Avira

Free Antivirus

Manual do usário

Marcas Registradas e Direitos Autorais

Marcas Registradas

Windows é uma marca registrada da Microsoft Corporation nos Estados Unidos e em outros países.
Todas as outras marcas e nomes de produtos são marcas comerciais ou marcas registradas de seus respectivos proprietários.
As marcas comerciais protegidas não são marcadas como tal neste manual. No entanto, isso não significa que elas podem ser usadas livremente.

Informações sobre direitos autorais

Um código fornecido por provedores de terceiros foi usado para o Avira Free Antivirus. Agradecemos os detentores dos direitos autorais por disponibilizar o código para nós.
Para informações detalhadas sobre direitos autorais, consulte Licenças de Terceiros.

Contrato de Licença de Usuário Final - EULA

http://www.avira.com/pt-br/license-agreement

Política de privacidade

http://www.avira.com/pt-br/general-privacy

Sumário

1. Introdução

Seu produto Avira protege seu computador contra vírus, worms, cavalos de Troia, adware e spyware e outros riscos. Neste manual, eles são referidos como vírus ou malware (software nocivo) e programas indesejados.

O manual descreve a instalação e a operação do programa.

Para obter opções e informações adicionais, visite nosso site:
http://www.avira.com/pt-br

O site da Avira permite:

- acessar informações sobre outros programas da área de trabalho da Avira
- fazer download dos programas da área de trabalho da Avira mais recentes
- fazer download dos manuais de produto mais recentes no formato PDF
- fazer download de ferramentas gratuitas de suporte e reparo
- acessar nosso abrangente banco de dados de conhecimento e perguntas frequentes para solução de problemas
- acessar endereços de suporte específicos do país.

Sua Equipe Avira

1.1 Ícones e ênfases

Os seguintes ícones são usados:

Ícone / designação	Explicação
✓	Colocado antes de uma condição que deve ser cumprida antes da execução de uma ação.
▸	Colocado antes de uma ação executada por você.
↪	Colocado antes de um evento que segue a ação anterior.
Aviso	Colocado antes de um aviso quando pode ocorrer a perda de dados críticos.

Observação	Colocado antes de um link para informações particularmente importantes ou uma dica que torna o produto Avira mais fácil de usar.

As seguintes ênfases são usadas:

Ênfase	Explicação
Itálico	Dados do nome de arquivo ou do caminho.
	Elementos de interface de software exibidos (por exemplo, seção da janela ou mensagem de erro).
Negrito	Elementos de interface de software clicáveis (por exemplo, item de menu, área de navegação, caixa de opção ou botão).

2. Informações do produto

Este capítulo contém todas as informações relevantes para a compra e o uso de seu produto Avira:

- consulte o Capítulo: Escopo da Entrega
- consulte o Capítulo: Requisitos do Sistema
- consulte o Capítulo: Licenciamento e Atualização

Os produtos Avira são ferramentas abrangentes e flexíveis que protegem seu computador contra vírus, malware, programas indesejados e outros perigos.

▸ Observe o seguinte:

Aviso
A perda de dados valiosos normalmente tem consequências dramáticas. Até mesmo o melhor programa de proteção contra vírus não pode fornecer proteção total contra a perda de dados. Faça cópias regularmente (backups) de seus dados por motivos de segurança.

Observação
Um programa só pode fornecer proteção confiável e eficiente contra vírus, malwares, programas indesejados e outros perigos se estiver atualizado. Verifique se seu produto Avira está atualizado com atualizações automáticas. Configure o programa conforme necessário.

2.1 Escopo da Entrega

Seu produto Avira possui as seguintes funções:

- Centro de Controle para monitorar, gerenciar e controlar o programa inteiro
- Configuração centralizada com opções padrão e avançadas amigáveis e ajuda contextual
- Scanner (varredura por demanda) com varredura configurável e controlada por perfis de todos os tipos conhecidos de vírus e malwares
- A integração no Controle de Conta de Usuário do Windows permite que você realize tarefas que exigem direitos de administrador.
- Real-Time Protection (varredura no acesso) para monitoramento contínuo de todas as tentativas de acesso ao arquivo

- Avira SearchFree Toolbar, uma barra de ferramentas de procura integrada no navegador da web que fornece opções de procura rápidas e convenientes. Também inclui widgets das funções da Internet mais comuns.
- Web Protection (apenas para usuários do Avira Free Antivirus em combinação com o Avira SearchFree) para monitorar dados e arquivos transferidos da internet usando o protocolo HTTP (monitoramento das portas 80, 8080 e 3128)
- O aplicativo Avira Free Android Security não está somente focado em medidas antirroubo. O aplicativo ajuda a recuperar o seu dispositivo móvel em caso de perda, ou pior, em caso de furto. Além disso, o aplicativo permite bloquear chamadas recebidas ou SMS. O Avira Free Android Security protege celulares e smartphones com o sistema operacional Android.
- Gerenciamento de quarentena integrado para isolar e processar arquivos suspeitos
- Rootkits Protection para detectar malware oculto instalado em seu sistema de computador (rootkits)
  (Não disponível no Windows XP de 64 bits)
- Acesso direto para informações detalhadas sobre os vírus e malwares detectados via Internet
- Atualizações simples e rápidas para o programa, definições de vírus e mecanismo de procura por meio da Atualização de Único Arquivo e atualizações incrementais de VDF por meio de um servidor da web na Internet
- Agendamento Integrado para planejar trabalhos individuais ou recorrentes, como atualizações ou verificações
- Altíssima taxa de detecção de vírus e malware com uma inovadora tecnologia de varredura (mecanismo de varredura), incluindo o método de varredura heurística
- Detecção de todos os tipos convencionais de arquivos, inclusive detecção de arquivos aninhados e detecção inteligente de extensões
- Função de multithreading de alto desempenho (varredura simultânea de vários arquivos em alta velocidade)

2.2 Requisitos do Sistema

2.2.1 Requisitos do sistema do Avira Free Antivirus

O Avira Free Antivirus tem os seguintes requisitos necessários para o uso bem sucedido do sistema:

Sistema operacional

- Windows 8, SP mais recente (32 ou 64 bits) ou
- Windows 7, SP mais recente (32 ou 64 bits) ou
- Windows XP, SP mais recente (32 ou 64 bits)

Hardware

- Computador com processador Pentium ou superior de pelo menos 1 GHz
- Pelo menos 150 MB de espaço livre de memória no disco rígido (mais se for usada a quarentena para armazenamento temporário)
- Pelo menos 1024 MB de RAM no Windows 8, Windows 7
- Pelo menos 512 MB de RAM no Windows XP

Outros requisitos

- Para a instalação do programa: Direitos de administrador
- Para todas as instalações: Windows Internet Explorer 6.0 ou superior
- Conexão com a Internet, se apropriado (consulte Preparando para instalação)

2.2.2 Requisitos do sistema do Avira SearchFree Toolbar

Os seguintes requisitos devem ser cumpridos para o uso correto do Avira SearchFree Toolbar:

Sistema operacional

- Windows 8, SP mais recente (32 ou 64 bits) ou
- Windows 7, SP mais recente (32 ou 64 bits) ou
- Windows XP, SP mais recente (32 ou 64 bits)

Navegador da Web

- Windows Internet Explorer 6.0 ou superior
- Mozilla Firefox 3.0 ou superior
- Google Chrome 18.0 ou superior

Observação
Se necessário, desinstale quaisquer barras de ferramenta de pesquisa instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.

2.2.3 Direitos de Administrador (a partir do Windows Vista)

No Windows XP, muitos usuários trabalham com direitos de administrador. No entanto, isso não é desejável do ponto de vista de segurança, pois facilita a invasão de vírus e programas indesejados nos computadores.

Por isso, a Microsoft introduziu o "Controle de Conta de Usuário" (UAC). O Controle de Conta de Usuário é parte dos seguintes sistemas operacionais:

- Windows Vista
- Windows 7

- Windows 8

O Controle de Conta de Usuário oferece maior proteção a usuários que estão conectados como administradores. No entanto, o administrador possui apenas os privilégios de um usuário normal, a princípio. Ações para as quais os direitos de administrador são necessárias estão claramente marcadas no sistema operacional com um ícone de informações. Além disso, o usuário deve confirmar explicitamente a ação necessária. Os privilégios aumentam e a tarefa administrativa é realizada pelo sistema operacional após a obtenção dessa permissão.

O Avira Free Antivirus requer direitos de administrador para algumas ações. Essas ações são marcadas com o símbolo a seguir:  . Se esse símbolo também aparecer em um botão, os direitos de administrador serão necessários para realizar essa ação. Se a sua conta de usuário atual não tem direitos de administrador, a caixa de diálogo de Controle de Conta de Usuário do Windows solicitará a inserção da senha de administrador. Se você não tiver uma senha de administrador, não poderá realizar essa ação.

2.3 Licenciamento e Atualização

Para poder usar seu produto Avira, é necessária uma licença. Ao usar a licença, você aceita os termos da licença.

A licença é emitida através de uma licença digital na forma de um arquivo.*KEY*. Esse arquivo de licença digital é a chave de sua licença pessoal. Ele contém detalhes exatos sobre os programas que foram licenciados para você e por quanto tempo. Portanto, o arquivo de licença digital também pode conter a licença de mais de um produto.

Se você adquiriu seu produto Avira na Internet, ou por meio de um CD/DVD do programa, o arquivo de licença digital será enviado para você por e-mail.

Um código de ativação válido já está contido no Avira Free Antivirus. Por este motivo, a ativação do produto não é necessária.

3. Instalação e desinstalação

Este capítulo contém informações relacionadas à instalação do Avira Free Antivirus.

3.1 Preparando para instalação

- ✓ Antes da instalação, verifique se seu computador preenche todos os Requisitos mínimos do sistema.
- ✓ Feche todos os aplicativos em execução.
- ✓ Verifique se nenhuma outra solução de proteção contra vírus está instalada. As funções de proteção automática de várias soluções de segurança podem interferir umas nas outras (para opções automáticas, consulte Removendo software incompatível).
- ✓ Se necessário, desinstale quaisquer barras de ferramenta de pesquisa instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.
- ✓ Estabeleça uma conexão com a Internet.
- A conexão é necessária para realizar as seguintes etapas de instalação:
  - Download do arquivo do programa e do mecanismo de pesquisa atuais, bem como dos arquivos de definição de vírus mais recentes através do programa de instalação (para instalação baseada na Internet)
  - Ativando o programa
  - Registrando como um usuário
  - Quando apropriado, realizar uma atualização após a conclusão da instalação
- ✓ Mantenha o código de ativação ou arquivo de licença para o seu Avira Free Antivirus acessível para quando desejar ativar o programa.
- ✓ Para ativação ou registro do produto, o Avira Free Antivirus usa protocolo HTTP e Porta 80 (comunicação na Web), bem como protocolo de criptografia SSL e Porta 443 para comunicaçã com os servidores Avira. Se estiver usando um firewall, certifique-se de que as conexões necessárias e/ou os dados de entrada ou de saída não estejam bloqueados pelo firewall.

3.2 Instalando software baixado do Avira Shop

- Vá para www.avira.com/download.

  Selecione o produto e clique em **Download**.

  Salve o arquivo baixado no seu sistema.

  Clique duas vezes no arquivo de instalação avira_free_antivirus_en.exe.

  Se a janela de Controle de conta do usuário aparecer, clique em Sim

  O programa verifica softwares incompatíveis (mais informações aqui: Removendo software incompatível).

  O arquivo de instalação será extraído. A rotina de instalação será iniciada.

  Continue com Selecionando um tipo de instalação.

3.3 Removendo software incompatível

O Avira Free Antivirus procurará qualquer sotware incompatível possível em seu computador. Se algum software potencialmente incompatível for detectado, o Avira Free Antivirus gerará uma lista desses programas. É recomendado remover esses programas de software para não arriscar a estabilidade de seu computador.

- Selecione na lista as caixas de seleção de todos os programas que devem ser removidos automaticamente de seu computador e clique em **Avançar**.

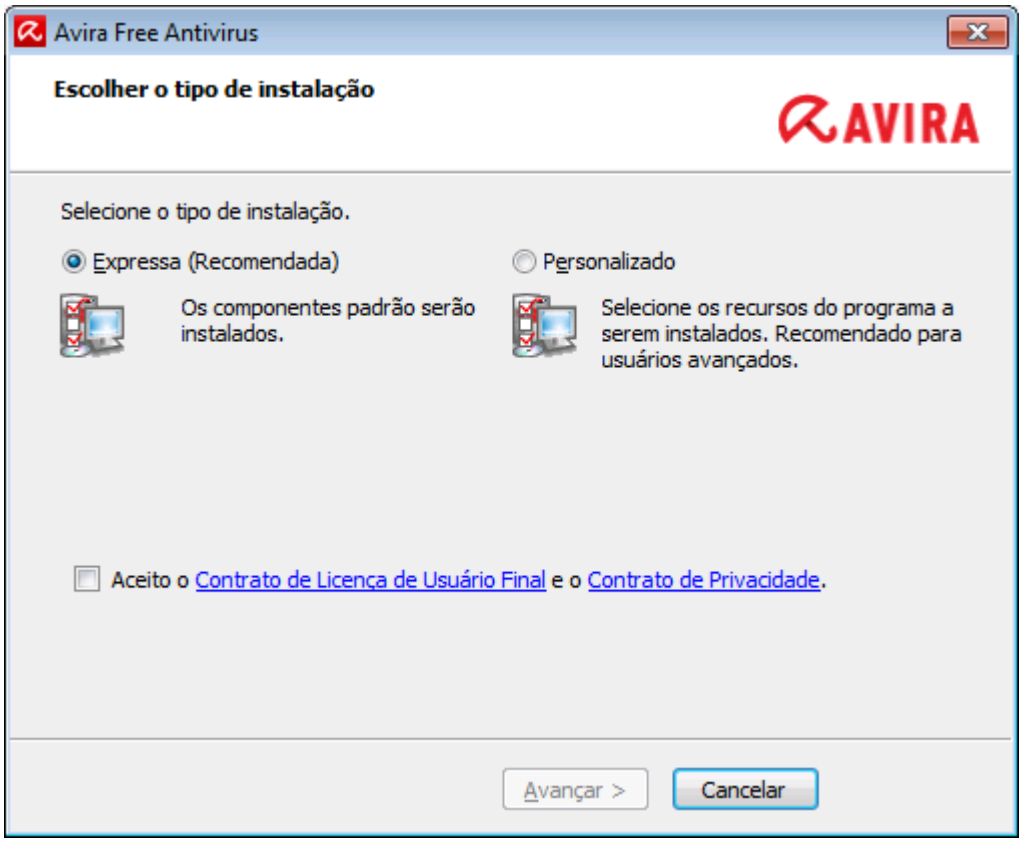
  Para alguns produtos, a desinstalação precisa ser confirmada manualmente.

