), use a seta no canto superior esquerdo desse diálogo

12.2. Resultado da Proteção Residente

O serviço **Proteção Residente** é parte do componente [Computador](#) e verifica arquivos à medida que eles 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:

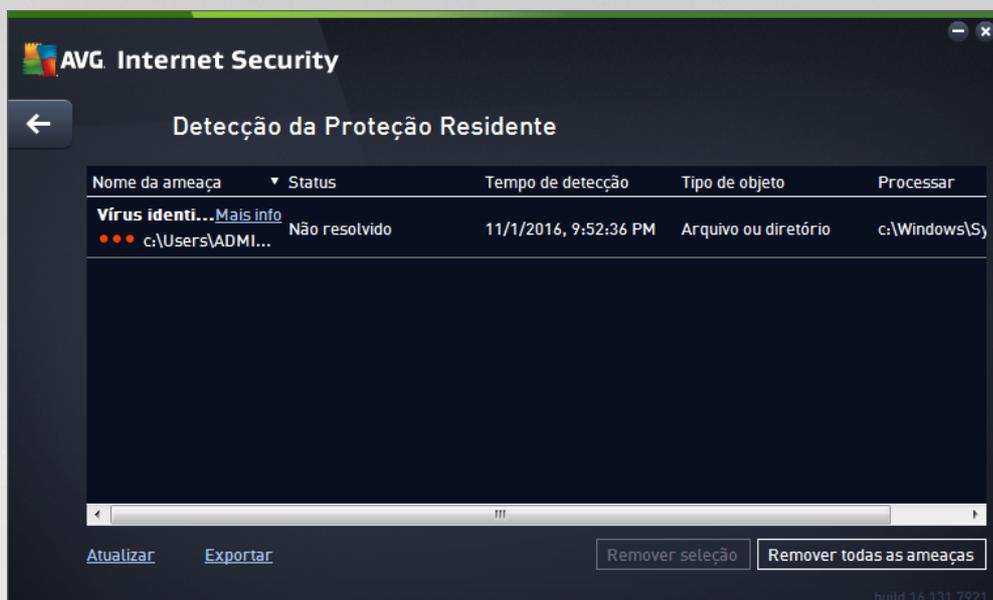


Nessa caixa de diálogo de aviso, você encontrará informações sobre o objeto detectado e classificado como infectado (*Ameaça*), e alguns fatos descritivos sobre a infecção reconhecida (*Descrição*). O link *Mais informações* acessa uma página que fornece informações detalhadas sobre a ameaça detectada na [enciclopédia de vírus online](#), caso ela seja conhecida. Na caixa de diálogo, você também verá um resumo das soluções disponíveis sobre como tratar a ameaça detectada. Uma das alternativas será rotulada como recomendada: **Me proteja (recomendada)**. **Se for possível, você deve sempre utilizar essa opção!**

Obs.: pode acontecer que o tamanho do objeto detectado exceda 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 modificado. 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 parte inferior do diálogo você pode encontrar o link **Mostrar detalhes**. Clique para abrir uma nova janela com informações detalhadas sobre o processo executado durante a detecção da infecção e a identificação do processo.

Uma lista de todas as detecções da Proteção Residente está disponível no diálogo **Detecção da Proteção Residente**. A caixa de diálogo é acessada através do item de menu **Opções / Histórico / Detecção da Proteção Residente** na linha superior de navegação da [janela principal](#) do AVG Internet Security. Essa caixa de diálogo oferece uma **visão geral dos objetos detectados pela proteção residente**, avaliados como perigosos e recuperados ou movidos para a [Quarentena de vírus](#).



Para cada objeto detectado, as seguintes informações são fornecidas:

- **Nome da ameaça** – descrição (possivelmente também o nome) do objeto detectado e sua localização. O link *Mais informações* acessa uma página que fornece informações detalhadas sobre a ameaça detectada na [enciclopédia de vírus online](#).
- **Status** – ação executada pelo objeto detectado
- **Tempo de detecção** – data e hora em que a ameaça foi detectada e bloqueada
- **Tipo de objeto** – tipo do objeto detectado
- **Processo** – qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

