AVG AntiVirus 2014

Manual do Usuário

Revisão do documento 2014.01 (03/09/2013)

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

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

Conteúdo

1. Introdução 5

2. Requisitos de instalação do AVG 6

2.1 Sistemas operacionais suportados 6
2.2 Requisitos de HW mínimos e recomendados 6

3. Processo de instalação do AVG 7

3.1 Bem-vindo: seleção de idioma 7
3.2 Bem-vindo: contrato de licença 8
3.3 Ative a sua Licença 9
3.4 Selecionar tipo de instalação 10
3.5 Opções personalizadas 11
3.6 Instalar o AVG Security Toolbar 12
3.7 Progresso da Instalação 13
3.8 Parabéns! 14

4. Após a instalação 15

4.1 Registro do produto 15
4.2 Acesso à interface do usuário 15
4.3 Verificação de todo o computador 15
4.4 Teste Eicar 15
4.5 Configuração padrão do AVG 16

5. Interface de usuário do AVG 17

5.1 Linha superior de navegação 18
5.2 Informações sobre status de segurança 21
5.3 Visão geral dos componentes 22
5.4 Meus aplicativos 23
5.5 Verificar / Atualizar links rápidos 24
5.6 Ícone da bandeja do sistema 24
5.7 Gadget AVG 26
5.8 AVG Advisor 27
5.9 AVG Accelerator 29

6. Componentes do AVG 30

6.1 Proteção para o computador 30
6.2 Proteção de navegação da Web 34
6.3 Identity protection 36

6.4 Proteção de email 37
6.5 Quick Tune componente 39

7. AVG Security Toolbar 42

8. AVG Do Not Track 45

8.1 Interface do AVG Do Not Track 45
8.2 Informações sobre processos de rastreamento 47
8.3 Bloqueio de processos de rastreamento 47
8.4 Configurações do AVG Do Not Track 48

9. Configurações avançadas do AVG 49

9.1 Aparência 49
9.2 Sons 52
9.3 Desativar temporariamente a proteção do AVG 53
9.4 Proteção para o computador 54
9.5 Verificador de Email 59
9.6 Proteção de navegação da Web 69
9.7 Identity Protection 72
9.8 Verificações 73
9.9 Programações 79
9.10 Atualizar 87
9.11 Exceções 91
9.12 Quarentena de Vírus 93
9.13 Auto Proteção do AVG 94
9.14 Preferências de Privacidade 94
9.15 Ignorar status de erro 97
9.16 Advisor – Redes conhecidas 98

10. Verificação do AVG 99

10.1 Verificações predefinidas 101
10.2 Verificando o Windows Explorer 112
10.3 Verificação de linha de comando 113
10.4 Programação de verificação 116
10.5 Resultados da verificação 123
10.6 Detalhes dos resultados da verificação 125

11. AVG File Shredder 126

12. Quarentena de Vírus 127

13. Histórico 129

13.1 Resultados da verificação 129
13.2 Resultado da Proteção Residente 130
13.3 Resultados do Identity Protection 133
13.4 Resultados da Proteção de Email 134
13.5 Resultado da Proteção Online 135
13.6 Histórico de Eventos 137

14. Atualizações do AVG 138

14.1 Iniciar atualização 138
14.2 Níveis de atualização 138

15. Perguntas frequentes e Suporte técnico 140

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG AntiVirus 2014**.

O **AVG AntiVirus 2014** oferece proteção em tempo real contra as ameaças mais sofisticadas atualmente. Você pode bater papo, baixar e trocar arquivos com confiança; jogar e assistir vídeos sem preocupações ou interrupções; baixar e compartilhar arquivos e enviar mensagens com segurança; aproveitar as redes sociais ou navegar e pesquisar com uma proteção em tempo real.

Você pode também usar outras fontes de informações:

- ***Arquivo de ajuda***: uma seção da *Solução de problemas* está disponível diretamente do arquivo de ajuda incluso no **AVG AntiVirus 2014** *(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 levem 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 ***Centro de Suporte***, você pode encontrar uma visão geral estruturada sobre grupos temáticos que lidam com problemas técnicos e relacionados a vendas.

- ***Perguntas frequentes***: no site do AVG (*http://www.avg.com/*) você também pode encontrar uma seção separada e de estrutura elaborada com perguntas frequentes. Esta seção pode ser acessada através da opção de menu ***Centro de Suporte/Perguntas frequentes e tutoriais***. Novamente, todas as perguntas são divididas de maneira organizada nas categorias técnica, de vendas e de vírus.

- ***AVG ThreatLabs***: um website específico relacionado ao AVG (*http://www.avgthreatlabs.com/website-safety-reports/*) 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://forums.avg.com.

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais suportados

O **AVG AntiVirus 2014** destina-se à proteção de estações de trabalho com os seguintes sistemas operacionais:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64,todas as edições)
- Windows 7 (x86 e x64, todas as edições)
- Windows 8 (x32 e x64)

(e possíveis service packs posteriores para sistemas operacionais específicos)

***Observação**: o componente Identidade não é suportado no Windows XP x64. Nesses sistemas operacionais, é possível instalar AVG AntiVirus 2014,·mas sem o componente IDP.*

2.2. Requisitos de HW mínimos e recomendados

Requisitos mínimos de hardware para **AVG AntiVirus 2014**:

- 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 recomendados de hardware para **AVG AntiVirus 2014**:

- 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 AntiVirus 2014** em seu computador, você precisa obter o arquivo de instalação mais recente. Para garantir que você esteja instalando a versão atualizada do **AVG AntiVirus 2014**, recomenda-se baixar o arquivo de instalação no site do AVG (http://www.avg.com/). A seção ***Suporte/Download*** fornece uma visão geral estruturada dos arquivos de instalação para cada edição do AVG.

Se você não tiver certeza de quais arquivos precisa baixar e instalar, poderá usar o serviço ***Selecionar produto*** na parte inferior da página da Web. Depois que você responder a três simples perguntas, o serviço definirá exatamente os arquivos de que precisa. Clique no botão ***Continuar*** para ser redirecionado a uma lista completa de arquivos para download que foram personalizados para suas necessidades.

Depois de fazer download 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: seleção de idioma

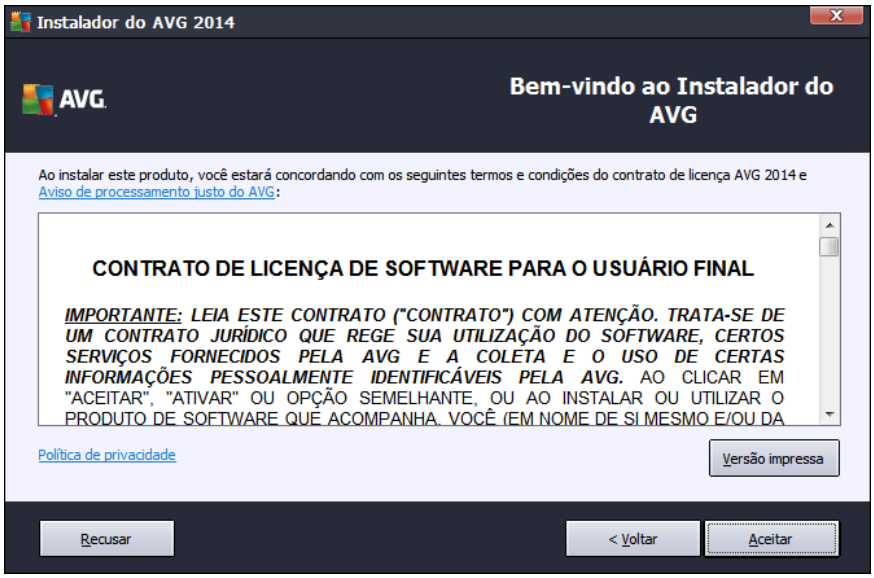
O processo de instalação é iniciado com a caixa de diálogo ***Bem-vindo ao Instalador do AVG***:

Neste diálogo você pode selecionar o idioma usado no processo de instalação. Clique na caixa de combinação e role o menu de idiomas. Selecione o idioma desejado, e o processo de instalação continuará no idioma de sua escolha.

Atenção: no momento, você está somente selecionando o idioma do processo de instalação. O aplicativo AVG AntiVirus 2014 será instalado no idioma selecionado e em inglês, que é sempre instalado automaticamente. No entanto, é possível ter mais idiomas instalados e trabalhar com o AVG AntiVirus 2014 em qualquer um desses. Você será solicitado a confirmar a seleção completa dos idiomas alternativos em uma das seguintes caixas de diálogo de configuração Opções personalizadas.

3.2. Bem-vindo: contrato de licença

A caixa de diálogo ***Bem-vindo ao Instalador do AVG*** fornece a versão completa do contrato de licença do AVG:



Leia todo o texto com atenção. Para confirmar que leu, compreendeu e aceita o contrato, pressione o botão ***Aceitar***. Se você não concordar com o contrato de licença, pressione o botão Recusar e o processo de instalação será encerrado imediatamente.

Política de Privacidade do AVG

Além do contrato de licença, essa caixa de diálogo de instalação oferece a opção de saber mais sobre o ***Aviso de Processamento Íntegro da AVG***, ***Personalização do AVG*** e a ***Política de Privacidade da AVG*** *(todas as funções mencionadas são exibidas no diálogo na forma de um hyperlink ativo que o leva para o website dedicado onde é possível encontrar informações detalhadas)*. Clique no respectivo link para ser direcionado para o website da AVG (http://www.avg.com/) onde você pode encontrar a versão completa dessas declarações.

Botões de controle

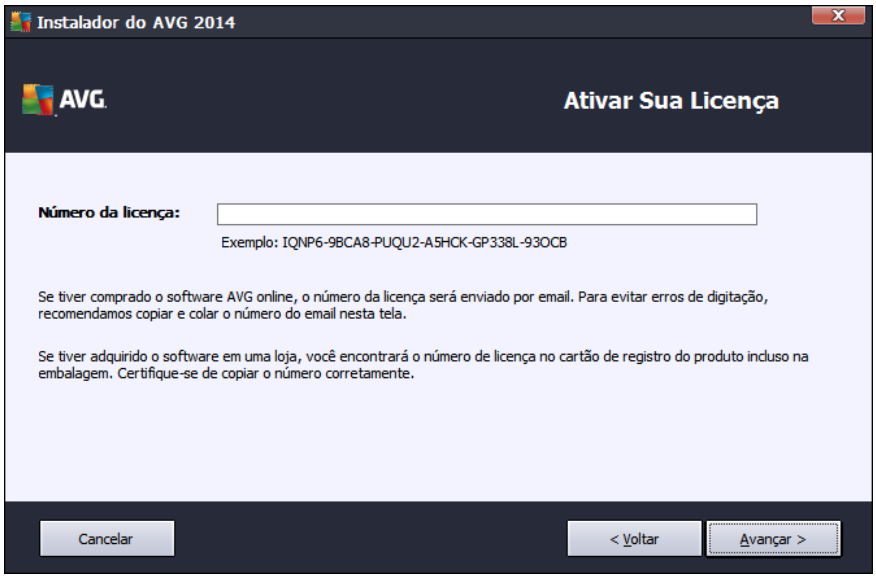
Na primeira caixa de diálogo de instalação, há somente dois botões de controle disponíveis:

- ***Versão impressa*** – clique no botão para exibir a versão completa do contrato de licença da AVG em uma versão de interface web, bem organizada para ser impressa.
- ***Recusar*** – clique para recusar o contrato de licença. O processo de configuração será encerrado imediatamente. **AVG AntiVirus 2014** não será instalado!
- ***Voltar*** – clique para voltar à caixa de diálogo de instalação anterior.
- ***Aceitar*** – clique para confirmar que você leu, compreendeu e aceitou o contrato de licença.

A instalação continuará e você avançará para a próxima caixa de diálogo de configuração.

3.3. Ative a sua Licença

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



Onde encontrar o número de licença

O número de vendas pode ser encontrado na embalagem do CD na caixa do **AVG AntiVirus 2014**. O número da licença está no email de confirmação recebido depois da aquisição do AVG AntiVirus 2014 **online.** Digite o número exatamente como mostrado. 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 de copiar e colar.

O uso do método de ***copiar e colar*** para inserir seu número de licença do **AVG AntiVirus 2014** no programa garante que o número seja inserido corretamente. Por favor siga esses passos:

- 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 a tecla ***C***. Desse modo, o número é copiado.
- Aponte e clique no local em que você deseja colar o número copiado.
- Mantenha pressionada a tecla ***Ctrl*** enquanto pressiona a tecla ***V***. Desse modo, o número é

colado no local selecionado.

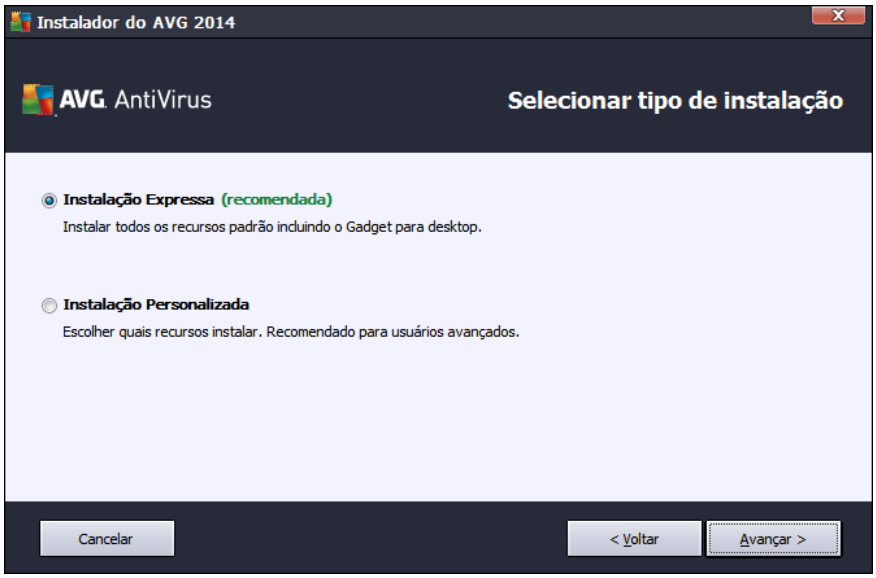
Botões de controle

Como na maioria das caixas de diálogo de instalação, há três botões de controle disponíveis.

- ***Cancelar*** – clique para sair do processo de instalação imediatamente. O **AVG AntiVirus 2014** não será instalado!
- ***Voltar*** – clique para voltar uma etapa para a caixa de diálogo de instalação anterior.
- ***Avançar*** – clique para continuar a instalação e avançar uma etapa.

3.4. Selecionar tipo de instalação

A caixa de diálogo ***Selecionar tipo de instalação*** oferece duas opções de instalação: ***Expressa*** e ***Personalizada***:



Instalação Expressa

Para a maioria dos usuários, é altamente recomendado manter a instalação padrão ***Expressa***. Assim, você instala o **AVG AntiVirus 2014** de modo totalmente automático, com configurações predefinidas pelo fornecedor do programa, incluindo o AVG Gadget. Essa configuração fornece o máximo de segurança combinado com o uso ideal dos recursos. No futuro, se houver necessidade de alterar a configuração, você sempre terá a opção de fazer isso diretamente no aplicativo **AVG AntiVirus 2014**.

Pressione o botão ***Avançar*** para prosseguir para o diálogo seguinte do processo de instalação.

Instalação personalizada

A ***Instalação personalizada*** deve ser usada somente por usuários experientes que tenham um motivo válido para instalar o **AVG AntiVirus 2014** com uma configuração não padrão; por exemplo, para adequar-se a requisitos de sistema específicos. Se você se decidir por esta opção, uma nova seção chamada ***Pasta de Destino*** será exibida no diálogo. Neste caso, você deverá especificar o local onde o **AVG AntiVirus 2014** deve ser instalado. Por padrão, o **AVG AntiVirus 2014** será instalado na pasta de arquivos de programa localizada na unidade C:, conforme apresentado no campo de texto no diálogo. Se você desejar alterar esse local, use o botão ***Procurar*** para exibir a estrutura da unidade e selecionar a pasta respectiva. Para reverter para o destino padrão predefinido pelo fornecedor do software, use o botão ***Padrão***.

Depois, pressione o botão ***Avançar*** para prosseguir para a caixa de diálogo Opções Personalizadas .

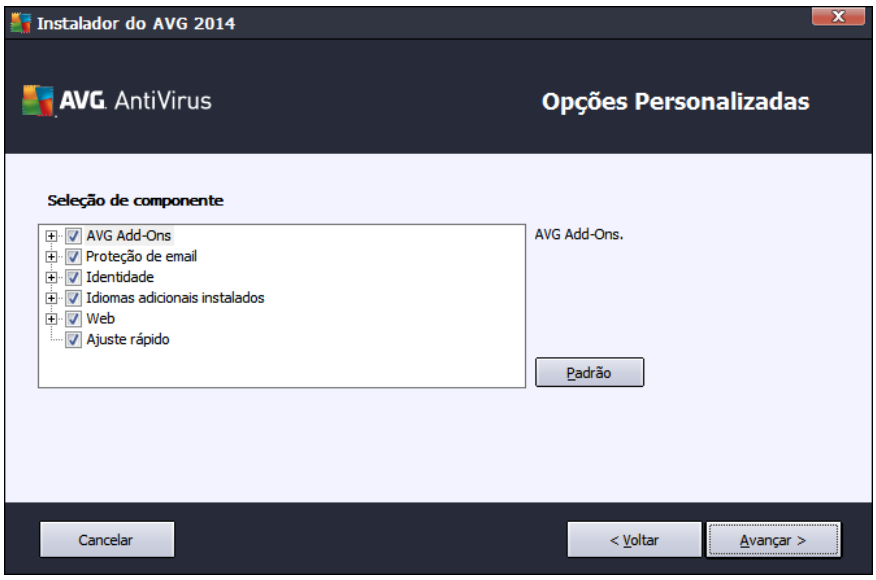
Botões de controle

Como a maioria das caixas de diálogo de instalação, há três botões de controle disponíveis.

- ***Cancelar*** – clique para sair do processo de instalação imediatamente. O **AVG AntiVirus 2014** não será instalado!
- ***Voltar*** – clique para voltar uma etapa para a caixa de diálogo de instalação anterior.
- ***Avançar*** – clique para continuar a instalação e avançar uma etapa.

3.5. Opções personalizadas

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



A seção ***Seleção de Componente*** exibe uma visão geral de todos os componentes **AVG AntiVirus 2014** que podem ser instalados. Se as configurações padrão não forem adequadas para você, é possível remover/adicionar componentes específicos. ***Entretanto, só é possível selecionar os componentes incluídos na edição do AVG que você adquiriu!*** Selecione qualquer item na lista ***Seleção de Componente***, e uma breve descrição do respectivo componente será exibida no lado direito desta seção. Para informações detalhadas sobre a funcionalidade de cada componente, consulte o capítulo Visão Geral de Componentes dessa documentação. Para reverter para a configuração padrão predefinida pelo fornecedor do software, use o botão ***Padrão***.

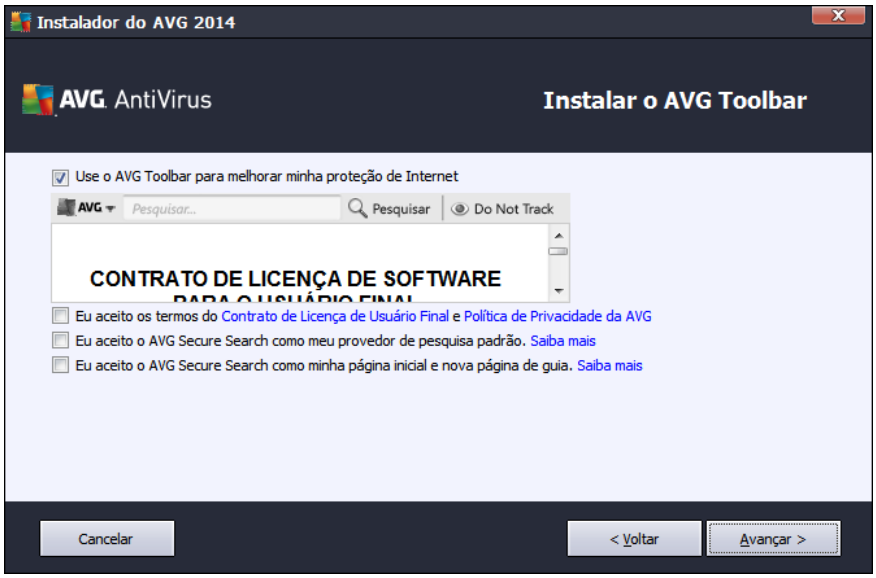
Botões de controle

Como na maioria das caixas de diálogo de instalação, há três botões de controle disponíveis.

- ***Cancelar*** – clique para sair do processo de instalação imediatamente. O **AVG AntiVirus 2014** não será instalado!
- ***Voltar*** – clique para voltar uma etapa para a caixa de diálogo de instalação anterior.
- ***Avançar*** – clique para continuar a instalação e avançar uma etapa.

3.6. Instalar o AVG Security Toolbar

Na janela ***Instalar o AVG Security Toolbar***, decida se deseja instalar o recurso ***AVG Security Toolbar***. Se você não alterar as configurações padrão, esse componente será instalado automaticamente no navegador de Internet padrão (*navegadores atualmente suportados são Microsoft Internet Explorer versão 6.0 ou mais recente e Mozilla Firefox versão 3.0 ou mais recente*), para lhe fornecer proteção online abrangente enquanto estiver navegando pela Internet. No momento, os navegadores da Internet suportados são o Internet Explorer (*versão 6.0 e mais recente*) e Mozilla Firefox (*versão 3.0 e mais recente*). Nenhum outro navegador é suportado *(se você estiver usando um navegador da Internet alternativo, como o Avant Browser, poderá perceber um comportamento inesperado).*

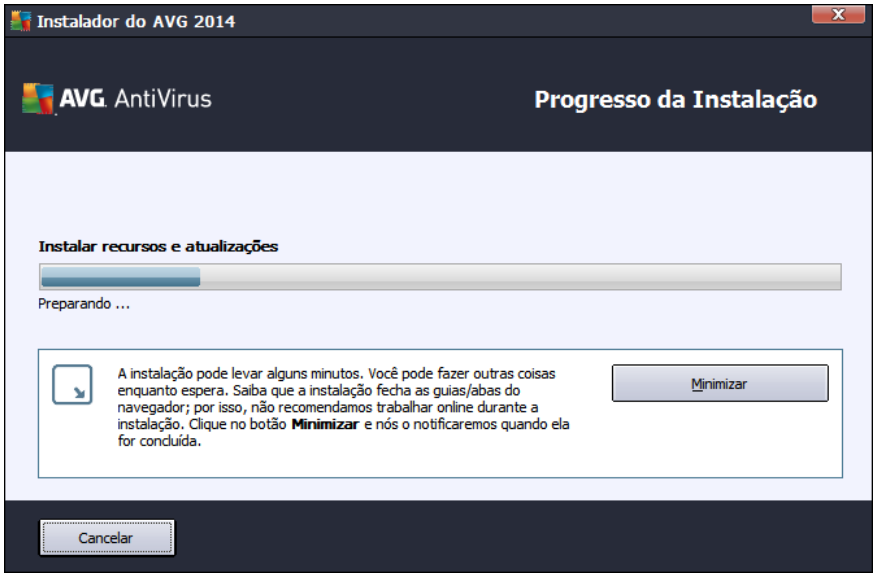


Na caixa de diálogo, você tem as opções para decidir sobre as seguintes configurações:

- ***Eu aceito os termos do Contrato de Licença de Usuário Final e da Política de Privacidade da AVG*** – esta opção deve ser confirmada para que a instalação prossiga!
- ***Eu aceito o AVG Secure Search como meu provedor de pesquisa padrão*** – marque para confirmar que você deseja usar o mecanismo AVG Secure Search, que colabora intimamente com o componente Link Scanner Surf Shield para oferecer a máxima segurança online.
- ***Eu aceito o AVG Secure Search como minha página inicial e nova página de guia.***

3.7. Progresso da Instalação

A caixa de diálogo ***Progresso da Instalação*** mostra o andamento do processo de instalação e não requer intervenção:



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

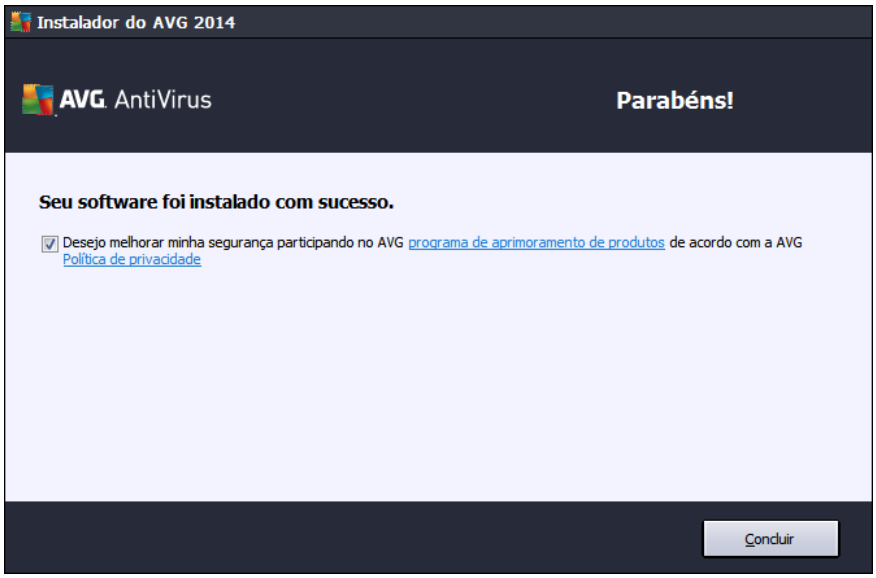
Botões de controle

Há dois botões de controle disponíveis nessa caixa de diálogo:

- ***Minimizar*** – o processo de instalação pode levar alguns minutos. Clique no botão para minimizar a janela do diálogo em um ícone visível na barra do sistema. O diálogo é exibido novamente assim que a instalação é concluída.
- ***Cancelar*** – este botão deve ser usado somente se você desejar interromper o processo de instalação atual. Tenha em mente que neste caso seu **AVG AntiVirus 2014** não será instalado!

3.8. Parabéns!

A caixa de diálogo ***Parabéns!*** confirma que o **AVG AntiVirus 2014** foi totalmente instalado e configurado:



Programa de Aprimoramento de Produto da e Política de Privacidade

Aqui você pode optar por participar do ***Programa de Aprimoramento de Produto*** (*para obter os detalhes, consulte o capítulo Configurações Avançadas do AVG / Programa de Aprimoramento de Produto*), que coleta informações anônimas sobre ameaças detectadas para aumentar o nível geral de segurança na Internet. Todos os dados são tratados como confidenciais e em conformidade com a Política de Privacidade da AVG; clique no link ***Política de Privacidade*** para ser redirecionado ao website da AVG (http://www.avg.com/) onde você pode encontrar a Política de Privacidade da AVG completa. Se concordar, mantenha a opção marcada *(como padrão, a opção está confirmada)*.

Para finalizar o processo de instalação pressione o botão ***Concluir***.

4. Após a instalação

4.1. Registro do produto

Quando a instalação do **AVG AntiVirus 2014** 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 AntiVirus 2014**. 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.

4.2. 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 de sistema do AVG
- clique duas vezes no ícone do AVG na área de trabalho
- no menu ***Iniciar / Todos os Programas / AVG 2014***

4.3. Verificação de todo o computador

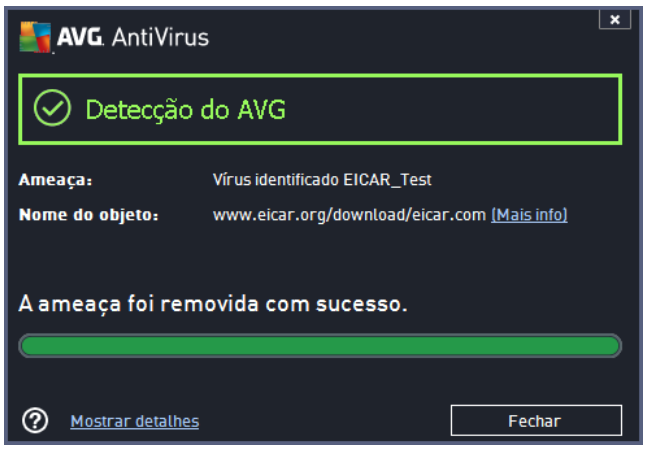
Existe um risco potencial de um vírus de computador ter sido transmitido ao seu computador antes da instalação do **AVG AntiVirus 2014**. Por esse motivo, você deve executar uma verificação de todo o computador para assegurar que seu PC não esteja infectado. A primeira verificação levará algum tempo *(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.

4.4. Teste Eicar

Para confirmar que **AVG AntiVirus 2014** foi instalado corretamente, você pode executar o teste EICAR.

O Teste Eicar é um método padrão 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 reagem 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 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 AntiVirus 2014** reagirá a ele com um aviso. Esse aviso demonstra que o AVG está instalado corretamente em seu computador.



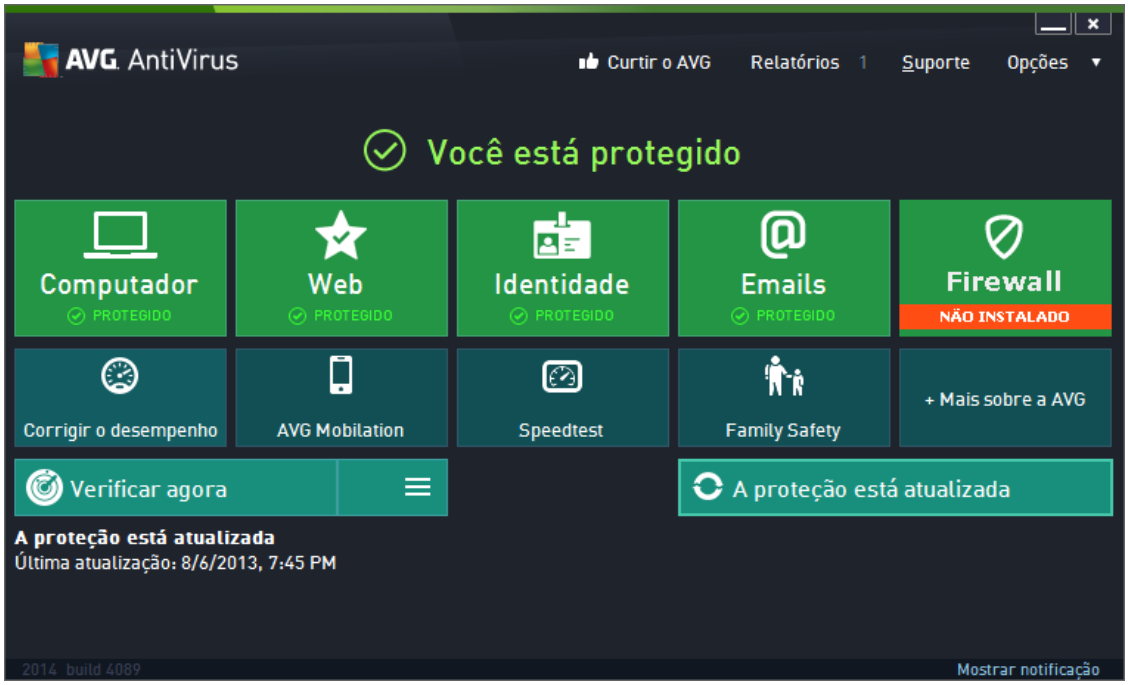
Se o AVG falhar na identificação do teste EICAR como sendo um vírus, você deverá verificar novamente a configuração do programa.

4.5. Configuração padrão do AVG

A configuração padrão (*isto é, como o aplicativo é configurado logo após a instalação*) de **AVG AntiVirus 2014**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

O **AVG AntiVirus 2014** é aberto com 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 *(Curtir o AVG, Relatórios, Suporte, Opções).* Detalhes >>
- ***Informações do Status de Segurança*** fornece informações básicas sobre o status atual do seu **AVG AntiVirus 2014**. Detalhes >>
- ***A visão geral dos componentes instalados*** pode ser encontrado 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 AntiVirus 2014** 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 AntiVirus 2014**, há mais dois elementos de controle que podem ser usados 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 AntiVirus 2014**. Detalhes >>

- ***O Gadget AVG***, que pode ser acessado da barra lateral do Windows (*suportado apenas no SO Windows Vista/7/8*), permite acesso rápido à verificação e atualização no **AVG AntiVirus 2014**. Detalhes >>

5.1. Linha superior de navegação

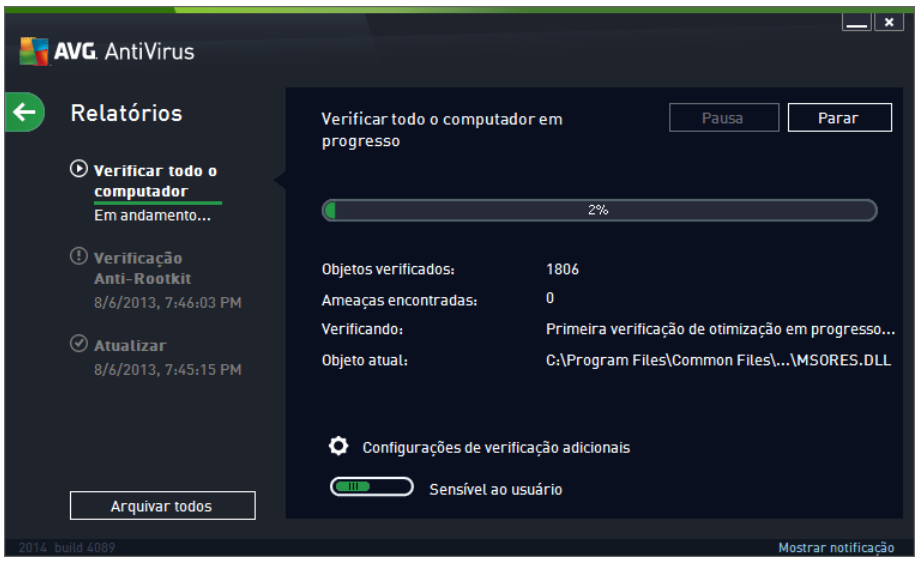
A ***linha superior de navegação*** abrange vários links ativos alinhados na seção superior da janela principal. A navegação contém os seguintes botões:

5.1.1. Junte-se a nós no Facebook

Clique no link para se conectar à comunidade da AVG no Facebook e compartilhar as mais recentes informações, notícias, dicas e truques para maximizar sua segurança na Internet.