  Selecione os programas e clique em **Avançar**.

  A desinstalação de um ou mais programas selecionados pode requerer a reinicialização do computador. Após a reinicialização, a instalação começará.

3.4 Selecionando um tipo de instalação

Durante a instalação, você pode escolher um tipo de instalação no assistente de instalação. O assistente de instalação é projetado para guiá-lo de modo fácil na instalação.



Tópicos relacionados:

- consulte Executando uma Instalação Expressa
- consulte Executando uma instalação personalizada

3.4.1 Executando uma Instalação Expressa

A *Instalação Expressa* é a rotina de instalação recomendada.

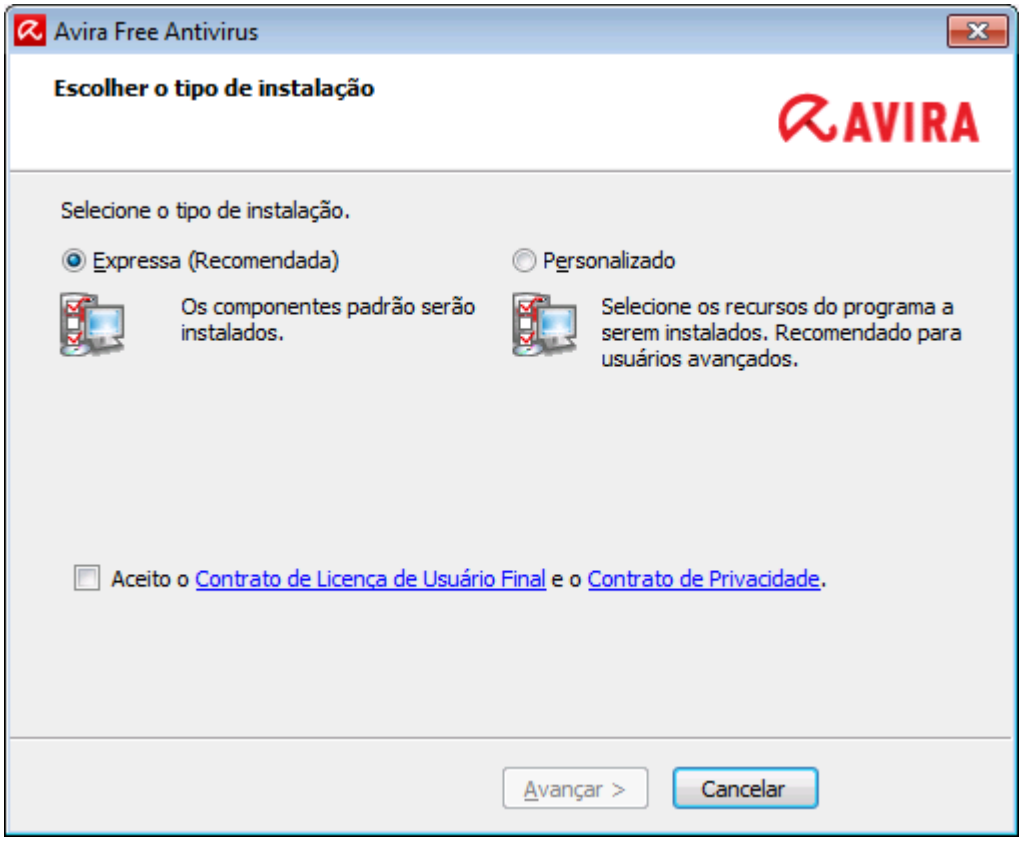
- Ela instala todos os componentes padrão do Avira Free Antivirus. As configurações de nível de segurança recomendadas do Avira são usadas.
- Como padrão, um dos caminhos de instalação a seguir é escolhido:
  - *C:\Program Files\Avira* (para versões Windows 32 bits) ou
  - *C:\Program Files (x86)\Avira* (para versões Windows 64 bits)
- Aqui, você pode encontrar todos os arquivos relacionados ao Avira Free Antivirus.
- Se escolher este tipo de instalação, você poderá efetuar uma instalação apenas clicando em **Avançar** até concluir.
- Este tipo de instalação é projetado especialmente para os usuários que não se sentem confortáveis em configurar ferramentas de software.

3.4.2 Executando uma instalação personalizada

A *Instalação Personalizada* permite configurar a instalação. Isso só é recomendado para usuários avançados que estejam bem familiarizados com softwares e hardwares, assim como com questões de segurança.

- Você pode escolher instalar componentes de programa individuais.
- Uma pasta de destino pode ser selecionada para os arquivos de programa a serem instalados.
- Você pode desativar **Criar um ícone na área de trabalho e grupo de programa no menu Iniciar**.
- Usando o assistente de configuração, você pode definir as configurações para o Avira Free Antivirus. Você também pode escolher o nível de segurança com o qual esteja confortável.
- Após a instalação, você pode iniciar uma pequena varredura de sistema que é efetuada automaticamente após a instalação.

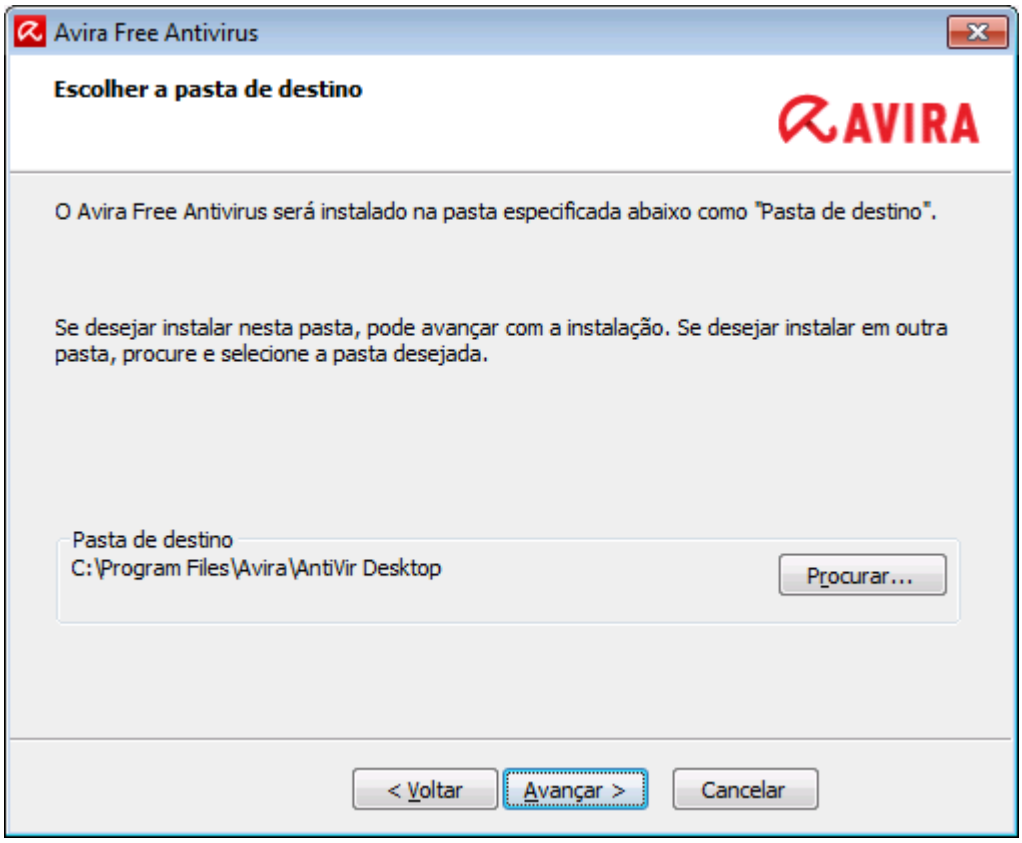
3.5 Instalando o Avira Free Antivirus



Confirme se aceita o **Contrato de Licença do Usuário Final**. Para ler o texto detalhado do **Contrato de Licença do Usuário Final**, clique no link.

3.5.1 Escolhendo uma pasta de destino

A instalação personalizada permite escolher a pasta na qual deseja instalar o Avira Free Antivirus.



- Clique em **Procurar** e navegue até o local onde deseja instalar o Avira Free Antivirus.

  Selecione a pasta na qual deseja instalar o Avira Free Antivirus na janela **Escolher pasta de destino**.

  Clique em **Avançar**.

3.5.2 Instalando o Avira SearchFree Toolbar

Ao fim da instalação, você pode instalar o Avira SearchFree Toolbar.

O Avira SearchFree Toolbar inclui dois componentes principais: o Avira SearchFree e a Barra de ferramentas.

Com o Avira SearchFree, você pesquisa na Internet inúmeros termos. Este mecanismo de pesquisa exibe todos os resultados na janela do navegador, classificando seu nível de segurança. Isso permite uma navegação mais segura aos usuários do Avira.

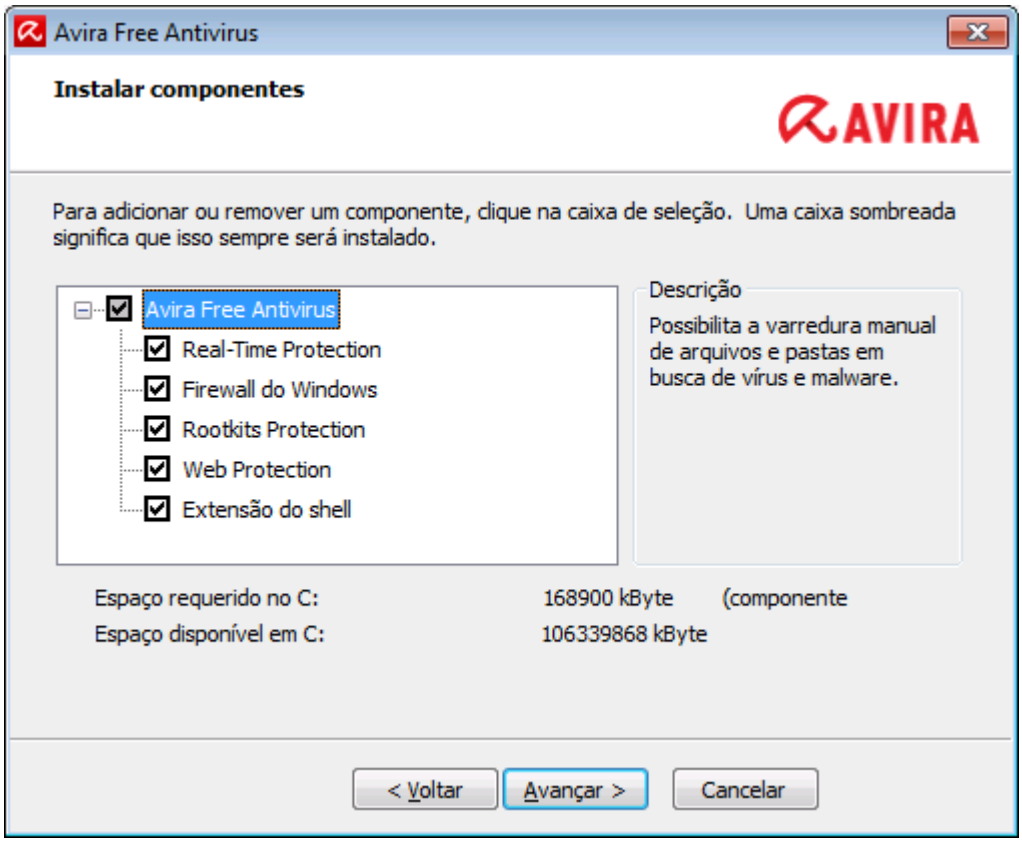
A Barra de ferramentas oferece três widgets para as funções mais importantes relacionadas à Internet. Com um clique, você tem acesso direto ao Facebook e ao seu e-mail ou pode garantir navegação segura na web (somente Firefox e Internet Explorer).

Se você não quiser instalar o Avira SearchFree Toolbar, desmarque as caixas de marcação das opções **Definir e manter o Ask como meu provedor de pesquisa padrão** e **Definir e manter o Avira SearchFree (avira.search.ask.com) como a página inicial do navegador e a nova página de aba do navegador.**

Se você recusar, somente a instalação do Avira SearchFree Toolbar será cancelada. A instalação do Avira Free Antivirus, entretanto, será concluída.

3.5.3 Escolhendo componentes de instalação

Em uma instalação personalizada ou uma modificação de instalação, os componentes de instalação a seguir podem ser selecionados, adicionados ou removidos.



Selecione ou cancele componentes da lista na caixa de diálogo de Instalar componentes.

- **Avira Free Antivirus**
  Ele contém todos os componentes necessários para uma instalação bem-sucedida do Avira Free Antivirus.
  - **Real-Time Protection**
    O Avira Real-Time Protection é executado em segundo plano. Ele monitora e repara, se possível, os arquivos durante operações como abrir, gravar e copiar no "modo de acesso". O modo de acesso significa que, sempre que o usuário realiza uma operação de arquivo (por exemplo, carregar documento, executar, copiar), o Avira Free Antivirus verifica o arquivo automaticamente. Renomear o arquivo, entretanto, não dispara uma verificação pelo Avira Real-Time Protection.
  - **Firewall do Windows** (a partir do Windows 7)
    Este componente gerencia o Firewall do Windows a partir do Avira Free Antivirus.
  - **Rookits Protection**
    O Avira Rookits Protection verifica se há software já instalado no computador que não possa mais ser detectado com métodos convencionais de proteção contra malware depois da invasão do sistema do computador.
  - **ProActiv** O componente ProActiv monitora ações do aplicativo e alerta os usuários quanto ao comportamento de aplicativo suspeito. Esse reconhecimento baseado em comportamento permite que você se proteja contra malware desconhecido. O componente ProActiv está integrado ao Avira Real-Time Protection.
  - **Web Protection** (para usuários do Avira Free Antivirus, somente em combinação com o Avira SearchFree Toolbar)
    Ao navegar pela Internet, você está usando seu navegador da Web para solicitar