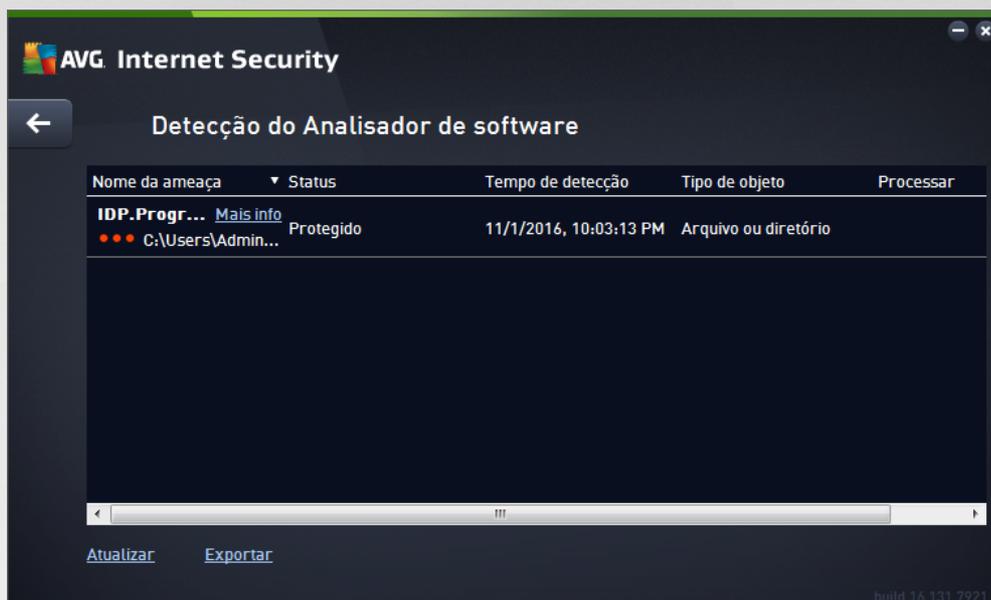
Botões de controle

- **Atualizar** – atualiza a lista de detecções feitas pela **Proteção Online**
- **Exportar** – exporta toda a lista de objetos detectados em um arquivo
- **Remover selecionados** – na lista você pode destacar registros selecionados e usar esse botão para os excluir
- **Remover todas as ameaças** – use o botão para excluir todos os registros listados nesse diálogo
-  – para voltar ao [diálogo principal AVG padrão](#) (visão geral dos componentes), use a seta no canto superior esquerdo desse diálogo



12.3. Resultados do Identity Protection

A caixa de diálogo **Resultados do Analisador de Software** é acessada através do item de menu **Opções / Histórico / Resultados do Analisador de Software**, na linha superior de navegação da janela principal do AVG Internet Security .



O diálogo fornece uma lista de todas as descobertas detectadas pelo componente [Analisador de Software](#) . Para cada objeto detectado, as seguintes informações são fornecidas:

- **Nome da ameaça** - descrição (*possivelmente também o nome*) do objeto detectado e sua localização. O link *Mais informações* acessa uma página que fornece informações detalhadas sobre a ameaça detectada na [enciclopédia de vírus online](#).
- **Status** – ação executada pelo objeto detectado
- **Tempo de detecção** – data e hora em que a ameaça foi detectada e bloqueada
- **Tipo de objeto** – tipo do 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, abaixo da lista, se encontram informações sobre o número total de objetos detectados listados acima. Também é possível 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 **Resultados do Analisador de Software** são os seguintes:

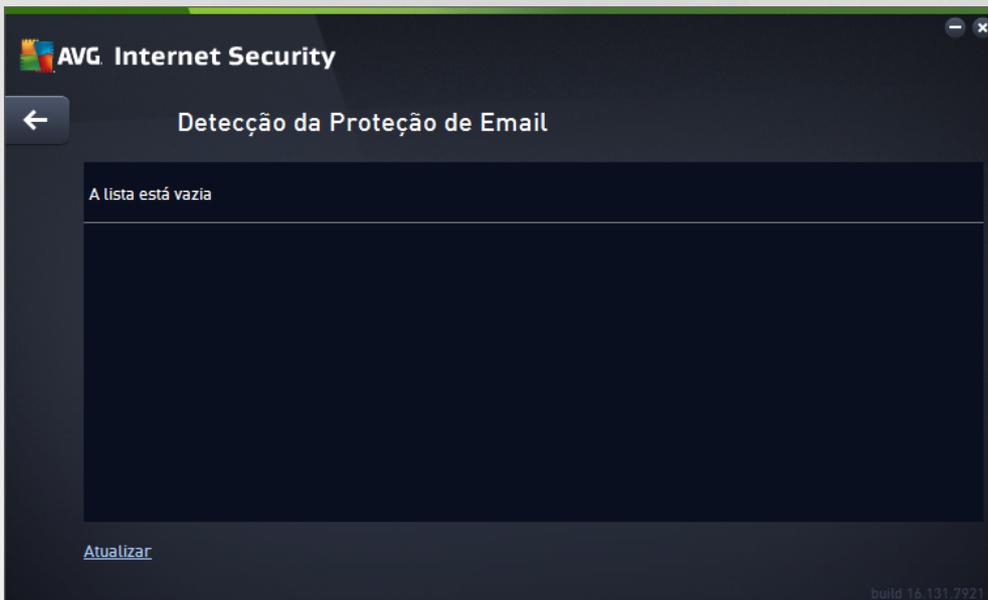
- **Atualizar lista** – atualiza a lista de ameaças detectadas