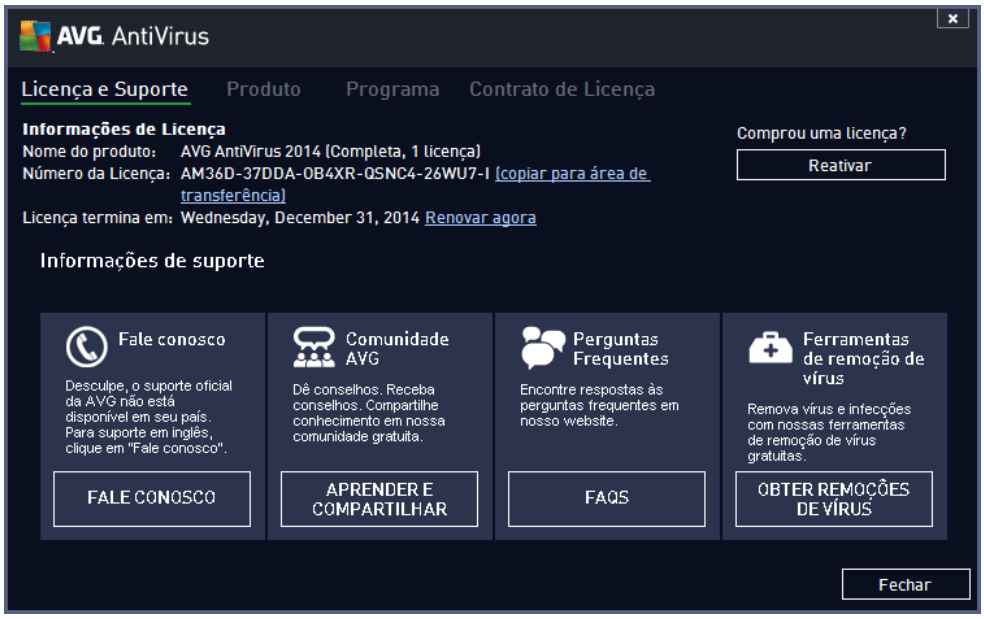
5.1.2. Relatórios

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 circulo 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 AntiVirus 2014**:



- ***Licença e suporte*** – a guia fornece informações sobre o nome do produto, número da 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 AntiVirus 2014)* 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 do 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 AntiVirus 2014** 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 **AVG AntiVirus 2014** dados técnicos mais importantes referentes às informações do produto, componentes instalados, proteção de email instalada e informações do sistema.

- ***Programa*** – nesta guia é possível encontrar informações sobre a versão do arquivo do programa e sobre o código de terceiros usados no produto.

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

5.1.4. Opções

A manutenção do **AVG AntiVirus 2014** 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 nesta 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 AntiVirus 2014**.
- ***Atualizar a partir do diretório...*** – executa o processo de atualização a partir dos arquivos de atualização localizados em uma pasta específica do disco local. Entretanto, esta opção é recomendada somente como emergência, ou seja, em situações em que não há conexão com a Internet (por exemplo, seu computador está infectado e desconectado da Internet; seu computador está conectado a uma rede sem acesso à Internet, etc.). Na nova janela aberta, selecione a pasta na qual colocou o arquivo de atualização anteriormente e inicialize o processo de atualização.
- ***Quarentena de Vírus*** – abre a interface do espaço de quarentena (Quarentena de Vírus) no qual o AVG remove todas as infecções detectadas que, por algum motivo, não podem ser resolvidas automaticamente. No espaço de quarentena, os arquivos infectados são isolados, 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.
    - *Detecção da Proteção Residente* – abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela Proteção Residente.
    - *Detecção do Identity Protection* – abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela Proteção de Identidade.
    - *Detecção do Verificador de email* – abre uma caixa de diálogo com uma visão geral dos anexos de email detectados como perigosos pelo componente Verificador de Email.
    - *Detecção da Proteção Online* – abre uma caixa de diálogo com uma visão geral das ameaças detectadas pelo Proteção Online.
    - *Log de histórico de eventos* – abre a interface de log de histórico com uma visão

geral de todas as ações registradas **AVG AntiVirus 2014** .

- ***Configurações avançadas...*** – abre a caixa de diálogo Configurações avançadas do AVG, na qual é possível editar a configuração **AVG AntiVirus 2014**. Em geral, é recomendável manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.

- ***Conteúdo da Ajuda*** – abre os arquivos de ajuda do AVG.

- ***Obter suporte*** – abre o website da AVG (*http://www.avg.com/*) na página do centro de atendimento ao cliente.

- ***Sua Web AVG*** – abre o site do AVG (*http://www.avg.com/*).

- ***Sobre vírus e ameaças*** – abre a Enciclopédia de vírus on-line, na qual é possível procurar informações sobre o vírus identificado.

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

- ***Registre-se agora / 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 AVG poderão receber suporte técnico gratuito. Observação: se estiver utilizando a versão de teste do **AVG AntiVirus 2014**, os dois últimos itens aparecerão como ***Comprar agora*** e ***Ativar***, permitindo que você compre a versão completa do programa imediatamente. Para **AVG AntiVirus 2014** instalado com um número de vendas, o itens são exibidos como ***Registrar e*** Ativar***.***

- ***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.

5.2. Informações sobre status de segurança

A seção ***Informações sobre Status de Segurança*** está localizada na parte superior da janela principal do **AVG AntiVirus 2014**. Nessa seção, você encontrará informações sobre o status de segurança atual do **AVG AntiVirus 2014.** Observe uma visão geral dos ícones possivelmente ocultos dessa seção e seus significados:

– O ícone verde indica que seu ***AVG AntiVirus 2014 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 nenhum problema crítico no **AVG AntiVirus 2014** e você provavelmente decidiu desativar alguns componentes 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 AntiVirus 2014** e não quer ser avisado novamente sobre isso. Talvez seja necessário usar esta opção em uma situação específica, mas é fortemente recomendável desativar a opção ***Ignorar status de erro*** o mais rápido possível!

Alternativamente, o ícone amarelo será também exibido se o **AVG AntiVirus 2014** precisar reiniciar o computador (***Reinicialização necessária***). Preste atenção a este aviso e reinicie seu PC.

– O ícone laranja indica que o ***AVG AntiVirus 2014 se encontra em estado crítico***! Um ou mais componentes não estão funcionando corretamente e o **AVG AntiVirus 2014** não pode proteger 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 AntiVirus 2014 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 AntiVirus 2014 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!

Nota: *as informações sobre o status do AVG AntiVirus 2014 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 encontrado 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. ***Recomenda-se fortemente 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 do 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 AntiVirus 2014** a seção ***Visão geral dos componentes*** contém informações sobre os

seguintes componentes:

- ***Computador*** – esse componente abrange dois serviços: ***Antivírus*** que detecta vírus, spyware, worms, trojans, 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 >>

- ***Web*** – protege contra ataques baseados na Web, enquanto você faz pesquisas ou navega na Internet. Detalhes >>

- ***Identidade*** – o componente executa o serviço ***Identity Shield*** que que está protegendo constantemente seus ativos digitais de ameaças novas e desconhecidas na Internet. Detalhes >>

- ***Emails*** – verifica as mensagens de email recebidas em busca de SPAM, além de bloquear vírus, ataques de phishing ou outras ameaças. 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 própria interface do componente com as informações sobre o status atual do componente 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 LiveKive*** se dedica a fazer backup de dados online em servidores seguros. O LiveKive faz backup automático de todos os arquivos, fotos e músicas em um local seguro, permitindo que você os compartilhe com a família e amigos e os acesse de qualquer dispositivo habilitado da web, incluindo dispositivos iPhones e Android.

- ***A Proteção para a Família*** ajuda a proteger seus filhos contra conteúdo de mídia, pesquisas on-line e sites inapropriados, além de enviar relatórios sobre as atividades que eles realizam on-line. O AVG Family Safety usa a tecnologia de rastreamento da tecla clicada para monitorar as atividades de seu filho em salas de bate-papo e em sites de redes sociais. Se ele reconhecer palavras, frases ou linguagens conhecidas por serem usadas para vitimar crianças online, você será notificado imediatamente através de SMS ou de email. O aplicativo permite definir o nível apropriado de proteção para cada um de seus filhos e monitorá-los individualmente por meio de logins exclusivos.

- ***O aplicativo PC Tuneup*** é uma ferramenta avançada para correção e análise detalhada do sistema, tendo como objetivo o aprimoramento da velocidade e do desempenho geral de seu computador.

- ***MultiMi*** reúne todas suas contas de email e de rede sociais em um único local seguro, tornando mais fácil entrar em contato com sua família e amigos, navegar na Internet, compartilhar fotos, vídeos e arquivos. O MultiMi contém o serviço LinkScanner que protege contra o número crescente de ameças na web, analisando as páginas web por trás dos links em qualquer página web que você esteja exibindo, para ter certeza que elas são seguras.

- ***AVG Toolbar*** está disponível diretamente em seu navegador de Internet e garante sua segurança máxima ao navegar na Internet.

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

5.5. Verificar / Atualizar links rápidos

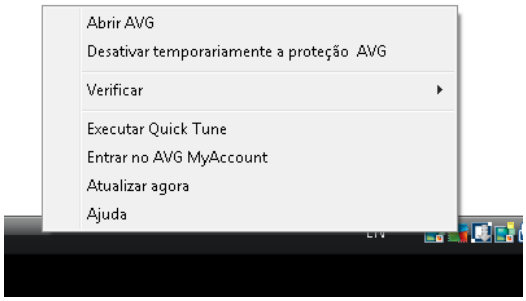
Links rápidos está localizados na linha inferior de botões na interface do usuário do **AVG AntiVirus 2014**. Esses links permitem que você tenha acesso imediato aos recursos do aplicativo mais importantes e mais usados, como a verificação e a atualização. Os links rápidos podem ser acessados em todas 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)*

- ***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 AntiVirus 2014**. Ele está sempre visível na bandeja do sistema, estando a interface de usuário do seu **AVG AntiVirus 2014** aberta ou fechada:



Exibição do ícone da bandeja do sistema do AVG

- Quando exibido em preto e branco, sem elementos adicionais, o ícone indica que todos os componentes do **AVG AntiVirus 2014** 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 ter confirmado 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 AntiVirus 2014** em execução no momento.

Informações do ícone da bandeja do sistema do AVG

O ***ícone da bandeja do sistema AVG*** também informa sobre atividades atuais do seu **AVG AntiVirus 2014** e possíveis mudanças de status no programa (*por ex., início automático de uma verificação ou atualização agendada, , alteração do status do componente, ocorrência de status de erro, ...*) por uma janela pop-up aberta pelo ícone 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 AntiVirus 2014**, clicando duas vezes no ícone. Ao clicar com o botão direito do mouse no ícone, você abre um menu de contexto breve com as opções a

seguir:

- ***Abrir AVG*** – clique para abrir a interface de usuário do **AVG AntiVirus 2014**.

- ***Desativar temporariamente a proteção do AVG*** – a opção permite desligar toda a proteção fornecida pelo seu **AVG AntiVirus 2014** 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 AntiVirus 2014** 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. Se for necessário desativar temporariamente o **AVG AntiVirus 2014**, você deverá reativá-lo assim que concluir a tarefa que solicitou a desativação. Se você estiver conectado à Internet ou a uma rede durante o período em que o software antivírus está desativado, o computador ficará vulnerável a ataques.

- ***Verificações*** – clique para abrir o menu de contexto das verificações predefinidas (*Verificar todo o computador* e *Verificar arquivos ou pastas específicos*) e selecione a verificação necessária. Ela será iniciada imediatamente.

- ***Executando verificações...*** – este item será exibido apenas se uma verificação estiver sendo executada no momento em seu computador. Para essa verificação, você pode definir sua prioridade ou, como segunda opção, interromper ou pausar a verificação em execução. Além disso, as seguintes ações estão acessíveis: *Definir prioridade para todas as verificações, Pausar todas as verificações* ou *Interromper todas as verificações*.

- ***Executar o Quick Tune*** – clique para iniciar o componente Quick Tune.

- ***Login no AVG MyAccount*** – abre a página inicial MyAccount onde é possível gerenciar os produtos que você assina, comprar mais proteção, baixar arquivos de instalação, verificar seus pedidos e faturas anteriores e gerenciar suas informações pessoais.

- ***Atualizar agora*** – inicia uma atualização imediata.

- ***Ajuda*** – abre o arquivo de ajuda da página de inicialização.

5.7. Gadget AVG

O ***gadget AVG*** é exibido na área de trabalho do Windows (*barra lateral do Windows*). Esse aplicativo é compatível apenas com os sistemas operacionais Windows Vista, Windows 7 e Windows 8. O ***gadget AVG*** oferece um acesso imediato às funções mais importantes do **AVG AntiVirus 2014**, por exemplo, verificação e atualização:

Controles do gadget AVG

Se necessário, o gadget AVG permite iniciar imediatamente uma verificação ou atualização. Ele fornece um link rápido que conecta você com as principais redes sociais *(Facebook, Twitter),* e oferece pesquisa rápida. A seguir, você pode encontrar uma visão geral dos controles disponíveis:

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

- ***Atualizar agora*** – clique no link ***Atualizar agora*** **AVG AntiVirus 2014** para iniciar a atualização do diretamente do gadget:

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

- ***Link do Facebook*** – abre o navegador no site do Facebook, especificamente na página da ***Comunidade da AVG.***

- ***Link do Quick Tune*** – abre o componente Quick Tune pronto para análise imediata do seu computador.

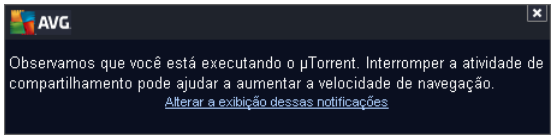
- ***Caixa de Pesquisa*** – digite uma palavra-chave e obtenha os resultados da pesquisa imediatamente em uma nova janela aberta com o seu navegador padrão.

5.8. AVG Advisor

O ***AVG Advisor*** foi projetado para detectar problemas que podem estar desacelerando seu computador ou colocando-o em risco e para recomendar uma ação para solucionar a situação. Se você notar que seu computador ficou lento subitamente *(navegação na Internet, desempenho geral)*, geralmente não é óbvio definir exatamente o culpado e, subsequentemente, resolver o problema. Neste ponto, o ***AVG Advisor*** entra em cena: ele exibe uma notificação na bandeja do sistema

informando-o sobre qual é o provável problema e sugerindo como corrigi-lo. O ***AVG Advisor*** monitora possíveis problemas em todos os processos que são executados em seu PC, oferecendo dicas para evitar estes problemas.

O ***AVG Advisor*** é visível na forma de um pop-up deslizante sobre a bandeja do sistema:



Especificamente, o ***AVG Advisor*** monitora o seguinte:

- ***O estado de qualquer navegador web aberto no momento***. Os navegadores web podem sobrecarregar a memória, especialmente se várias abas ou janelas estiverem abertas ao mesmo tempo, além de consumir muitos recursos do sistema, e.x. deixando seu computador mais lento. Em tal situação, geralmente ajuda reiniciar o navegador web.

- ***Conexões peer-to-peer em funcionamento***. Às vezes, após usar o protocolo P2P para compartilhar arquivos, a conexão pode continuar ativa, usando certa quantidade da sua banda larga. Como resultado, a navegação na web pode ficar lenta.

- ***Rede desconhecida com nome familiar***. Geralmente, isso se aplica apenas aos usuários que conectam-se a várias redes, comumente com computadores portáteis: se uma nova rede desconhecida tiver o mesmo nome de uma rede conhecida e usada frequentemente *(por exemplo, Casa ou MeuWifi)*, pode ocorrer uma confusão e você se conectar acidentalmente a 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***. Assim ela não será reportada novamente no futuro.

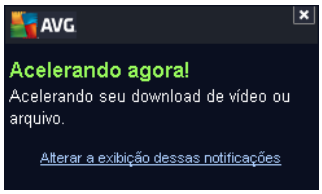
Em cada uma destas situações, o ***AVG Advisor*** avisa sobre possíveis problemas que possam ocorrer e fornece o nome e ícone do processo ou aplicativo em conflito. Também, o ***AVG Advisor*** sugere qual o procedimento para evitar os possíveis problemas.

Navegadores web suportados

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

5.9. 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.



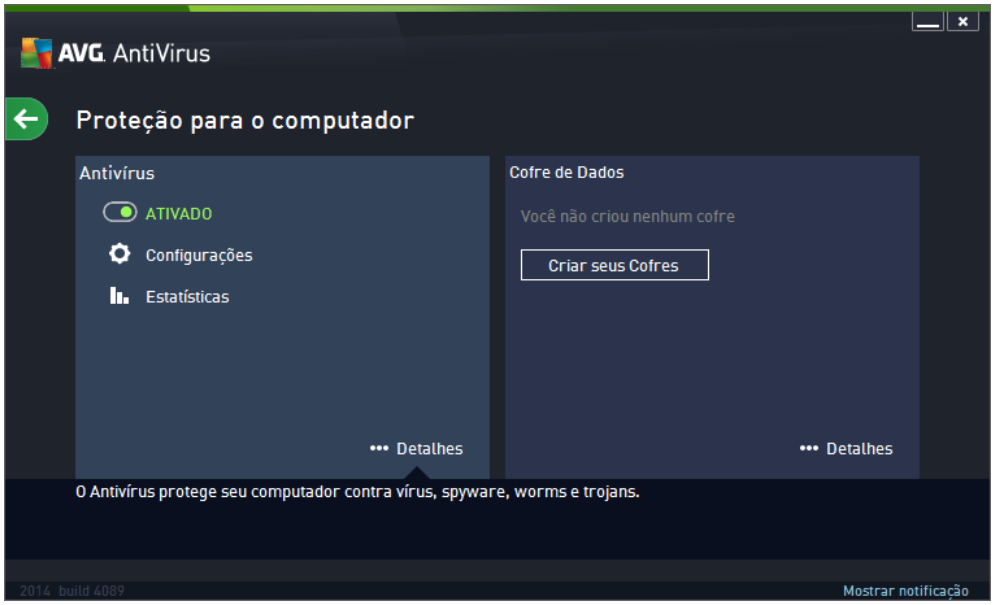
6. Componentes do AVG

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 verifica se há vírus conhecidos. Todos os vírus detectados serão bloqueados e não poderão realizar nenhuma ação. Eles também serão limpos e colocados na Quarentena de Vírus. Você nem se dará conta do processo, já que essa proteção residente é executada "em segundo plano". O Antivírus utiliza também verificação heurística, onde é verificado se os arquivos possuem características típicas de vírus. Isso significa que o Antivírus pode detectar um novo e desconhecido vírus se este contiver algumas características típicas dos vírus existentes. **AVG AntiVirus 2014** 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 o tratamento de todos os itens potencialmente prejudiciais como qualquer outra infecção.

- O ***Cofre de Dados*** permite criar cofres virtuais seguros para armazenar dados valiosos ou sensíveis. O conteúdo de um Cofre de Dados é criptografado e protegido com 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 destacada 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 *Antivírus ou Cofres de Dados)*:

Ativado / Desativado – o botão pode lembrar um semáforo, tanto em aparência quanto em funcionalidade. É só clicar para alternar entre as duas posições. A cor verde representa ***Ativado***, o que significa que o serviço de segurança do Antivírus 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 para 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 sobre o possível risco pelo 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, Antivírus. Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG AntiVirus 2014**, mas qualquer configuração só pode ser recomendada para usuários experientes!

Estatísticas – clique no botão para ser redirecionado para a página dedicada no website da AVG (*http://www.avg.com/*). Nessa página, é possível encontrar um resumo estatístico detalhado de todas as atividades realizadas pelo em seu computador em um período específico e ao todo.

Detalhes – clique o botão e uma breve descrição do serviço destacado aparecerá na parte inferior do diálogo.

– 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:

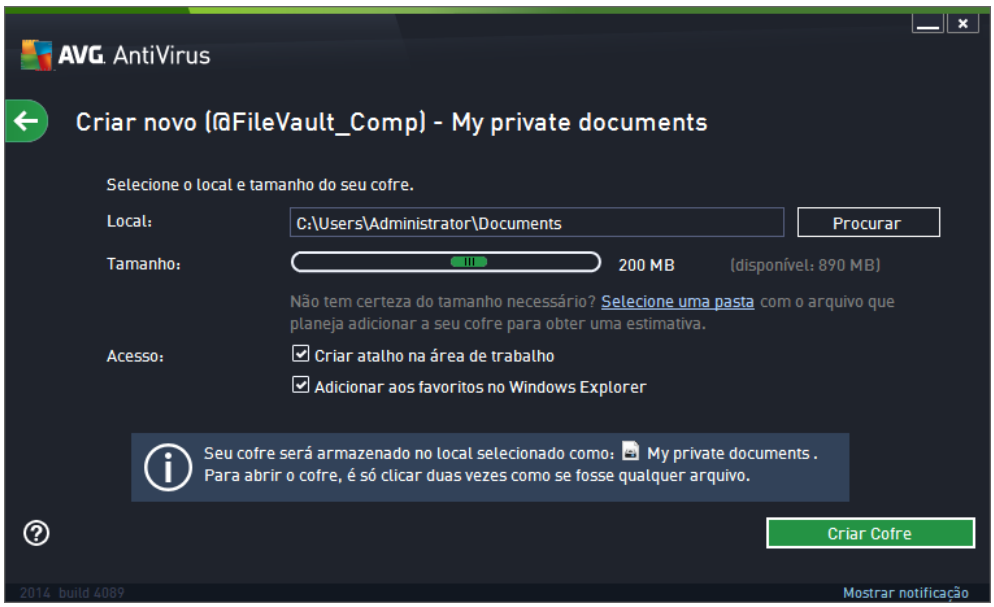
Primeiro, é necessário especificar o nome do seu cofre e criar uma senha forte:

- ***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 desejável incluir seu nome, além de uma indicação do conteúdo do cofre, por exemplo, *Emails do papai*.

- ***Criar senha / Redigitas senha*** – crie uma senha para seu cofre de dados e digite-a nos campos de texto respectivos. O indicador gráfico à direita dirá se sua senha é fraca *(relativamente fácil de ser quebrada com ferramentas especiais de software)* ou forte. Recomendamos escolher uma senha, pelo menos, de força média. Você pode fortalecer sua senha incluindo letras maiúsculas, números e outros caracteres como pontos, barras, etc. Se desejar se certificar que você digitou a senha que desejava, é possível marcar a caixa ***Mostrar senha*** *(claro, ninguém mais deverá 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:

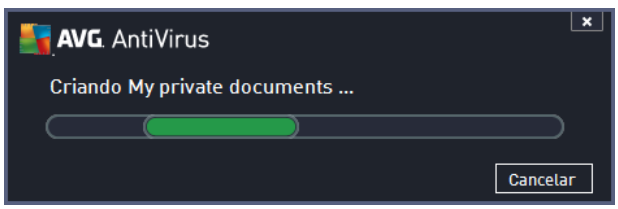
- ***Local*** informa onde o cofre de dados será colocado fisicamente. Procure por um destino adequado em seu disco rígido ou você poderá manter o local predefinido, que é sua pasta *Documentos*. Observe que assim que você criar um cofre de dados, não será possível alterar seu local.

- ***Tamanho*** – é possível predefinir o tamanho do seu cofre de dados, 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 suas necessidades.

- ***Acesso*** – as caixas de seleção nessa seção permitem que você crie atalhos convenientes para seu cofre de dados.

Como desbloquear seu cofre de dados

Quando estiver satisfeito com as configurações, clique no botão ***Criar cofre***. Você será solicitado a desbloquear seu novo cofre de dados com a senha escolhida e depois ele estará pronto para receber os arquivos:



- ***Abrir*** – para usar seu novo cofre de dados, é necessário primeiro desbloqueá-lo. Ao ser

desbloqueado, o cofre de dados será exibido em seu computador como um novo disco virtual. Atribua uma letra a sua escolha do menu suspenso. Normalmente, você não terá permissão de escolher o C *(geralmente atribuído ao seu disco rígido)*, A *(unidade de disco flexível)*, ou D *(unidade de DVD)*. Observe que a cada vez que você desbloquear um cofre de dados, você poderá escolher uma letra de unidade disponível diferente.

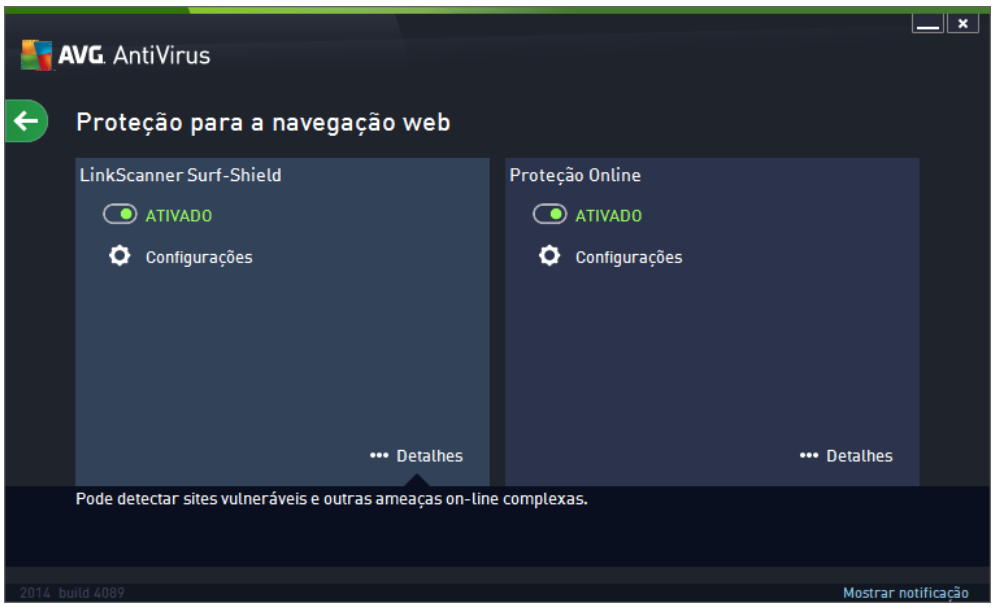
- ***Senha*** – no campo de texto, digite sua senha para se autorizar e clique no botão ***Desbloquear***. Se precisar de ajuda para se lembrar da senha, clique em ***Dica*** para exibir a dica de senha que você definiu ao criar o cofre de dados. O novo cofre de dados aparecerá na visão geral dos seus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

6.2. Proteção de navegação da Web

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

- O ***LinkScanner Surf-Shield*** protege contra o crescente número de ameaças atuais e que estão surgindo na Web. Essas ameaças podem estar escondidas em qualquer tipo de site, de governamentais a grandes marcas bem conhecidas, a pequenas empresas, e raramente permanecem nesses locais mais de 24 horas. O LinkScanner protege analisando as páginas da web que estão por trás de todos os links em qualquer página da Web que esteja vendo e garantindo que são seguras só no momento que importa – quando você está prestes a clicar nesse link. ***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 paginas da Web visitadas (e possíveis arquivos incluídos nelas) mesmo antes destas serem exibidas no navegador da Web ou baixadas no computador. A Proteção Online detecta que a página que você está prestes a visitar inclui um javascript perigoso e impede a exibição da pagina. Além disso, ela reconhece malware contido em uma página e interrompe seu download imediatamente, para que nunca entre no seu computador. 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 pode lembrar um semáforo, tanto em aparência quanto em funcionalidade. 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 para 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 sobre o possível risco pelo 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 AntiVirus 2014**, mas qualquer configuração só pode ser recomendada para usuários experientes!

Estatísticas – clique no botão para ser redirecionado para a página dedicada no website da AVG (*http://www.avg.com/*). Nessa página, é possível encontrar um resumo estatístico detalhado de todas as atividades realizadas pelo em seu computador em um período específico e ao todo.

Detalhes – clique o botão e uma breve descrição do serviço destacado aparecerá na parte inferior do diálogo.

– 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. Identity protection

O componente ***Identity Protection*** executa o serviço ***Identity Shield*** que que está protegendo constantemente seus ativos digitais de ameaças novas e desconhecidas na Internet:

- O ***Identity Protection*** é um serviço anti-malware que o protege de todos os tipos de malware (*spyware, robôs, roubo de identidade...*) usando tecnologias comportamentais e que fornece proteção imediata contra novos vírus. 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 sendo executados em seu PC ou em sua rede compartilhada estão operando corretamente. O Identity Protection aponta e bloqueia comportamento suspeito em base contínua, além de proteger seu computador de todos os novos malware. O Identity Protection 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, assim como pode determinar se algo mal-intencionado está ocorrendo em seu sistema.* Por isso, pode revelar ameaças ainda não descritas no banco de dados de vírus. Quando um código desconhecido chega ao seu computador, é imediatamente vigiado por comportamento malicioso e monitorado. Se o arquivo for considerado mal-intencionado, o Identity Protection 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. Esta tecnologia é bastante proativa, raramente precisa ser atualizada e está sempre de prontidão.

Controles da caixa de diálogo

Na caixa de diálogo, você pode encontrar os seguintes controles:

Ativado / Desativado – o botão pode lembrar um semáforo, tanto em aparência quanto em funcionalidade. É só clicar para alternar entre as duas posições. A cor verde representa ***Ativado***, o que significa que o serviço de segurança Identity Protection 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 para 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 sobre o possível risco pelo 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, Identity Protection. Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG AntiVirus 2014**, mas qualquer configuração só pode ser recomendada para usuários experientes!

Detalhes – clique o botão e uma breve descrição do serviço destacado aparecerá na parte inferior do diálogo.

– 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 AntiVirus 2014** o serviço Identity Alert não está incluído. 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.

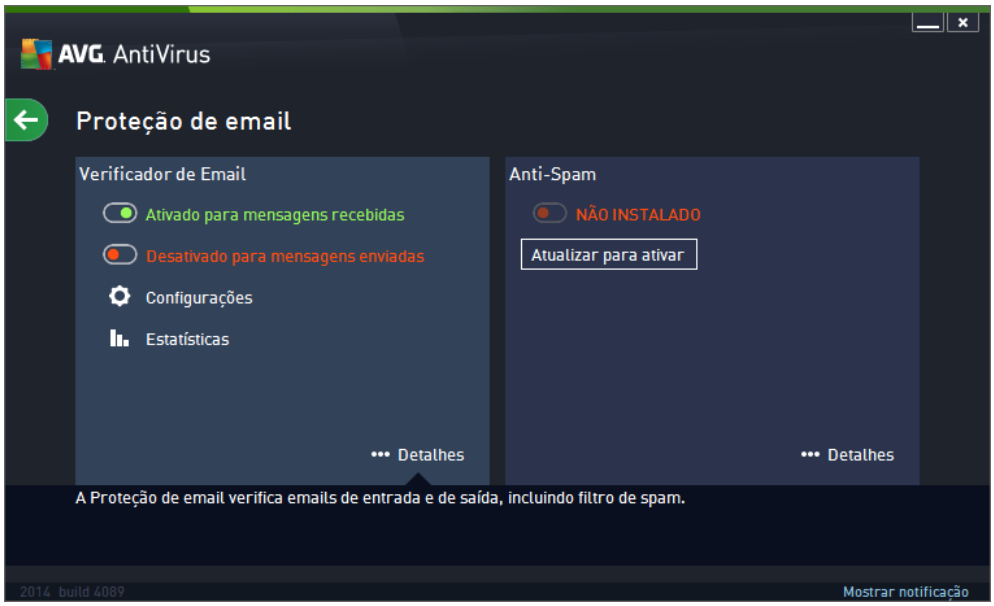
6.4. Proteção de email

O componente ***Proteção de Email*** abrange os dois serviços de segurança a seguir: ***Verificador de Email*** e ***Anti-Spam***:

- ***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 de email.* 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 destacada 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 pode lembrar um semáforo, tanto em aparência quanto em funcionalidade. 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 para 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 sobre o possível risco pelo 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!***

Na seção Verificador de Email, é possível ver dois botões de "semáforo". Desta maneira, é possível especificar se você deseja que o Verificador de Email verifique mensagens recebidas, enviadas, ou ambas. Como padrão, a verificação está ativada para mensagens recebidas e desativada para mensagens enviadas, onde o risco de infecção é baixo.

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, i.e. Verificador de email ou Anti-Spam. Na interface de configurações avançadas, é possível editar todas as configurações de cada serviço de segurança no **AVG AntiVirus 2014**, mas qualquer configuração só pode ser recomendada para usuários experientes!