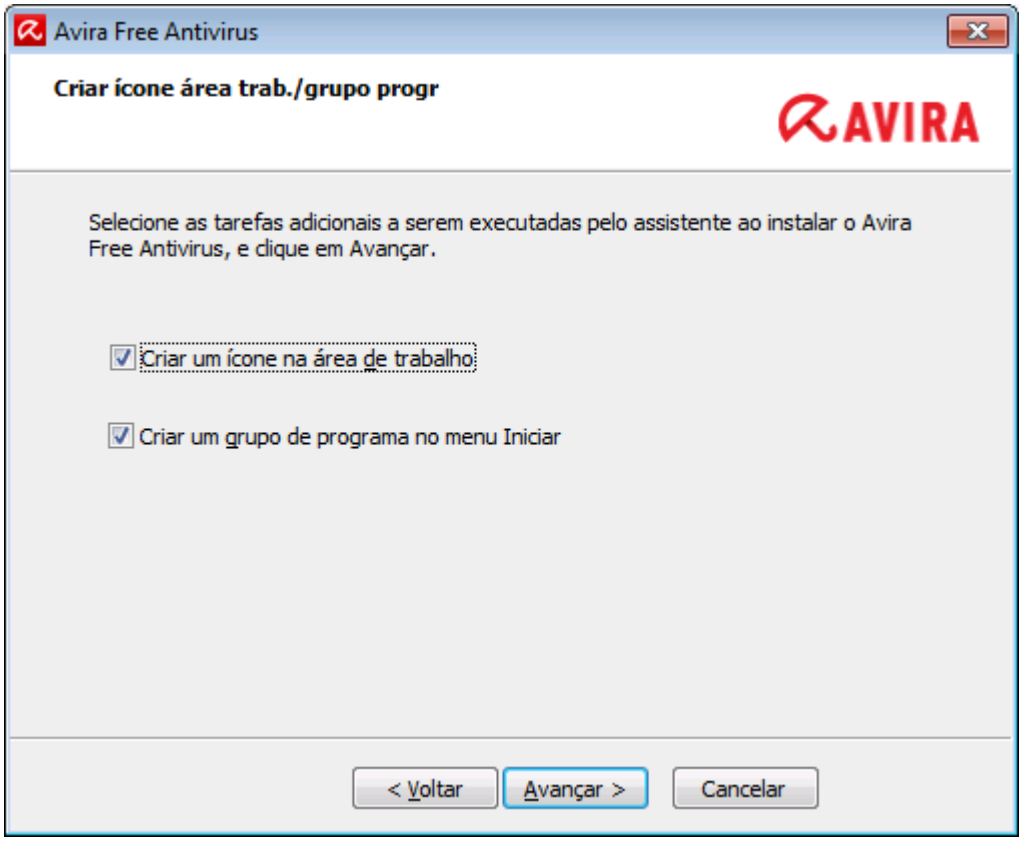
dados de um servidor da Web. Os dados transferidos do servidor da Web (arquivos HTML, arquivos de script e de imagem, arquivos Flash, fluxos de vídeo e música, etc.) em geral são movidos diretamente no cache do navegador para serem exibidos no navegador da Web, de forma que uma verificação de acesso realizada pelo Avira Real-Time Protection não é possível. Isso poderia permitir o acesso de vírus e programas indesejados ao sistema do computador. O Web Protection é um proxy HTTP que monitora as portas usadas para transferência de dados (80, 8080, 3128) e verifica os dados transferidos em busca de vírus e programas indesejados. Dependendo da configuração, o programa pode processar os arquivos afetados automaticamente ou solicitar uma ação específica ao usuário.

- **Extensão do shell**
  O Extensão do shell gera uma entrada **Varredura de arquivos selecionados com o Avira** no menu contextual do Windows Explorer (botão direito do mouse). Com essa entrada, é possível verificar arquivos ou diretórios diretamente.

Tópicos relacionados:
Alterando uma instalação

3.5.4 Criando atalhos para o Avira Free Antivirus

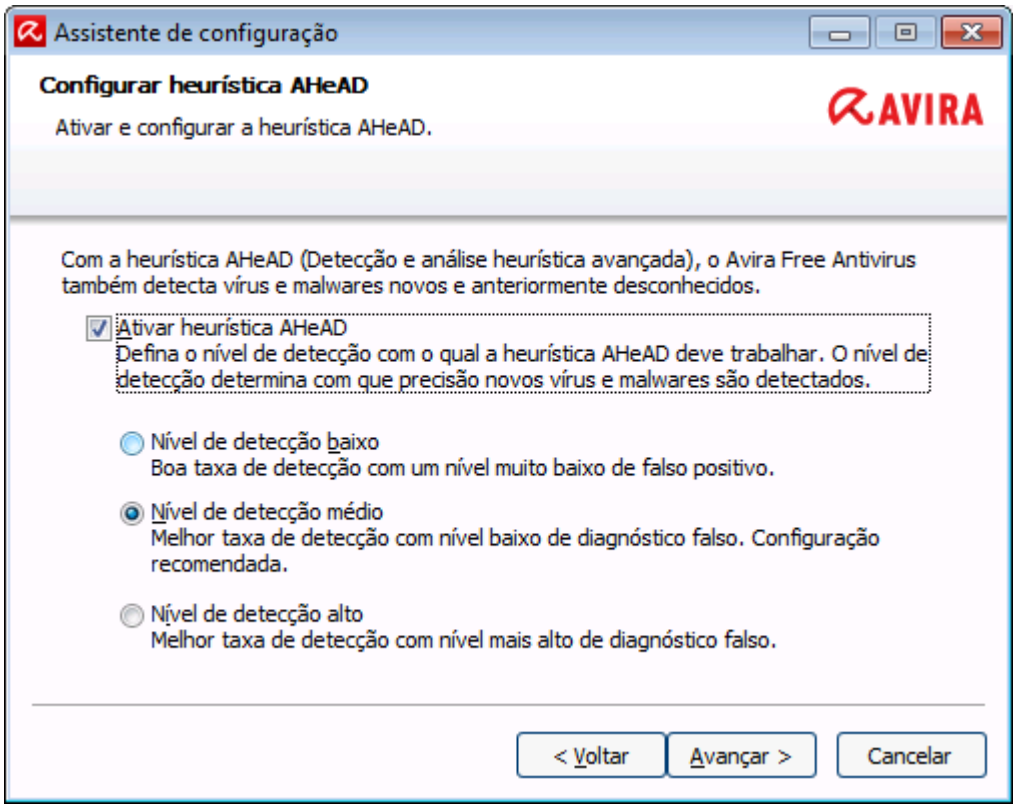
Um ícone na área de trabalho e/ou um grupo de programa no menu Iniciar ajudam você a acessar o Avira Free Antivirus de modo mais fácil e rápido.



- Para criar um atalho na área de trabalho para o Avira Free Antivirus e/ou um grupo de programa no **menu Iniciar** deixe a opção ativada.

3.5.5 Configurando o nível de detecção heurística (AHeAD)

O Avira Free Antivirus possui uma ferramenta muito poderosa na forma de tecnologia Avira AHeAD (*Análise e Detecção Heurística Avançada*). Essa tecnologia usa técnicas de reconhecimento de padrões para detectar malwares desconhecidos (novos) a partir da análise anterior de outros malwares.

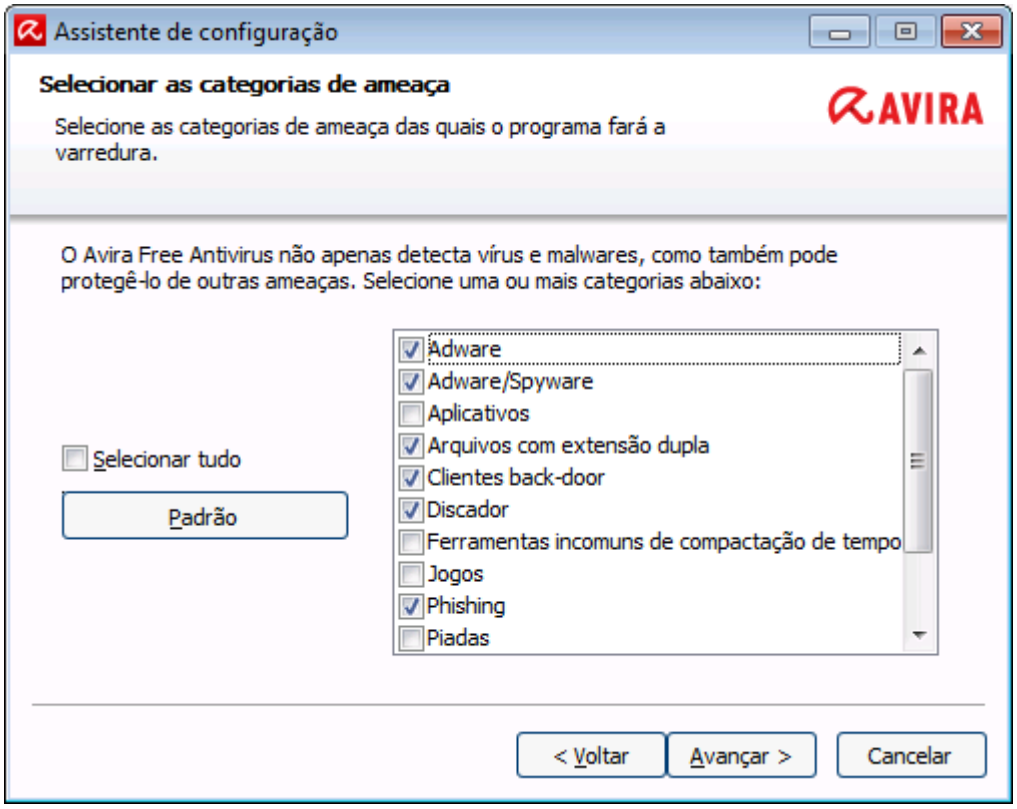


- Selecione um nível de detecção na caixa de diálogo **Configurar AHeAD** e clique em **Avançar**.

  O nível de detecção selecionado é usado para as configurações da tecnologia AHeAD System Scanner (verificação por demanda) e Real-Time Protection (verificação por acesso).

3.5.6 Selecionando categorias de ameaça estendida

Vírus e malware não são ameaças que representam perigo apenas ao sistema do computador. Nós definimos uma lista de riscos e os classificamos em categorias de ameaça estendida para você.



- Um número de categorias de ameaças já é pré-selecionado por padrão.

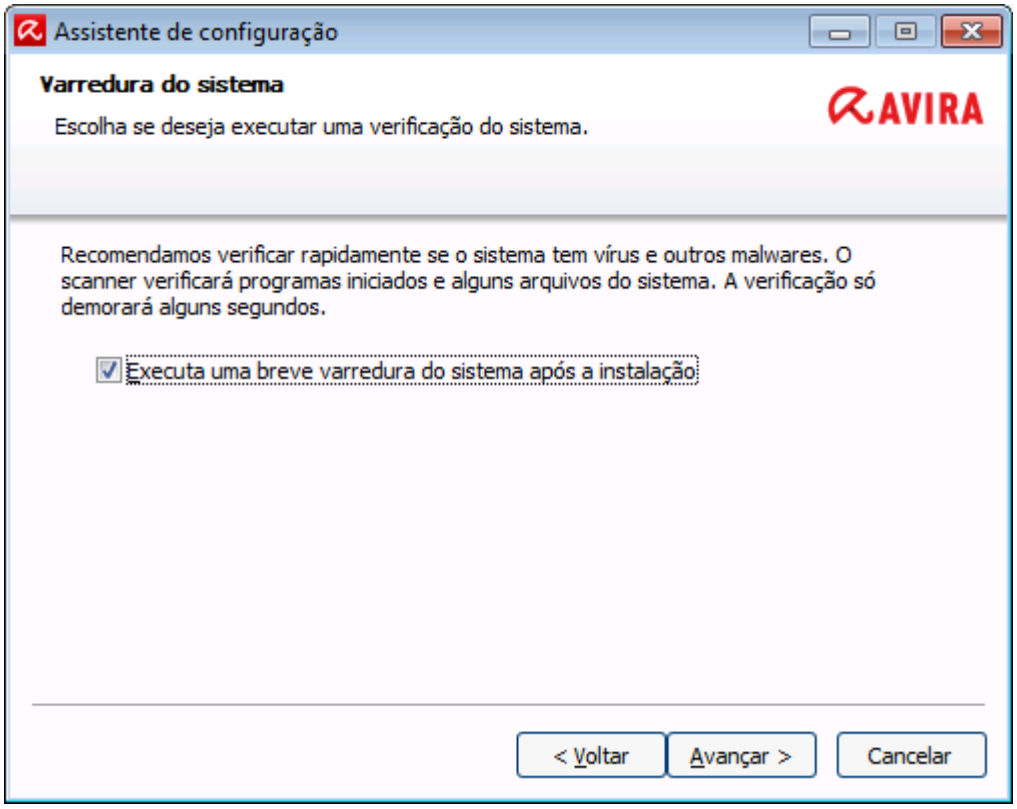
  Onde seja adequado, ative mais categorias de ameaça na caixa de diálogo **Selecionar categorias de ameaça estendida**.

  Se você mudar de ideia, reverta para os valores recomendados clicando no botão **Valores padrão**.

  Continue a instalação clicando em **Avançar**.

3.5.7 Iniciando uma varredura após a instalação

Para verificar o estado de segurança atual do computador, uma varredura rápida do sistema pode ser efetuada após a configuração ser concluída e antes do computador ser reinicializado. O System Scanner verifica os programas em execução e os arquivos de sistema mais importantes em busca de vírus e malware.



- Se você quiser efetuar uma varredura rápida do sistema, deixe a opção **Varredura rápida do sistema** ativada.

  Clique em **Avançar**.

  Complete a configuração clicando em **Concluir**.

  Se você não desativar a opção **Varredura rápida do sistema**, a janela *Luke Filewalker* abre.

  O System Scanner executa uma varredura rápida do sistema.

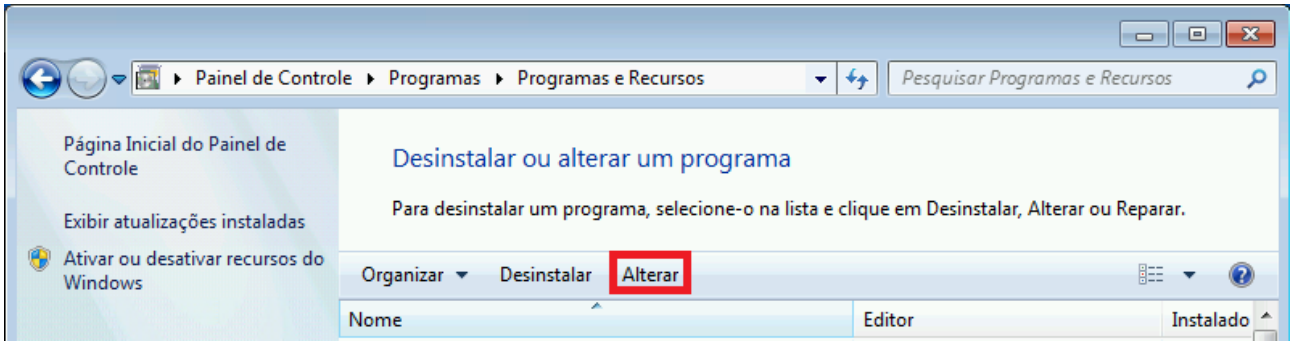
3.6 Alterando a instalação

Se quiser adicionar ou remover módulos da instalação atual, você pode fazer isso sem precisar desinstalar o Avira Free Antivirus. Segue o guia:

- Alterando uma instalação no Windows 8
- Alterando uma instalação no Windows 7
- Alterando uma instalação no Windows XP

3.6.1 Alterando uma instalação no Windows 8

Você tem a opção de adicionar ou remover componentes de programa individuais na instalação do Avira Free Antivirus (consulte Escolhendo componentes de instalação).