-  – para voltar ao [diálogo principal AVG padrão](#) (*visão geral dos componentes*), use a seta no canto superior esquerdo desse diálogo

12.4. Resultados da Proteção de Email

A caixa de diálogo **Resultados da Proteção de Email** é acessada através do item de menu **Opções / Histórico / Resultados da Proteção de Email**, na linha superior de navegação da janela principal do **AVG Internet Security**.



O diálogo fornece uma lista de todas as descobertas detectadas pelo componente [Verificador de Email](#). Para cada objeto detectado, as seguintes informações são fornecidas:

- **Nome da detecção** – descrição (*possivelmente também o nome*) do objeto detectado e sua origem
- **Resultado** – ação executada pelo objeto detectado
- **Hora da detecção** – data e hora em que o objeto suspeito foi detectado
- **Tipo de objeto** – tipo do 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, abaixo da lista, se encontram informações sobre o número total de objetos detectados listados acima. Também é possível 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 da **Detecção do Verificador de Email** são os seguintes:

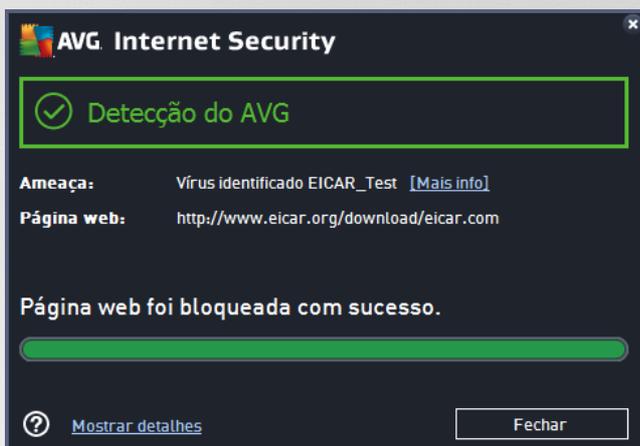
- **Atualizar listas** – atualiza a lista de ameaças detectadas



-  – para voltar ao [diálogo principal AVG padrão](#) (*visão geral dos componentes*), use a seta no canto superior esquerdo desse diálogo

12.5. Resultado da Proteção Online

A **Proteção Online** verifica o conteúdo de páginas da Web visitadas e possíveis arquivos inclusos 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:



Nesse diálogo de aviso, você encontrará informações sobre o objeto detectado e classificado como infectado (*Ameaça*), e alguns fatos descritivos sobre a infecção reconhecida (*Nome do objeto*). O link *Mais informações* redirecionará para a [enciclopédia de vírus online](#) onde é possível encontrar informações detalhadas sobre a infecção detectada, se for conhecida. Essa caixa de diálogo fornece os seguintes botões de controle:

- **Mostrar detalhes** – clique no botão Mostrar detalhes para abrir uma nova janela pop-up, 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 web suspeita não será aberta e a detecção da ameaça será registrada na lista **Detecções da Proteção Online**. Essa visão geral de ameaças detectadas é acessada através do item de menu **Opções / Histórico / Detecções da Proteção Online** na linha superior de navegação da janela principal do **AVG Internet Security**.