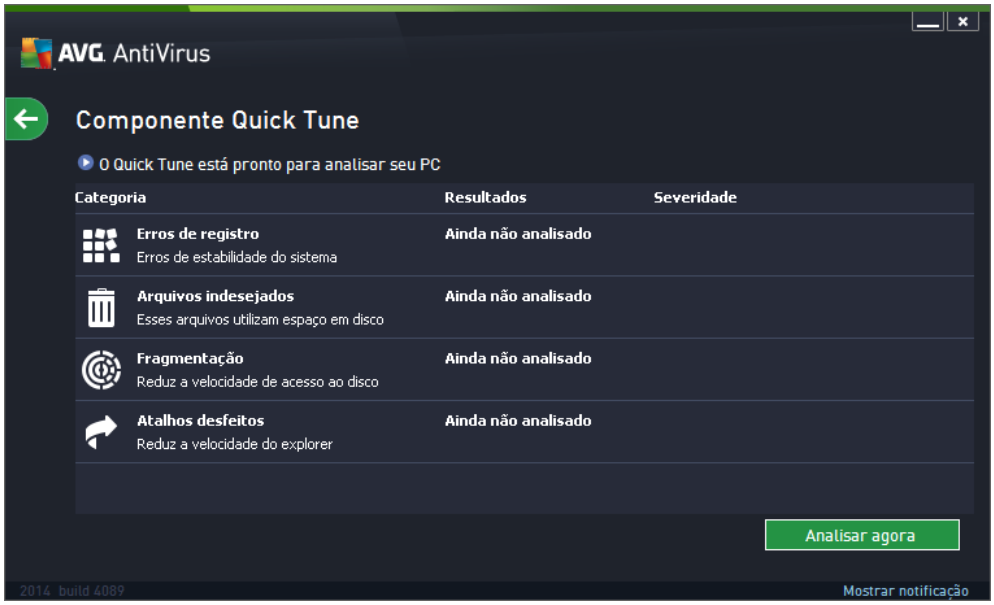
Estatísticas – clique no botão para ser redirecionado para a página dedicada no website da AVG (http://www.avg.com/). Nessa página, é possível encontrar um resumo estatístico detalhado de todas as atividades realizadas pelo em seu computador em um período específico e ao todo.

Detalhes – clique o botão e uma breve descrição do serviço destacado aparecerá na parte inferior do diálogo.

– 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. Quick Tune componente

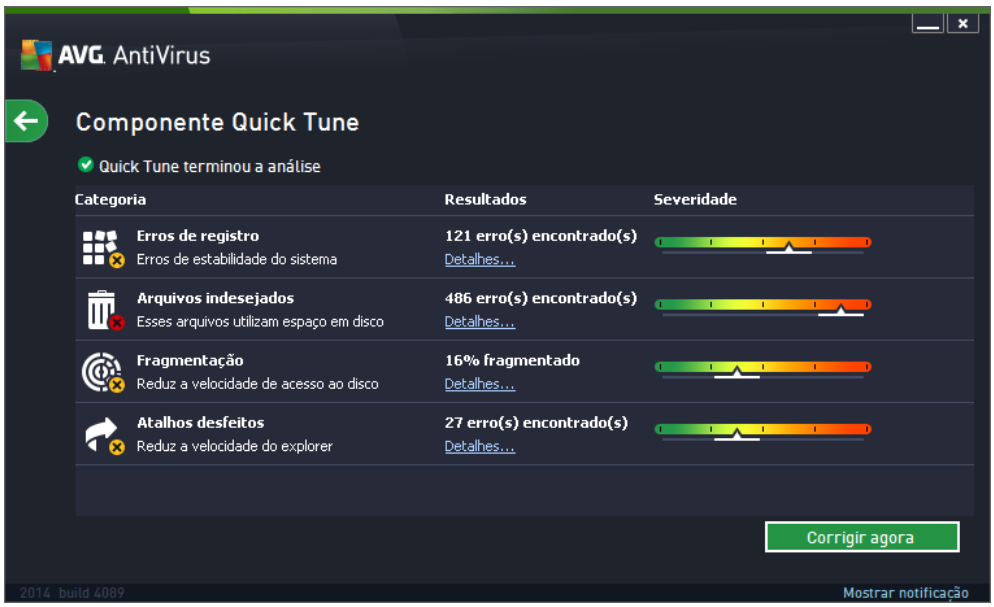
O componente ***Quick Tune*** é uma ferramenta avançada para análise detalhada e correção do sistema, sobre como a velocidade e o desempenho geral do seu computador pode ser aprimorado. Ele abre a partir da interface de usuário principal através do item ***Corrigir o desempenho***:



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

- ***Erros de registro*** irá fornecer 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*** fornecerá 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.
- ***Atalhos Desfeitos*** notificará sobre atalhos que não funcionam mais, que levam a locais não existentes, etc.

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



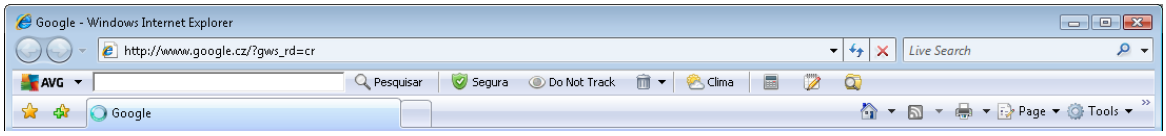
A visão geral de resultados apresenta o número de problemas de sistema detectados, divididos de acordo com as respectivas categorias testadas. Os resultados da análise serão também exibidos graficamente em um eixo na coluna ***Gravidade***.

Botões de controle

- ***Analisar agora*** (*é exibido antes do início da análise*) – pressione este botão para iniciar a análise imediata do computador
- ***Corrigir agora*** *(exibido após a análise ser concluída*) – pressione o botão para corrigir todos os erros encontrados. Você terá uma visão geral do resultado assim que o processo de correção estiver terminado.
- ***Parar análise*** – pressione este botão para interromper a análise em execução ou retornar à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*) quando a análise for concluída

7. AVG Security Toolbar

O ***AVG Security Toolbar*** é uma ferramenta que coopera intimamente com o serviço LinkScanner Surf-Shield e que o protege ao máximo durante a navegação na Internet. No **AVG AntiVirus 2014**, a instalação do ***AVG Security Toolbar*** é opcional. Durante o processo de instalação você é convidado a optar pela instalação ou não do componente. O ***AVG Security Toolbar*** está disponível diretamente no seu navegador de Internet. No momento, os navegadores da Internet suportados são o Internet Explorer (*versão 6.0 e mais recente*) e Mozilla Firefox (*versão 3.0 e mais recente*). Nenhum outro navegador é suportado *(se você estiver usando um navegador da Internet alternativo, como o Avant Browser, poderá perceber um comportamento inesperado).*



O ***AVG Security Toolbar*** consiste no seguinte:

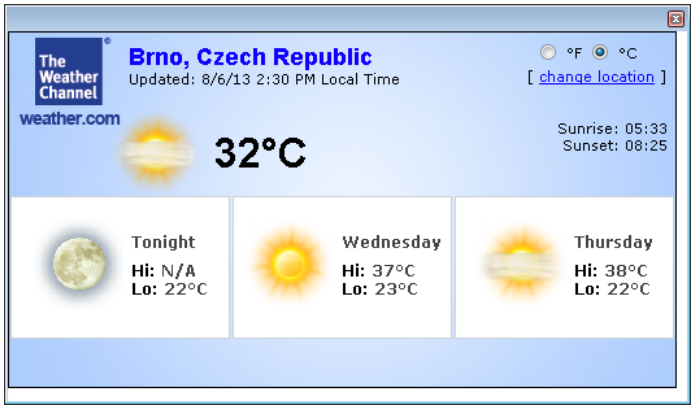
- ***Logotipo do AVG*** com o menu suspenso:
  - ***Nível atual de ameaças*** – abre a página da Web do AVG Virus Lab, com uma exibição gráfica do nível atual de ameaças na Web.
  - ***AVG Threat Labs*** – abre o website específico do ***AVG Threat Lab*** *(em http://www.avgthreatlabs.com)* onde você pode encontrar informações online sobre a segurança de websites e o nível de ameças atuais.
  - ***Ajuda da Barra de Ferramentas*** – abre a ajuda online, cobrindo todos os recursos do ***AVG Security Toolbar***.
  - ***Enviar um Comentário sobre o Produto*** – abre uma página da Internet com um formulário que você pode preencher para dar a sua opinião sobre o ***AVG Security Toolbar***.
  - ***Contrato de Licença do Usuário Final*** – abre o website da AVG na página fornecendo o texto completo do contrato de licença relacionado ao seu uso do **AVG AntiVirus 2014**.
  - ***Política de Privacidade*** – abre o website da AVG na página em que encontra o texto completo da Política de Privacidade da AVG.
  - ***Desinstalar o AVG Security Toolbar*** – abre uma página da Internet que apresenta uma descrição detalhada de como desativar o ***AVG Security Toolbar*** em cada um dos navegadores suportados.
  - ***Sobre...*** – abre uma nova janela com informações relativas à versão do ***AVG Security Toolbar*** que está instalada.
- ***Campo de pesquisa*** – pesquise na Internet com o ***AVG Security Toolbar*** para ficar completamente seguro e tranquilo, uma vez que todos os resultados da pesquisa apresentados serão cem por cento seguros. Digite uma palavra-chave ou expressão no campo de pesquisa e clique no botão ***Pesquisar*** *(ou pressione Enter)*.

- ***Segurança do Site*** – este botão abre um novo diálogo fornecendo informações sobre o nível de ameaça atual (*Seguro*) da página que você está visitando. Esta breve visão geral pode ser expandida e exibida com todos os detalhes de todas as atividades de segurança relacionadas à página na janela do navegador (*Relatório completo do website*):

- ***Do Not Track*** – o serviço DNT ajuda a identificar websites que coletam dados sobre suas atividades online, e lhe fornece a escolha de permitir ou impedir isso. Detalhes >>

- ***Excluir*** – o botão "lixeira" oferece um menu suspenso onde é possível selecionar se você deseja excluir as informações sobre sua navegação, downloads, formulários online ou excluir todo seu histórico de pesquisa de uma vez.

- ***Tempo*** – o botão abre uma nova caixa de diálogo que fornece informações sobre o tempo em seu local e sobre a previsão meteorológica para os dois próximos dias. Essas informações são atualizadas regularmente de cada 3 a 6 horas. Na caixa de diálogo, você pode alterar o local desejado manualmente e decidir se deseja ver informações sobre a temperatura em Celsius ou Fahrenheit.



- ***Facebook*** – este botão permite que você se conecte à rede social Facebook diretamente a partir do ***AVG Security Toolbar***.

- Botões de atalho para o acesso rápido a esses aplicativos: ***Calculadora***, ***Bloco de Notas***, ***Windows Explorer***.

8. AVG Do Not Track

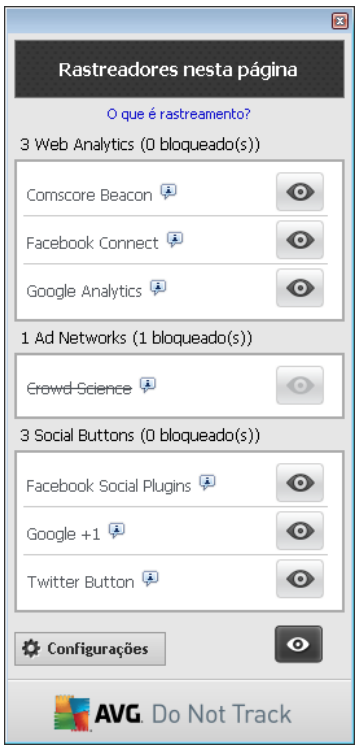
O ***AVG Do Not Track*** ajuda a identificar websites que estão coletando dados sobre suas atividades online. O ***AVG Do Not Track***, incluído no AVG Security Toolbar, mostra os websites ou anunciantes que coletam dados relativos à sua atividade online e fornece a opção de permitir ou não a coleta de dados.

- O ***AVG Do Not Track*** fornece informações adicionais sobre a política de privacidade correspondente a cada serviço, assim como um link direto para cancelar o serviço, se estiver disponível.
- Além disso, o ***AVG Do Not Track*** suporta o protocolo W3C DNT para notificar os sites automaticamente que você não deseja ser rastreado. Esta notificação está ativada como padrão, mas pode ser alterada a qualquer momento.
- O ***AVG Do Not Track*** é fornecido sob estes termos e condições.
- Como padrão, o ***AVG Do Not Track*** está ativado, mas pode ser facilmente desativado a qualquer momento. As instruções podem ser encontradas no artigo da FAQ Desativação do recurso AVG Do Not Track.
- Para obter mais informações sobre o ***AVG Do Not Track***, visite nosso website.

No momento, a funcionalidade ***AVG Do Not Track*** é suportada nos navegadores Mozilla Firefox, Chrome e Internet Explorer.

8.1. Interface do AVG Do Not Track

Quando estiver online, ***AVG Do Not Track*** alertará assim que qualquer tipo de atividade de coleta de dados for detectada. Nesse caso, o ícone do ***AVG Do Not Track*** localizado no AVG Security Toolbar muda de aspecto; um número pequeno é exibido ao lado do ícone fornecendo informações sobre o número de serviços de coleta de dados detectado: Clique no ícone para ver a seguinte caixa de diálogo:



Todos os serviços de coleta de dados estão listados no resumo ***Rastreadores nesta página***. Existem três tipos de atividades de coleta de dados reconhecidos pelo ***AVG Do Not Track***:

- ***Web Analytics*** *(permitido como padrão):*serviços usados para melhorar o desempenho e experiência do respectivo website. Nesta categoria, você encontra serviços como o Google Analytics, Omniture ou Yahoo Analytics. Recomendamos não bloquear os serviços web, pois o website pode não funcionar como planejado.

- ***Ad Networks*** *(alguns bloqueados como padrão):* serviços que coletam ou compartilham dados sobre sua atividade online em vários sites, de forma direta ou indireta, para oferecer publicidade personalizada no lugar de publicidade baseada no conteúdo. Isto é determinado baseado na política de privacidade de cada Ad network, conforme disponibilizado em seus websites. Como padrão, alguns ad networks estão bloqueados.

- ***Social Buttons*** *(permitido como padrão):* elementos projetados para melhorar a experiência de redes sociais. Os Social buttons são oferecidos pelas redes sociais no site que você está visitando. Eles coletam dados sobre sua atividade online enquanto estiver logado. Alguns exemplos de botões sociais: plugins sociais do Facebook, botão do Twitter, Google +1.

Obs.: *dependendo dos serviços executados em segundo plano no website, algumas das três seções descritas acima podem não aparecer no diálogo do AVG Do Not Track.*

Controles da caixa de diálogo

- ***O que é rastreamento?*** – clique neste link na seção superior da caixa de diálogo para ser redirecionado para a página web dedicada que fornece explicações detalhadas sobre os princípios do rastreamento e uma descrição de tipos específicos de rastreamento.

- ***Bloquear Tudo*** – clique no botão localizado na seção inferior do diálogo para informar que você não gostaria de nenhuma atividade de coleta de dados *(para obter detalhes, consulte o capítulo Bloquear processos de rastreamento).*

- ***Configurações do Do Not Track*** – clique neste botão na seção inferior do diálogo para ser redirecionado para a página web dedicada onde é possível definir configurações específicas de vários parâmetros do ***AVG Do Not Track*** *(consulte o capítulo Configurações do AVG Do Not Track para obter informações mais detalhadas)*

8.2. Informações sobre processos de rastreamento

A lista de serviços de coleta de dados detectados fornece apenas o nome do serviço específico. Para tomar uma decisão bem informada e decidir se o respectivo serviço deve ser bloqueado, é necessário saber mais sobre ele. Mova seu mouse sobre o respectivo item da lista. Um balão de informações será exibido fornecendo dados detalhados sobre o serviço. Você ficará sabendo se o serviço coleta seus dados pessoais ou outros dados disponíveis; se os dados estão sendo compartilhados com terceiros; e se os dados coletados estão sendo arquivados para uso futuro:

Na seção inferior do balão de informações, está o hyperlink da ***Política de Privacidade*** que redireciona para o website dedicado à política de privacidade do respectivo serviço detectado.

8.3. Bloqueio de processos de rastreamento

Com as listas de todas os Ad Networks / Social Buttons / Web Analytics, você tem agora a opção de controlar quais serviços devem ser bloqueados. Existem dois caminhos:

- ***Bloquear Tudo*** – clique neste botão localizado na seção inferior do diálogo para informar que você não gostaria de nenhuma atividade de coleta de dados. *(Entretanto, tenha em mente que esta ação pode quebrar o funcionamento da respectiva webpage onde o serviço é executado!)*

- – Se você não desejar bloquear todos os serviços detectados de uma vez, é possível especificar individualmente se o serviço deve ser bloqueado ou permitido. Você pode permitir a execução de alguns sistemas de detecção *(por exemplo, Web Analytics):* estes sistemas costumam coletar dados para a otimização do website ao qual pertencem, ajudando assim a melhorar o ambiente comum de Internet para todos os usuários. No entanto, ao mesmo tempo, você pode bloquear as atividades de coleta de dados de todos os processos classificados como Ad Networks. É só clicar no ícone ao lado do respectivo serviço para bloquear a coleta de dados *(o nome do processo aparecerá riscado)* , ou permitir novamente a coleta de dados.

8.4. Configurações do AVG Do Not Track

A caixa de diálogo ***Opções do Do Not Track*** oferece as seguintes opções de configuração:

- ***Do Not Track está ativado*** – por padrão, o serviço DNT está ativo.*(chave LIGADA)*. Para desativar o serviço, mova a chave para a posição DESLIGADA.

- Na seção central da caixa de diálogo, você pode ver uma caixa com uma lista dos serviços de coleta de dados conhecidos que podem ser classificados como Ad Networks. Como padrão, o ***Do Not Track*** bloqueia algumas Ad Networks automaticamente e você continua decidindo se o resto também deveria ser bloqueado, ou não. Para isso, é só clicar no botão ***Bloquear tudo*** abaixo da lista. Ou, você pode usar o botão ***Padrão*** para cancelar todas as alterações de configuração executadas, e para retornar à configuração original.

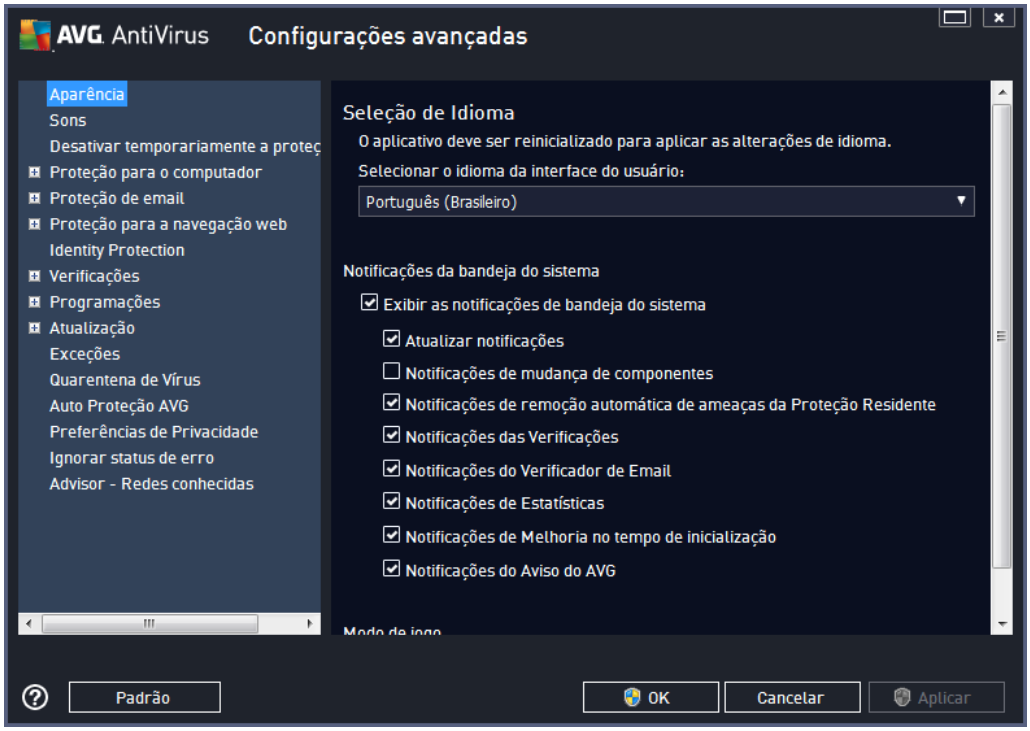
- ***Notificar websites...*** – nessa sessão você pode ligar/desligar a opção ***Notifique os websites que eu não desejo ser rastreado*** *(ativada por padrão).* Mantenha essa opção marcada para confirmar que você deseja que o ***Do Not Track*** informe o provedor de um serviço de coleta de dados detectado que você não deseja ser rastreado.

9. Configurações avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG AntiVirus 2014** 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.

9.1. Aparência

O primeiro item na árvore de navegação, ***Aparência***, refere-se às configurações gerais da interface de usuário do **AVG AntiVirus 2014** e fornece algumas opções básicas do comportamento do aplicativo:



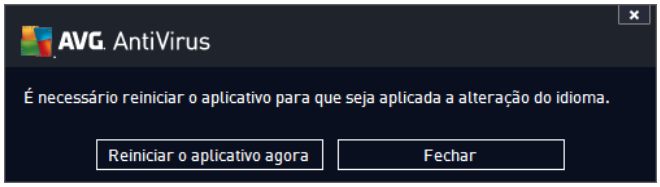
Seleção de idioma

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 AntiVirus 2014**. 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 AntiVirus 2014**, é necessário reiniciar o aplicativo. Por favor siga esses passos:

- 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 AntiVirus 2014**

- 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:

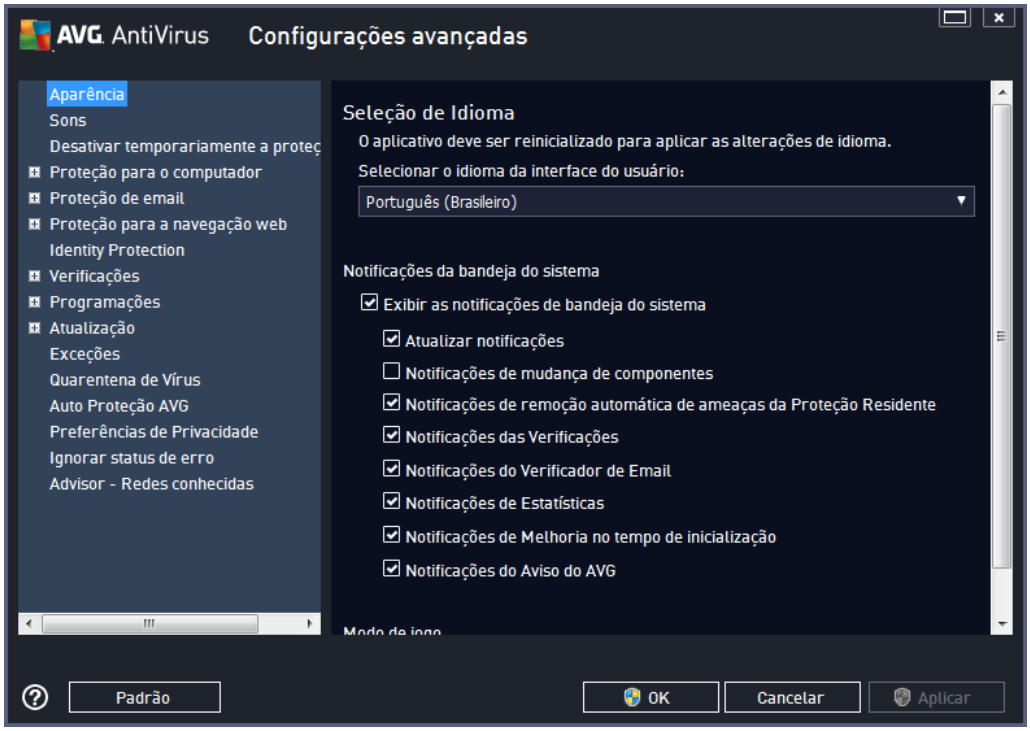


Notificações da bandeja do sistema

Nesta seção, é possível ocultar as notificações na bandeja do sistema sobre o status do aplicativo **AVG AntiVirus 2014**. Por 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 AntiVirus 2014**. 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 AntiVirus 2014)*, poderá definir e especificar suas preferências marcando/desmarcando as seguintes opções:

- ***Exibir as notificações de bandeja do sistema*** *(ativada por padrão)* – todas as notificações são exibidas por 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 por padrão)* – decide se as informações relacionadas ao **AVG AntiVirus 2014** início, andamento ou à finalização do processo de atualização do devem ser exibidas.

- ***Notificações de mudança dos componentes*** *(desativada, por padrão)* – decide se devem ser exibidas informações referentes à atividade/inatividade de componentes ou a problemas potenciais. Ao relatar o status de falha de um componente, esta opção é equivalente à função informativa do ícone na bandeja do sistema, informando um problema em qualquer componente do **AVG AntiVirus 2014**.

- ***Notificações de remoção automática de ameaças da Proteção Residente*** *(ativada por 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 por padrão)* – decide se devem ser exibidas as informações sobre o início automático da verificação agendada, seu andamento e resultados.

- ***Notificações do Verificador de Email*** *(ativada por padrão)* – decide se as informações sobre a verificação de todas as mensagens de email de entrada e saída devem ser exibidas.

- ***Notificações de estatísticas*** *(ativada por padrão)* – mantenha a opção selecionada para permitir que notificações regulares de análises estatísticas sejam exibidas na bandeja do sistema.

- ***Notificações de Melhoria no tempo de inicialização*** *(desativada por padrão)* – decide se você deseja ser informado sobre a aceleração do tempo de inicialização

do seu computador.

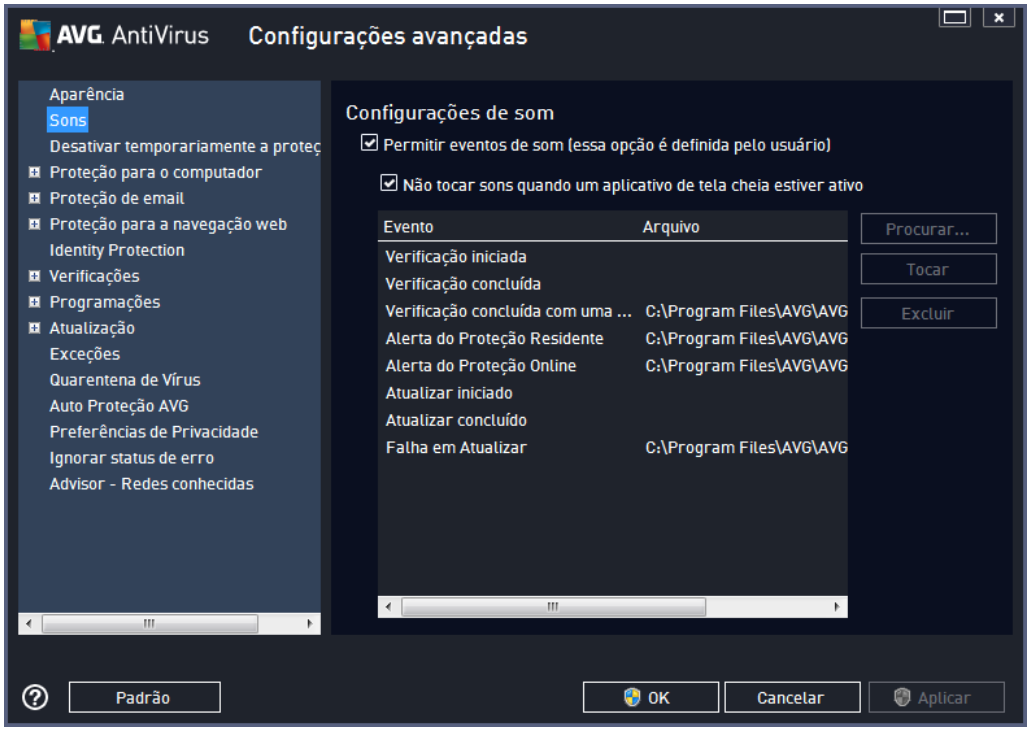
- ***Notificações do AVG Advisor*** *(ativado por padrão)* – decide as informações sobre as atividades do AVG Advisor devem ser exibidas no painel deslizante da bandeja do sistema.

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*).

9.2. Sons

Na caixa de diálogo ***Configurações de som***, é possível especificar se deseja receber informações sobre ações especificas do **AVG AntiVirus 2014** por meio de uma notificação sonora:



As configurações são válidas somente para o usuário de conta atual, ou seja, cada usuário do computador pode ter suas próprias configurações 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)*.

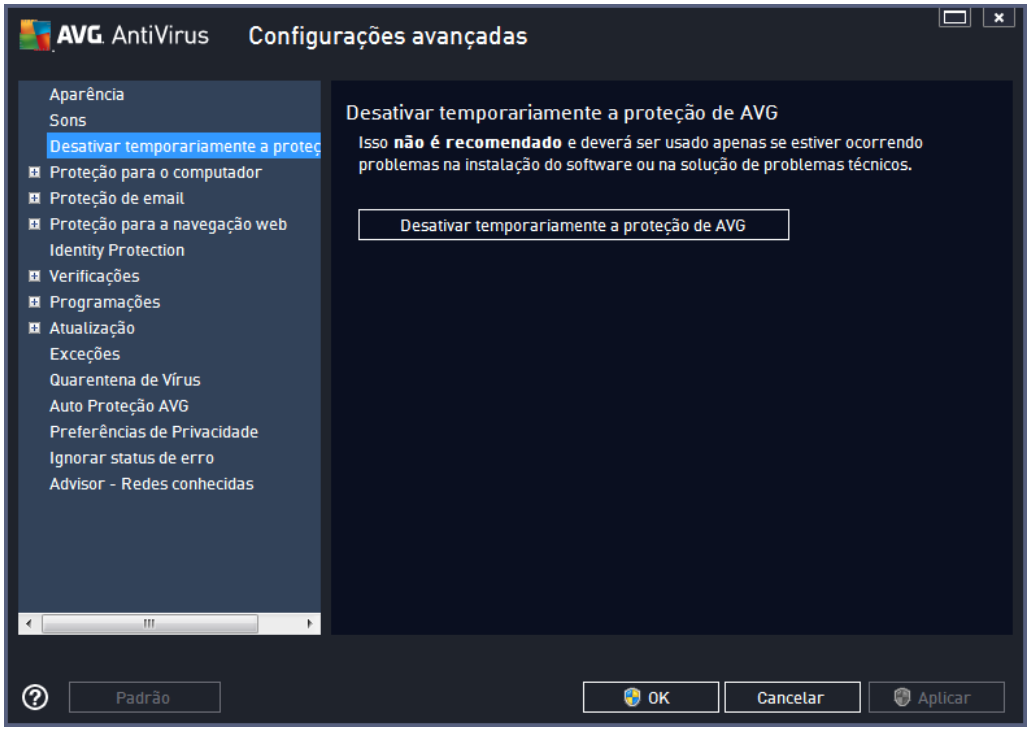
Botões de controle

- ***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.

9.3. 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 AntiVirus 2014** de uma vez.

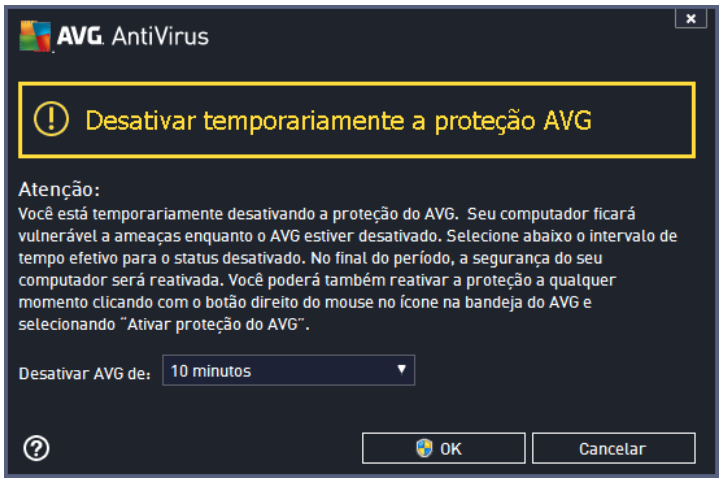
Lembre-se de que você não deve usar essa opção, a menos que ela seja absolutamente necessária!



Na maioria dos casos, ***não é necessário*** desativar o **AVG AntiVirus 2014** antes de instalar novo software ou novos drivers, nem mesmo se o instalador ou assistente de software sugerir que programas e aplicativos em execução devem ser encerrados primeiro para garantir que não haja interrupções indesejadas durante o processo de instalação. Caso você tenha problemas durante a instalação, tente desativar a proteção residente (*Habilitar Proteção Residente*) primeiro. Se for necessário desativar temporariamente o **AVG AntiVirus 2014**, 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

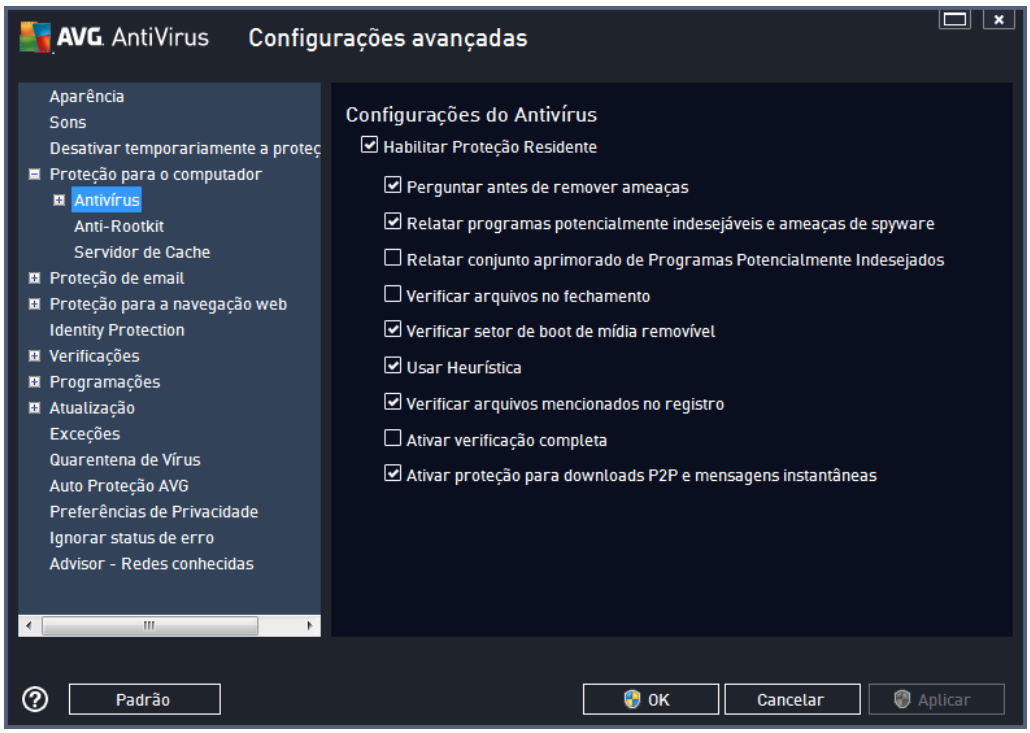
Marque a caixa de seleção ***Desativar temporariamente a proteção AVG*** e confirme sua opção, pressionando o botão ***Aplicar***. Na caixa de diálogo recém aberta, ***Desativar temporariamente a proteção AVG***, especifique por quanto tempo você deseja manter o **AVG AntiVirus 2014** desativado. Por padrão, a proteção ficará desativada por 10 minutos, o que deve ser suficiente para qualquer tarefa comum, como instalação de novo software etc. Você pode decidir um período de tempo mais longo, no entanto essa opção não é recomendada se não for absolutamente necessária. Depois, todos os componentes desativados serão ativados automaticamente. No máximo, é possível desativar a proteção do AVG até a próxima reinicialização do computador.