Se você quiser adicionar ou remover módulos da instalação atual, você poderá usar a opção **Desinstalar programas** no **Painel de Controle do Windows** para **Alterar/Desinstalar** programas.

- Clique com o botão direito do mouse na tela.

  O símbolo **Todos os aplicativos** aparecerá.

  Clique no símbolo e procure na seção *Aplicativos - Sistema Windows* o **Painel de Controle**.

  Clique duas vezes no símbolo do **Painel de Controle**.

  Clique em **Programas - Desinstalar um programa**.

  Clique em **Programas e Recursos - Desinstalar um programa**.

  Selecione Avira Free Antivirus e clique em **Alterar**.

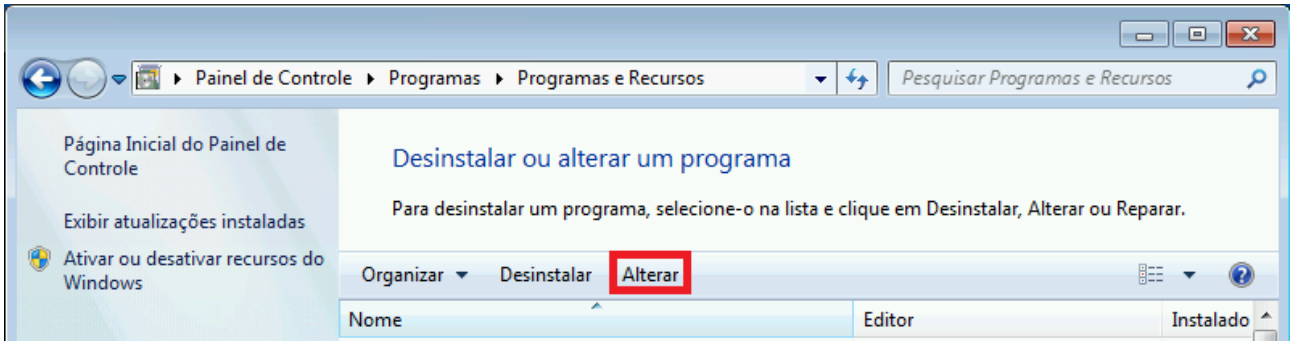
  No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

Observação
Se você desinstalar o Avira SearchFree Toolbar, o Web Protection também será desinstalado.

Tópicos relacionados:
Escolhendo componentes de instalação

3.6.2 Alterando uma instalação no Windows 7

Você tem a opção de adicionar ou remover componentes de programa individuais na instalação do Avira Free Antivirus (consulte Escolhendo componentes de instalação).



Se desejar adicionar ou remover módulos da instalação atual, você poderá usar a opção **Adicionar ou Remover Programas** no **Painel de Controle do Windows** para **Alterar/Remover** programas.

- Abra o **Painel de Controle** através do menu **Iniciar** do Windows.

  Clique duas vezes em **Programas e Recursos**.

  Selecione Avira Free Antivirus e clique em **Alterar**.

  No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

Observação
Se você desinstalar o Avira SearchFree Toolbar, o Web Protection também será desinstalado.

Tópicos relacionados:
Escolhendo componentes de instalação

3.6.3 Alterando uma instalação no Windows XP

Você tem a opção de adicionar ou remover componentes de programa individuais na instalação do Avira Free Antivirus (consulte Escolhendo módulos de instalação).

Se desejar adicionar ou remover módulos da instalação atual, você poderá usar a opção **Adicionar ou Remover Programas** no **Painel de Controle do Windows** para **Alterar/Remover** programas.

- Abra o **Painel de Controle** através do menu **Iniciar > Configurações** do Windows.

  Clique duas vezes em **Adicionar ou Remover Programas**.

  Selecione Avira Free Antivirus e clique em **Alterar**.

  No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

Observação
Se você desinstalar o Avira SearchFree Toolbar, o Web Protection também será desinstalado.

Tópicos relacionados:
Escolhendo componentes de instalação

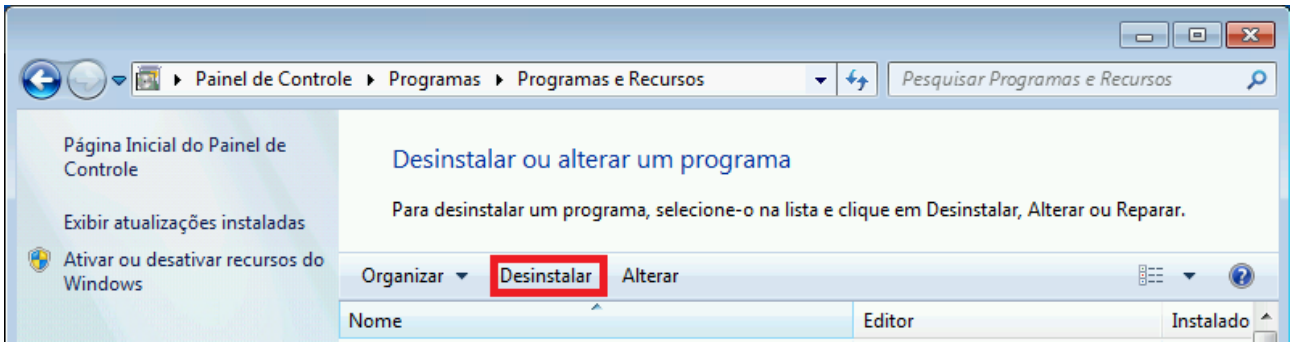
3.7 Desinstalação

Se você achar que precisa desinstalar o Avira Free Antivirus, aqui está como fazer isso:

- Desinstalando Avira Free Antivirus no Windows 8
- Desinstalando Avira Free Antivirus no Windows 7
- Desinstalando Avira Free Antivirus no Windows XP

3.7.1 Desinstalando o Avira Free Antivirus no Windows 8

Para desinstalar o Avira Free Antivirus do seu computador, use a opção **Programas e Recursos** no Painel de Controle do Windows.



- Clique com o botão direito do mouse na tela.

  O símbolo **Todos os aplicativos** aparecerá.

  Clique no símbolo e procure na seção *Aplicativos - Sistema Windows* o **Painel de Controle**.

  Clique duas vezes no símbolo do **Painel de Controle**.

  Clique em **Programas - Desinstalar um programa**.

  Clique em **Programas e Recursos - Desinstalar um programa**.

  Selecione Avira Free Antivirus na lista e clique em **Desinstalar**.

  Ao ser perguntado se deseja realmente remover o aplicativo e todos os seus componentes, clique em **Sim** para confirmar.

Ao ser perguntado se deseja ativar o Firewall do Windows (o Avira FireWall será desinstalado), clique em **Sim** para confirmar e manter ao menos alguma proteção no seu sistema.

Todos os componentes do programa serão removidos.

Clique em **Concluir** para concluir a desinstalação.

Se uma caixa de diálogo aparecer recomendando a reinicialização do computador, clique em **Sim** para confirmar.

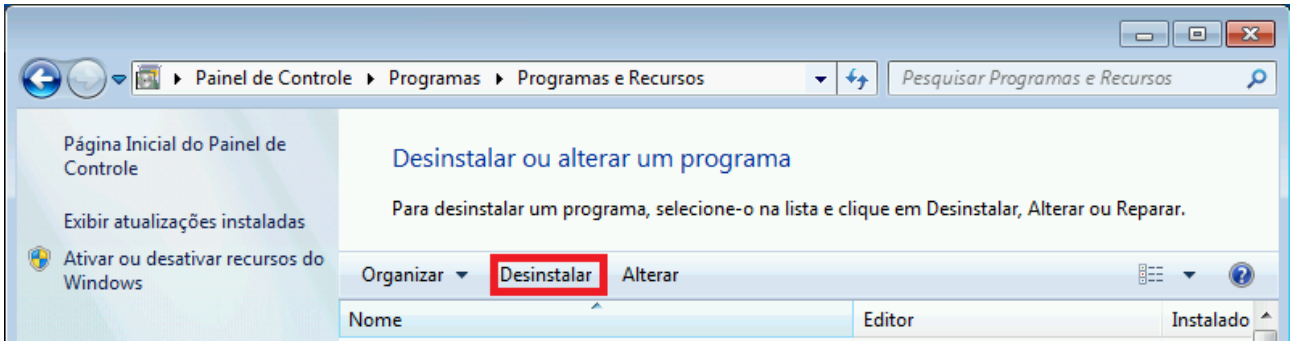
O Avira Free Antivirus agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

Observação
O Avira SearchFree Toolbar não está incluído no programa de desinstalação e deve ser desinstalado separadamente.

Observação
Se você desinstalar o Avira SearchFree Toolbar, o Web Protection também será desinstalado.

3.7.2 Desinstalando o Avira Free Antivirus no Windows 7

Para desinstalar o Avira Free Antivirus do seu computador, use a opção **Programas e Recursos** no Painel de Controle do Windows.



- Abra o **Painel de Controle** através do menu **Iniciar** do Windows.

  Clique em **Programas e Recursos**.

  Selecione Avira Free Antivirus na lista e clique em **Desinstalar**.

  Ao ser perguntado se deseja realmente remover o aplicativo e todos os seus componentes, clique em **Sim** para confirmar.

Ao ser perguntado se deseja ativar o Firewall do Windows (o Avira FireWall será desinstalado), clique em **Sim** para confirmar e manter ao menos alguma proteção no seu sistema.

Todos os componentes do programa serão removidos.

Clique em **Concluir** para concluir a desinstalação.

Se uma caixa de diálogo aparecer recomendando a reinicialização do computador, clique em **Sim** para confirmar.

O Avira Free Antivirus agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

Observação
O Avira SearchFree Toolbar não está incluído no programa de desinstalação e deve ser desinstalado separadamente.

Observação
Se você desinstalar o Avira SearchFree Toolbar, o Web Protection também será desinstalado.

3.7.3 Desinstalando o Avira Free Antivirus no Windows XP

Para desinstalar o Avira Free Antivirus do seu computador, use a opção **Alterar ou Remover Programas** no Painel de Controle do Windows.

- Abra o **Painel de Controle** através do menu **Iniciar > Configurações** do Windows.

  Clique duas vezes em **Adicionar ou Remover Programas**.

  Selecione Avira Free Antivirus na lista e clique em **Remover**.

  Ao ser perguntado se deseja realmente remover o aplicativo e todos os seus componentes, clique em **Sim** para confirmar.

  Todos os componentes do programa serão removidos.

  Clique em **Concluir** para concluir a desinstalação.

  Se uma caixa de diálogo aparecer recomendando a reinicialização do computador, clique em **Sim** para confirmar.

  O Avira Free Antivirus agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

Observação
O Avira SearchFree Toolbar não está incluído no programa de desinstalação e deve ser desinstalado separadamente.

Observação
Se você desinstalar o Avira SearchFree Toolbar, o Web Protection também será desinstalado.

3.7.4 Instalando o Avira SearchFree Toolbar

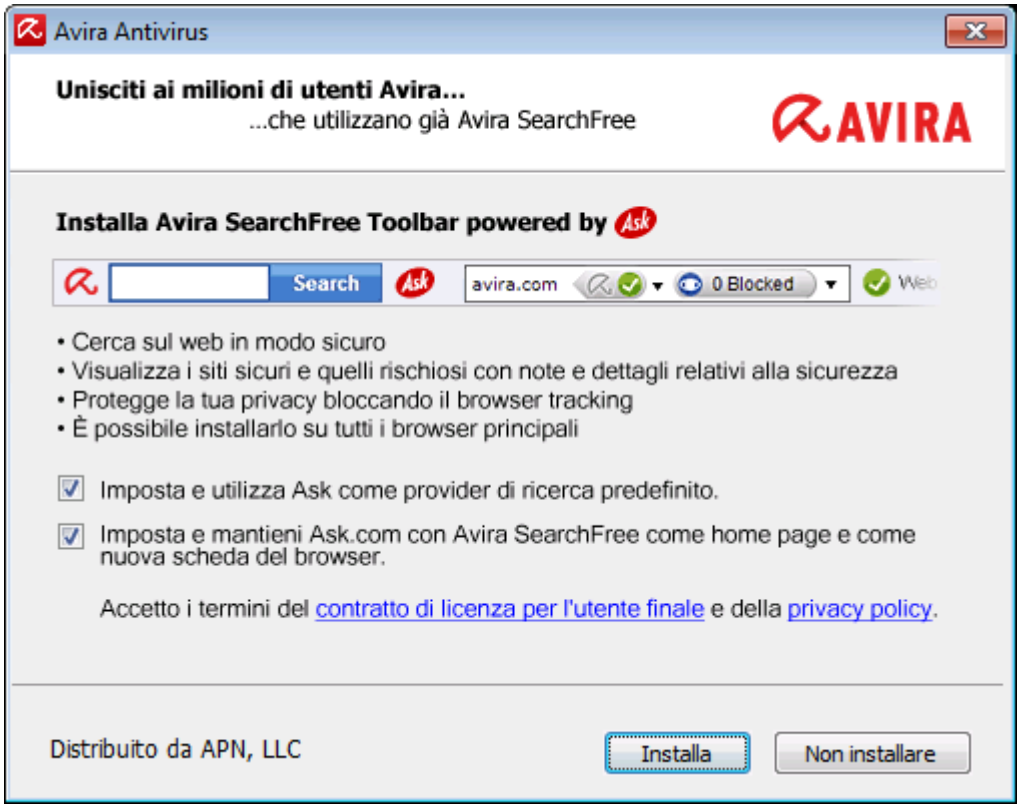
Instalando o Avira SearchFree Toolbar

Ao fim da instalação, você pode instalar o Avira SearchFree Toolbar.

O Avira SearchFree Toolbar inclui dois componentes principais: o Avira SearchFree e a Barra de ferramentas.

Com o Avira SearchFree, você pesquisa na Internet inúmeros termos. Este mecanismo de pesquisa exibe todos os resultados na janela do navegador, classificando seu nível de segurança. Isso permite uma navegação mais segura aos usuários do Avira.

A Barra de ferramentas oferece três widgets para as funções mais importantes relacionadas à Internet. Com um clique, você tem acesso direto ao Facebook e ao seu e-mail ou pode garantir navegação segura na web (somente Firefox e Internet Explorer).



Se você não quiser instalar o Avira SearchFree Toolbar, desmarque as caixas de marcação das opções **Definir e manter o Ask como meu provedor de pesquisa padrão** e **Definir e manter o Avira SearchFree (avira.search.ask.com) como a página inicial do navegador e a nova página de aba do navegador.**

Se você recusar, somente a instalação do Avira SearchFree Toolbar será cancelada. A instalação do Avira Free Antivirus, entretanto, será concluída.