Para cada objeto detectado, as seguintes informações são fornecidas:

- **Nome da ameaça** – descrição (possivelmente, até mesmo o nome) do objeto detectado e sua fonte (página web). O link *Mais informações* acessa uma página que fornece informações detalhadas sobre a ameaça detectada na [enciclopédia de vírus online](#).
- **Status** – ação executada pelo objeto detectado
- **Tempo de detecção** – data e hora em que a ameaça foi detectada e bloqueada
- **Tipo de objeto** – tipo do objeto detectado

Botões de controle

- **Atualizar** – atualiza a lista de detecções feitas pela **Proteção Online**
- **Exportar** – exporta toda a lista de objetos detectados em um arquivo
-  – para voltar ao [diálogo principal AVG padrão](#) (visão geral dos componentes), use a seta no canto superior esquerdo desse diálogo



12.6. Histórico de Eventos



O diálogo de **Histórico de eventos** é acessado através do item de menu **Opções / Histórico / Histórico de eventos** na linha superior de navegação da janela principal do **AVG Internet Security**. Nesta caixa de diálogo, você encontrará um resumo dos eventos importantes que ocorreram durante a operação do **AVG Internet Security**. A caixa de diálogo fornece registros dos seguintes tipos de eventos: informações sobre a atualização do aplicativo da AVG; informações sobre início, término e interrupção de verificações (*incluindo testes executados automaticamente*); informações sobre eventos relacionados com detecção de vírus (*tanto pela proteção residente quanto pela [verificação](#)*) incluindo local de ocorrência; e 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.
- O campo **Usuário** informa o nome do usuário conectado no momento em que ocorreu o evento.
- O campo **Fonte** fornece informações sobre o componente de origem ou outra parte do sistema AVG que acionou o evento.
- **Descrição do evento** fornece um breve resumo do que realmente aconteceu.

Botões de controle

- **Atualizar lista** – clique no botão para atualizar todas as entradas na lista de eventos
- **Fechar** – pressione o botão para voltar para a janela principal do **AVG Internet Security**

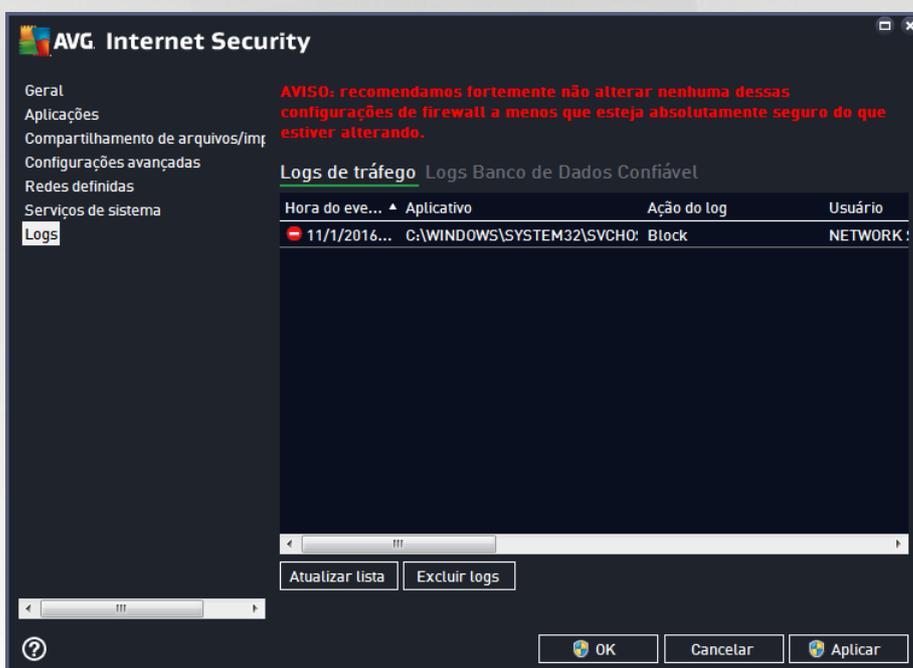


12.7. Log do firewall

Esta caixa de diálogo foi planejada para a configuração por um especialista e recomendamos não alterar nenhuma das configurações, a menos que você esteja absolutamente seguro sobre a alteração!

A caixa de diálogo **Logs** permite rever a lista de todas as ações e eventos registrados do Firewall com uma descrição detalhada de parâmetros relevantes exibida em duas guias:

- **Logs de tráfego** – essa guia oferece informações sobre atividades de todos os aplicativos que tentaram se conectar à rede. Para cada item, você encontrará informações sobre o horário do evento, nome do aplicativo, ação de log respectiva, nome do usuário, PID, direção do tráfego, tipo de protocolo, números das portas remotas e locais, e informações sobre o endereço IP local e remoto.



- **Logs do banco de dados confiável** – o banco de dados 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. Na 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 dados confiável e, se o aplicativo estiver listado, ele receberá acesso automático à rede. Somente depois disso, desde que não haja informações sobre o aplicativo disponíveis no banco de dados, você será solicitado a especificar em uma caixa de diálogo à parte se deseja permitir que esse aplicativo acesse a rede.