9.4. Proteção para o computador

9.4.1. Antivírus

O ***Antivírus*** junto com a ***Proteção Residente*** protegem seu computador de forma contínua 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 por padrão*). Além disso, você pode selecionar os recursos da proteção residente que devem ser ativados:

- ***Perguntar antes de remover ameaças*** (*ativado por 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 AntiVirus 2014** irá recuperar automaticamente a infecção e, se não for possível, o objeto será movido para a Quarentena de Vírus.

- ***Relatar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois ele aumenta a segurança do computador.

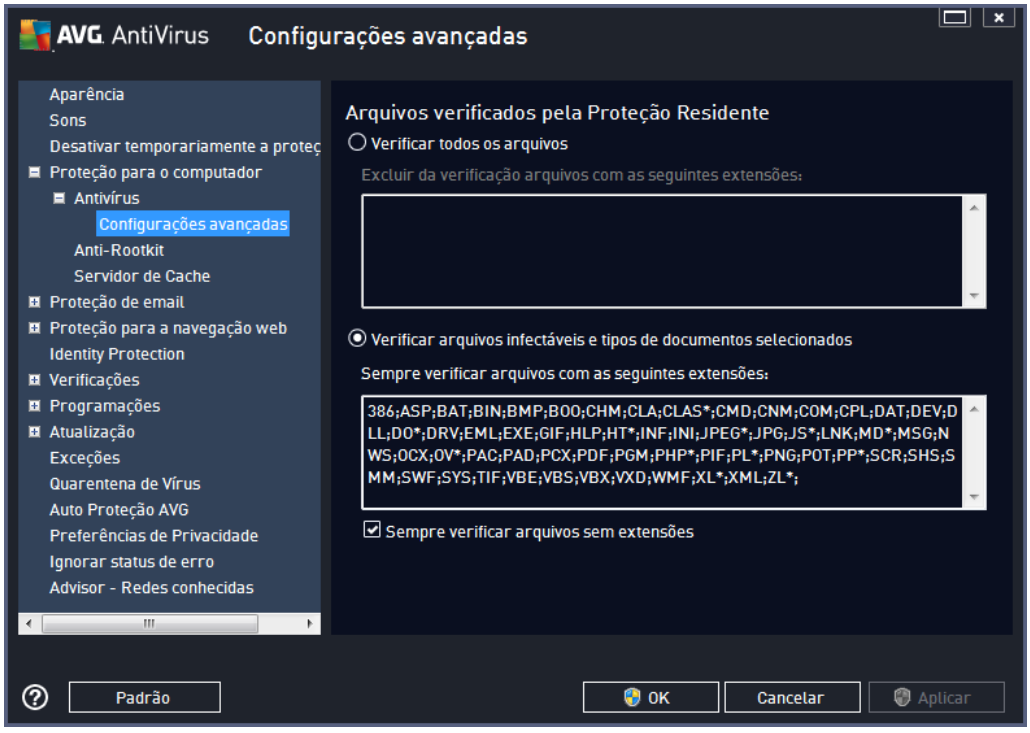
- ***Relatar conjunto aprimorado de programas potencialmente indesejáveis*** (*desativada por padrão*) – marque para detectar os pacotes estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar arquivos no fechamento*** (*desativado por 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*** (*ativada por padrão*)
- ***Usar Heurística*** (*ativado por padrão*) – a análise heurística será usada para detecção (*emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual*).
- ***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 consome bastante tempo.
- ***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, ...*) 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.

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

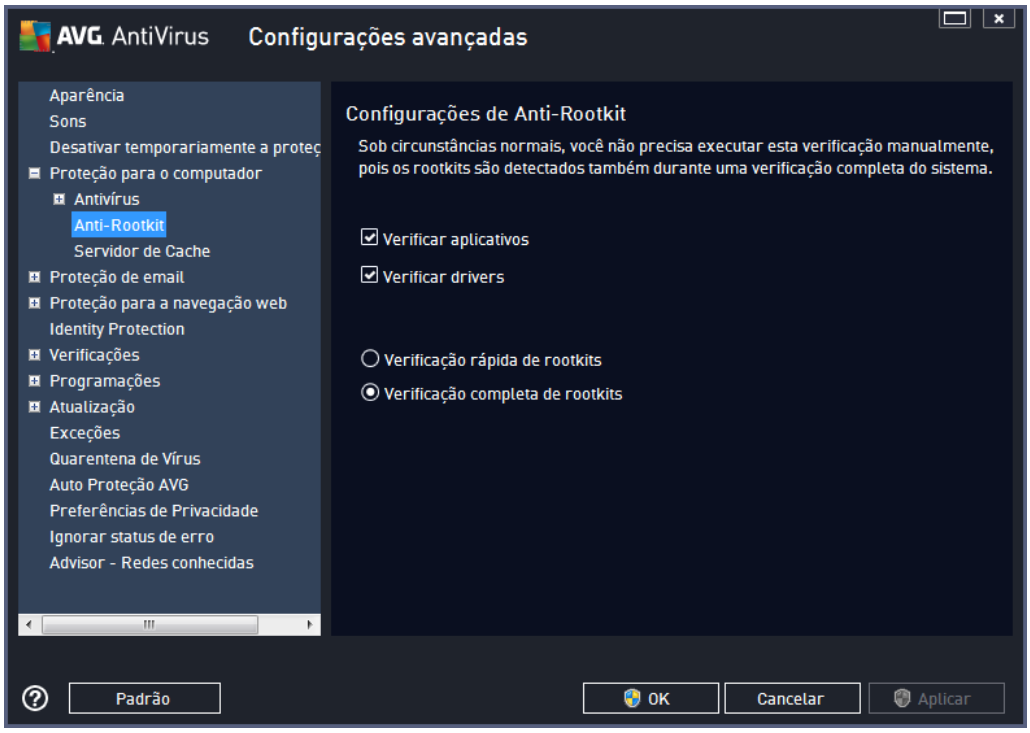


Marque a caixa de seleção respectiva para decidir se deseja ***Verificar todos os arquivos*** ou ***Verificar arquivos infectáveis e tipos de documentos selecionados*** somente. Para acelerar a verificação e fornecer o nível máximo de proteção, recomendamos manter as configurações padrão. Desta forma, 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.

9.4.2. 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:

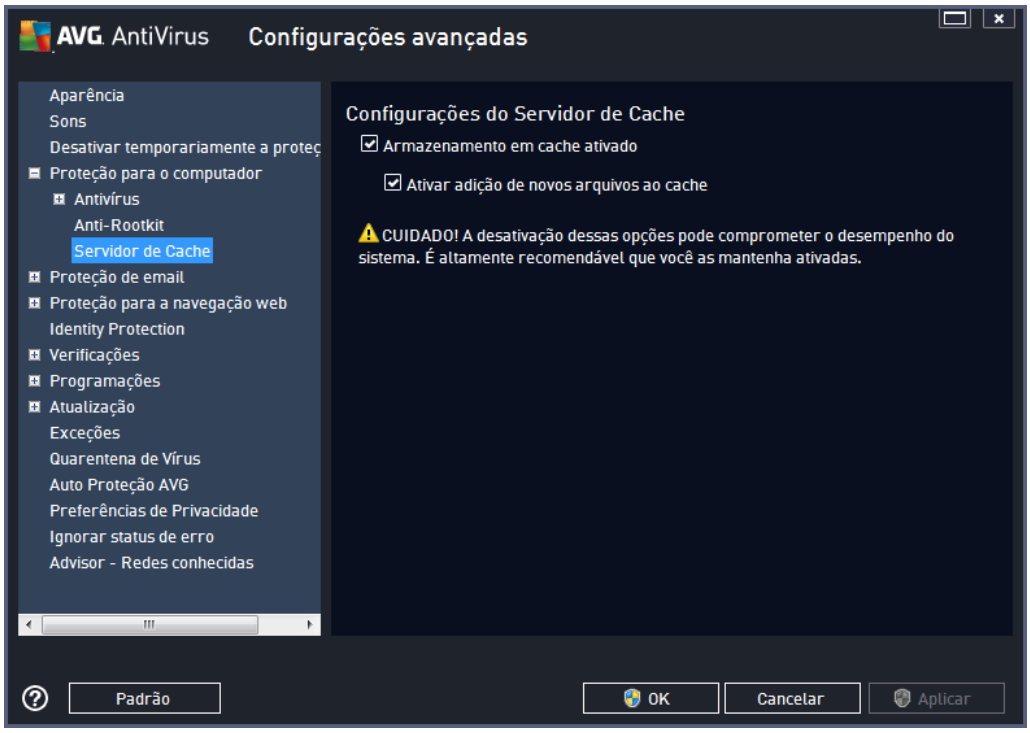


A Verificação de aplicativos e a ***Verificação de drivers*** permitem que você especifique em detalhes o que deve ser incluído na verificação Anti-Rootkit. Essas configurações são direcionadas a usuários avançados; recomendamos que você mantenha todas as opções ativadas. Você também pode selecionar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

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

9.4.3. 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 AntiVirus 2014**:



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:

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

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

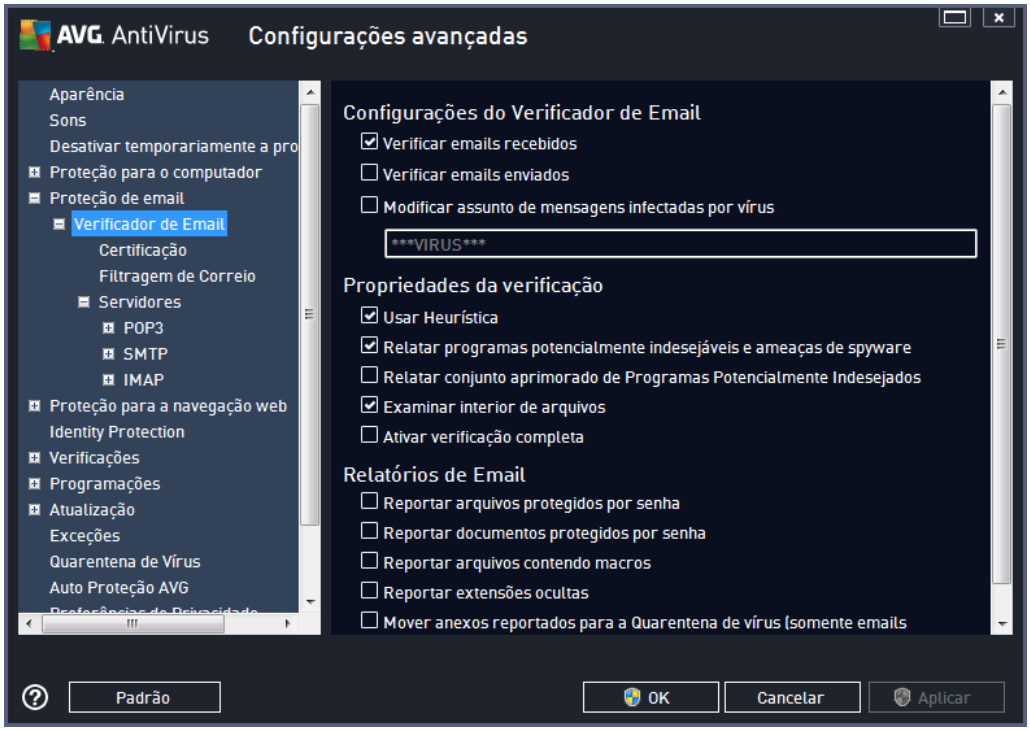
A menos que você tenha um bom motivo para desativar o servidor de cache, recomendamos manter as configurações padrão e deixar as opções ativadas! Caso contrário, você poderá sentir uma redução significativa na velocidade e no desempenho de seu sistema.

9.5. Verificador de Email

Nessa seção, é possível editar configurações detalhadas do Verificador de Email e do Anti-Spam:

9.5.1. Verificador de Email

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



Verificando 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 infecciosa, 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 correio.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) – marque para detectar os pacotes estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar dentro de arquivos*** (*ativada por padrão*) – marque para verificar os conteúdos de arquivos anexados às mensagens de 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 consome bastante tempo.

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

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

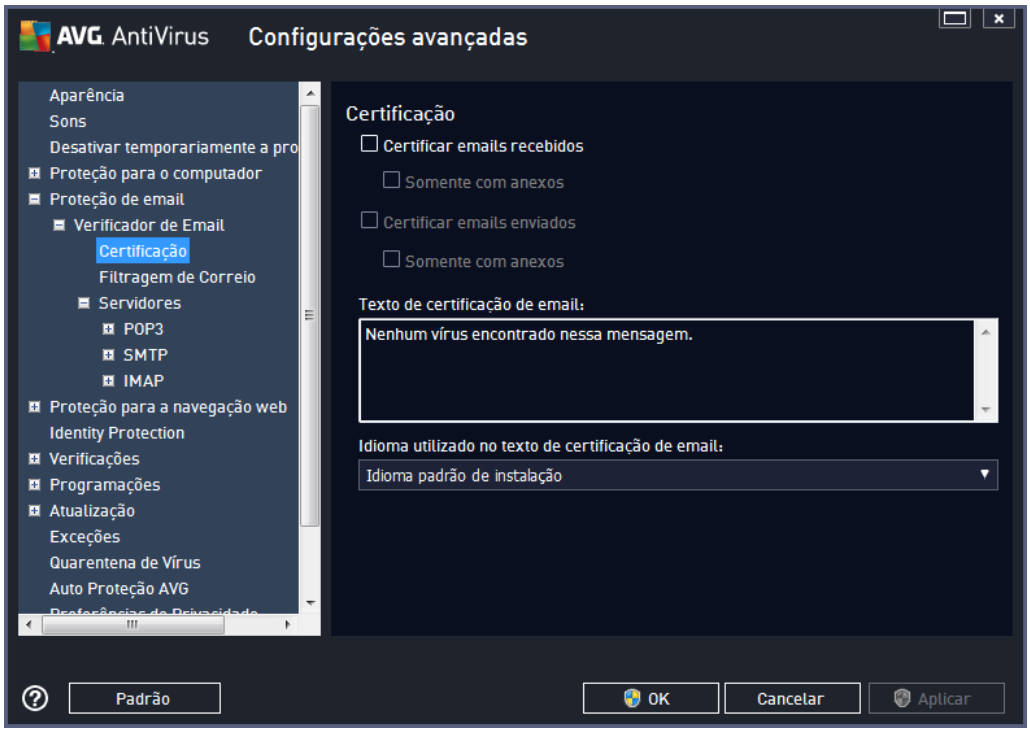
- ***Reportar arquivos contendo macros*** – uma macro é uma sequência predefinida de etapas com o objetivo de executar certas tarefas mais fáceis para um usuário (*as macros de MS Word são amplamente conhecidas*). Dessa forma, uma macro pode conter instruções potencialmente perigosas e convém você marcar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

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

potencialmente perigosos.

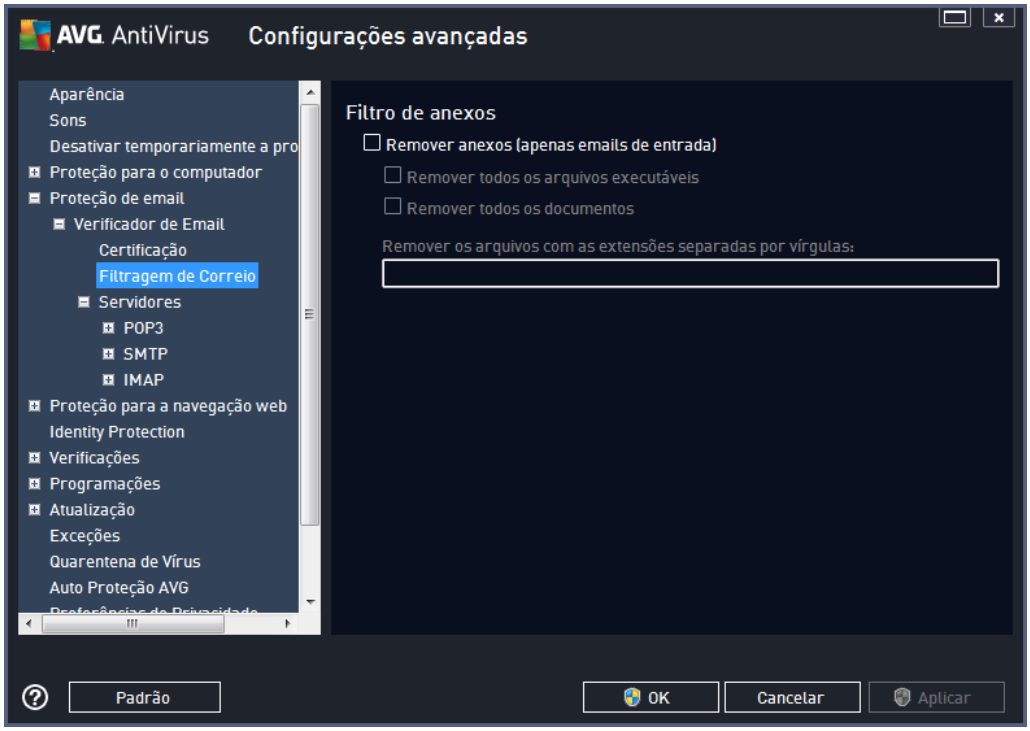
- ***Mover anexos de email relatados para a área de Quarentena*** – especifique se você deseja ser notificado por email sobre arquivos protegidos por senha, documentos protegidos por senha, arquivos contendo macros e/ou arquivos com extensão oculta detectados como um anexo de uma mensagem de email verificada.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

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:



Por padrão, o texto de certificação consiste em informações básicas com o aviso *Nenhum vírus encontrado nesta 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.*



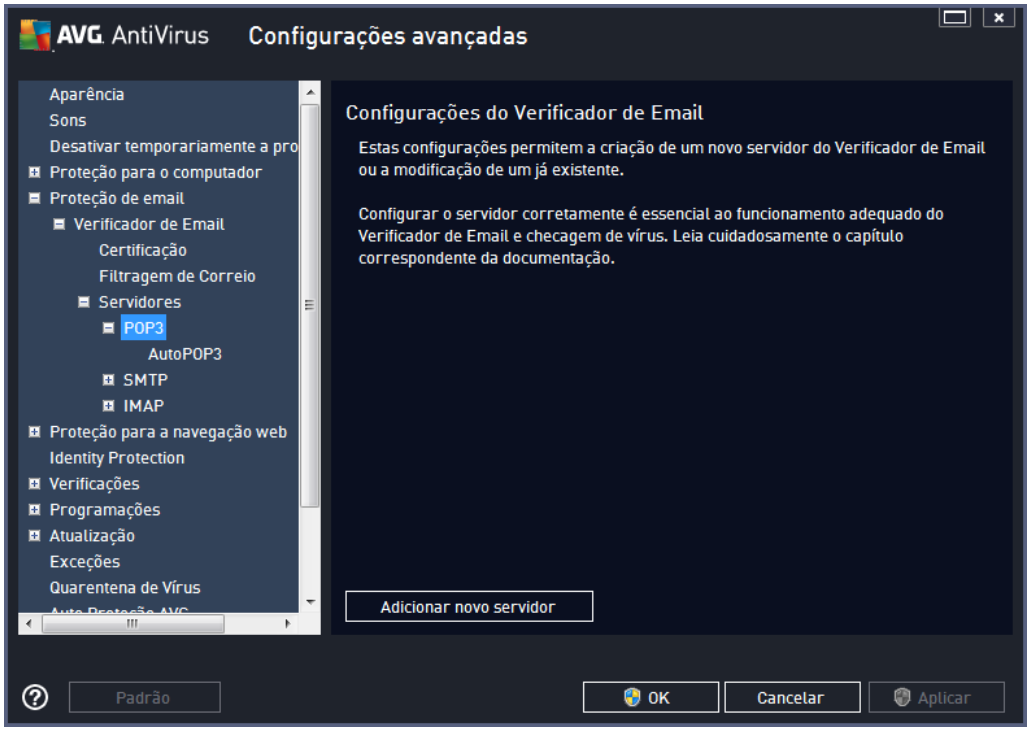
A caixa de diálogo ***Filtro de anexos*** permite definir os parâmetros da verificação dos anexos das mensagens de email.Por padrão, a opção ***Remover anexos*** está desativada. Se decidir ativá-la, todos os anexos de mensagem de email detectados como infectados ou potencialmente perigosos serão removidos automaticamente. Se você desejar especificar os tipos de anexo que devem ser removidos, selecione a opção apropriada:

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

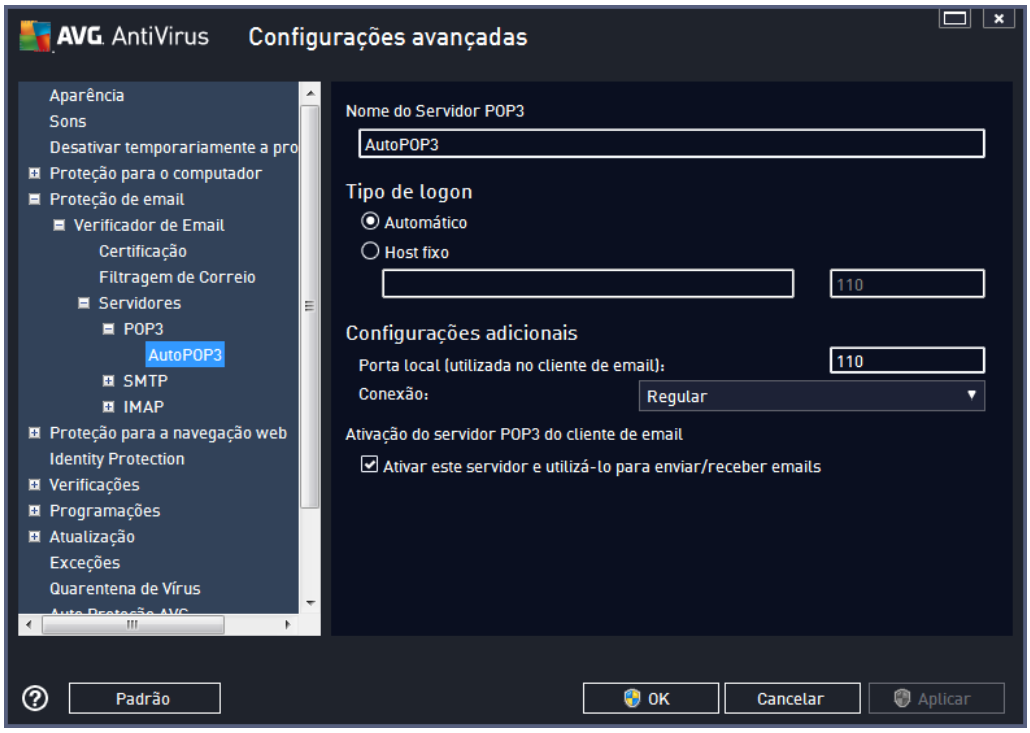
Na seção ***Servidores***, você pode editar parâmetros dos servidores do Verificador de Email:

- POP3
- SMTP
- IMAP

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



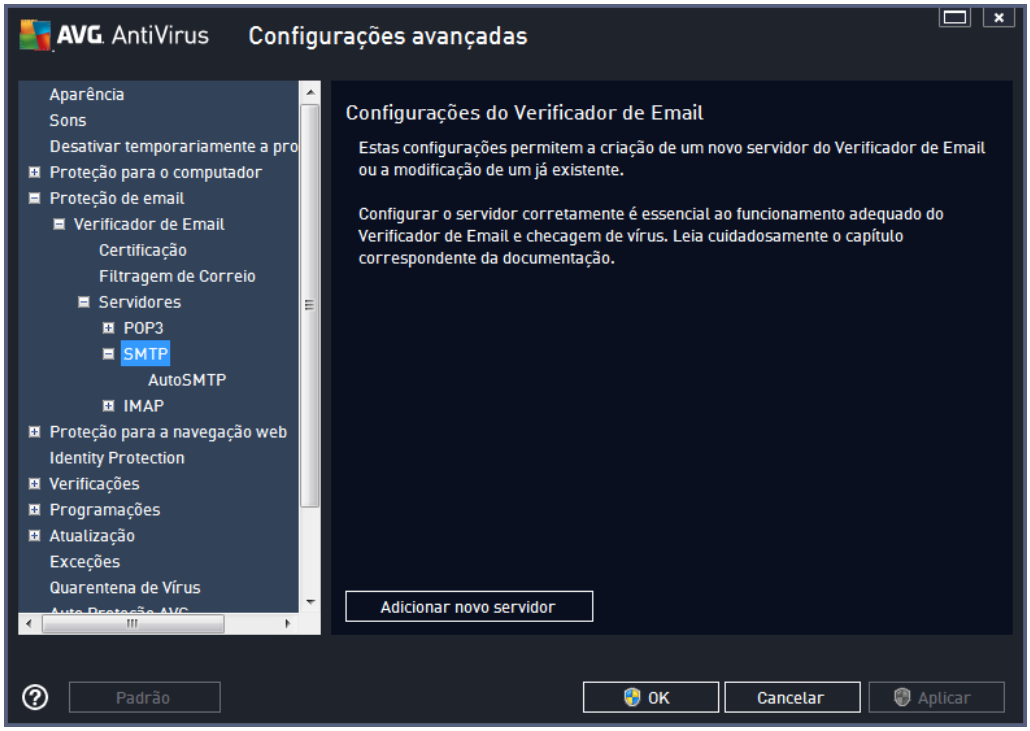
Nessa caixa de diálogo, você pode configurar um novo servidor do Verificador de Email usando o protocolo POP3 para emails recebidos:



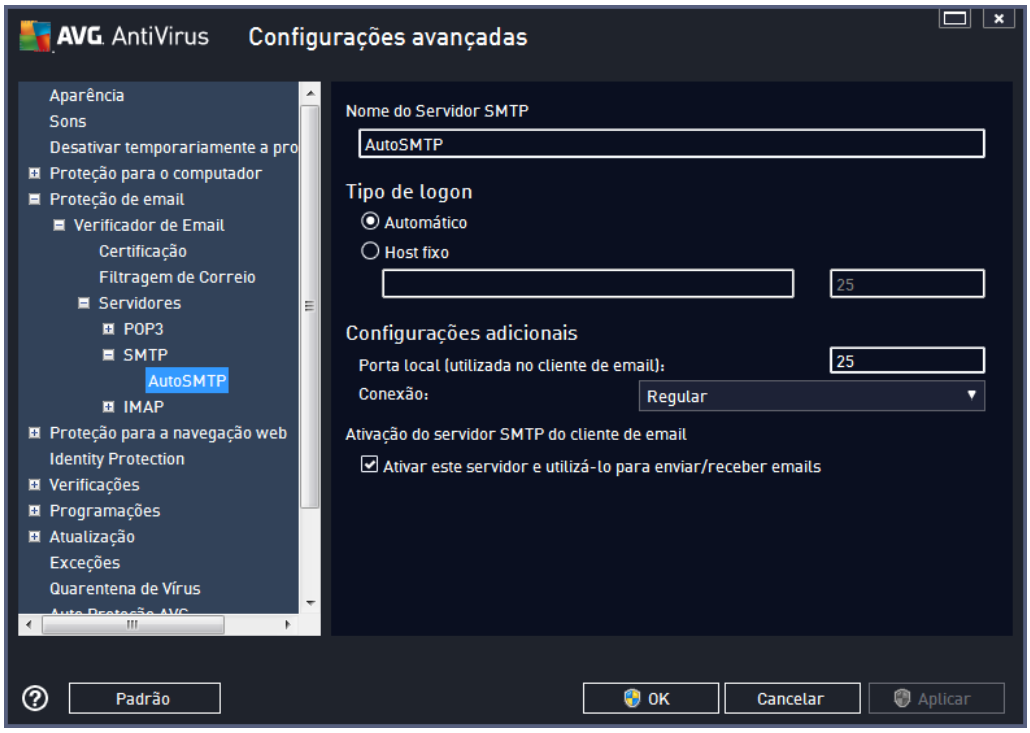
- ***Nome do Servidor POP3*** – neste campo, é possível especificar o nome dos servidores

recém-adicionados (*para adicionar um servidor POP3, clique com o botão direito do mouse sobre o item POP3 do menu de navegação esquerdo*). Para os servidores "AutoPOP3" criados automaticamente, este campo fica desativado.