Desinstalando o Avira SearchFree Toolbar no Windows 8

Para desinstalar o Avira SearchFree Toolbar:

- Feche o navegador da Web.

  Clique com o botão direito do mouse em um dos cantos inferiores da tela.

  O símbolo **Todos os aplicativos** aparecerá.

  Clique no símbolo e procure na seção *Aplicativos - Sistema Windows* o **Painel de Controle**.

  Clique duas vezes no símbolo do **Painel de Controle**.

  Clique em **Programas - Desinstalar um programa**.

  Clique em **Programas e Recursos - Desinstalar um programa**.

  Selecione Avira SearchFree Toolbar plus Web Protection na lista e clique em **Desinstalar**.

  Será perguntado se você realmente deseja desinstalar este produto.

Clique em **Sim** para confirmar.

O Avira SearchFree Toolbar plus Web Protection é desinstalado e todos os diretórios, arquivos e entradas do registro para o Avira SearchFree Toolbar plus Web Protection são excluídos quando o seu computador for reiniciado.

Desinstalando o Avira SearchFree Toolbar no Windows 7

Para desinstalar o Avira SearchFree Toolbar:

- Feche o seu navegador da Web.

  Abra o **Painel de Controle** através do menu **Iniciar** do Windows.

  Clique duas vezes em **Programas e Recursos**.

  Selecione o Avira SearchFree Toolbar plus Web Protection na lista e clique em **Desinstalar**.

  Será perguntado se você realmente deseja desinstalar este produto.

  Clique em **Sim** para confirmar.

  O Avira SearchFree Toolbar plus Web Protection é desinstalado e todos os diretórios, arquivos e entradas do registro para o Avira SearchFree Toolbar plus Web Protection são excluídos quando o seu computador for reiniciado.

Desinstalando o Avira SearchFree Toolbar no Windows XP

Para desinstalar o Avira SearchFree Toolbar:

- Feche o seu navegador da Web.

  Abra o **Painel de Controle** através do menu **Iniciar > Configurações** do Windows.

  Clique duas vezes em **Adicionar ou Remover Programas**.

  Selecione Avira SearchFree Toolbar plus Web Protection na lista e clique em **Remover**.

  Será perguntado se você realmente deseja desinstalar este produto.

  Clique em **Sim** para confirmar.

  O Avira SearchFree Toolbar plus Web Protection é desinstalado e todos os diretórios, arquivos e entradas do registro para o Avira SearchFree Toolbar plus Web Protection são excluídos quando o seu computador for reiniciado.

Desinstalando o Avira SearchFree Toolbar através do navegador da Web

Você também pode desinstalar o Avira SearchFree Toolbar diretamente no navegador. Esta opção está disponível somente no Firefox e Internet Explorer:

- Abra o seu navegador da Web.

  Na barra de ferramentas de pesquisa, abra o menu **Opções**.

  Clique em **Desinstalar barra de ferramentas a partir do navegador**.

Ao ser perguntado se deseja instalar o produto, clique em **Sim** para confirmar.

Você será solicitado, agora, a fechar o navegador da Web.

Feche o navegador da Web e clique em **Tentar novamente**.

Avira SearchFree Toolbar plus Web Protection é desinstalado e todos os diretórios, arquivos e entradas do registro para o Avira SearchFree Toolbar plus Web Protection são excluídos quando o seu computador for reiniciado.

Observação
Para desinstalar o Avira SearchFree Toolbar, a barra de ferramentas deve ser ativada no Add-On Manager.

Desinstalando o Avira SearchFree Toolbar através do Add-On Manager

Como a barra de ferramentas é instalada como um complemento, ela também pode ser desinstalada como um:

Firefox

- Clique em **Ferramentas > Complementos > Extensões**. Ali, é possível gerenciar o Avira Add-on: ativar ou desativar a barra de ferramentas e desinstalar.

Internet Explorer

- Ir para **Gerenciar Complementos > Barras de ferramentas e Extensões**. Aqui, você pode ativar e desativar o Avira SearchFree Toolbar ou desinstalá-lo.

Google Chrome

- Clique em **Opções > Extensões** e gerencie facilmente sua barra de ferramentas: ative, desative ou desinstale-a.

4. Visão geral do Avira Free Antivirus

Este capítulo contém uma visão geral da funcionalidade e operação de seu produto Avira.

- consulte o Capítulo Interface de Usuário e Operação
- consulte o Capítulo Avira SearchFree Toolbar
- consulte o Capítulo Como...?

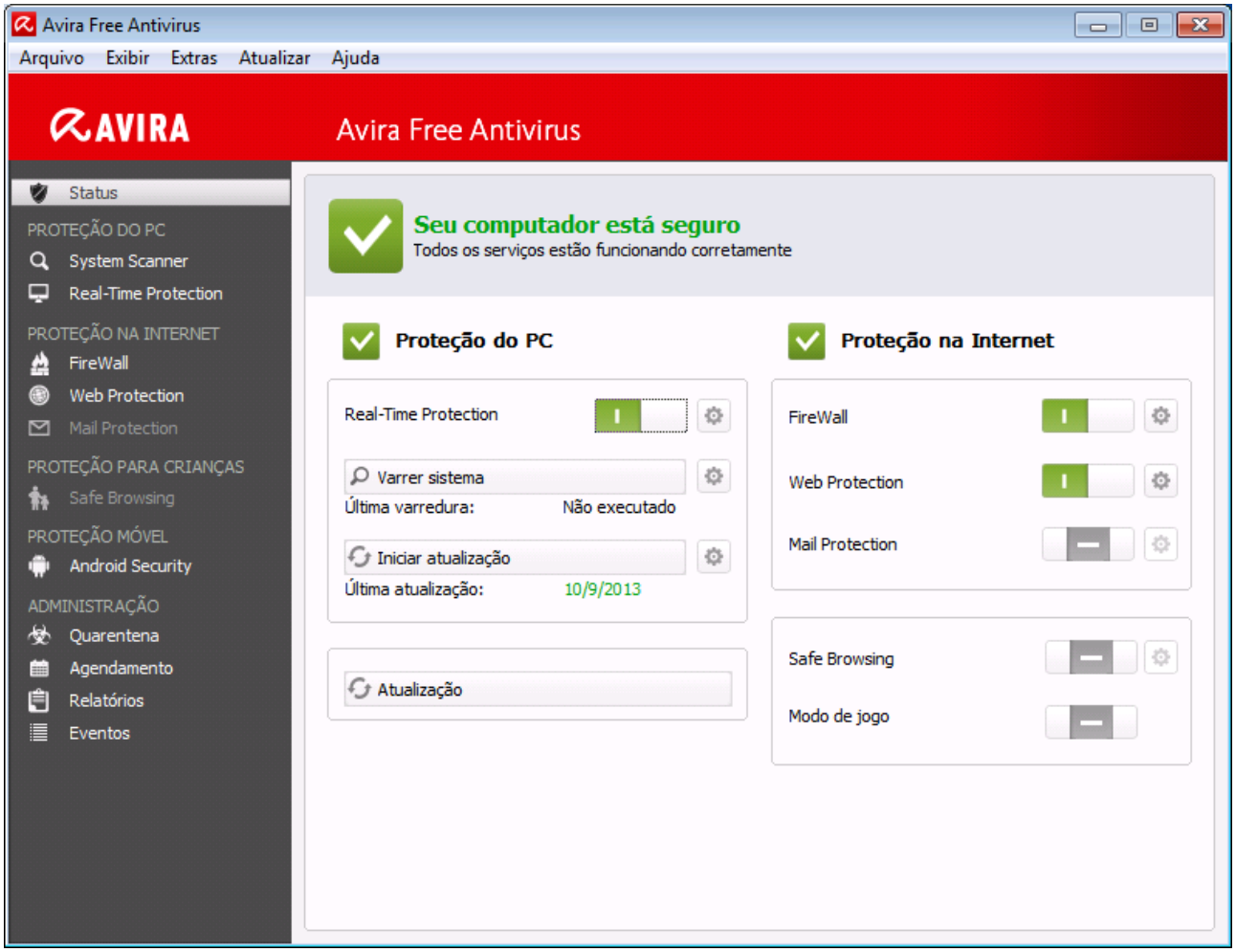
4.1 Interface de Usuário e Operação

Você opera seu produto Avira por meio de três elementos da interface do programa:

- Centro de Controle: monitorando e controlando o produto Avira
- Configuração: Configurando o produto Avira
- Ícone de Bandeja na bandeja do sistema da barra de tarefas: Abrindo o Centro de Controle e outras funções

4.1.1 Centro de controle

O Centro de Controle foi desenvolvido para monitorar o status de proteção de sistemas de computador e para controlar e operar os componentes e as funções de proteção do produto Avira.



A janela Centro de Controle é dividida em três áreas: a **Barra de Menus**, a **Área de Navegação** e a janela de detalhes **Status**:

- **Barra de Menus:** Na barra de menus do Centro de Controle, você pode acessar funções gerais do programa e informações sobre o programa.
- **Área de Navegação:** Na área de navegação, você pode alternar facilmente entre as seções individuais do Centro de Controle. As seções individuais contêm informações e funções dos componentes do programa e são organizadas na barra de navegação de acordo com a atividade. Exemplo: Atividade *PROTEÇÃO DO PC* - Seção **Real-Time Protection**.
- **Status:** O Centro de Controle é aberto com a exibição **Status**, na qual você pode ver rapidamente se seu computador está saguro e você tem uma visão geral dos módulos ativos, a data do último backup e a data da última varredura do sistema. A exibição **Status** também contém botões para iniciar recursos ou ações, tal como iniciar ou parar o **Real-Time Protection**.

Iniciando e fechando o Centro de Controle

Para iniciar o Centro de controle, as seguintes opções estão disponíveis:

- Clique duas vezes no ícone do programa na área de trabalho

- Através da entrada do programa no menu **Iniciar > Programas**.
- Através do Ícone da Bandeja de seu produto Avira.

Feche o Centro de Controle com o comando de menu **Fechar** no menu **Arquivo** ou clicando na guia Fechar no Centro de Controle.

Operar o Centro de Controle

Para navegar no Centro de Controle

- Selecione uma atividade na barra de navegação.
  - ↪ A atividade é aberta e outras seções são exibidas. A primeira seção da atividade é selecionada e exibida na visualização.
- Se necessário, clique em outra seção para exibi-la na janela de detalhes.

> **Observação**
> Você pode ativar a navegação do teclado na barra de menus com a ajuda da tecla [**Alt**]. Se a navegação estiver ativada, você poderá percorrer o menu com as teclas de **seta**. Com a tecla **Voltar** você ativa o item de menu ativo.
> Para abrir ou fechar menus no Centro de Controle ou para navegar dentro dos menus, você também pode usar as seguintes combinações de teclas: [**Alt**] + letra sublinhada no menu ou comando de menu. Mantenha pressionada a tecla [**Alt**] se desejar acessar um menu, um comando de menu ou um submenu.

Para processar dados ou objetos exibidos na janela de detalhes:

- Realce os dados ou o objeto que deseja editar.

  Para destacar vários elementos (elementos nas colunas), mantenha pressionada a tecla **Ctrl** ou **Shift** enquanto seleciona os elementos.
- Clique no botão apropriado na barra superior da janela de detalhes para editar o objeto.

Visão Geral do Centro de Controle

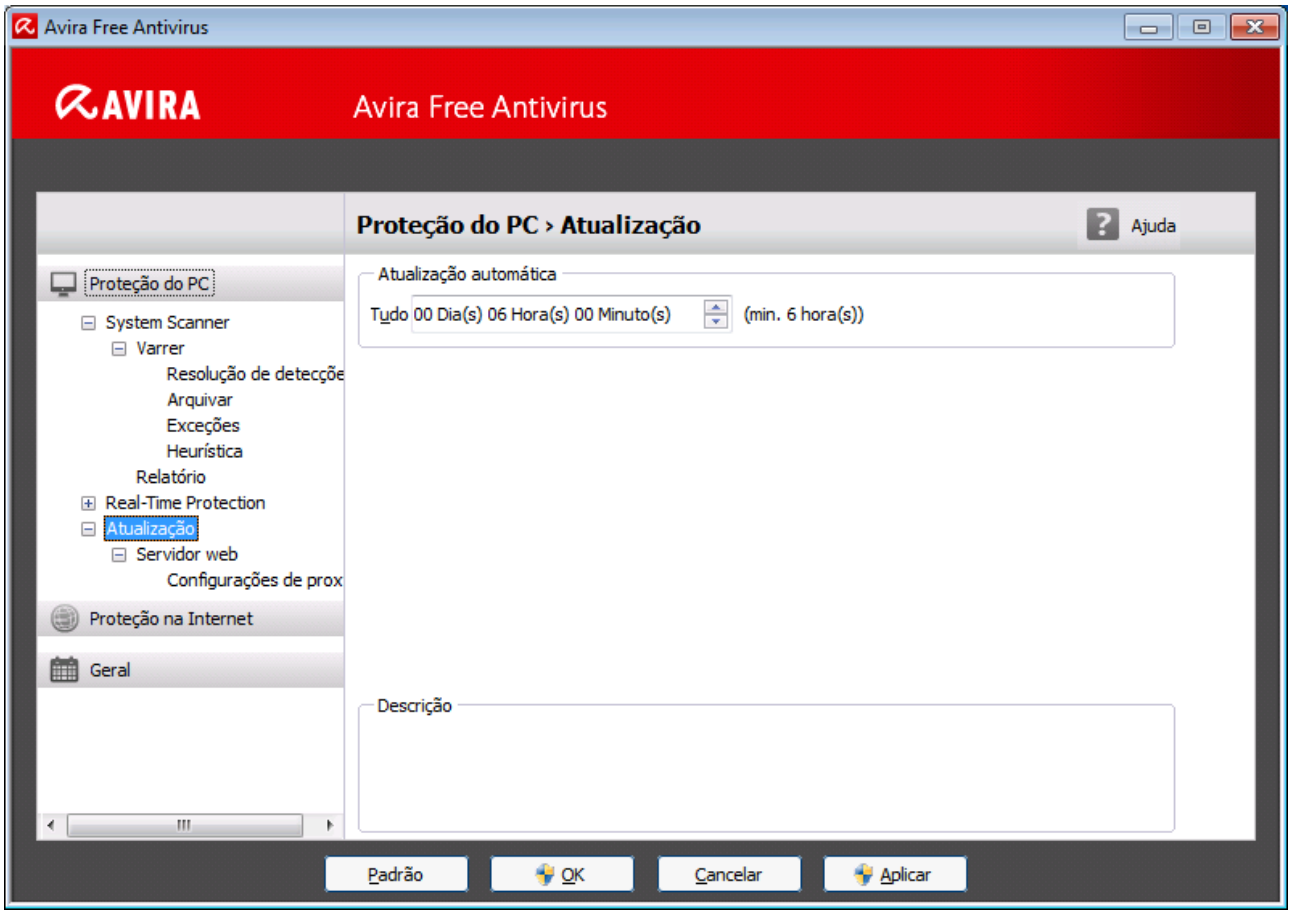
- **Status**: Clicar na barra **Status** fornece uma visão geral da funcionalidade do produto e do desempenho (consulte Status).
  - A seção **Status** permite ver rapidamente quais módulos estão ativos e fornece informações sobre a última atualização realizada.
- *PROTEÇÃO DO PC*: Nesta seção você localizará os componentes para verificar os arquivos em seu sistema do computador em busca de vírus e malwares.
  - A seção Scanner permite configurar e iniciar facilmente uma varredura por demanda. Perfis predefinidos ativa uma varredura com opções padrão já adaptadas. Do mesmo modo, é possível adaptar a varredura de vírus e programas indesejados de acordo com seus requisitos pessoais com a ajuda da seleção manual (será salva).