Botões de controle

- **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.



- **Excluir logs** – pressione esta opção para excluir todas as entradas exibidas.



13. Atualizações do AVG

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. Considerando todas as ameaças ao computador recentemente descobertas e a velocidade com que se disseminam, é absolutamente crucial atualizar o **AVG Internet Security** regularmente. A melhor solução é manter as configurações padrão do programa onde a atualização automática está configurada. Saiba que, se o banco de dados de vírus de seu **AVG Internet Security** não estiver atualizado, o programa não poderá detectar as ameaças mais recentes!

É fundamental atualizar o AVG regularmente! As atualizações das definições de vírus essenciais devem ser feitas diariamente, se possível. Atualizações de programas menos urgentes podem ser feitas semanalmente.

Para proporcionar o máximo de segurança disponível, o **AVG Internet Security** é programado para verificar se há novas atualizações do banco de dados de vírus a cada quatro horas. Como as atualizações do AVG não são lançadas de acordo com uma programação fixa, mas em resposta à quantidade e severidade de novas ameaças, essa verificação é altamente importante para garantir que o banco de dados de vírus do seu AVG fique atualizado o tempo todo.

Se desejar verificar se há novos arquivos de atualização imediatamente, use o link rápido [Atualizar agora](#), na interface de usuário principal. Esse link está sempre disponível em qualquer caixa de diálogo da [interface de usuário](#). Ao iniciar a atualização, o AVG primeiro verifica se há novos arquivos de atualização disponíveis. Se houver, o **AVG Internet Security** começará a baixá-los e executará o processo de atualização. Você será informado sobre os resultados da atualização no diálogo deslizante acima do ícone do AVG na bandeja do sistema.

Se desejar reduzir a frequência das atualizações, você poderá configurar seus próprios parâmetros de inicialização. No entanto, **é altamente recomendável iniciar a atualização, pelo menos, uma vez ao dia!** A configuração pode ser editada na seção [Configurações avançadas/Programações](#), especificamente nas seguintes caixas de diálogo:

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



14. Perguntas frequentes e Suporte técnico

Caso tenha problemas técnicos ou relacionados a vendas com o aplicativo **AVG Internet Security**, há várias maneiras de obter ajuda. Selecione entre as opções abaixo:

- **Obter suporte:** diretamente do aplicativo AVG, é possível chegar a uma página dedicada ao suporte ao cliente no website da AVG (<http://www.avg.com/>). Selecione o item **Ajuda / Obter suporte** do menu principal para ser redirecionado ao website da AVG com as vias de suporte disponíveis. Para prosseguir, siga as instruções na página da Web.
- **Suporte** (link no menu principal): o menu do aplicativo AVG (na parte superior da interface de usuário principal) inclui o link **Suporte** que abre uma nova caixa de diálogo com todos os tipos de informações de que você precisa enquanto obtém ajuda. A caixa de diálogo inclui dados básicos sobre o programa AVG instalado (versão do banco de dados/programa), detalhes da licença e uma lista de links rápidos de suporte.
- **Solução de problemas no arquivo de ajuda:** uma nova seção da **Solução de problemas** está disponível diretamente do arquivo de ajuda incluso no **AVG Internet Security** (para abrir o arquivo de ajuda, pressione a tecla F1 em qualquer diálogo do aplicativo). Esta seção fornece uma lista das situações mais frequentes quando um usuário deseja buscar ajuda profissional para um problema técnico. Selecione a situação que melhor descreve seu problema e clique nela para abrir instruções detalhadas que levam a solucionar o problema.
- **Centro de suporte do site do AVG:** como alternativa, você pode buscar a solução de problemas no site do AVG (<http://www.avg.com/>). Na seção **Suporte**, é possível encontrar uma visão geral de grupos temáticos que tratam de problemas técnicos e de venda, uma seção estruturada com perguntas frequentes e todos os contatos disponíveis.
- **AVG ThreatLabs:** um website específico relacionado ao AVG (<http://www.avg.com/about-viruses>) dedicado a problemas de vírus que fornece uma visão geral estruturada de informações relacionadas a ameaças online. Você também pode encontrar instruções sobre a remoção de vírus, spyware e dicas sobre como permanecer protegido.
- **Fórum de discussões:** você também pode usar o fórum de discussões de usuários do AVG em <http://community.avg.com/>.