- ***Tipo de login*** – 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 sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de email. O nome de login permanecerá inalterado. Para um nome, você pode usar um nome de domínio (*por exemplo, pop. acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*). Se o servidor de 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 você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso estará disponível somente quando houver suporte no servidor de email de destino.
- ***Ativação do servidor POP3 do cliente de email*** – marque/desmarque esse item para ativar ou desativar o servidor POP3 especificado



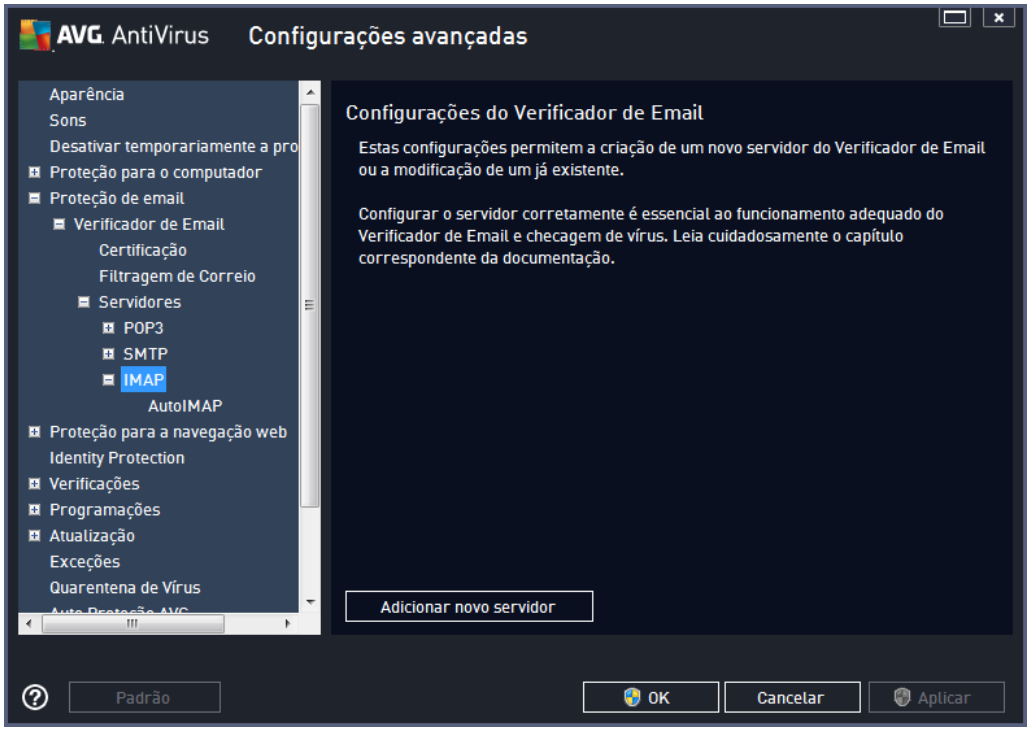
Nessa caixa de diálogo, você pode configurar um novo servidor do Verificador de Email usando o protocolo SMTP para mensagens enviadas:



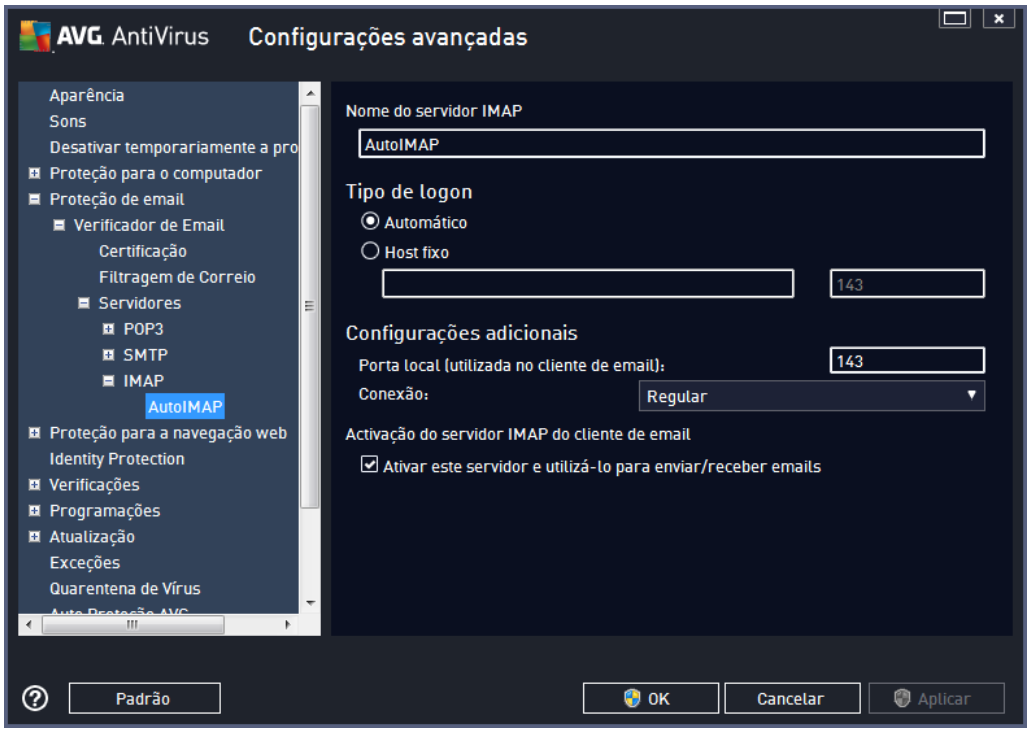
- ***Nome do Servidor SMTP*** – neste campo, é possível especificar o nome dos servidores

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*) para um 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 25 é.
- ***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*** – no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso está disponível somente quando houver suporte no servidor de 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:



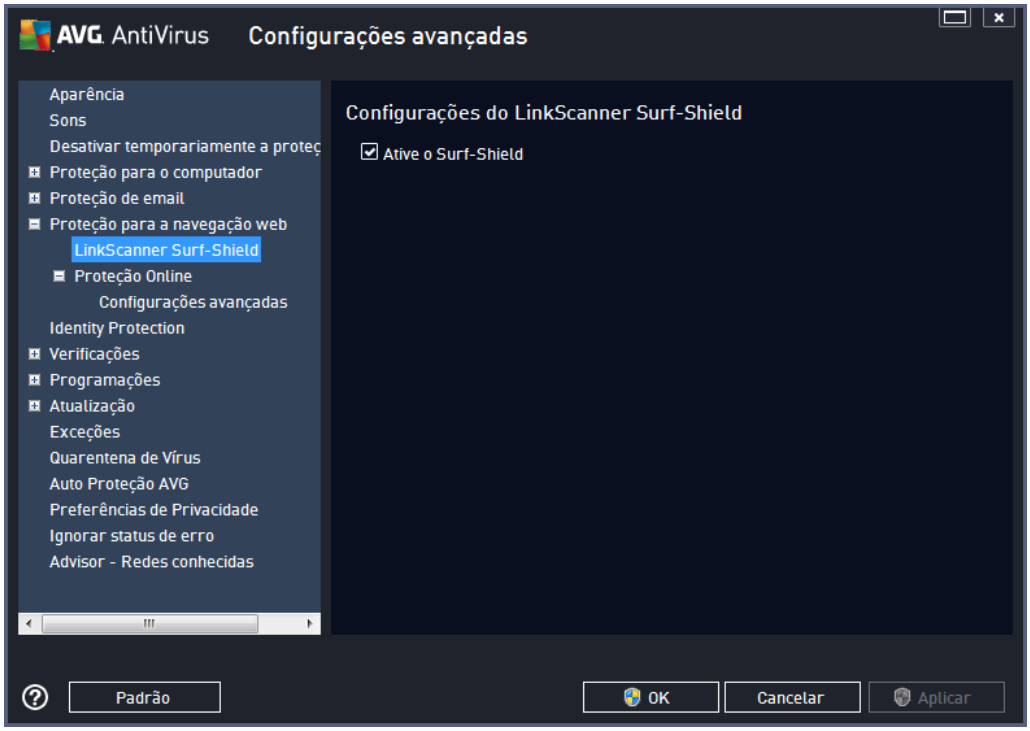
- ***Nome do Servidor IMAP*** – neste campo, é possível especificar o nome dos servidores

recém-adicionados (*para adicionar um servidor IMAP, clique com o botão direito do mouse sobre o item IMAP do menu de navegação esquerdo*). Para os servidores "AutoIMAP" criados 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*) para um 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 usada em*** – 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

9.6. Proteção de navegação da Web

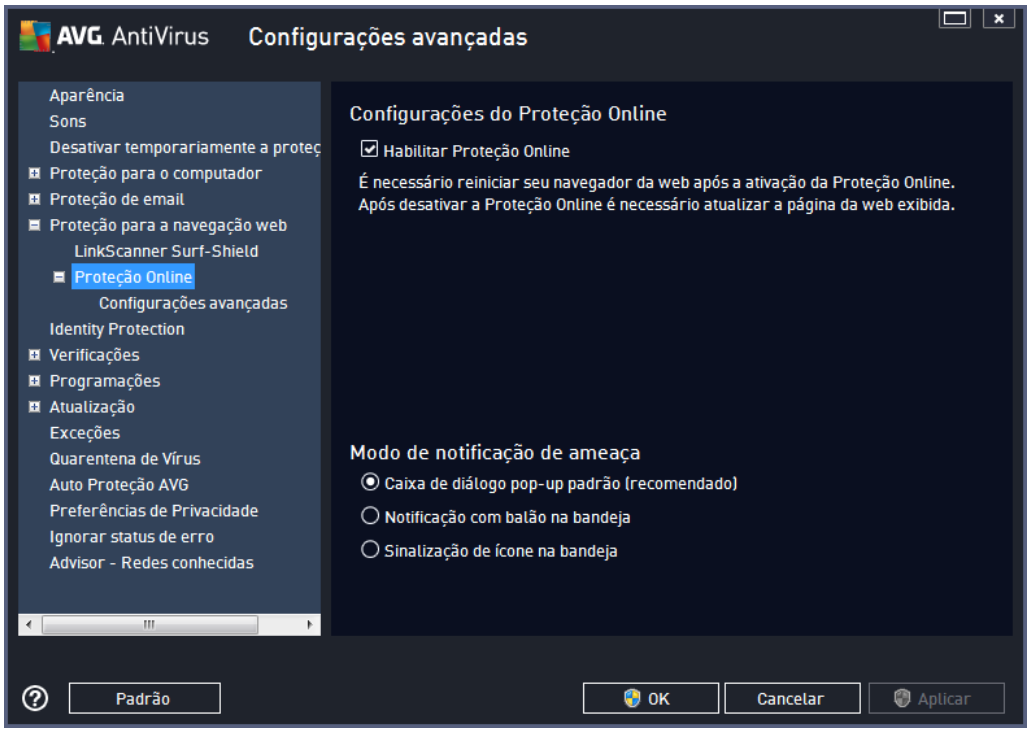
O diálogo de ***configurações do LinkScanner*** permite marcar/desmarcar os seguintes recursos:



- ***Ative o Surf-Shield*** – (*ativo por 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*).

- ***Adicione "Protegido por LinkScanner"*** – (*como padrão desligado*): marque essa opção para garantir que todas as mensagens enviadas das redes sociais Facebook / MySpace e que contenham hyperlinks ativos sejam certificadas como verificadas pelo LinkScanner.

9.6.1. Proteção Online

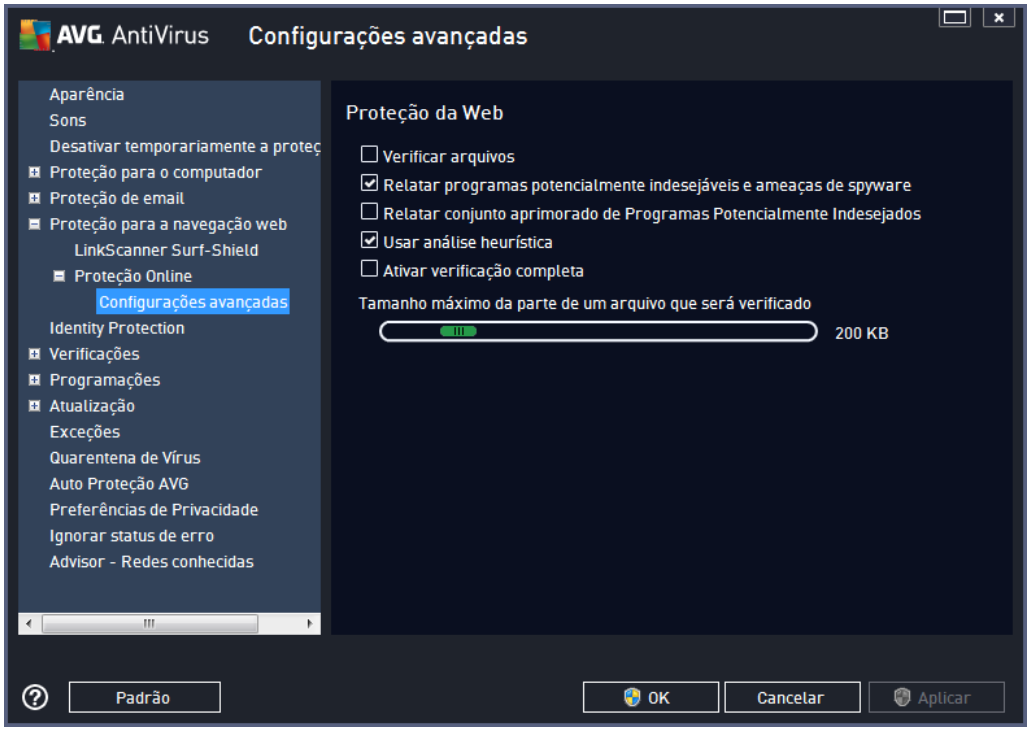


O diálogo ***Proteção Online*** oferece as seguintes opções:

- ***Habilitar Proteção Online*** *(ativado por 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.

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:

- ***Ativar Proteção da Web*** – essa opção confirma que a ***Proteção Online*** deve realizar a verificação do conteúdo das páginas www. Desde que essa proteção esteja ativada (*padrão*), você também pode ligar/desligar esses itens:
    - ***Verificar arquivos*** – (*desativada por padrão*): verifique o conteúdo dos arquivos possivelmente incluídos na página www 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 ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.
    - ***Relatar conjunto aprimorado de programas potencialmente indesejáveis*** – (*desativada por padrão*): marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, portanto, é desativada por padrão.
    - ***Usar análise heurística*** – (*ativada por padrão*): verifique o conteúdo da página a ser exibida usando o método de análise heurística (*emulação dinâmica das instruções*

do objeto verificado em um ambiente de computador virtual).

- **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 consome bastante tempo.

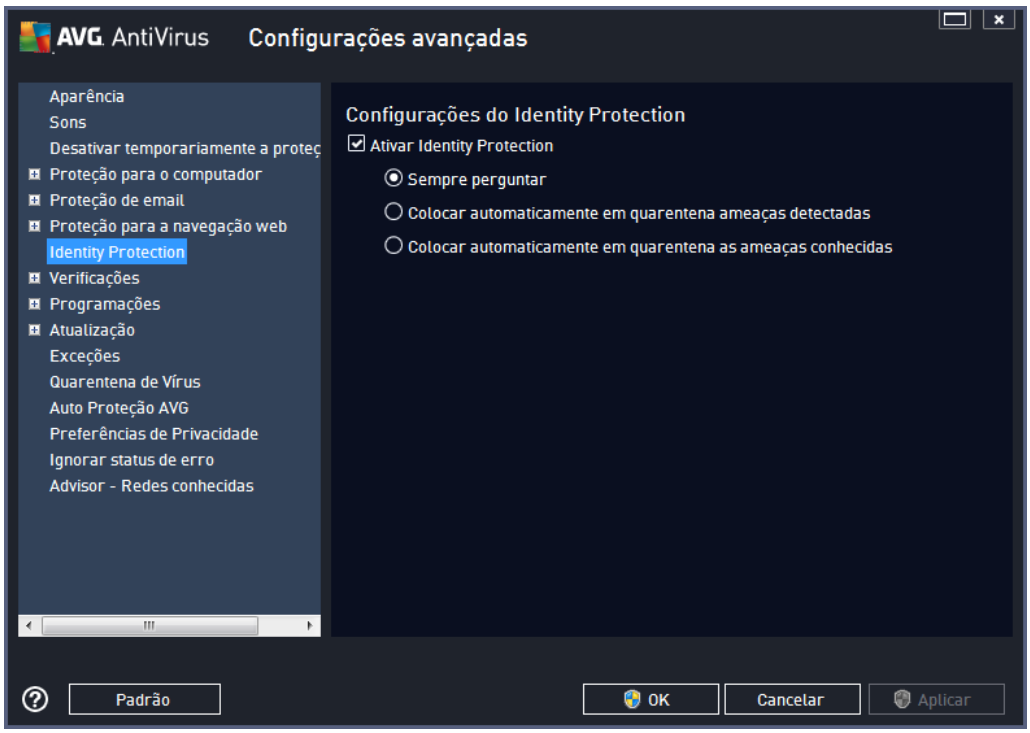
- **Tamanho máximo de um arquivo a ser verificado** – se os arquivos incluídos estiverem presentes na página exibida, você também poderá verificar o conteúdo deles, mesmo antes que serem baixados para seu computador. Entretanto, a verificação de arquivos grandes pode levar tempo e o download da página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

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

9.7. Identity Protection

O **AVG Identity** é um componente anti-malware que o protege de todos os tipos de malware (*spyware, robôs, roubo de identidade...*) usando tecnologias comportamentais e que fornece proteção imediata contra novos vírus *(para obter uma descrição detalhada das funcionalidades dos componentes, consulte o capítulo Proteção de Identidade*).

A caixa de diálogo **Configurações do Identity Protection** permite ativar/desativar os recursos elementares do componente Identity Protection:



Ativar Identity (*ativada por padrão*) – desmarque para desativar o componente Identity Protection.

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

Quando o Identity Protection está ativado, você pode especificar o que fazer quando uma ameaça é detectada:

- ***Perguntar sempre*** (*ativado por padrão*) – quando uma ameaça for detectada, será perguntado se deseja movê-la para a quarentena para assegurar que aplicativos que você deseja executar não sejam removidos.
- ***Colocar 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*** – marque esse item se desejar que todos os aplicativos detectados como possíveis malware sejam movidos automaticamente e imediatamente para a Quarentena de Vírus.

9.8. Verificações

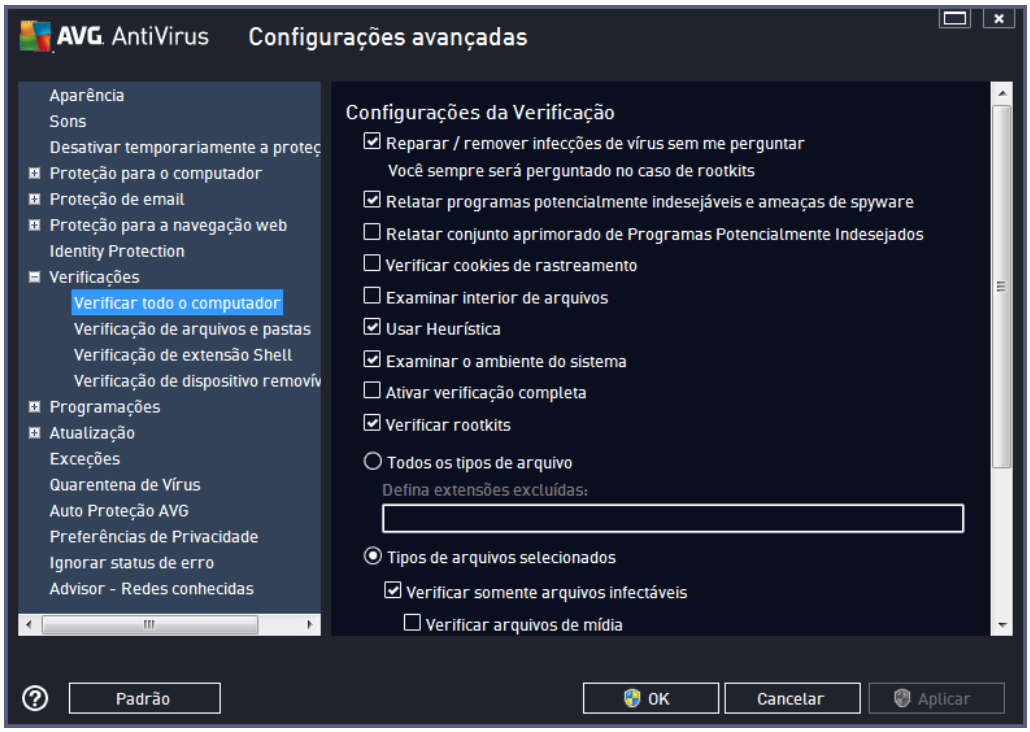
As configurações de verificação avançadas estão divididas em três categorias referentes a tipos específicos de verificação, conforme definido pelo fornecedor do software:

- 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

9.8.1. 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, poderá ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.
- ***Relatar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) – marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente.

Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Relatar conjunto aprimorado de programas potencialmente indesejados*** (*desativada 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 mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, 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 consome bastante tempo.

- ***Verificar rootkits*** (*ativado como padrão*) – a verificação Anti-Rootkit procura possíveis rootkits em seu computador, e.x. 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 pontos e vírgula*) dos arquivos de extensão que não devem ser verificados;

- ***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*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser

verificados.

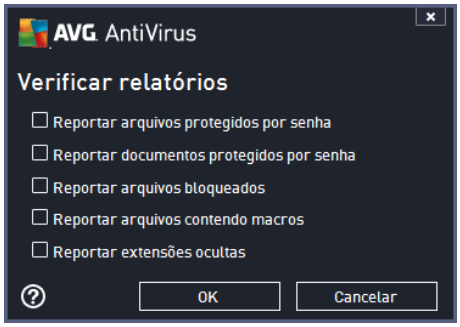
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensões*** – essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção ***Ajustar a velocidade de conclusão da verificação***, você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas 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.

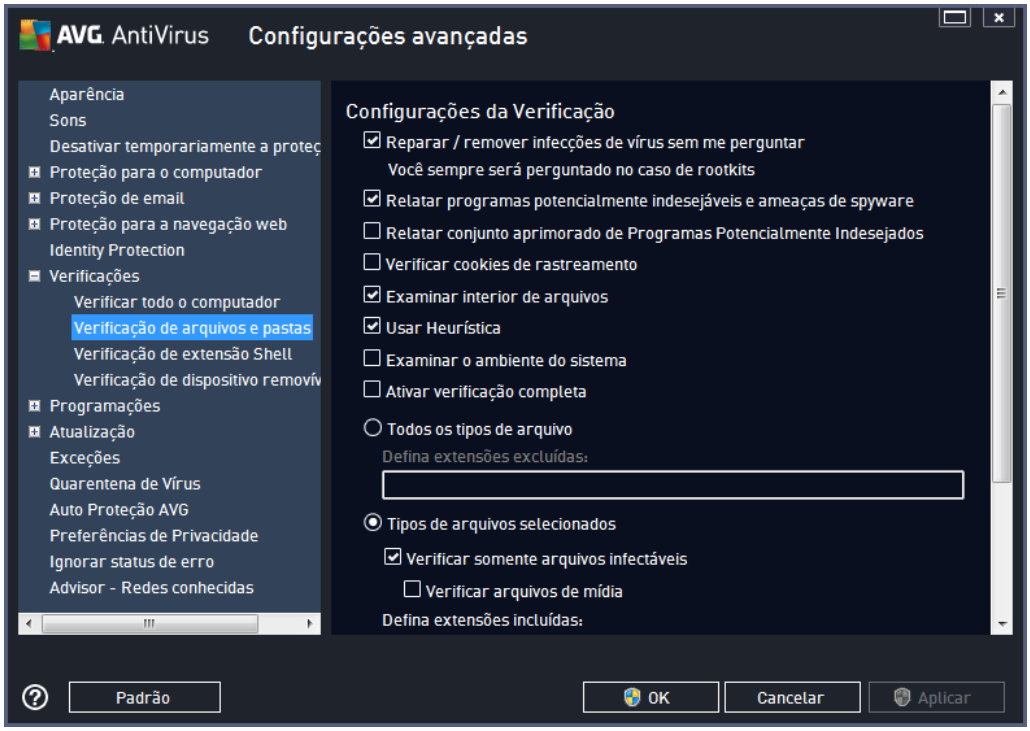
Defina relatórios de verificação adicionais...

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:



9.8.2. Verificação de arquivos e pastas

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

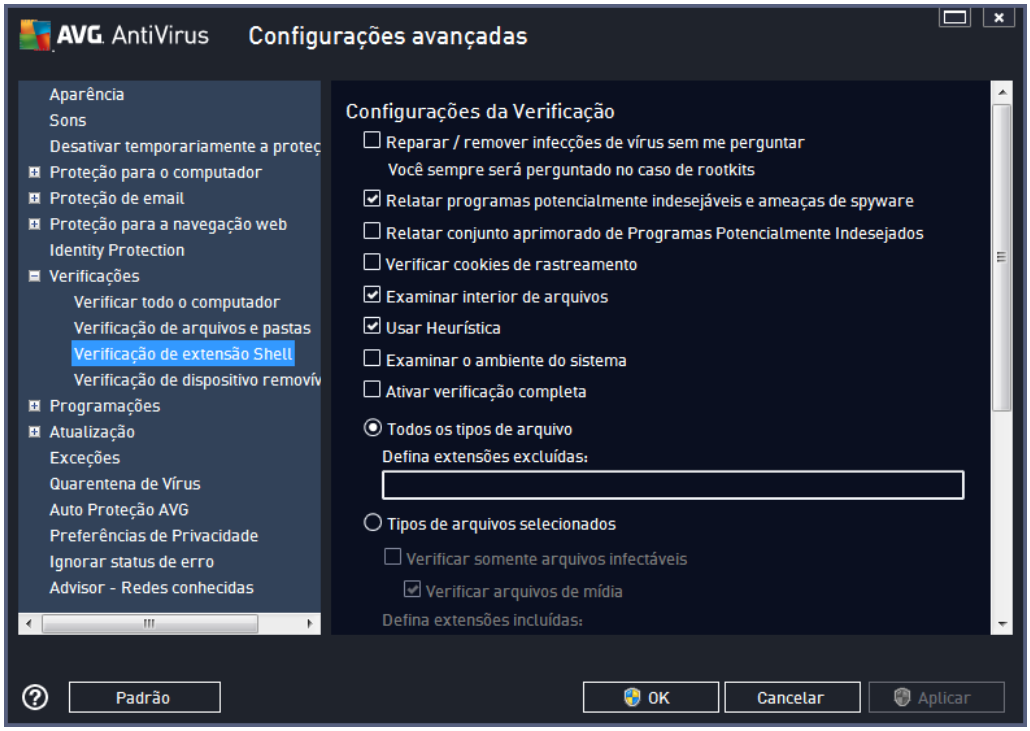


Todos os parâmetros definidos nesta caixa de diálogo de configuração aplicam-se apenas às áreas selecionadas para verificação com Verificar arquivos ou pastas!

Observação: *para obter uma descrição dos parâmetros específicos, consulte o capítulo Configurações avançadas do AVG/Verificações/Verificar todo o computador.*

9.8.3. 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:



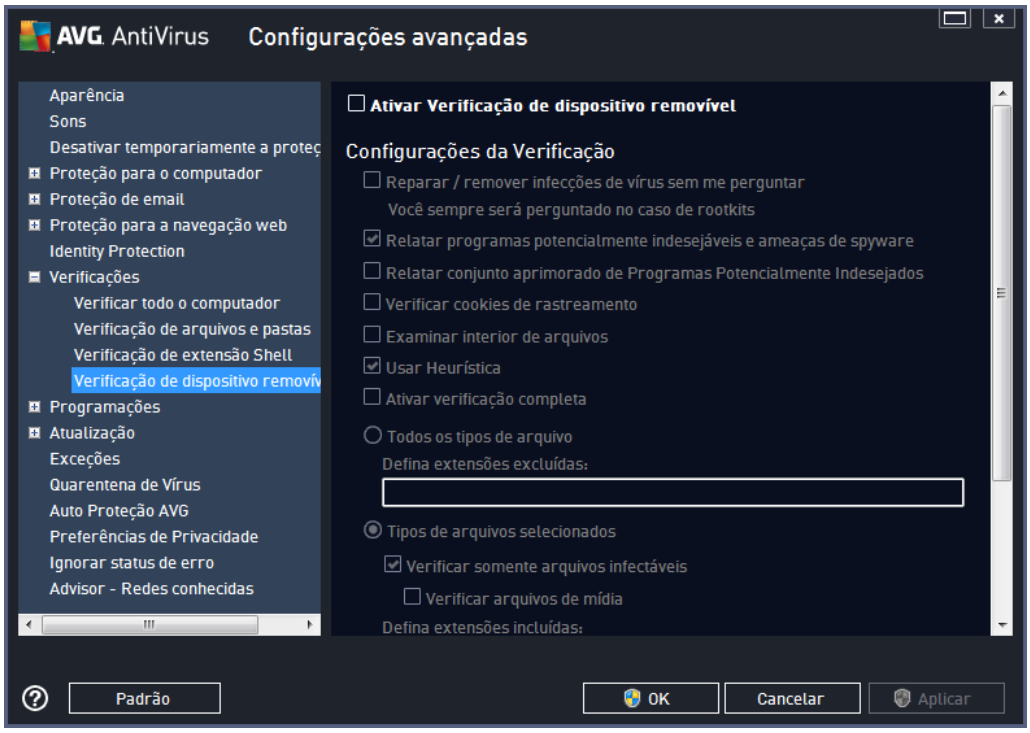
A lista de parâmetros é idêntica à disponível para Verificar todo o computador. Entretanto, as configurações padrão são diferentes (*por exemplo, Verificar todo o computador, por padrão, não verifica os arquivos, mas verifica o ambiente de sistema; com a Verificação da Extensão Shell, é ao contrário*).

Observação: *para obter uma descrição dos parâmetros específicos, consulte o capítulo Configurações avançadas do AVG/Verificações/Verificar todo o computador.*

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

9.8.4. Verificação de Dispositivo Removível

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



A ***Verificação de dispositivo removível*** é ativada automaticamente quando você conecta um dispositivo removível ao computador. 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***.

Observação: *para obter uma descrição dos parâmetros específicos, consulte o capítulo Configurações avançadas do AVG/Verificações/Verificar todo o computador.*

9.9. Programações

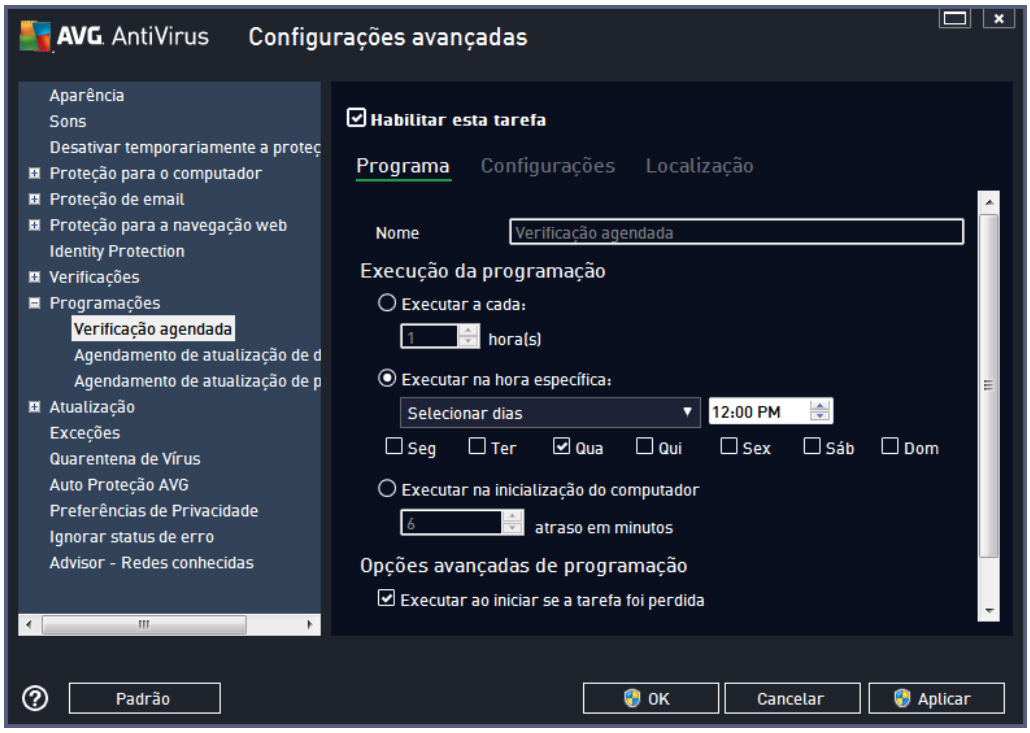
Na seção ***Agendamentos***, é possível editar as configurações padrão de:

- Verificação programada
- Agendamento de atualização de definições
- Programação de atualização de programa

9.9.1. Verificação programada

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

necessário:



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 programada*** *na área de navegação esquerda*), você pode especificar o seu próprio nome e, nesse caso, o campo de texto ficará aberto para edição. Tente sempre usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

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

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

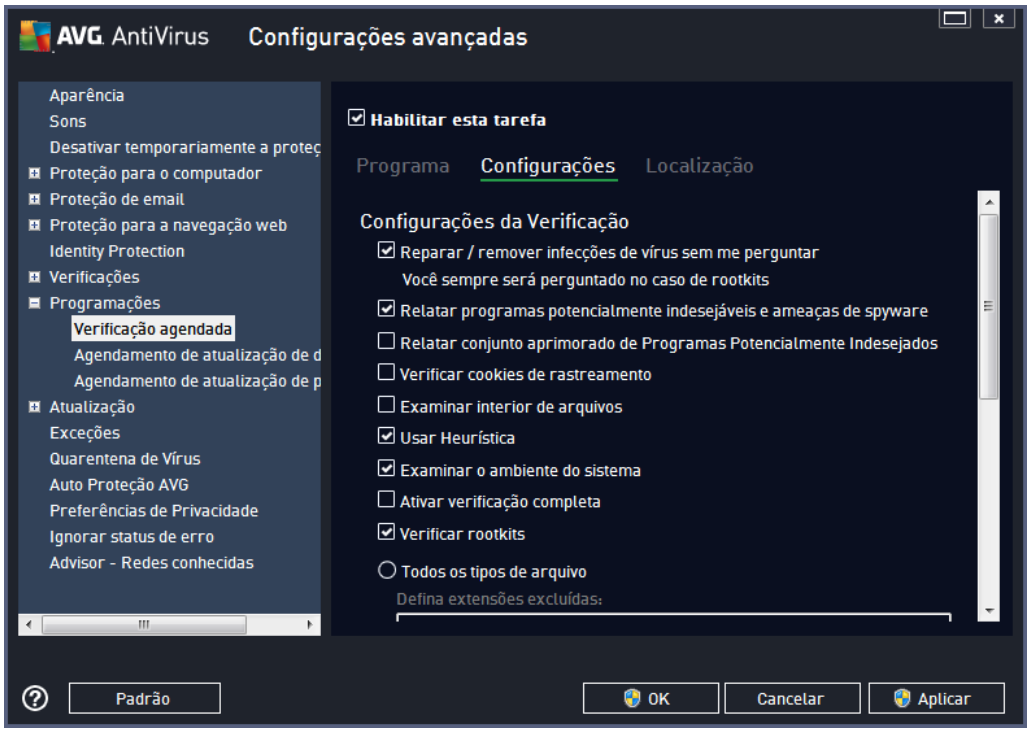
Execução da programação

Aqui, você pode especificar intervalos de tempo para a ativação da verificação recém-programada. O tempo pode ser definido pela repetição da execução da verificação depois de um determinado período (***Executar a cada ...***), pela definição de uma data e hora exatas (***Executar em uma 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 AVG na bandeja do sistema.

Um novo ícone AVG na bandeja do sistema aparece (*em cores e com um holofote*) informando que uma verificação agendada está em execução. Clique com o botão direito do mouse no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e também alterar a prioridade da verificação em execução.



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

- ***Reparar ou remover o vírus sem me consultar*** *(ativada por padrão):* se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** *(ativada como padrão):* marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente.

Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Relatar conjunto aprimorado de Programas Potencialmente Indesejados*** (*desativada 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 mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, 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 consome bastante tempo.

- ***Verificar rootkits*** *(ativada como padrão): a verificação* Anti-Rootkit procura possíveis rootkits em seu computador, e.x. 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 pontos e vírgula*) dos arquivos de extensão que não devem ser verificados;

- ***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*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

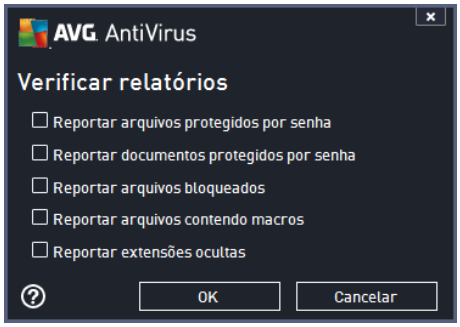
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensões*** – essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção 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:



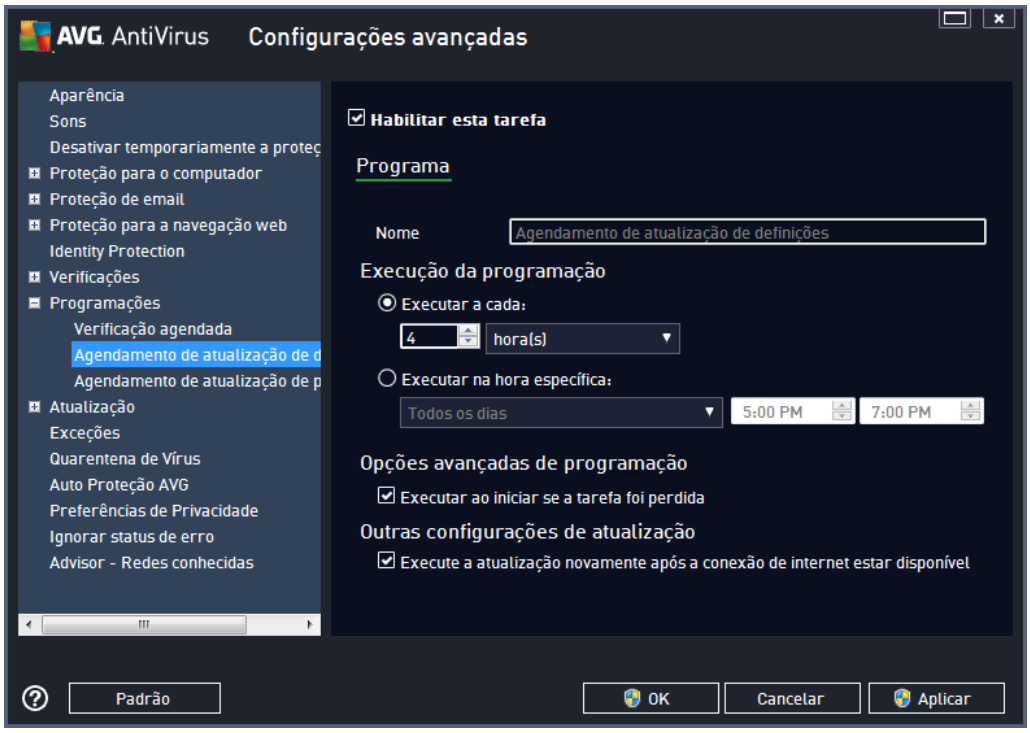
Opções de desligamento do computador

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.