- A seção Real-Time Protection exibe informações sobre arquivos verificados, assim como outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".

- *PROTEÇÃO NA INTERNET*: Nesta seção você localizará os componentes para proteger seu sistema do computador contra vírus e malwares da Internet e contra acesso à rede não autorizado.
  - A seção FireWall permite configurar as configurações básicas do FireWall. Além disso, são exibidos a taxa de transferência de dados atual e todos os aplicativos ativos que usam uma conexão de rede.
  - A seção Web Protection apresenta informações sobre URLs verificados e vírus detetados e outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite o acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".
- *PROTEÇÃO MÓVEL*: Desta seção você será redirecionado ao acesso on-line para dispositivos Android.
  - Avira Free Android Security gerencia todos os dispositivos baseados em Android.
- *ADMINISTRAÇÃO*: Nesta seção você localizará ferramentas para isolar e gerenciar arquivos suspeitos ou infectados e para planejar tarefas recorrentes.
  - A seção Quarentena contém o conhecido gerenciador de quarentena. Este é o ponto central para os arquivos já colocados na quarentena ou para os arquivos suspeitos que deseja colocar na quarentena. Também é possível enviar um arquivo selecionado para o Avira Malware Research Center por e-mail.
  - A seção Agendamento permite configurar trabalhos programados de varredura e atualização, bem como trabalhos de backup, e adaptar ou excluir os trabalhos existentes.
  - A seção Relatórios permite visualizar os resultados de ações executadas.
  - A seção Eventos permite visualizar os eventos gerados por determinados módulos do programa.

4.1.2 Configuração

Você pode definir configurações para seu produto Avira na Configuração. Após a instalação. seu produto Avira é definido com configurações padrão, assegurando a proteção ideal para seu sistema do computador. No entanto, seu sistema do computador ou seus requisitos específicos para o produto Avira podem exigir que você adapte os componentes de proteção do programa.



A Configuração abre uma caixa de diálogo: Você pode salvar suas definições de configuração por meio dos botões **OK** ou **Aplicar**, excluir suas configurações clicando no botão Cancelar ou restaurar suas configurações padrão usando o botão **Padrão**. Você pode selecionar seções de configuração individuais na barra de navegação à esquerda.

Acessando a Configuração

Você tem várias opções para acessar a configuração:

- por meio do Painel de Controle do Windows.
- através da Central de Segurança do Windows - no Windows XP Service Pack 2.
- por meio do Ícone da Bandeja de seu produto Avira.
- no Centro de Controle através do item de menu Extras > Configuração.
- no Centro de Controle através do botão Configuração.

Observação
Se estiver acessando a configuração através do botão **Configuração** no Centro de Controle, vá até o registro de Configuração da seção que está ativa no Centro de Controle. O

Operação de Configuração

Navegue na janela de configuração como faria no Windows Explorer:

- Clique em uma entrada na estrutura em árvore para exibir essa seção de configuração na janela de detalhes.
- Clique no símbolo de adição na frente da entrada para expandir a seção de configuração e exibir subseções de configuração na estrutura em árvore.
- Para ocultar subseções de configuração, clique no símbolo de subtração na frente da seção de configuração expandida.

> **Observação**
> Para ativar ou desativar opções de Configuração e usar os botões, você também pode usar as seguintes combinações de tecla: [**Alt**] + letra sublinhada no nome da opção ou na descrição do botão.

Para confirmar as definições de Configuração:

- Clique em **OK**.
  - ↪ A janela de configuração é fechada e as configurações são aceitas.

  - OU -
- Clique em **Aplicar**.
  - ↪ As configurações são aplicadas. A janela de configuração permanece aberta.

Para concluir a configuração sem confirmar as definições:

- Clique em **Cancelar**.
  - ↪ A janela de configuração é fechada e as configurações são descartadas.

Para restaurar todas as definições de configurações aos valores padrão:

- Clique em **Valores padrão**.
  - ↪ Todas as opções da configuração são restauradas aos valores padrão. Todas as correções e entradas personalizadas são perdidas quando as configurações padrão são restauradas.

Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:

- **Scanner**: Configuração da varredura por demanda
  - Opções de varredura
  - Resolução de na detecções
  - Opções de varredura do arquivo

- Exceções de varredura do sistema
- Heurística de varredura do sistema
- Configuração da função de registro

- **Real-Time Protection**: configuração de uma varredura durante o acesso
  - Opções de varredura
  - Resolução de na detecções
  - Mais ações
  - Exceções de varredura durante o acesso
  - Heurística de varredura durante o acesso
  - Configuração da função de registro
- **Atualização**: Configuração das configurações de atualização
  - Fazer download através do servidor Web
  - Configurações de proxy
- **Web Protection**: Configuração da Web Protection
  - Opções de varredura, ativação e desativação da Web Protection
  - Resolução de na detecções
  - Acesso bloqueado: Tipos de arquivo e tipos MIME indesejados
  - Exceções de varredura da Web Protection: URLs, tipos de arquivo, tipos MIME
  - Heurística de Web Protection
  - Configuração da função de registro
- **Geral**:
  - Categorias de ameaça para o Scanner e o Real-Time Protection
  - Filtro de aplicativos: bloquear ou permitir aplicativos
  - Proteção com senha para acesso ao Centro de controle e à Configuração
  - Segurança: bloquear função autostart, proteção do produto, proteger arquivo hosts do Windows
  - WMI: Ativar o suporte a WMI
  - Configuração do registro de eventos
  - Configuração das funções de registro
  - Configuração dos diretórios usados
  - Configuração de alertas acústicos emitidos quando malwares são detectados

4.1.3 Ícone de bandeja

Após a instalação, você verá o ícone de bandeja do produto Avira na bandeja do sistema, na barra de tarefas:

Ícone	Descrição
	O Avira Real-Time Protection é ativado
	O Avira Real-Time Protection é desativado

O ícone de bandeja exibe o status do serviço do Real-Time Protection .

As funções centrais de seu produto Avira podem ser acessadas rapidamente através do menu contextual do **ícone de bandeja**. Para abrir o menu contextual, clique no **ícone de bandeja** com o botão direito do mouse.

Entradas no menu contextual

- **Ativar Real-Time Protection**: Ativa ou desativa o Avira Real-Time Protection.
- **Ativar Web Protection**: Ativa ou desativa o Avira Web Protection.
  - **Ativar Firewall do Windows**: Ativa ou desativa o Firewall do Windows (esta funcionalidade está disponível a partir do Windows 8).
- **Iniciar Avira Free Antivirus**: Abre o Centro de Controle.
- **Configurar Avira Free Antivirus**: Abre a Configuração.
- **Minhas mensagens**: Abre um slide com as informações atuais sobre seu produto Avira.
- **Iniciar atualização** Inicia uma atualização.
- **Ajuda**: abre a ajuda online.
- **Sobre o Avira Free Antivirus:** Abre uma caixa de diálogo com informações sobre seu produto Avira: Informações do produto, Informações da versão, Informações de licença.
- **Avira na Internet**: Abre o portal da Web da Avira na Internet. Para isso, é necessário ter uma conexão ativa com a Internet.

4.2 Avira SearchFree Toolbar

O Avira SearchFree Toolbar inclui dois componentes principais: o Avira SearchFree e o Toolbar.

O Avira SearchFree Toolbar é instalado como um complemento. Quando o navegador for acessado pela primeira vez (no Firefox e Internet Explorer), será exibida uma mensagem perguntando se você tem permissão para instalar a barra de ferramentas. Você precisará aceitar para concluir uma instalação com êxito do Avira SearchFree Toolbar.

O Avira SearchFree é um mecanismo de pesquisa e contém um logotipo clicável do Avira para o site do Avira e canais da web, de imagem e vídeo. Isto permite uma navegação na Internet mais segura aos usuários do Avira.

A barra de ferramentas, integrada em seu navegador da web, consiste em uma caixa de pesquisa, um logotipo do Avira vinculado ao site da Avira, duas exibições de status, três widgets e o menu **Opções**.

- Barra de Ferramentas de Pesquisa
  Use a barra de ferramentas de pesquisa gratuitamente para pesquisar rapidamente a Internet usando o mecanismo de pesquisa da Avira.
- Exibição de Status
  As exibições de status fornecem informações sobre o status do Web Protection e o status de atualização atual de seu produto Avira e o ajuda a identificar quais ações você precisa executar para proteger seu PC.
- Widgets
  O Avira oferece três widgets para as funções mais importantes relacionadas à Internet. Com um clique, você tem acesso direto ao Facebook e ao seu e-mail ou pode garantir a navegação na web segura (apenas Firefox e Internet Explorer).
- Opções
  Você pode usar o menu **Opções** para acessar as opções da barra de ferramentas, limpar o histórico, localizar a ajuda e informações da barra de ferramentas e também desinstalar o Avira SearchFree Toolbar diretamente através do navegador da web (apenas Firefox e Internet Explorer).

4.2.1 Uso

Avira SearchFree

Você pode usar o Avira SearchFree para definir qualquer número de termos para procurar na Internet.

Insira o termo na caixa de pesquisa e pressione a tecla **Enter** ou clique em **Pesquisar**. O mecanismo Avira SearchFree, então, pesquisa a Internet para você e exibe todas as ocorrências na janela do navegador.

Para descobrir como customizar a configuração do Avira SearchFree no Internet Explorer, Firefox e Chrome, vá para **Opções**.

Exibição de Status

Web Protection

É possível usar os seguintes ícones e mensagens para identificar quais ações você precisa executar para proteger seu PC:

Ícone	Exibição de Status	Descrição
	*Web Protection*	Se você mover o cursor sobre o ícone, as seguinte mensagem é exibida: *O Avira Web Protection está ativo. Sua navegação está protegida.* Nenhuma ação adicional é necessária.
	*Web Protection inativo*	Se você mover o cursor sobre o ícone, as seguinte mensagem é exibida: *O Avira Web Protection está desligado. Clique para saber como ligá-lo.* ↪ Você será redirecionado para um dos artigos da nossa Base de Conhecimento.
	*Sem Web Protection*	Se você mover o cursor sobre o ícone, uma das seguintes mensagens aparecerá: • *Você não tem Avira Web Protection instalado. Clique para saber como proteger sua navegação.* Essa mensagem aparecerá se você instalar incorretamente ou desinstalar o Avira Antivirus. • *O Web Protection é incluído gratuitamente com o antivírus Avira. Clique para saber como instalá-lo.* Essa mensagem aparecerá se você não instalar o Web Protection ou se desinstalá-lo. ↪ Nos dois casos você será redirecionado à home page da Avira, onde poderá fazer download do produto Avira.
	*Erro*	Se você mover o cursor sobre o ícone, a seguinte mensagem aparecerá: *O Avira relatou um erro. Clique para entrar em contato com o Suporte e obter ajuda.* ▸ Clique no ícone ou texto cinza para ir para a página Suporte do Avira.

Widgets

O Avira SearchFree contém três widgets com as funções mais importantes para a navegação da web na Internet atualmente: Facebook, E-mail e Navegador de segurança.

Facebook

Esta função permite receber todas as mensagens do Facebook e estar sempre atualizado.

E-mail

Se você clicar no símbolo de e-mail na barra de ferramentas, será mostrada uma lista suspensa. Você pode escolher entre os provedores de e-mail usados mais comumente.

Navegador de segurança

Este widget foi concebido para ofeecerr em um clique todas as opções de segurança na Internet necessárias diariamente. Esta opção está disponível apenas para Firefox e Internet Explorer. Além disso, os nomes das funções às vezes, mudam de um navegador para outro:

- *Bloqueador de Pop-up*

Se esta opção estiver ativada, todas as janelas pop-up serão bloqueadas.

- *Bloquear Cookies*

Se você ativar esta opção, nenhum cookie será salvo em seu computador.

- *Navegação Privada (Firefox) / Navegação InPrivate (Internet Explorer)*

Ative esta opção se você não desejar deixar nenhuma informação pessoal na Internet enquanto navega. Esta opção não está disponível para o Internet Explorer 7 e 8.

- *Limpar Histórico Recente (Firefox) / Excluir Histórico de Navegação (Internet Explorer)*

Com esta opção você apagará todos os rastros de suas atividades na Internet.

Website Safety Advisor

O Website Safety Advisor oferece uma classificação de segurança durante a navegação. Você pode avaliar a reputação do site que está sendo visitado e verificar se ele apresenta risco baixo ou alto para sua segurança.
Este widget também fornece informações adicionais sobre o site, como quem é o proprietário do domínio ou a razão pela qual o site foi categorizado como seguro ou arriscado.

O status do Website Safety Advisor é exibido no Toolbar e nos resultados da pesquisa, como um ícone de bandeja do Avira em combinação com outros ícones:

Ícone	Exibição de Status	Descrição
	*Seguro*	Uma marca de seleção verde para sites seguros.
	*Baixo Risco*	Um ponto de exclamação amarelo para sites que representam baixo risco.
	*Alto Risco*	Um sinal de pare vermelho para sites que representam alto risco para a sua segurança.
	*Desconhecido*	Um ponto de interrogação cinza aparece quando o status for desconhecido.
	*Verificação*	Este sinal aparecerá durante a verificação do status de um site.

Browser Tracking Blocker

Com o Browser Tracking Blocker, é possível parar a coleta de informações sobre você pelos controladores enquanto você está navegando.
O widget permite escolher quais controladores bloquear e quais permitir.

As empresas de controle são classificadas em três categorias:

- Redes sociais
- Redes de anúncios
- Outras empresas

4.2.2 Opções

O Avira SearchFree Toolbar é compatível com o Internet Explorer, o Firefox e o Google Chrome e pode ser configurado nos três navegadores da web:

- Opções de Configuração do Internet Explorer
- Opções de Configuração do Firefox
- Opções de Configuração do Google Chrome

Internet Explorer

No Internet Explorer, as seguintes opções de configuração para o Avira SearchFree Toolbar estão disponíveis no menu **Opções**:

Opções do Toolbar

Pesquisar

Selecionar Avira

No menu **Selecionar Avira**, é possível selecionar qual mecanismo de pesquisa usar para a pesquisa. Os mecanismos de pesquisa estão disponíveis para os Estados Unidos Brasil, Alemanha, Espanha, Europa, França, Itália, os Países Baixos, Rússia e o Reino Unido.

Abrir as buscas em

Na opção de menu **Abrir as buscas em**, você pode selecionar onde o resultado da pesquisa deve ser exibido; na janela Atual, em uma janela Novo ou em uma guia Novo.

Exibir buscas recentes

Se a opção **Exibir buscas recentes** estiver ativada, você poderá exibir termos de pesquisa na caixa de entrada de texto da barra de ferramentas de pesquisa.

Limpar automaticamente o histórico de buscas recentes ao fechar o navegador

Ative a opção **Limpar automaticamente o histórico de buscas recentes ao fechar o navegador** se não desejar salvar pesquisas anteriores e desejar limpar o histórico ao fechar o navegador da web.

Mais opções

Idioma da barra

Em **Idioma da barra** é possível selecionar o idioma no qual o Avira SearchFree Toolbar é exibido. A barra de ferramentas está disponível em Inglês, Alemão, Espanhol, Francês, Italiano, Português e Holandês.

Observação
Onde possível, o idioma padrão do Avira SearchFree Toolbar corresponde ao de seu programa. Se a barra de ferramentas não estiver disponível em seu idioma, o idioma padrão será o Inglês.

Mostrar rótulos de texto dos botões

Desative a opção **Mostrar rótulos de texto dos botões** se desejar ocultar o texto ao lado dos ícones do Avira SearchFree Toolbar.

Limpar histórico

Ative a opção **Limpar histórico** se não desejar salvar pesquisas anteriores e desejar limpar o histórico imediatamente.

Ajuda

Clique em **Ajuda** para acessar o site contendo as perguntas frequentes (FAQs) relacionadas à barra de ferramentas.

Desinstalar

Você também pode desinstalar o Avira SearchFree Toolbar diretamente no Internet Explorer: Desinstalação Através do Navegador da Web

Sobre

Clique em **Sobre** para exibir qual versão do Avira SearchFree Toolbar está instalada.

Firefox

No navegador da web Firefox, as seguintes opções de configuração para o Avira SearchFree Toolbar estão disponíveis no menu **Opções**:

Opções do Toolbar

Pesquisar

Selecionar Avira

No menu **Selecionar Avira**, é possível selecionar qual mecanismo de pesquisa usar para a pesquisa. Os mecanismos de pesquisa estão disponíveis para os Estados Unidos Brasil, Alemanha, Espanha, Europa, França, Itália, os Países Baixos, Rússia e o Reino Unido.

Exibir buscas recentes

Se a opção **Exibir buscas recentes** estiver ativada, você poderá exibir termos de pesquisa anteriores clicando na seta na barra de ferramentas de pesquisa. Selecione um termo se desejar exibir o resultado da pesquisa novamente.

Limpar automaticamente o histórico de buscas recentes ao fechar o navegador

Ative a opção **Limpar automaticamente o histórico de buscas recentes ao fechar o navegador** se não desejar salvar pesquisas anteriores e desejar limpar o histórico ao fechar o navegador da web.

Exibir os resultados da pesquisa da Ask quando eu digitar palavras chaves ou URLs inválidas na barra de endereço do navegador

Se esta opção estiver ativada, uma pesquisa será iniciada e o resultado da pesquisa exibido toda vez que você inserir palavras-chave ou uma URL inválida na barra de endereços do navegador da web.

Mais opções

Idioma da barra

Em **Idioma da barra** é possível selecionar o idioma no qual o Avira SearchFree Toolbar é exibido. A barra de ferramentas está disponível em Inglês, Alemão, Espanhol, Francês, Italiano, Português e Holandês.

> **Observação**
> Onde possível, o idioma padrão do Avira SearchFree Toolbar corresponde ao de seu programa. Se a barra de ferramentas não estiver disponível em seu idioma, o idioma padrão será o Inglês.

Mostrar rótulos de texto dos botões

Desative a opção **Mostrar rótulos de texto dos botões** se desejar ocultar o texto ao lado dos ícones do Avira SearchFree Toolbar.

Limpar histórico

Ative a opção **Limpar histórico** se não desejar salvar pesquisas anteriores e desejar limpar o histórico imediatamente.

Ajuda

Clique em **Ajuda** para acessar o site contendo as perguntas frequentes (FAQs) relacionadas à barra de ferramentas.

Desinstalar

Você também pode desinstalar o Avira SearchFree Toolbar diretamente no Firefox: Desinstalação Através do Navegador da Web.

Sobre

Clique em **Sobre** para exibir qual versão do Avira SearchFree Toolbar está instalada.

Google Chrome

No navegador da web Chrome, as seguintes opções de configuração para o Avira SearchFree Toolbar estão disponíveis no menu do guarda-chuva vermelho do Avira:

Ajuda

Clique em **Ajuda** para acessar o site contendo as perguntas frequentes (FAQs) relacionadas à barra de ferramentas.

Instruções para desinstalação

Aqui você será vinculado aos artigos que contêm todas as informações necessárias para desinstalar a barra de ferramentas.

Sobre

Clique em **Sobre** para exibir qual versão do Avira SearchFree Toolbar está instalada.

Mostrar/Ocultar o Avira SearchFree Toolbar

Clique aqui para ocultar ou mostrar o Avira SearchFree Toolbar em seu navegador da web.

4.2.3 Desinstalando o Avira SearchFree Toolbar no Windows 7

Para desinstalar o Avira SearchFree Toolbar:

- Feche o seu navegador da Web.

  Abra o **Painel de Controle** através do menu **Iniciar** do Windows.

  Clique duas vezes em **Programas e Recursos**.

  Selecione o Avira SearchFree Toolbar plus Web Protection na lista e clique em **Desinstalar**.

  Será perguntado se você realmente deseja desinstalar este produto.

  Clique em **Sim** para confirmar.

  O Avira SearchFree Toolbar plus Web Protection é desinstalado e todos os diretórios, arquivos e entradas do registro para o Avira SearchFree Toolbar plus Web Protection são excluídos quando o seu computador for reiniciado.

4.3 Como...?

Os capítulos "Como...?" Oferecem instruções breves sobre a licença e a ativação do produto e informações sobre as funções mais importantes do seu produto Avira. Os artigos resumidos selecionados servem como uma visão geral sobre a funcionalidade do produto Avira. Elas não substituem as informações detalhadas de cada seção deste centro de ajuda.

4.3.1 Executar atualizações automáticas

Para criar um trabalho com o Agendamento Avira para atualizar o produto Avira automaticamente:

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Agendamento**.
- Clique no ícone  **Inserir novo trabalho**.

↳ A caixa de diálogo **Nome e descrição do trabalho** é exibida.

- Dê um nome ao trabalho e, quando apropriado, uma descrição.
- Clique em **Avançar**.

↳ A caixa de diálogo **Tipo de trabalho** é exibida.

- Selecione **Trabalho de atualização** na lista.
- Clique em **Avançar**.

↳ A caixa de diálogo **Tempo do trabalho** é exibida.

- Selecione um horário para a atualização:

- **Imediatamente**
- **Daily**
- **Semanalmente**
- **Intervalo**
- **Única**

Observação
Recomendamos atualizações automáticas periódicas. O intervalo de atualização recomendado é: 6 horas.

- Quando apropriado, especifique uma data de acordo com a seleção.
- Quando apropriado, selecione opções adicionais (a disponibilidade depende do tipo de trabalho):

- **Repita o trabalho se o tempo expirou**
  São executados trabalhos passados que não puderam ser realizados no momento apropriado, por exemplo, porque o computador estava desligado.

- Clique em **Avançar**.

↳ A caixa de diálogo **Selecionar modo de exibição** é exibida.

- Selecione o modo de exibição da janela do trabalho:

- **Invisível**: Nenhuma janela de backup
- **Minimizar**: Somente barra de progresso
- **Maximizar**: Janela de trabalho inteira

- Clique em **Concluir**.

↳ Seu trabalho recém-criado aparece na página inicial da seção *ADMINISTRAÇÃO* **> Agendamento** com o status ativado (marca de seleção).

- Quando apropriado, desative os trabalhos que não devem ser realizados.

Use os ícones a seguir para definir seus trabalhos ainda mais:


Exibir propriedades de um trabalho

 Editar trabalho

 Excluir trabalho

 Iniciar trabalho

Interromper trabalho

4.3.2 Iniciar uma atualização manual

Você tem várias opções para iniciar uma atualização manualmente: quando uma atualização é iniciada manualmente, o arquivo de definição de vírus e o mecanismo de varredura são sempre atualizados.

Para iniciar uma atualização de seu produto Avira manualmente:

- Com o botão direito do mouse, clique no ícone de bandeja do Avira na barra de tarefas.
  - ↪ Um menu contextual é exibido.
- Selecione **Iniciar atualização**.
  - ↪ A caixa de diálogo **Atualizador** é exibida.

- OU -

- No Centro de Controle, selecione **Status**.
- No campo **Última atualização**, clique no link **Iniciar atualização**.
  - ↪ A caixa de diálogo Atualizador é exibida.

- OU -

- No Centro de controle, no menu **Atualizar**, selecione o comando de menu **Iniciar atualização**.
  - ↪ A caixa de diálogo Atualizador é exibida.

Observação
Recomendamos atualizações automáticas periódicas. O intervalo de atualização recomendado é: 6 horas.

Observação
Você também pode realizar uma atualização manual diretamente por meio da Central de Segurança do Windows.

4.3.3 Usando um perfil de verificação para verificar a presença de vírus e malwares

Um perfil de verificação é um conjunto de unidades e diretórios a serem verificados.

As seguintes opções estão disponíveis para verificação com um perfil de verificação:

Usar perfil de verificação predefinido

Se o perfil de verificação predefinido corresponder aos seus requisitos.

Personalizar e aplicar perfil de verificação (seleção manual)

Se desejar verificar com um perfil personalizado.

Dependendo do sistema operacional, vários ícones estão disponíveis para iniciar um perfil de verificação:

- No Windows XP:

   Este ícone inicia a verificação através de um perfil.

- No Windows Vista:

  No Microsoft Windows Vista, o Centro de Controle possui apenas direitos limitados no momento, por exemplo, para acessar diretórios e arquivos. Algumas ações e alguns acessos de arquivo só podem ser realizados no Centro de Controle com direitos de administrador estendidos. Esses direitos devem ser concedidos no início de cada verificação através de um perfil de verificação.

  -  Esse ícone inicia uma verificação limitada através de um perfil de verificação. Somente os diretórios e arquivos aos quais o sistema operacional concedeu direitos de acesso são verificados.
  -  Esse ícone inicia a verificação com direitos de administrador estendidos. Após a confirmação, todos os diretórios e arquivos no perfil de verificação selecionado são verificados.

Para verificar a presença de vírus e malwares com um perfil de verificação:

1. Vá para o Centro de Controle e selecione a seção *PROTEÇÃO DO PC* **> System Scanner**.

   ↪ Os perfis de verificação predefinidos são exibidos.

2. Selecione um dos perfis de verificação predefinidos.

   -OU-

   Adapte o perfil de verificação **Seleção Manual**.

3. Clique no ícone (Windows XP:  ou Windows Vista:  :).
4. A janela **Luke Filewalk**er é exibida e uma verificação por demanda é iniciada.

↳ Quando a verificação termina, os resultados são exibidos.

Se desejar adaptar um perfil de verificação:

- No perfil de verificação, expanda a árvore de arquivos **Seleção Manual** para que todas as unidades que deseja verificar sejam abertos:
- Realce os nós que deseja verificar clicando na relevante

4.3.4 Verificar presença de vírus e malware usando arrastar e soltar

Para verificar a presença de vírus e malware sistematicamente usando arrastar e soltar:

✓ O Centro de Controle de seu produto Avira foi aberto.

- Realce o arquivo que deseja verificar.
- Use o botão esquerdo do mouse para arrastar o arquivo realçado no **Centro de Controle**.
  - ↳ A janela **Luke Filewalker** aparece e uma verificação do sistema é iniciada.
  - ↳ Quando a verificação termina, os resultados são exibidos.

4.3.5 Verificar presença de vírus e malwares através do menu contextual

Para verificar a presença de vírus e malwares sistematicamente através do menu contextual:

- Clique com o botão direito do mouse (por exemplo. no Windows Explorer, na área de trabalho ou em um diretório aberto do Windows) no arquivo que deseja verificar.
  - ↳ O menu contextual do Windows Explorer é exibido.
- Selecione **Verificar arquivos selecionados com o Avira** no menu contextual.
  - ↳ A janela **Luke Filewalker** aparece e uma verificação do sistema é iniciada.
  - ↳ Quando a verificação termina, os resultados são exibidos.

4.3.6 Verificar presença de vírus e malwares automaticamente

Observação
Após a instalação, o trabalho de verificação **Verificação completa do sistema** é criado no Agendamento: Uma verificação completa do sistema é realizada automaticamente em um intervalo recomendado.

Para criar um trabalho de verificação automática da presença de vírus e malwares:

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Agendamento**.
- Clique no ícone  .

↳ A caixa de diálogo **Nome e descrição do trabalho** é exibida.

- Dê um nome ao trabalho e, quando apropriado, uma descrição.
- Clique em **Avançar**.

↳ A caixa de diálogo **Tipo de trabalho** é exibida.

- Selecione **Trabalho de verificação**.
- Clique em **Avançar**.

↳ A caixa de diálogo **Seleção do perfil** é exibida.

- Selecione o perfil a ser verificado.
- Clique em **Avançar**.

↳ A caixa de diálogo **Tempo do trabalho** é exibida.

- Selecione um horário para a verificação:

- **Imediatamente**
- **Diariamente**
- **Semanalmente**
- **Intervalo**
- **Única**

- Quando apropriado, especifique uma data de acordo com a seleção.
- Quando apropriado, selecione as seguintes opções adicionais (a disponibilidade depende do tipo de trabalho):

Repetir trabalho se o tempo já tiver expirado

São realizados os trabalhos antigos que não puderam ser realizados no tempo necessário, por exemplo porque o computador foi desligado.

- Clique em **Avançar**.

↳ A caixa de diálogo **Seleção do modo de exibição** é exibida.