9.9.2. Agendamento de atualização de definições

Se for ***realmente necessário***, você pode desmarcar o item ***Ativar 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

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

Opções avançadas de programação

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.

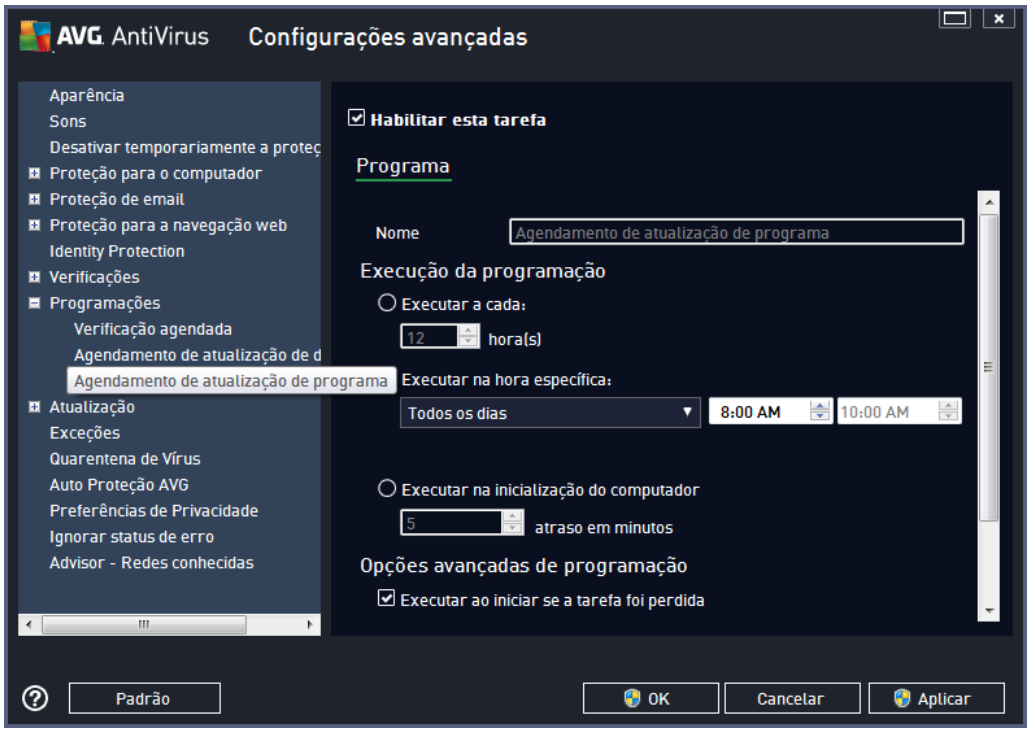
Outras configurações de atualização

Por fim, marque a opção ***Executar novamente a atualização 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 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*) .

9.9.3. Agendamento de atualização de programa

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



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

Opções avançadas de programação

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

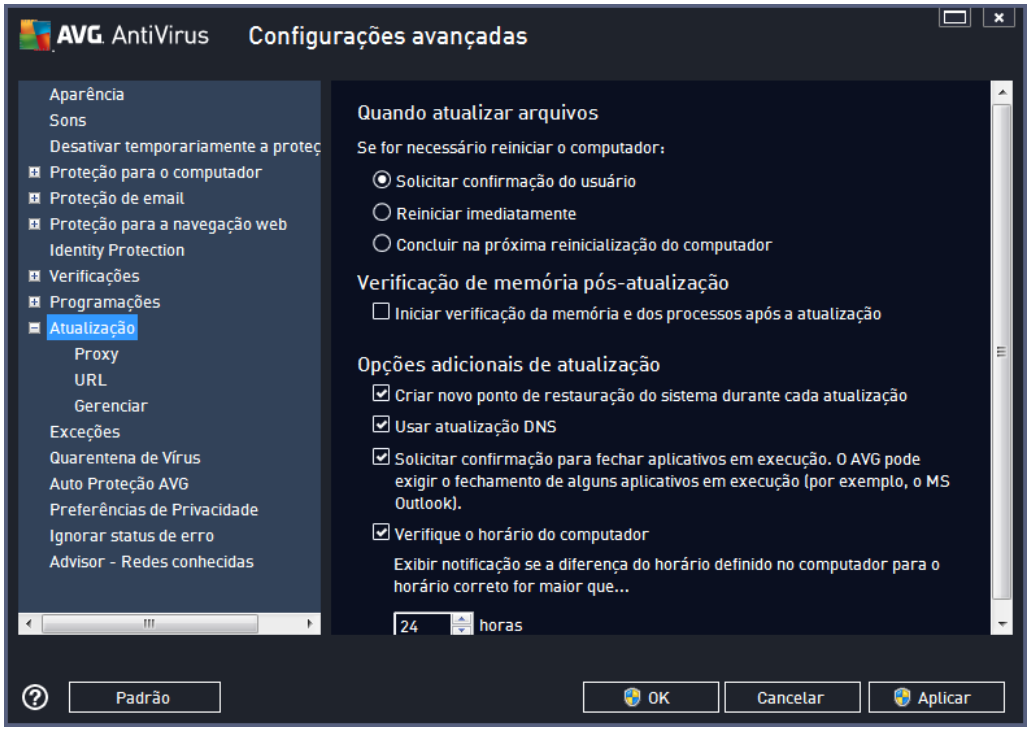
Outras configurações de atualização

Marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível*** para ter certeza de que, se a conexão com a Internet 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*).

Observação: *se o tempo de uma atualização de programa agendada e uma verificação agendada coincidirem, o processo de atualização terá maior prioridade, e a verificação será interrompida. Em tal caso, você será informado sobre o conflito.*

9.10. 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 requeira a reinicialização do PC. A finalização da atualização pode ser agendada para a próxima reinicialização do PC, ou você pode reiniciar imediatamente:

- ***Requer a confirmação do usuário*** *(por padrão)* – será solicitado que você aprove a reinicialização do PC necessária para finalizar o processo de atualização

- ***Reiniciar imediatamente*** – o computador será reiniciado automaticamente após a conclusão do processo de atualização, e sua aprovação não será necessária.

- ***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

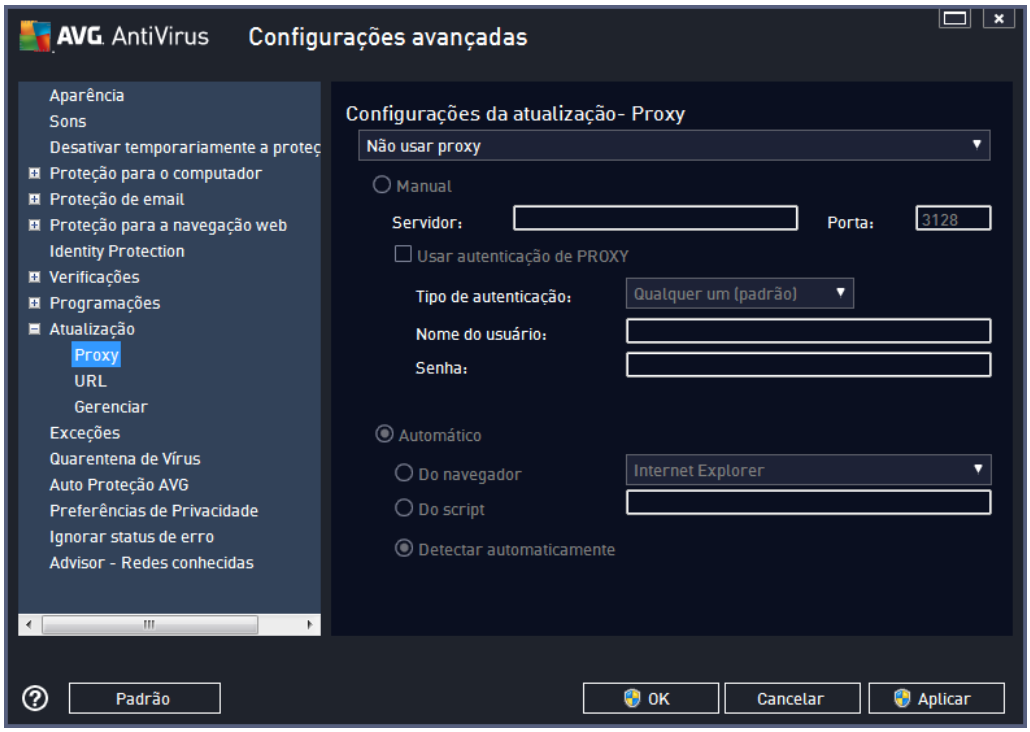
- ***Criar novo ponto de restauração do sistema durante cada atualização do programa*** (*como padrão*) – após cada ativação da atualização do programa AVG, um ponto de restauração do sistema é criado. No caso de falha no processo de atualização e do sistema operacional, você pode restaurar seu SO para 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*** (*ativada por padrão*) – com este item marcado, depois que a atualização é iniciada, o **AVG AntiVirus 2014** procura informações sobre a mais recente versão do banco de dados de vírus e sobre a versão mais recente do programa no servidor DNS. Então, somente os menores e mais indispensáveis arquivos de atualização são baixados e aplicados. Dessa forma, a quantidade total de dados baixados é reduzida e o processo de atualização é executado mais rapidamente.

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

- ***Marcar o horário definido do computador*** (*ativado por 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.

9.10.1. 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; as duas possibilidades também podem ser permitidas ao mesmo tempo. Em seguida, no primeiro item da caixa de diálogo ***Configurações da Atualização – Proxy***, você deverá selecionar o menu da caixa de combinação, se desejar:

- ***Não usar proxy*** – configurações padrão
- ***Usar proxy***
- ***Tentar conectar usando proxy e, se falhar, conectar 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 (*por padrão, esse número está definido como 3128, mas pode ser definido de forma diferente – se não tiver certeza, entre em contato com o administrador da rede*).

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

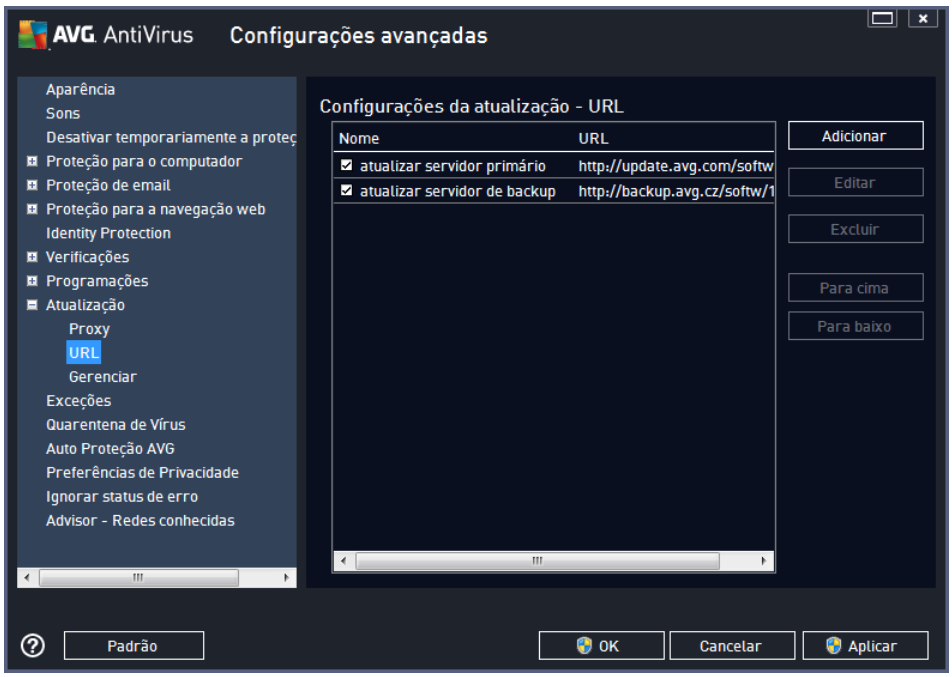
Configuração automática

Se você selecionar configuração automática (*marque a opção 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

9.10.2. URL

A caixa de diálogo ***URL*** oferece uma lista de endereços da Internet, a partir da qual você poderá baixar os arquivos de atualização:



Botões de controle

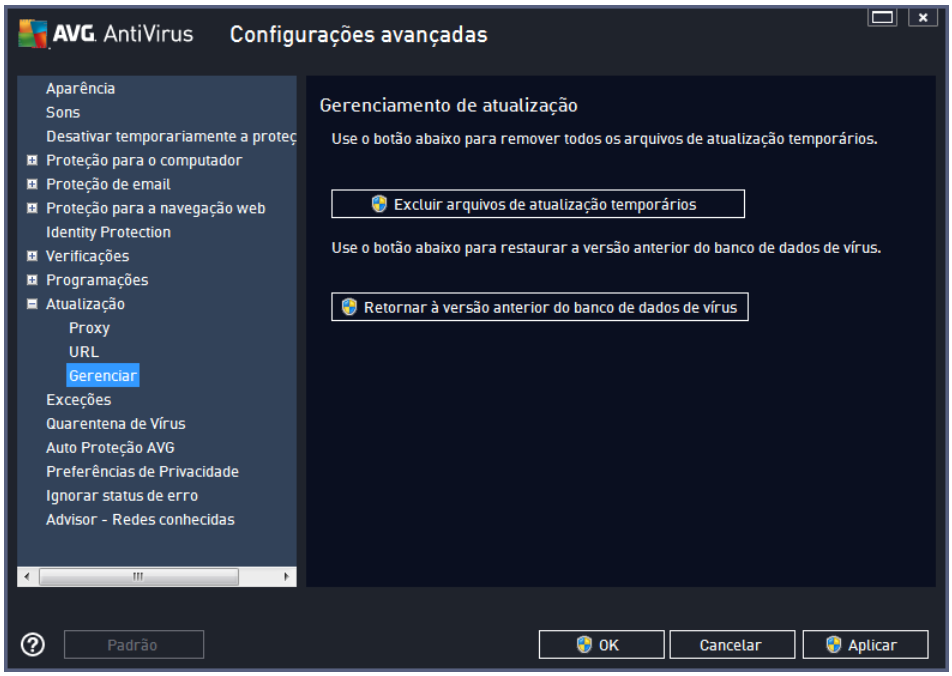
A lista e os itens podem ser modificados por meio dos seguintes botões de controle:

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

- ***Editar*** – abre uma caixa de diálogo na qual você poderá editar os parâmetros da URL selecionada
- ***Excluir*** – exclui a URL selecionada da lista
- ***Mover para cima*** – move a URL selecionada uma posição acima na lista
- ***Mover para baixo*** – move a URL selecionada uma posição abaixo na lista

9.10.3. Gerenciar

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



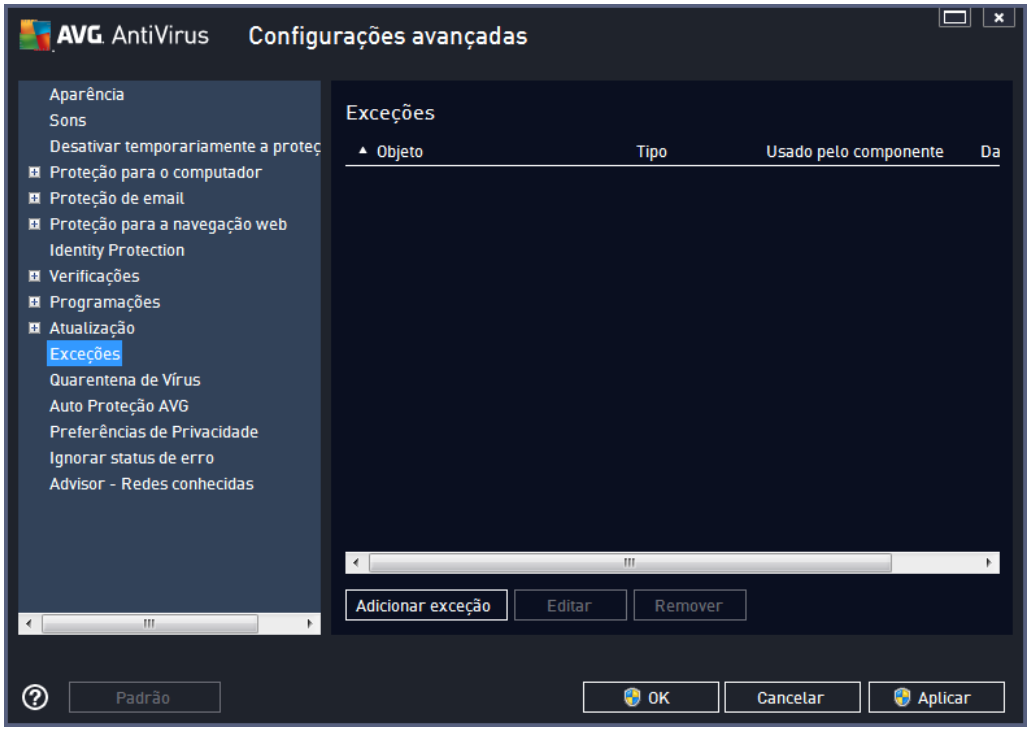
- ***Excluir arquivos de atualização temporários*** – pressione este botão para excluir todos os arquivos de atualização redundantes do seu disco rígido (*por padrão, eles são armazenados por 30 dias*)
- ***Retornar à versão anterior do banco de dados de vírus*** – pressione este botão para excluir a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

9.11. Exceções

No diálogo ***Exceções*** você pode definir exceções, isto é, itens que o **AVG AntiVirus 2014** 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.

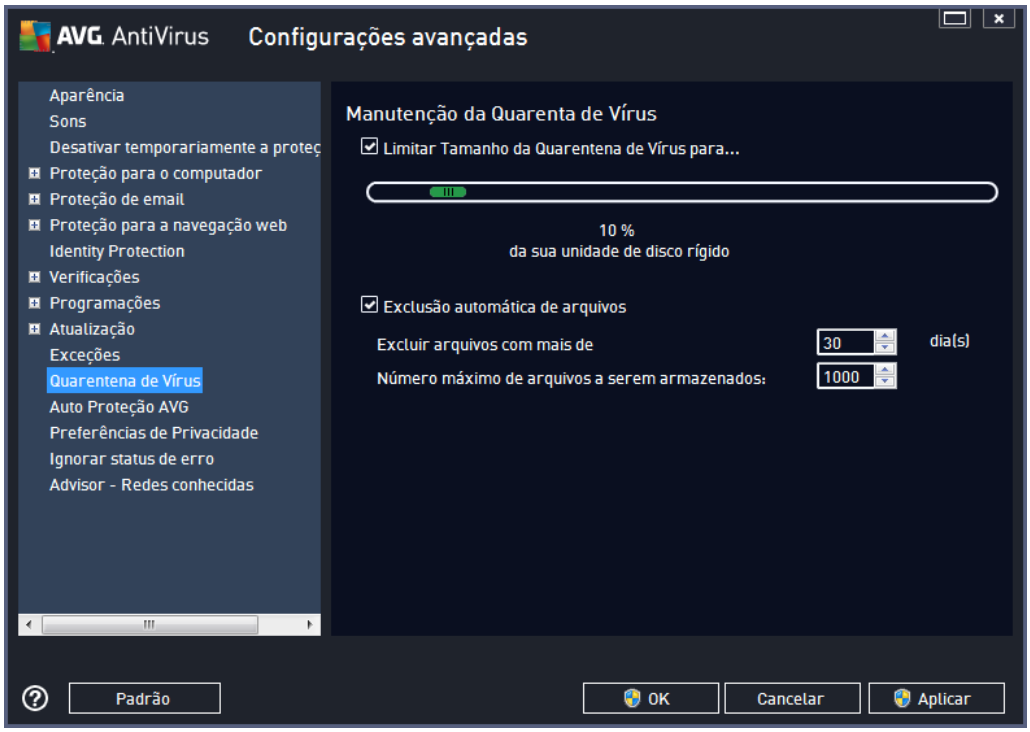
Botões de controle

- ***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 arquivo, pasta ou URL. Depois você terá que procurar no seu disco o caminho do respectivo objeto, ou digitar o URL. Finalmente, você pode selecionar quais recursos do AVG devem ignorar o objeto selecionado *(proteção residente, identidade, verificação, anti-rootkit)*.

- ***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!

9.12. Quarentena de Vírus

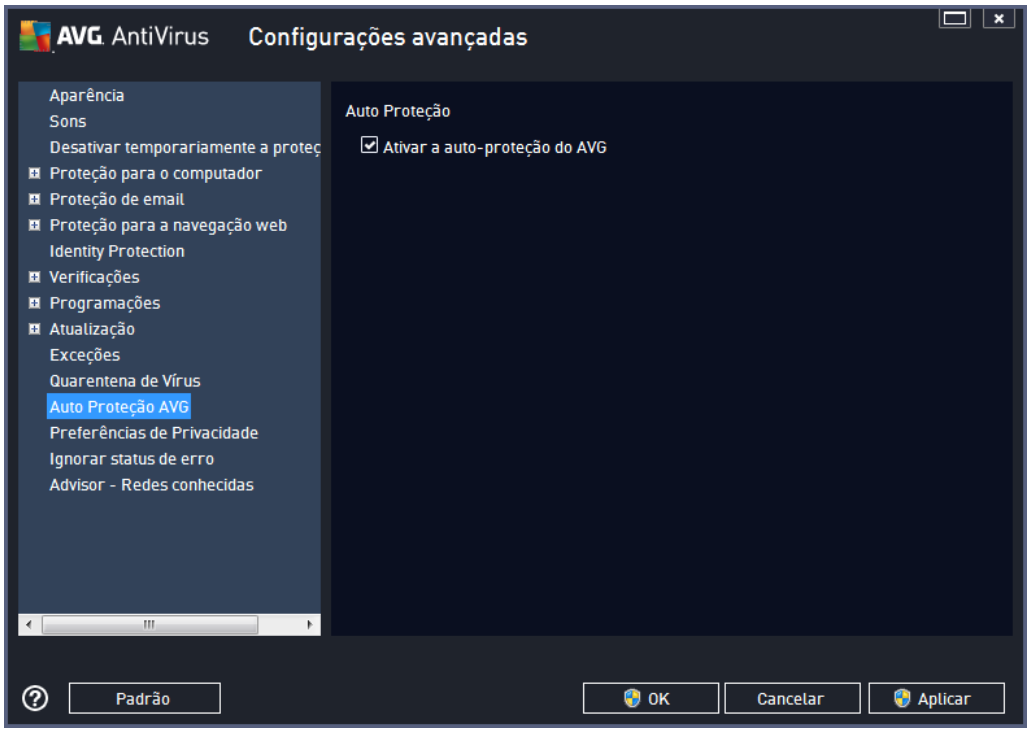


A caixa de diálogo ***Manutenção da quarentena*** permite definir vários parâmetros relativos à administração de objetos armazenados na Quarentena:

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

9.13. Auto Proteção do AVG

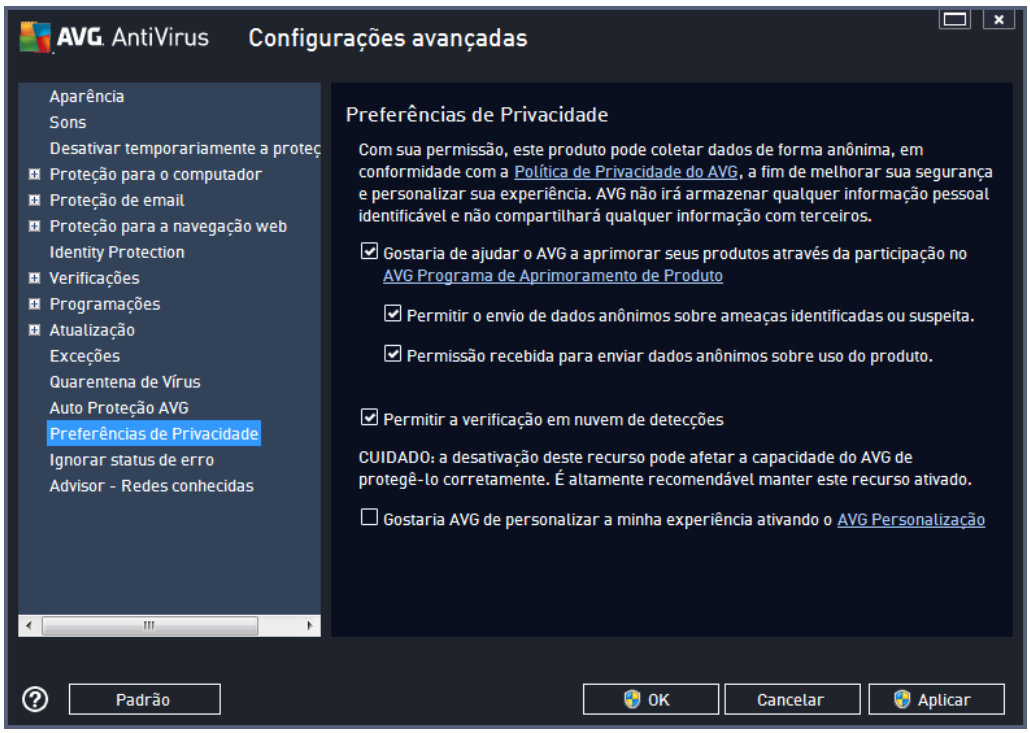


A ***Auto Proteção do AVG*** possibilita que o **AVG AntiVirus 2014** proteja seus próprios processos, arquivos, chaves de registro e drivers contra alteração e desativação. O principal motivo para este tipo de proteção é que algumas ameaças sofisticadas tentam desarmar a proteção antivírus e depois livremente causam danos a seu computador.

Nós recomendamos manter esse recurso ativado!

9.14. 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 Produto da AVG*** *(ativado como padrão)* – se desejar nos ajudar a aprimorar ainda mais o **AVG AntiVirus 2014**, 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 por 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 por 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 por padrão)* – envie estatísticas básicas sobre o uso do aplicativo, como número de detecções, verificações executadas, atualizações com ou sem sucesso, etc.
- ***Permitir verificação de detecções na nuvem*** *(ativada por 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. Baseado nessa análise, a AVG pode oferecer serviços direcionados diretamente às suas necessidades, para protegê-lo com segurança máxima.

Ameaças mais comuns

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

- ***Um vírus*** é um código mal-intencionado que se copia e se espalha, muitas vezes sem ser percebido, até que o estrago seja feito. Alguns vírus são uma ameaça séria, excluindo ou alterando deliberadamente arquivos no seu caminho, enquanto alguns vírus podem fazer algo aparentemente inofensivo, como reproduzir o trecho de uma música. No entanto, todos os vírus são perigosos devido à capacidade básica de se multiplicarem – mesmo um vírus simples pode ocupar toda a memória do computador em um instante e causar uma falha.

- ***O worm*** é uma subcategoria de vírus que, diferentemente de um vírus normal, não precisa de um objeto "transportador" ao qual se anexar. Ele se envia a outros computadores dentro de si mesmo, normalmente por email e, como resultado, frequentemente sobrecarrega servidores de email e sistemas de rede.

- ***Um Spyware*** normalmente é definido como uma categoria de malware (*malware = qualquer software mal intencionado, incluindo vírus*) que abrange programas – tipicamente Cavalos de Tróia – com o objetivo de roubar informações pessoais, senhas, números de cartão de crédito ou para se infiltrar em um computador e permitir que o atacante controle-o remotamente; é claro que tudo isso sem o conhecimento ou consentimento do dono do computador.

- ***Programas potencialmente indesejados*** são um tipo de spyware que pode ser (mas que não necessariamente é) perigoso ao computador. Um exemplo específico de um PPI é o adware, software projetado para distribuir propaganda, normalmente exibindo pop-ups de anúncio; é irritante, mas não diretamente prejudicial.

- ***Os cookies de rastreamento*** podem também ser contados como um tipo de spyware, uma vez que esses pequenos arquivos, armazenados no navegador da Web e enviados automaticamente ao site "pai" quando você visitá-lo novamente, podem conter dados como seu histórico de navegação e outras informações similares.

- ***Vulnerabilidade*** é um código mal intencionado que se aproveita de uma falha ou vulnerabilidade em um sistema operacional, navegador da Internet ou outro programa essencial.

- ***Phishing*** é uma tentativa de adquirir dados pessoais confidenciais simulando uma organização confiável e bem conhecida. Normalmente, as possíveis vítimas são contatadas por um email em massa solicitando que elas, por exemplo, atualizem os detalhes da sua conta bancária. Para fazer isso, elas são convidadas a seguir o link fornecido que leva a um site falso do banco.

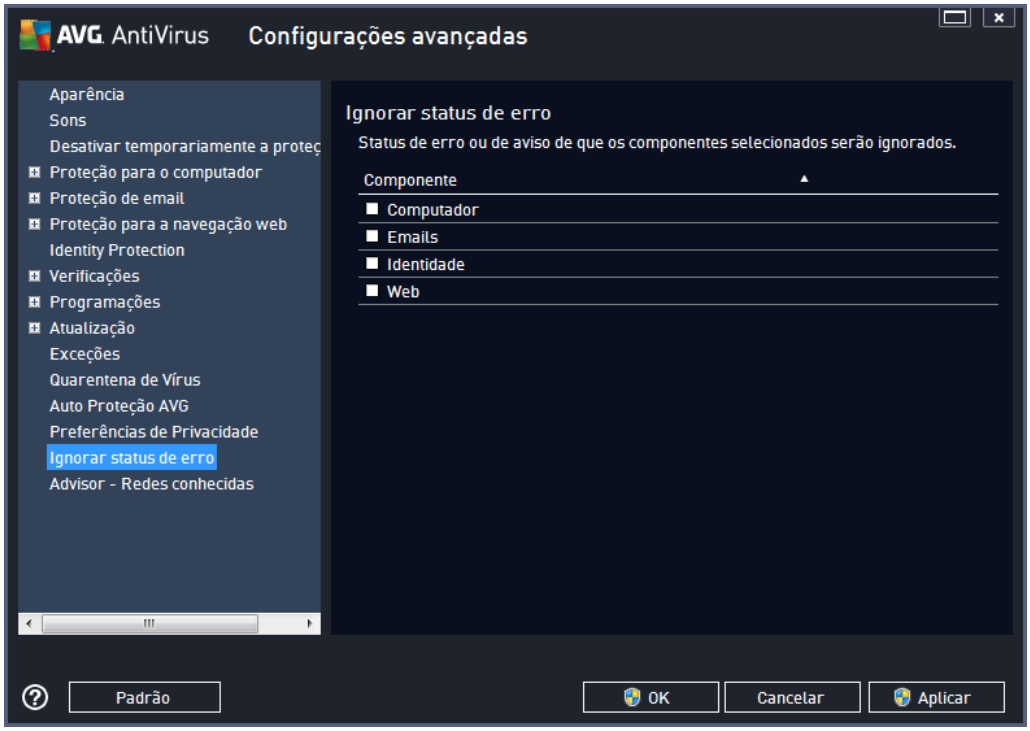
- ***Hoax*** é um email em massa contendo informações perigosas, alarmantes ou apenas irritantes e inúteis. Muitas das ameaças acima usam o email hoax para se espalharem.

- ***Sites mal-intencionados*** são aqueles que deliberadamente instalam software mal-intencionado no seu computador, e sites invadidos fazem o mesmo, a única diferença é que esses sites são legítimos, foram invadidos e infectam os visitantes.

Para protegê-lo de todos esses diferentes tipos de ameaças, o AVG AntiVirus 2014 inclui componentes especializados. Para obter uma breve descrição desses componentes, consulte o capítulo Visão geral dos componentes.

9.15. Ignorar status de erro

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



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

- ícone da bandeja do sistema – enquanto todos os componentes do AVG estão funcionando adequadamente, o ícone é exibido em quatro cores; entretanto, se ocorrer um erro, os ícones aparecem com um ponto de exclamação amarelo,

- descrição textual do problema na seção Informações sobre Status de Segurança na janela principal do AVG

Pode 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

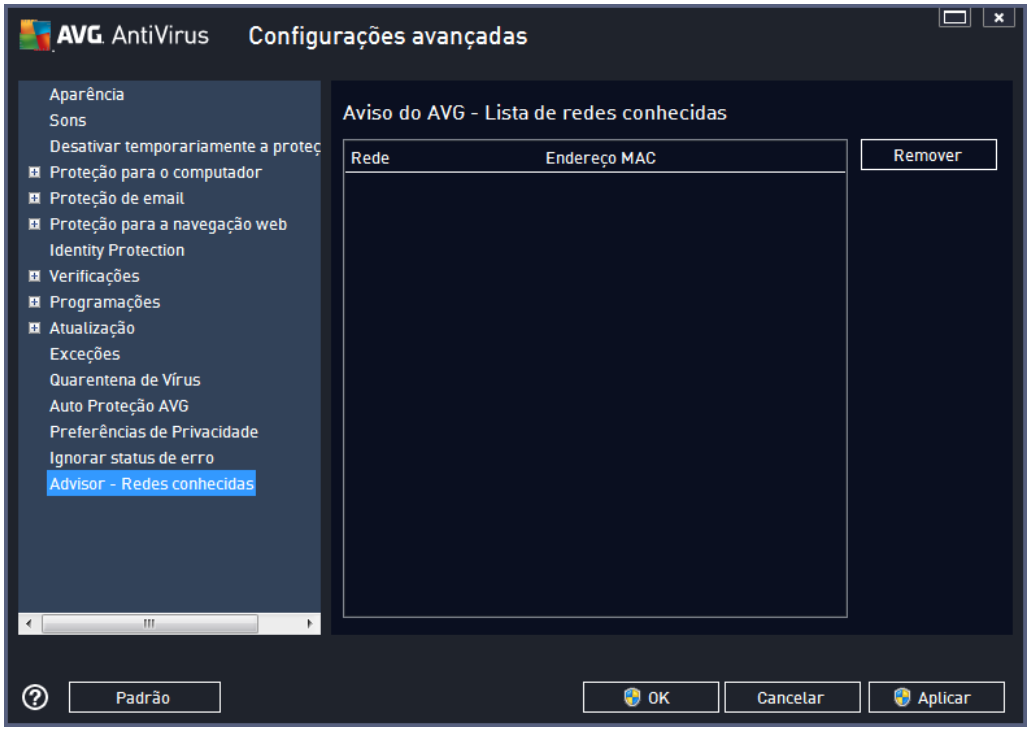
ícone da bandeja do sistema relata automaticamente o status de erro do componente. Entretanto, neste caso em particular, não se pode falar de um erro, pois você deliberadamente o induziu, e está ciente do provável risco. Ao mesmo tempo, assim que é exibido em cinza, o ícone não pode relatar qualquer 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.***

9.16. Advisor – Redes conhecidas

O AVG Advisor contém um recurso que monitora as redes nas quais você se conecta e, se um 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.

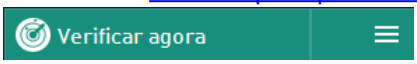
Na janela da caixa de diálogo, é possível verificar quais redes são consideradas conhecidas:



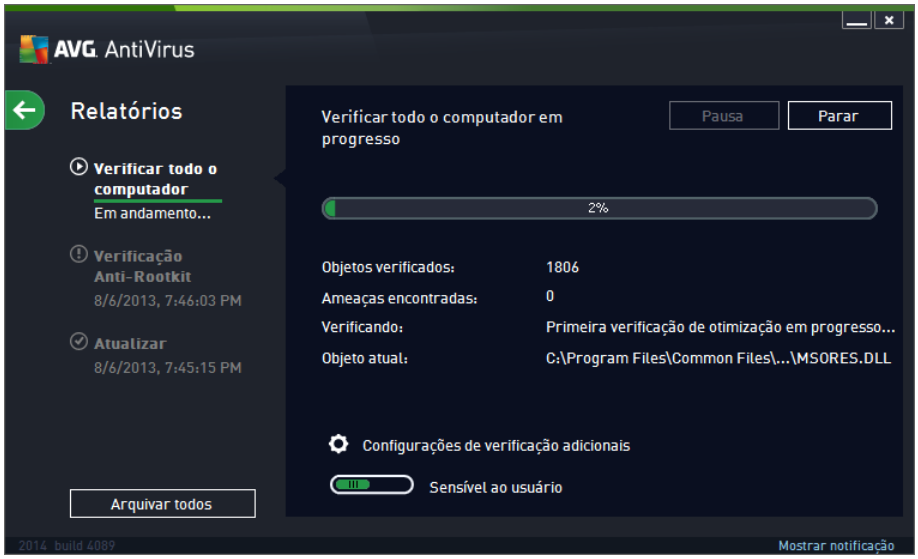
Observação: *o recurso de redes conhecidas no AVG Advisor não é compatível com o Windows XP 64-bit.*

10. Verificação do AVG

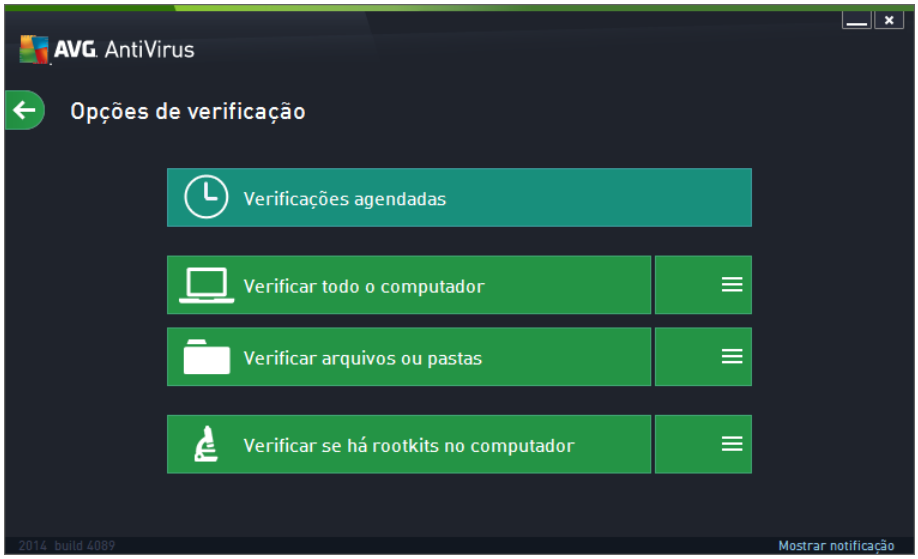
Como padrão, o **AVG AntiVirus 2014** não executa verificações, já que, após a verificação inicial *(que você será solicitado a iniciar*), você deverá estar totalmente protegido pelos componentes residentes do **AVG AntiVirus 2014**, que estão sempre prontos e não permitem que códigos mal intencionados 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*. Também é possível clicar em *Adicionar* 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 .

10.1. Verificações predefinidas

Um dos principais recursos do **AVG AntiVirus 2014** 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.

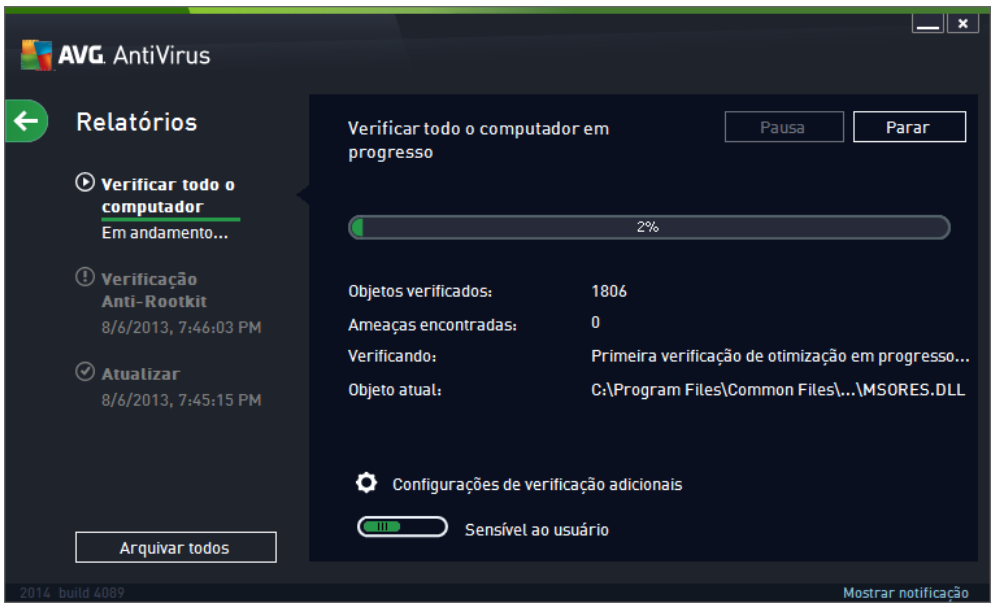
No **AVG AntiVirus 2014** você encontrará os seguintes tipos de verificação predefinidos pelo fornecedor do software:

10.1.1. Verificar todo o computador

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

Iniciar verificação

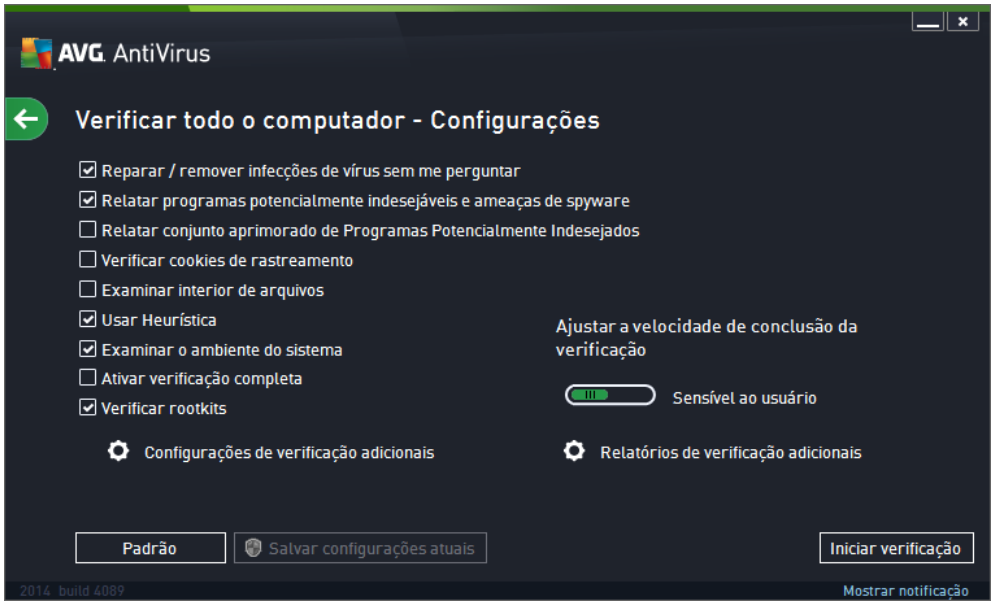
A ***verificação de todo o computador*** pode ser iniciada diretamente a partir da interface principal do usuário clicando no botão ***Verificar agora***. Nenhuma outra configuração deve ser definida para esse tipo de verificação; a verificação iniciará automaticamente. Na caixa de diálogo ***Verificar 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 / remover infecções de vírus sem me perguntar*** *(ativada por padrão)* – se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***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 ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Relatar conjunto aprimorado de programas 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. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, 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).*

- ***Verificar interior de arquivos*** *(desativada por padrão)* – esse parâmetro especifica que a

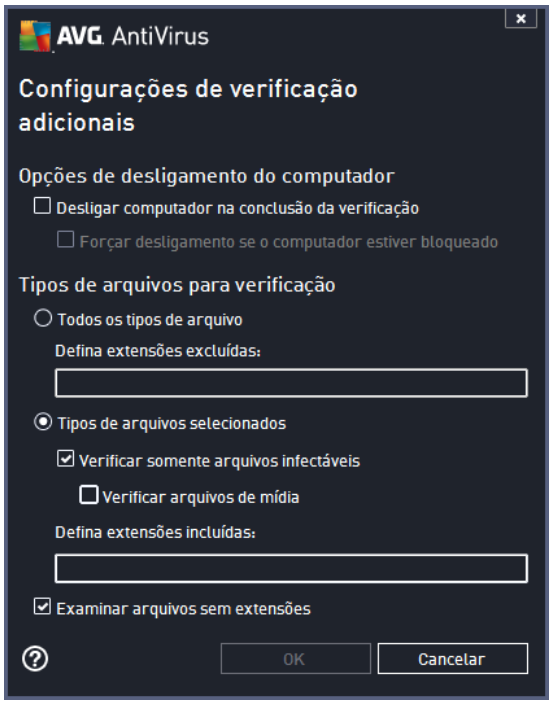
verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR, etc.

- ***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 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 consome bastante tempo.

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



  - ***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 na conclusão da verificação***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja 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

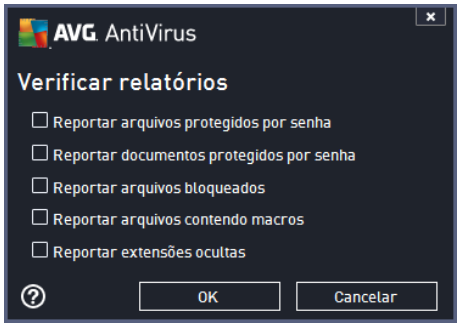
que não devem ser verificadas;

- ***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*). Mais uma vez, 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 por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Ajustar a velocidade de conclusão da verificação*** – você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, 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 (*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 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.*

10.1.2. Verificar arquivos ou pastas

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

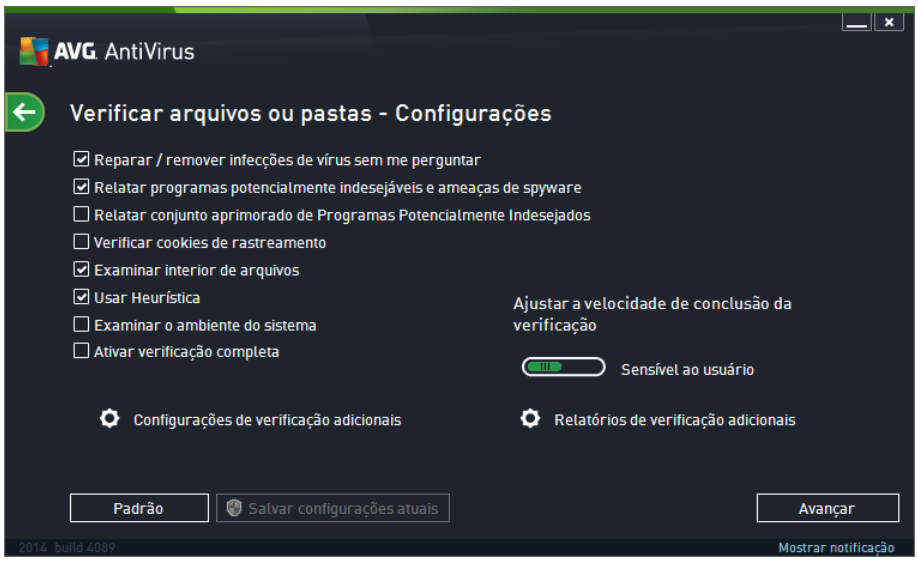
próprios testes e sua programação com base nas suas necessidades.

Iniciar verificação

A opção ***Verificar arquivos ou pastas*** pode ser iniciada diretamente a partir do 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. Também existe 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 da verificação a pasta inteira, use o parâmetro "**!**" . Finalmente, para iniciar a verificação, pressione o botão ***Iniciar verificação***; o processo de verificação será basicamente idêntico a Verificar todo o computador.

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 por padrão)* – se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***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 ele geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Relatar conjunto aprimorado de programas potencialmente indesejados*** *(desativada por padrão)* – marque para detectar os pacotes estendido de spyware: programas que são perfeitamente ok e inofensivos quando adquiridos diretamente do fabricante, mas que podem ser mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, 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*** (*ativada por padrão*) – esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

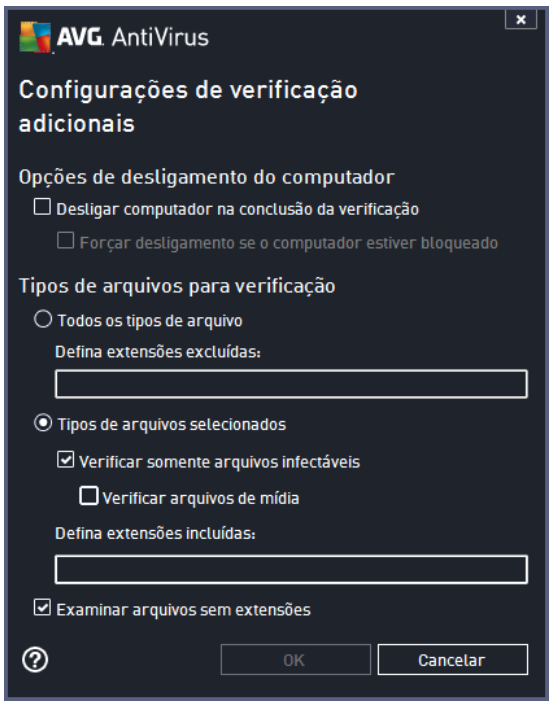
- ***Usar Heurística*** *(ativada por padrão)* – a análise heurística *(emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual)* será um dos métodos usados para detecção de vírus durante a verificação.

- ***Examinar o ambiente do sistema*** (*desativada 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 consome bastante tempo.

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



  - ***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 na conclusão da verificação***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja 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;

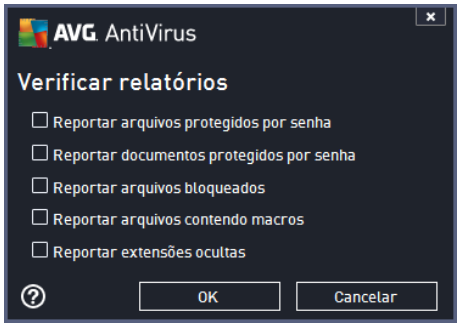
    - ***Tipos de arquivos selecionados*** – você pode especificar que deseja verificar apenas os arquivos que podem ser infectados (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*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). Mais uma vez, 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 por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Ajustar a velocidade de conclusão da verificação*** – você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, 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 (*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:



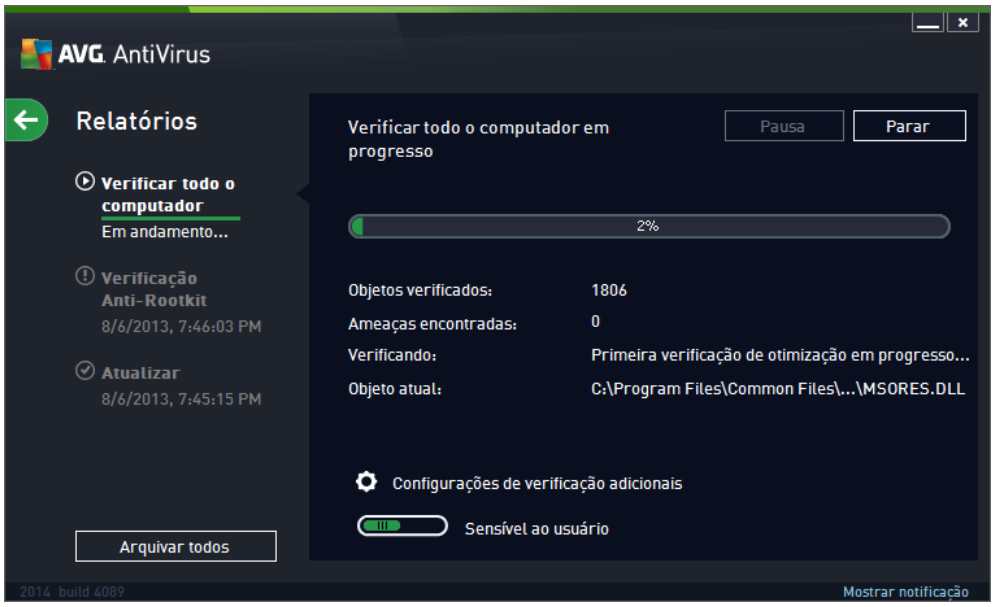
Aviso: *essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo Verificação do AVG/Programação da verificação/ Como verificar. Se você decidir alterar as configurações padrão de* ***Verificar arquivos ou pastas específicas****,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

10.1.3. 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.

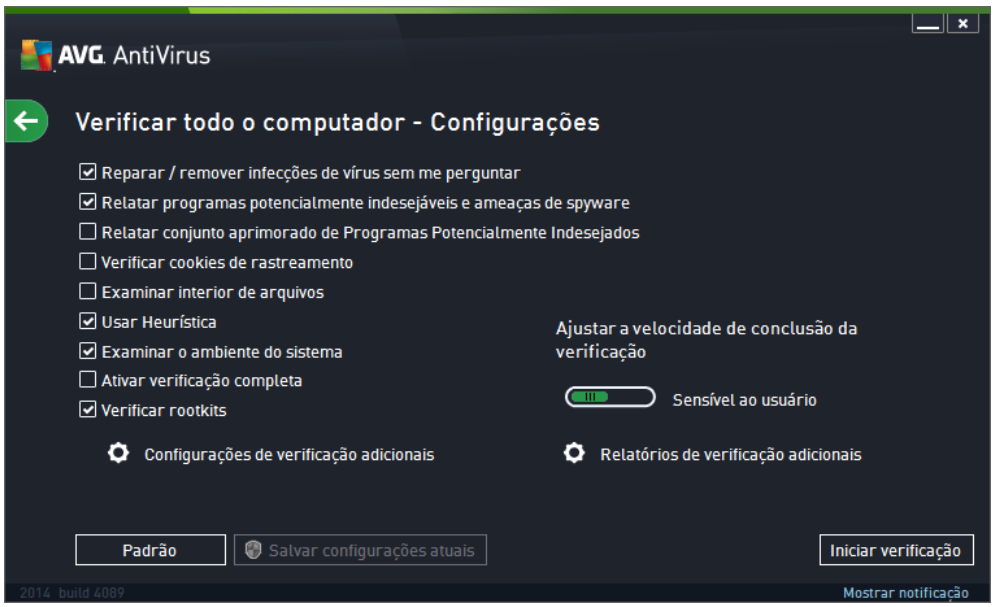
Iniciar verificação

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

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 / remover infecções de vírus sem me perguntar*** *(ativada por padrão)* – se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***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 ele geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente. Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Relatar conjunto aprimorado de programas potencialmente indesejados*** *(desativada 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 mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, 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)*.

- ***Verificar interior de arquivos*** *(desativada por padrão)* – esse parâmetro especifica que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR, etc.

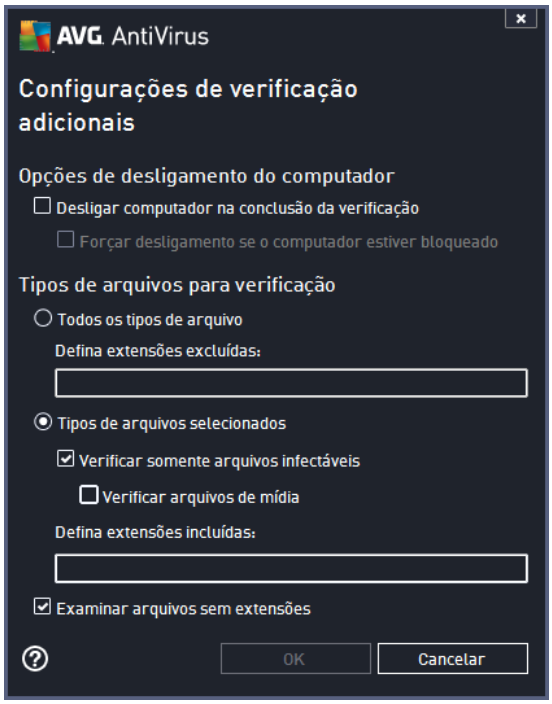
- ***Usar Heurística*** *(ativada por padrão)* – a análise heurística *(emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual)* será um dos

métodos usados para detecção de vírus durante a verificação.

- ***Examinar 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 consome bastante tempo.

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



  - ***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 na conclusão da verificação***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja 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*). Mais uma vez, 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 por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

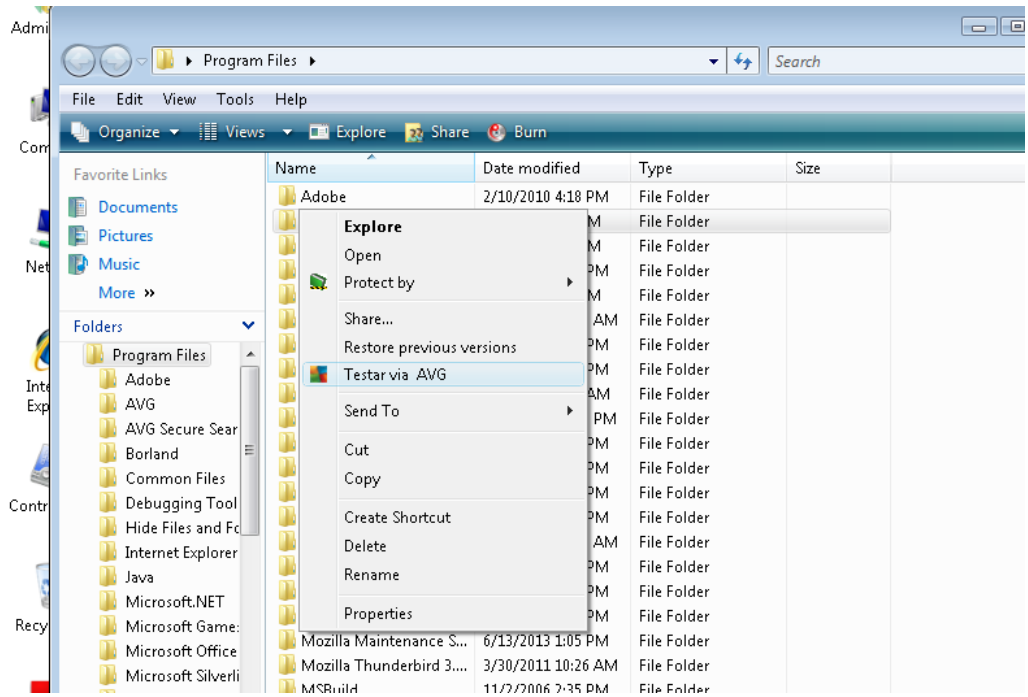
- ***Ajustar a velocidade de conclusão da verificação*** – você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, esse valor de opção é definido no nível *Sensível ao usuário de uso automático do recurso.* Se desejar, você pode executar o processo de 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 (*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 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.*

10.2. Verificando o Windows Explorer

Além das verificações predefinidas iniciadas em todo o computador ou em áreas selecionadas, o **AVG AntiVirus 2014** 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 AntiVirus 2014**

10.3. Verificação de linha de comando

No **AVG AntiVirus 2014** 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

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

Parâmetros de verificação

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

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

Verificação CMD iniciada pela interface gráfica

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

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

10.3.1. Parâmetros de verificação CMD

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

- /SCAN — Verifica arquivos ou pastas específicos /SCAN=caminho;caminho *(p. ex. /SCAN=C:\;D:\)*
- /COMP — Verifica todo o computador
- /HEUR — Usa análise heurística
- /EXCLUDE — Exclui caminho ou arquivo da verificação
- /@ — Arquivo de comando/nome de arquivo/
- /EXT — Verifica estas extensões/por exemplo, EXT=EXE,DLL
- /NOEXT — Não verifica estas extensões/por exemplo, NOEXT=JPG/
- /ARC — Verifica arquivos

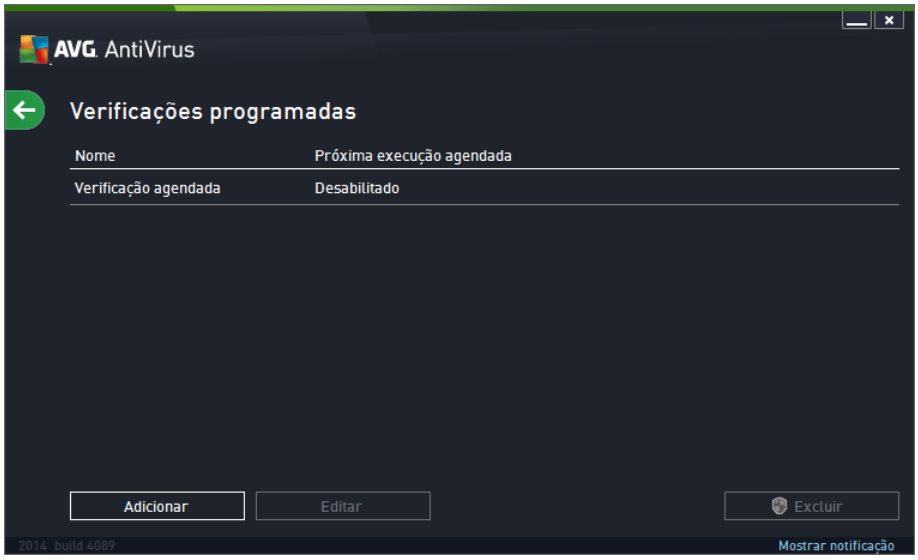
- /CLEAN Limpa automaticamente
- /TRASH Move arquivos infectados para a Quarentena de vírus
- /QT Teste rápido
- /LOG Gera um arquivo de resultado de verificação
- /MACROW Relata macros
- /PWDW Relata arquivos protegidos por senha
- /ARCBOMBSW Relata falhas de arquivos *(arquivos compactados repetidamente)*
- /IGNLOCKED Ignora arquivos bloqueados
- /REPORT Relata para arquivo/ nome de arquivo/
- /REPAPPEND Acrescenta ao arquivo de relatório
- /REPOK Relata arquivos não infectados como OK
- /NOBREAK Não permite abortar com CTRL-BREAK
- /BOOT Ativa verificação de MBR/BOOT
- /PROC Verifica processos ativos
- /PUP Relata "Programas potencialmente indesejáveis
- /PUPEXT Relata conjunto avançado de programas potencialmente indesejáveis
- /REG Verifica registro
- /COO Verifica cookies
- /? Exibe ajuda neste tópico
- /HELP Exibe ajuda neste tópico
- /PRIORITY Define a prioridade da verificação /Baixa, Automática, Alta/ *(consulte Configurações avançadas/Verificações)*
- /SHUTDOWN Desliga o computador na conclusão da verificação
- /FORCESHUTDOWN Força o computador a ser desligado na conclusão da verificação
- /ADS Verifica fluxos de dados alternativos *(apenas NTFS)*
- /HIDDEN Relata arquivos com extensão oculta
- /INFECTABLEONLY Verifica apenas os arquivos com extensões infectáveis

- /THOROUGHSCAN Ativa verificação completa
- /CLOUDCHECK Verifica a existência de falsos positivos
- /ARCBOMBSW Informa arquivos compactados novamente

10.4. Programação de verificação

Com o **AVG AntiVirus 2014**, é possível executar uma verificação sob demanda *(por exemplo, quando você suspeitar de uma infecção no seu computador) ou com base em um plano programado.* É altamente recomendável executar verificações com base em uma programação. Dessa forma, você pode assegurar que seu computador esteja protegido contra a possibilidade de infecção e não precisará se preocupar com a inicialização da verificação. Você deve Verificar todo o computador regularmente, pelo menos uma vez por semana. Mas, se possível, inicie a verificação de todo o computador diariamente, conforme definido na configuração padrão da programação da verificação. Se o computador estiver "sempre ligado", você poderá programar verificações fora dos horários de trabalho. Se o computador for desligado algumas vezes, programe verificações para 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 ***Verificações agendadas*** na caixa de diálogo Opções de verificação. Na nova caixa de diálogo ***Verificações programadas***, você pode ver uma visão geral completa de todas as verificações programadas:

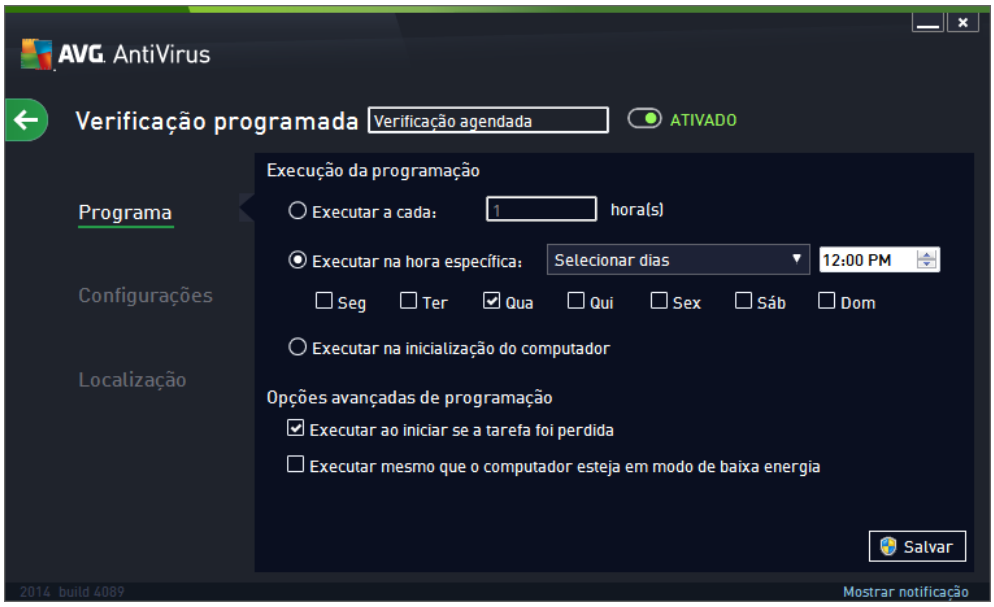


Na caixa de diálogo, é possível especificar suas próprias verificações. Também é possível clicar em ***Adicionar verificação programada*** para criar uma nova programação própria. Os parâmetros da verificação agendada podem ser editados (*ou uma nova configuração de agenda*) em três guias.

- Programa
- Configurações
- Localização

Em cada guia você pode simplesmente clicar no botão de "semáforo" para desativar o teste programado temporariamente e ativa-o novamente quando houver necessidade.

10.4.1. Programação



Na parte superior da guia ***Verificação programada***, 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 tornar seu reconhecimento mais fácil posteriormente. Exemplo: não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc.

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

- ***Execução programada*** – 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)*.

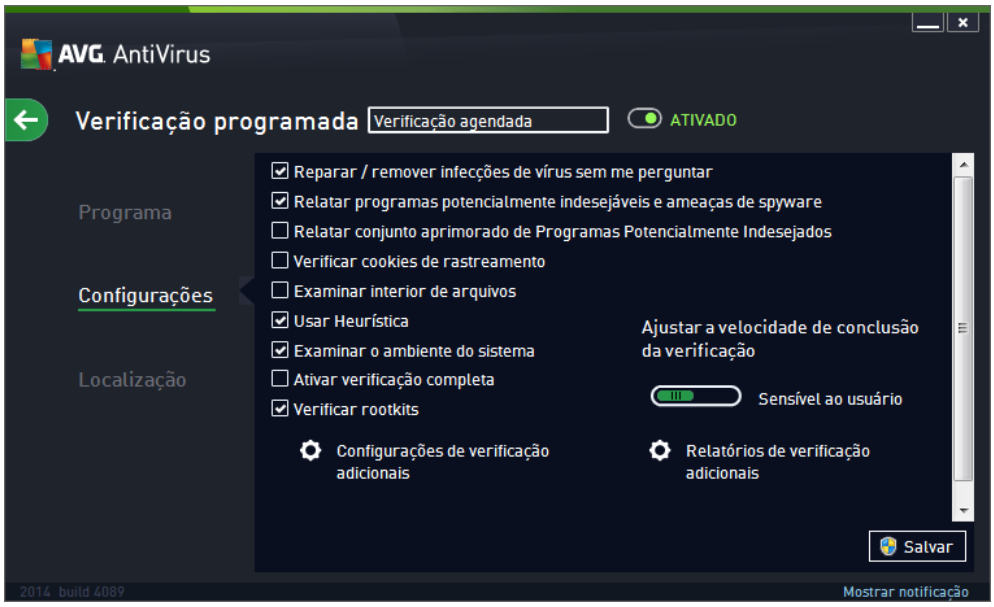
- ***Opções avançadas de programação*** – essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado. Uma vez que a verificação agendada é iniciada no horário que você especificou, você será informado deste fato por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema. Um novo ícone AVG na bandeja do sistema aparece (em cores e com um holofote) informando que uma verificação agendada está em execução. Clique com o botão direito do mouse no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e também alterar a prioridade da verificação em execução.

Controles no diálogo

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

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

10.4.2. 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 tornar seu reconhecimento mais fácil posteriormente. Exemplo: não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc.

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 ou remover o vírus sem me consultar*** *(ativada por padrão):* se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** *(ativada como padrão):* marque para ativar a verificação de spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas podem ser instalados intencionalmente.

Recomendamos que você mantenha esse recurso ativado, pois aumenta a segurança do computador.

- ***Relatar conjunto aprimorado de Programas Potencialmente Indesejados*** (*desativada 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 mal utilizados para finalidades mal intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode bloquear programas legais, e, 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;

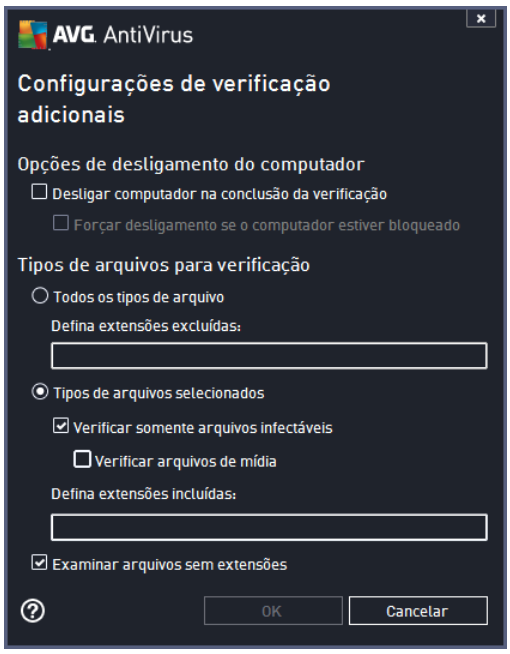
- ***Verificar ambiente do sistema*** (*ativada por padrão*): a verificação também atuará nas áreas do sistema do seu computador;

- ***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 consome bastante tempo.

- ***Verificar rootkits*** *(ativada como padrão): a verificação* Anti-Rootkit procura possíveis rootkits em seu computador, e.x. 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 que ele esteja 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*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

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

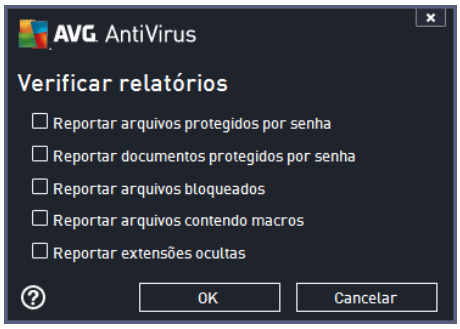
Ajustar a velocidade de conclusão da verificação

Na seção 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:

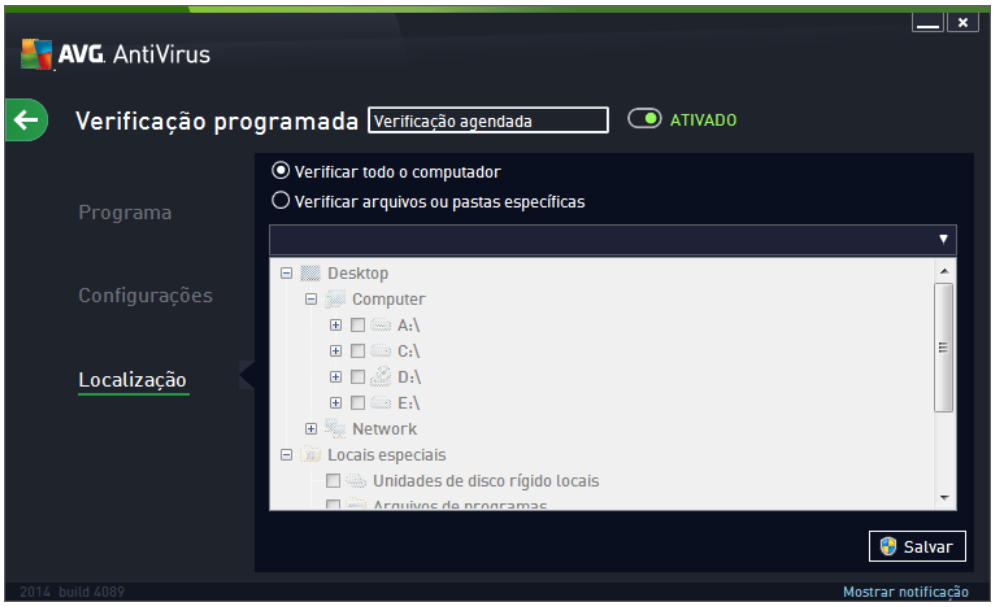


Controles no diálogo

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

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

10.4.3. 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 (expanda os itens clicando no nó de mais até encontrar a pasta que deseja verificar). Você pode selecionar várias pastas marcando as respectivas caixas. As pastas selecionadas aparecerão no campo de texto na parte superior da caixa de diálogo e o menu suspenso manterá o histórico das verificações selecionadas para um uso posterior. *Ou você pode inserir o caminho inteiro para a pasta desejada manualmente (se inserir vários caminhos, será necessário separar com pontos e vírgulas sem espaços extras*).

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

- ***Discos rígidos locais*** – todos os discos rígidos de seu computador
- ***Arquivos de programas***
    - C:\Arquivos de Programas\
    - *na versão de 64 bits* C:\Arquivos de Programas (x86)
- ***Pasta Meus documentos***
    - *para Windows XP:* C:\Documents and Settings\Usuário padrão\Meus documentos\
    - *para Windows Vista/7*: C:\Usuários\usuário\Documentos\
- ***Meus documentos (todos os usuários)***
    - *para Windows XP*: C:\Documents and Settings\Todos os usuários\Documentos\

- *para Windows Vista/7*: C:\Usuários\Público\Documentos\

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

- ***Outro***

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

  - *Pasta do sistema* – C:\Windows\System32\

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

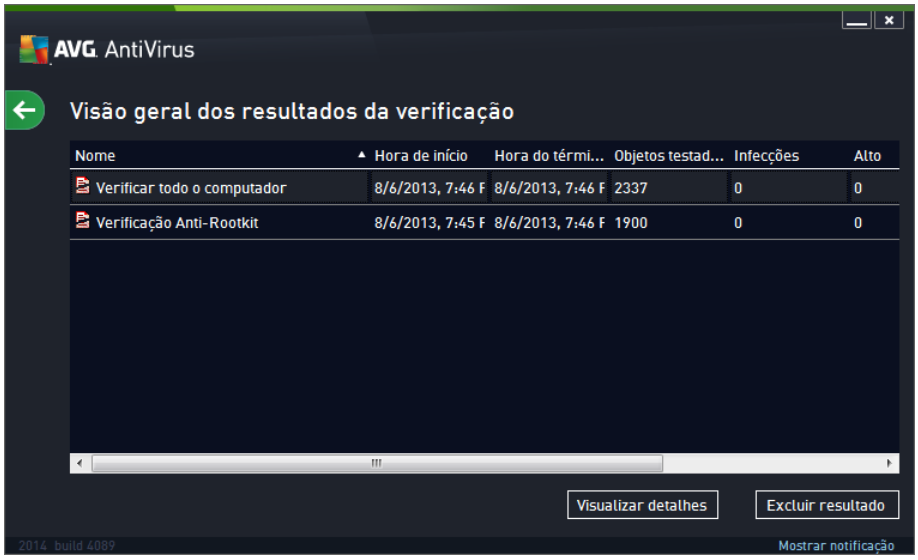
  - *Arquivos Temporários de Internet* – C:\Documents and Settings\Usuário\Configurações locais\Arquivos temporários de Internet\ (*Windows XP*); ou C:\Usuários\usuário\AppData\Local\Microsoft\Windows\Arquivos Temporários de Internet (*Windows Vista/7*)

Controles no diálogo

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

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

10.5. 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 completa.
  - Nenhuma infecção encontrada. A verificação foi interrompida antes da conclusão.
  - As infecções foram encontradas, mas não recuperadas. Verificação completa.
  - As infecções foram encontradas, mas não recuperadas. A verificação foi interrompida antes da conclusão.
  - As infecções foram encontradas e recuperadas ou removidas. Verificação completa.
  - As 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.
- ***Horário de início*** – a data e a hora exatas em que a verificação foi inicializada.
- ***Horário de 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.
- ***Alta / Média / Baixa*** – 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

Exibir 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.

10.6. 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:

- ***Resumo*** – a guia fornece informações básicas sobre a verificação: se ela foi concluída com sucesso, se foram encontradas ameaças 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.

- ***Detecções*** – 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 contém macros, documentos ou arquivos protegidos por uma senha, arquivos bloqueados, etc.

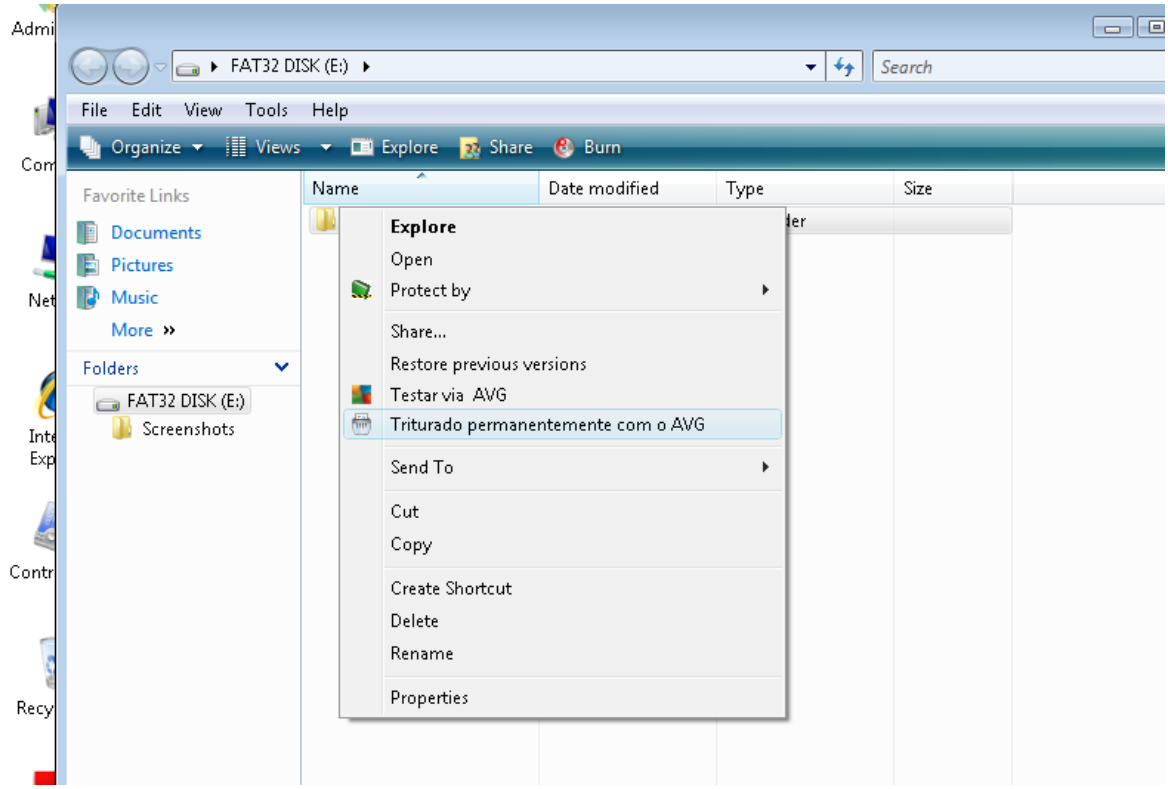
  Gravidade média: normalmente PPI *(Programas Potencialmente Indesejados, como adware*) ou cookies de rastreamento

  Gravidade alta: ameaças sérias como vírus, Cavalos de Tróia, explorações, etc. Além de objetos detectados pelo método de detecção Heurística, ou seja, ameaças que ainda não foram descritas no banco de dados de vírus.

11. AVG File Shredder

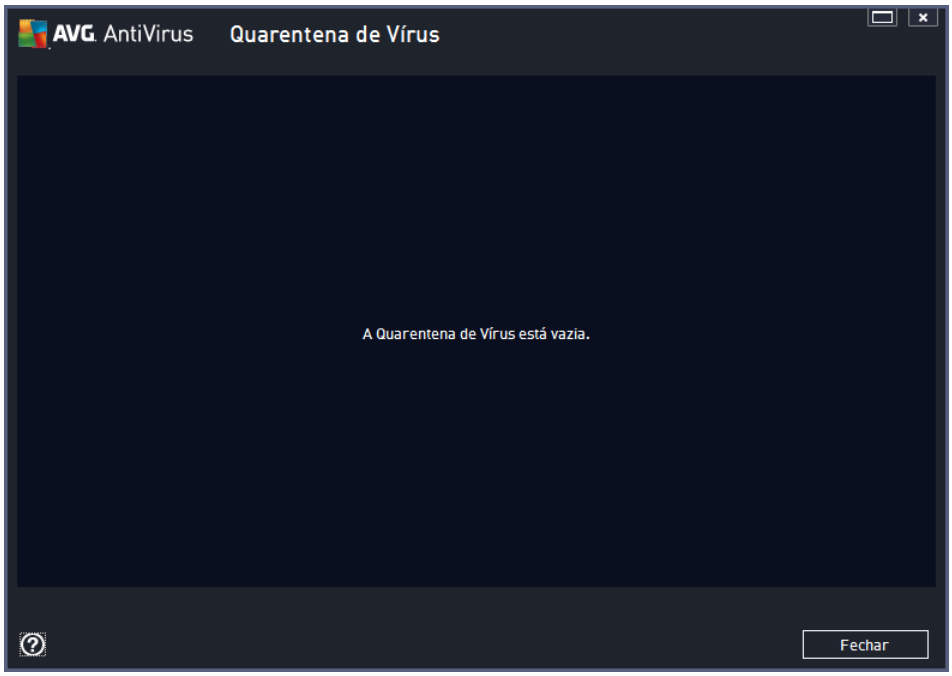
O ***AVG File Shredder*** foi projetado para excluir arquivos de forma absolutamente segura, ou seja, sem nenhuma chance de serem recuperados, mesmo por ferramentas de software avançadas que tenham essa finalidade.

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



Tenha sempre em mente que um arquivo triturado nunca mais poderá ser recuperado.

12. Quarentena de Vírus



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

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

- ***Data de adicionamento*** – fornece a data e hora em que o arquivo suspeito foi detectado e armazenado na Quarentena.
- ***Gravidade*** – caso você decida instalar o componente Identity no seu **AVG AntiVirus 2014**, uma identificação gráfica da respectiva gravidade da descoberta, em uma escala de quatro níveis que varia desde incensurável *(três pontos verdes)* até muito perigosa *(três pontos vermelhos)* será fornecida nesta seção; e as informações sobre o tipo de infecção (*com base em seu nível de infecção – todos os objetos listados podem estar positivamente ou potencialmente infectados*).
- ***Nome da ameaça*** – especifica o nome da infecção detectada de acordo com a Enciclopédia de vírus.
- ***Origem*** – especifica qual componente do **AVG AntiVirus 2014** detectou a respectiva ameaça.
- ***Mensagem*** – 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***:

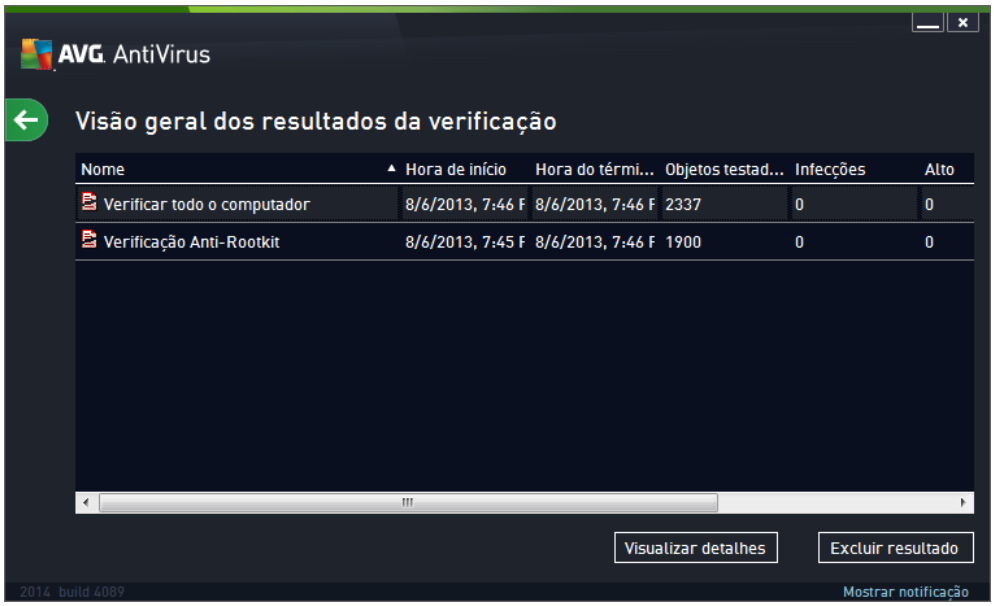
- ***Restaurar*** – remove o arquivo infectado de volta ao local original do disco.
- ***Restaurar como*** – move o arquivo infectado para a pasta selecionada.
- ***Detalhes*** – para obter informações detalhadas sobre ameaças específicas na ***Quarentena de Vírus***, destaque o item na lista e clique 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***.
- ***Esvaziar a Quarentena*** – remove completamente todo o conteúdo da ***Quarentena de Vírus***. Removendo os arquivos da ***Quarentena***, esses arquivos serão removidos de modo irreversível do disco (*e não para a Lixeira*).

13. Histórico

A seção ***Histórico*** contém informações sobre todos os eventos passados *(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
- Detecção da Proteção Residente
- Detecção da Proteção de Email
- Detecção da Proteção Online
- Log de histórico de eventos

13.1. 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 AntiVirus 2014**. A caixa de diálogo fornece uma lista de todas as verificações inicializadas anteriormente e as informações sobre seus resultados:

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

  – o ícone verde informa que não foram detectadas infecções durante a verificação

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

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

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

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

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

Botões de controle

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

- ***Exibir detalhes*** – pressione-o para ativar a caixa de diálogo Resultados da verificação para exibir dados detalhados na verificação selecionada
- ***Excluir resultado*** – pressione-o para remover o item selecionado a partir da visão geral dos resultados da verificação
- – para voltar ao diálogo principal AVG *padrão (visão geral dos componentes),* use a seta no canto superior esquerdo desse diálogo

13.2. 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:

Nesse diálogo de aviso, você encontrará informações sobre o objeto detectado e classificado como infectado (*Nome*), e alguns fatos descritivos sobre a infecção reconhecida (*Descrição*). O link Mostrar detalhes redirecionará para a enciclopédia de vírus online onde é possível encontrar informações detalhadas sobre a infecção detectada, se for conhecida. No diálogo, você também verá um resumo das soluções disponíveis sobre como tratar a ameaça detectada. Uma das alternativas será rotulada como recomendada: Proteja-me (recomendado) ***Se for possível, você deve sempre utilizar essa opção!***

Nota: *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***. O diálogo é acessado através do item de menu ***Opções / Histórico / Detecção da Proteção Residente*** na linha superior de navegação da janela principal do **AVG AntiVirus 2014. Esse diálogo oferece uma visão geral dos objetos detectados pela proteção residente, avaliados como perigosos e recuperados ou movidos para a** Quarentena de vírus.

Em cada objeto detectado, são fornecidas as seguintes informações:

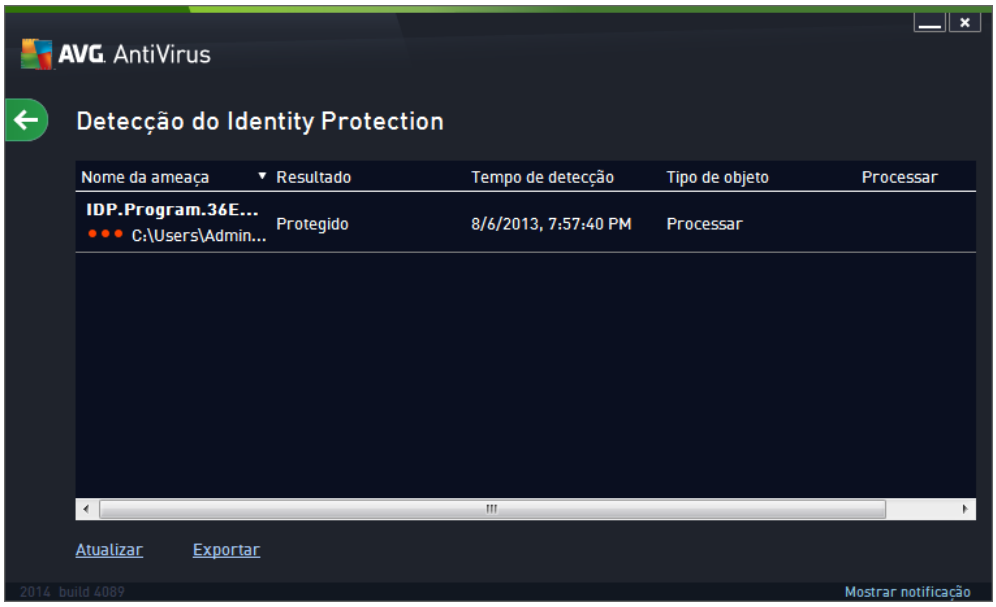
- ***Nome da ameaça*** – descrição (*possivelmente também o nome*) do objeto detectado e sua localização
- ***Resultado*** – ação executada pelo objeto detectado
- ***Hora da detecção*** – data e hora em que a ameaça foi detectada e bloqueada
- ***Tipo de Objeto*** – tipo de objeto detectado
- ***Processo***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

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

13.3. Resultados do Identity Protection

A caixa de diálogo ***Resultados do Identity Protection*** é acessada através do item de menu ***Opções / Histórico / Resultados do Identity Protection***, na linha superior de navegação da janela principal do **AVG AntiVirus 2014**.



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

- ***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 de objeto detectado
- ***Processo*** – qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

Na parte inferior da caixa de diálogo, 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***).

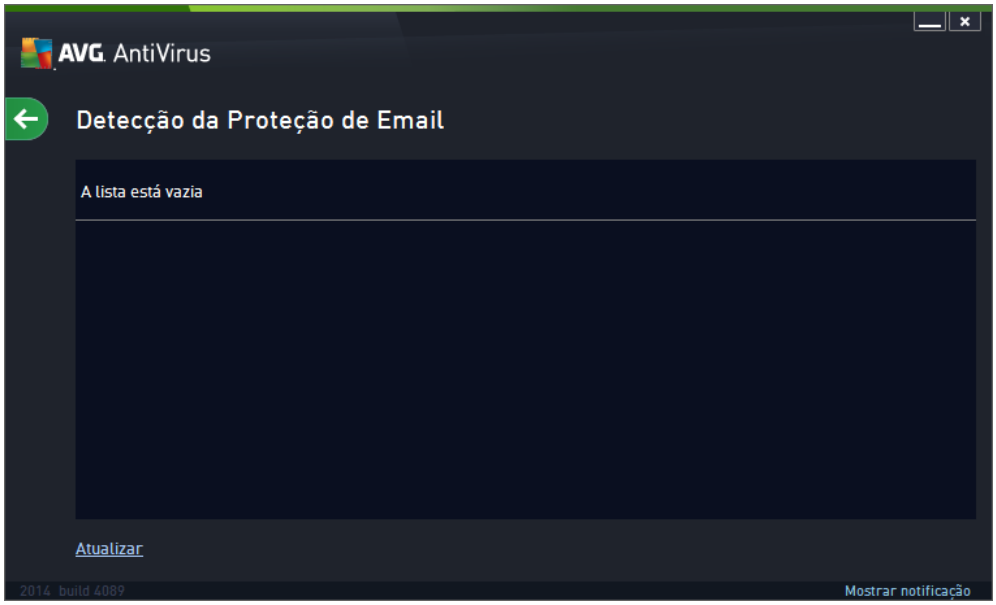
Botões de controle

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

13.4. Resultados da Proteção de Email

A caixa de diálogo ***Resultados da Proteção de Email*** é acessada através do item de menu ***Opções / Histórico / Resultados do Identity Protection***, na linha superior de navegação da janela principal do **AVG AntiVirus 2014**.



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

- ***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 de objeto detectado
- ***Processo*** – qual ação foi executada para ativar o objeto potencialmente perigoso de modo

a permitir que fosse detectado

Na parte inferior da caixa de diálogo, 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

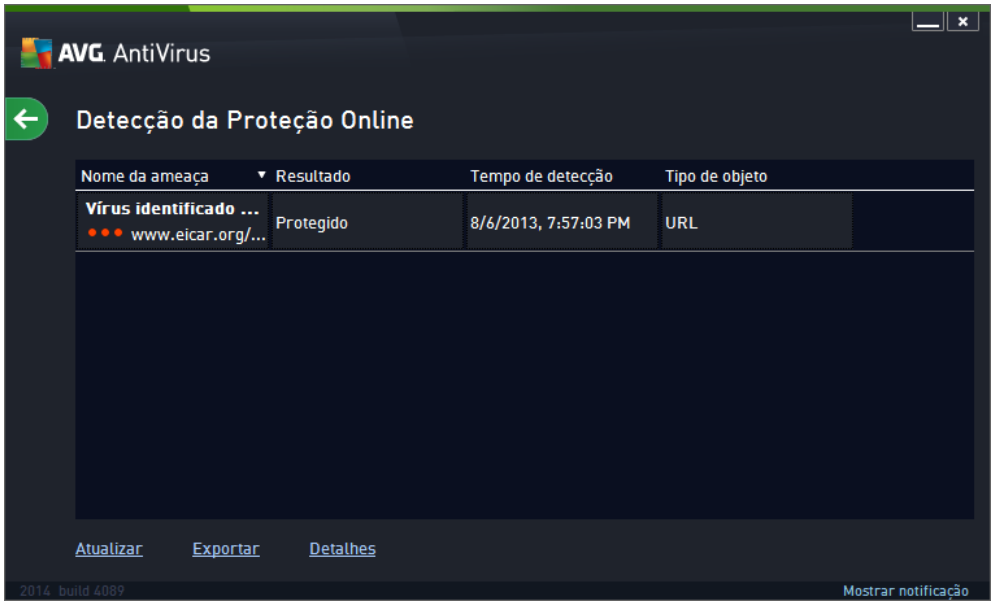
13.5. Resultado da Proteção Online

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

Nesse diálogo de aviso, você encontrará informações sobre o objeto detectado e classificado como infectado (*Nome*), 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 de ***Detecção da Proteção Online***. Essa visão geral de ameaças detectadas é acessada através do item de menu ***Opções / Histórico / Detecção da Proteção Online*** na linha superior de navegação da janela principal do **AVG AntiVirus 2014**.



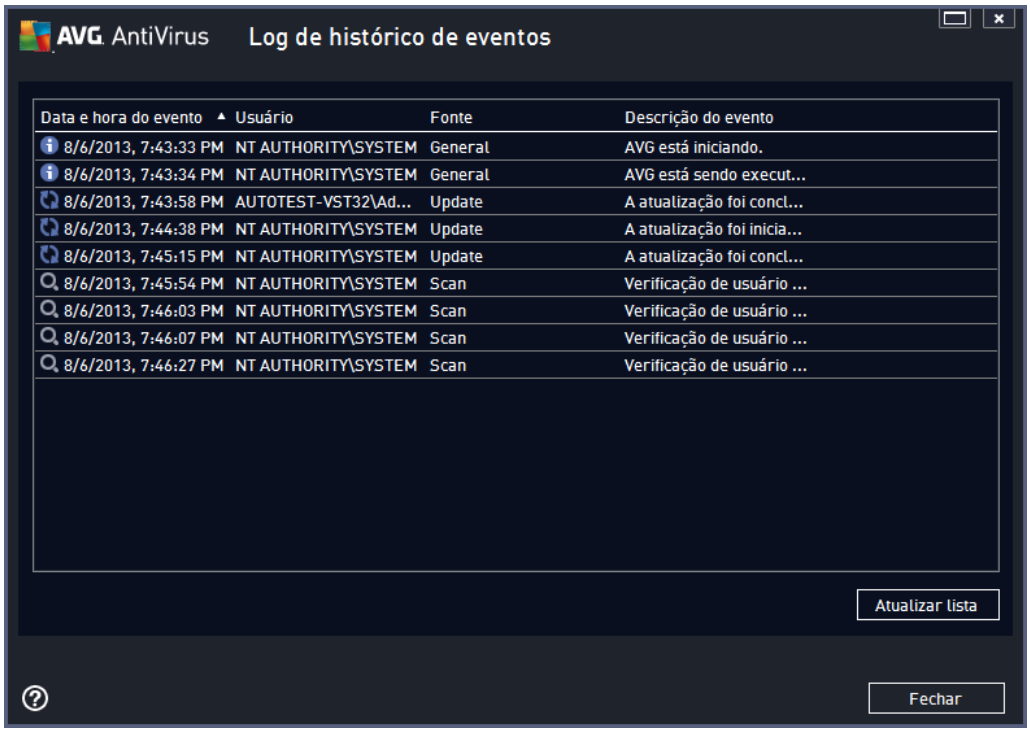
Em cada objeto detectado, são fornecidas as seguintes informações:

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

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

13.6. 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 AntiVirus 2014**. Nesta caixa de diálogo, você encontrará um resumo dos eventos importantes que ocorreram durante a operação do **AVG AntiVirus 2014**. O diálogo fornece registros dos seguintes tipos de eventos: i nformações 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 **AVG AntiVirus 2014** janela principal

14. 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 AntiVirus 2014** regularmente. A melhor solução é ater-se às configurações padrão do programa onde a atualização automática está configurada. Saiba que se o banco de dados de vírus de seu **AVG AntiVirus 2014** 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.

14.1. Iniciar atualização

Para proporcionar o máximo de segurança disponível, o **AVG AntiVirus 2014** 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. Quando você inicia a atualização, o AVG primeiro verifica se há novos arquivos de atualização disponíveis. Se houver, o **AVG AntiVirus 2014** 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 de programa

14.2. Níveis de atualização

O **AVG AntiVirus 2014** oferece dois níveis de atualização:

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

programa.

Ao agendar uma atualização, você pode definir parâmetros específicos para ambos os níveis de atualização:

- Agendamento de atualização de definições
- Agendamento de atualização de programa

Obs.: *se uma atualização programada e verificação programada do programa coincidirem, o processo de atualização tem maior prioridade e a verificação será interrompida. Neste caso, você será informado sobre o conflito.*

15. Perguntas frequentes e Suporte técnico

Caso tenha problemas técnicos ou relacionados a vendas com o aplicativo **AVG AntiVirus 2014**, 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 AntiVirus 2014** *(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 levem 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 ***Centro de Suporte***, você pode encontrar uma visão geral estruturada sobre grupos temáticos que lidam com problemas técnicos e relacionados a vendas.

- ***Perguntas frequentes***: no site do AVG (*http://www.avg.com/*) você também pode encontrar uma seção separada e de estrutura elaborada com perguntas frequentes. Esta seção pode ser acessada através da opção de menu ***Centro de Suporte/Perguntas frequentes e tutoriais***. Novamente, todas as perguntas são divididas de maneira organizada nas categorias técnica, de vendas e de vírus.

- ***AVG ThreatLabs***: um website específico relacionado ao AVG (*http://www.avgthreatlabs.com/website-safety-reports/*) 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://forums.avg.com.