- Selecione o modo de exibição da janela do trabalho:

- **Invisível**: Nenhuma janela de backup
- **Minimizado**: somente barra de progresso
- **Maximizado**: Janela de trabalho inteira

- Selecione a opção **Desligar o computador se o trabalho for concluído** se desejar que o computador seja desligado automaticamente quando a verificação for concluída. Essa opção está disponível apenas se o modo de exibição está definido como minimizado ou maximizado.
- Clique em **Concluir**.

↳ Seu trabalho recém-criado aparece na página inicial da seção *ADMINISTRAÇÃO* **> Agendamento** com o status ativado (marca de seleção).

- Quando apropriado, desative os trabalhos que não devem ser realizados.

Use os ícones a seguir para definir seus trabalhos ainda mais:

 Exibir propriedades de um trabalho

 Editar trabalho

 Excluir trabalho

 Iniciar trabalho

Interromper trabalho

4.3.7 Verificação direcionada para Rootkits e malware ativo

Para verificar rootkits ativos, use o perfil de verificação predefinido **Verificar rootkits e malware ativo**.

Para verificar rootkits ativos sistematicamente:

- Vá para o Centro de Controle e selecione a seção *PROTEÇÃO DO PC* **> System Scanner**.
  - ↪ Os perfis de verificação predefinidos são exibidos.
- Selecione o perfil de verificação predefinido **Verificar rootkits e malware ativo**.
- Quando apropriado, realce outros nós e diretórios a serem verificados clicando na caixa de seleção do nível de diretório.
- Clique no ícone (Windows XP:  ou Windows Vista: ).
  - ↪ A janela **Luke Filewalkerr** é exibida e uma verificação por demanda é iniciada.
  - ↪ Quando a verificação termina, os resultados são exibidos.

4.3.8 Reação aos vírus e malwares detectados

Para os componentes de proteção individuais de seu produto Avira, você pode definir como seu produto Avira reage a um vírus ou programa indesejado detectado na **Configuração** na seção **Resolução de detecções**.

Não existem opções de ação configuráveis com o componente Real-Time Protection. Quando um vírus ou programa indesejado for detectado, você receberá uma notificação de desktop. Na notificação de desktop, você pode remover o malware detectado ou encaminhá-lo usando o botão **Detalhes** no componente Scanner para o gerenciamento futuro do vírus. O Scanner abre a janela contendo a notificação da detecção, que fornece

a você várias opções para o gerenciamento do arquivo afetado por meio do menu contextual (consulte Detecção > Scanner):

Opções de ação para o Scanner:

Interativo

No modo de ação interativo, os resultados da varredura do Scanner são exibidos em uma caixa de diálogo. Essa opção é ativada como a configuração padrão.

No caso de uma **varredura do Scanner**, você receberá um alerta com uma lista dos arquivos afetados quando a varredura for concluída. Você pode usar o menu sensível ao contexto para selecionar uma ação a ser executada para os diversos arquivos afetados. Você pode executar as ações padrão para todos os arquivos infectados ou cancelar o Scanner.

Automático

No modo de ação automática, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente.

Opções de ação para Web Protection:

Interativo

No modo de ação interativo, se um vírus ou programa indesejado for detectado, uma caixa de diálogo será exibida, na qual é possível selecionar o que deve ser feito com o objeto infectado. Essa opção é ativada como a configuração padrão.

Automático

No modo de ação automática, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente.

No modo de ação interativo, você pode reagir aos vírus e programas indesejados detectados selecionando uma ação para o objeto infectado, exibido no alerta, e executando a ação selecionada ao clicar em **Confirmar**.

As seguintes ações estão disponíveis para manipular os objetos infectados:

Observação
Quais ações estão disponíveis para seleção depende do sistema operacional, dos componentes de proteção (Avira Real-Time Protection, Avira Mail Protection, Avira Web Protection) que relatam a deteção e do tipo de malware detectado.

Ações do Scanner:

Reparar

O arquivo é reparado.

Essa opção só estará disponível se for possível reparar o arquivo infectado.

Renomear

O arquivo é renomeado com uma extensão **.vir*. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. Os arquivos podem ser reparados e voltar a ter seus nomes originais posteriormente.

Quarentena

O arquivo é compactado em um formato especial (**.qua*) e movido para o diretório de Quarentena *INFECTED* em seu disco rígido para que o acesso direto não seja mais permitido. Os arquivos nesse diretório podem ser reparados na Quarentena posteriormente ou, se necessário, enviados para a Avira.

Excluir

O arquivo será excluído. Se um vírus de setor de inicialização for detectado, ele poderá ser excluído por meio da exclusão do setor de inicialização. Um novo setor de inicialização é gravado.

Ignorar

Nenhuma ação adicional é executada. O arquivo infectado permanece ativo em seu computador.

Aviso
Isto poderá resultar na perda de dados e em danos ao sistema operacional! Selecione a opção **Ignorar** somente em casos excepcionais.Selecione a opção Ignorar somente em casos excepcionais.

Sempre Ignorar

Opção de ação para detecções do Real-Time Protection: nenhuma outra ação é executada pelo Real-Time Protection. O acesso ao arquivo é permitido. Todo acesso posterior a esse arquivo é permitido e nenhuma outra notificação será fornecida até o computador ser reiniciado ou o arquivo de definição de vírus ser atualizado.

Copiar para quarentena

A opção de ação para a detecção de rootkits: a detecção é copiada na quarentena.

Reparar setor de inicialização | Baixar ferramenta de reparo

Opções de ação quando setores de inicialização infectados são detectados: Inúmeras opções estão disponíveis para reparar unidades de disquete infectadas. Se o produto

Avira não puder executar o reparo, você poderá baixar uma ferramenta especial para detecção e remoção dos vírus do setor de inicialização.

Observação
Se você executar ações em processos em execução, os processos em questão serão finalizados antes de as ações serem executadas.

O site solicitado do servidor da web e/ou todos os dados ou arquivos transferidos são movidos para a quarentena. O arquivo afetado pode ser recuperado do Gerenciador de quarentena se tiver valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

4.3.9 Manipulação de arquivos em quarentena (*.qua)

Para manipular os arquivos em quarentena:

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Quarentena**.
- Verifique quais arquivos estão envolvidos para que, se necessário, você possa recarregar o original no computador a partir de outro local.

Se desejar ver mais informações sobre um arquivo:

- Realce o arquivo e clique em  .
  - ↳ A caixa de diálogo **Propriedades** é exibida com mais informações sobre o arquivo.

Se desejar verificar um arquivo novamente:

É recomendado verificar um arquivo se o arquivo de definição de vírus do produto Avira tiver sido atualizado e houver uma suspeita de um falso-positivo. Desse modo, você pode confirmar o falso-positivo com uma nova verificação e restaurar o arquivo.

- Realce o arquivo e clique em  .
  - ↳ O arquivo é verificado em busca de vírus e malwares usando as configurações de verificação do sistema.
  - ↳ Após a verificação, a caixa de diálogo **Estatísticas da Nova Verificação** será exibida mostrando estatísticas sobre o status do arquivo antes e depois da nova verificação.

Para excluir um arquivo:

- Realce o arquivo e clique em  .

- Você precisa confirmar sua opção com **Sim**.

Se você quiser carregar o arquivo para um servidor da web do Avira Malware Research Center para análise:

- Realce o arquivo que deseja carregar.
- Clique em  .
  - ↳ Uma caixa de diálogo é aberta com um formulário para inserir seus dados de contato.
- Insira todos os dados necessários.
- Selecione um tipo: **Arquivo Suspeito** ou **Suspeita de Falso-Positivo**.
- Selecione um formato de resposta: **HTML**, **Texto**, **HTML e Texto**.
- Clique em **OK.**
  - ↳ O arquivo é carregado em um servidor da web do Avira Malware Research Center em formato compactado.

Observação
Nos casos a seguir, a análise pelo Avira Malware Research Center é recomendada:
Ocorrências de Heurística (Arquivo Suspeito): Durante uma verificação, um arquivo foi classificado como suspeito por seu produto Avira e movido para a quarentena: A análise do arquivo pelo Avira Malware Research Center foi recomendada na caixa de diálogo de detecção do vírus ou no arquivo de relatório gerado pela verificação.

Observação
O tamanho dos arquivos carregados é limitado a 20 MB descompactados ou 8 MB compactados.

Observação
Você pode carregar somente um arquivo por vez.

Se você desejar exportar as propriedades de um objeto em quarentena para um arquivo de texto:

- Realce o objeto em quarentena e clique em  .
  - ↳ O arquivo de texto *Quarentena - Bloco de Notas* é aberto contendo os dados do objeto em quarentena selecionado.

- Salve o arquivo de texto.

Você também pode restaurar os arquivos em quarentena (consulte Capítulo: Quarentena: Restaurar os arquivos em quarentena).

4.3.10 Restaurar os arquivos em quarentena

Ícones diferentes controlam o processo de restauração, dependendo do sistema operacional:

- No Windows XP:
  -  Esse ícone restaura os arquivos em seu diretório original.
  -  Esse ícone restaura os arquivos em um diretório de sua preferência.
- No Windows Vista:

  No Microsoft Windows Vista, o Centro de Controle possui apenas direitos limitados no momento, por exemplo, para acessar diretórios e arquivos. Algumas ações e alguns acessos de arquivo só podem ser realizados no Centro de Controle com direitos de administrador estendidos. Esses direitos devem ser concedidos no início de cada verificação através de um perfil de verificação.
  -  Esse ícone restaura os arquivos em um diretório de sua preferência.
  -  Esse ícone restaura os arquivos em seu diretório original. Se direitos de administrador estendidos forem necessários para acessar esse diretório, será exibida uma solicitação correspondente.

Para restaurar os arquivos em quarentena:

Aviso
Isto poderá resultar na perda de dados e em danos ao sistema operacional do computador! Use a função **Restaurar objeto selecionado** somente em casos excepcionais. Restaure somente os arquivos que podem ser reparados por uma nova verificação.

✓ Arquivo verificado novamente e reparado.

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Quarentena**.

Observação

Emails e anexos de email podem ser restaurados usando a opção  somente se a extensão do arquivo for **.eml*.

Para restaurar um arquivo ao seu local original:

- Realce o arquivo e clique no ícone (Windows XP:  , Windows Vista ).

Essa opção não está disponível para emails.

> **Observação**
>
> Emails e anexos de email podem ser restaurados usando a opção  somente se a extensão do arquivo for **.eml*.

  - ↪ Será exibida uma mensagem perguntando se você deseja restaurar o arquivo.
- Clique em **Sim**.
  - ↪ O arquivo é restaurado para o diretório em que estava antes de ser movido para a quarentena.

Para restaurar um arquivo em um diretório especificado:

- Realce o arquivo e clique em  .
  - ↪ Será exibida uma mensagem perguntando se você deseja restaurar o arquivo.
- Clique em **Sim**.
  - ↪ A janela padrão do Windows *Salvar Como* para selecionar o diretório é exibida.
- Selecione o diretório onde o arquivo será restaurado e confirme.
  - ↪ O arquivo é restaurado para o diretório selecionado.

4.3.11 Mover arquivos suspeitos para quarentena

Para mover um arquivo suspeito para a quarentena manualmente:

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Quarentena**.
- Clique em  .
  - ↪ A janela padrão do Windows para selecionar um arquivo é exibida.
- Selecione o arquivo e confirme com **Abrir**.
  - ↪ O arquivo é movido para a quarentena.

Você pode verificar arquivos na quarentena com o Avira System Scanner (consulte o Capítulo: Quarentena: Manipulando arquivos em quarentena (*.qua)).

4.3.12 Corrigir ou excluir tipo de arquivo em um perfil de varredura

Para especificar outros tipos de arquivo a serem verificados ou excluir determinados tipos da verificação em um perfil de verificação (possível apenas para seleção manual):

✓ No Centro de Controle, vá para a seção *PROTEÇÃO DO PC* **> System Scanner**.

- Com o botão direito do mouse, clique no perfil de verificação que deseja editar.
  - ↳ Um menu contextual é exibido.
- Selecione **Filtro de arquivo**.
- Expanda o menu contextual ainda mais clicando no pequeno triângulo à direita do menu contextual.
  - ↳ As entradas **Padrão**, **Verificar todos os arquivos** e **Definido pelo usuário** são exibidas.
- Selecione **Definido pelo usuário**.
  - ↳ A caixa de diálogo **Extensões do Arquivo** é exibida com uma lista de todos os tipos de arquivo a serem verificados com o perfil de verificação.

Se desejar excluir um tipo de arquivo da verificação:

- Realce o tipo de arquivo e clique em **Excluir**.

Se desejar adicionar um tipo de arquivo à verificação:

- Realce um tipo de arquivo.
- Clique em **Inserir** e insira a extensão do tipo de arquivo na caixa de entrada.

Use no máximo 10 caracteres e não insira nenhum ponto antes. Caracteres curinga (* e ?) são permitidos.

4.3.13 Criar atalho na área de trabalho para o perfil de verificação

Você pode iniciar uma verificação do sistema diretamente a partir de sua área de trabalho através de um atalho na área de trabalho para um perfil de verificação sem acessar o Centro de Controle de seu produto Avira.

Para criar um atalho na área de trabalho para o perfil de verificação:

✓ No Centro de Controle, vá para a seção *PROTEÇÃO DO PC* **> System Scanner**.

- Selecione o perfil de verificação para o qual deseja criar um atalho.
- Clique no ícone  .
  - ↳ O atalho é criado na área de trabalho.

4.3.14 Filtrar Eventos

Eventos que foram gerados por componentes do programa de seu produto Avira são exibidos no Centro de Controle em *ADMINISTRAÇÃO* **> Eventos** (análogo à exibição de evento de seu sistema operacional Windows). Os componentes do programa, em ordem alfabética, são os seguintes:

- Serviço de ajuda
- Real-Time Protection
- Agendamento
- Scanner
- Atualizador
- Web Protection

Os seguintes tipos de evento são exibidos:

- *Informações*
- *Aviso*
- *Erro*
- *Detecção*

Para filtrar os eventos exibidos:

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Eventos**.
- Marque a caixa dos componentes do programa para exibir os eventos dos componentes ativados.

  - OU -

  Desmarque a caixa dos componentes do programa para ocultar os eventos dos componentes desativados.
- Marque a caixa de tipo de evento para exibir esses eventos.

  - OU -

  Desmarque a caixa de tipo de evento para ocultar estes eventos.

5. Detecção

5.1 Visão Geral

Quando um vírus é detectado, o Avira pode executar automaticamente algumas ações ou responder de forma interativo. No modo de ação interativa, uma caixa de diálogo é aberta quando um vírus é detectado; nessa caixa é possível controlar ou iniciar as etapas subsequentes de manipulação do vírus (excluir, ignorar etc). No modo automático, existe uma opção para exibir um alerta quando um vírus é detectado. A ação que foi executada automaticamente é exibida na mensagem.

Este capítulo contém informações abrangentes sobre as mensagens de detecção, organizadas de acordo com o módulo.

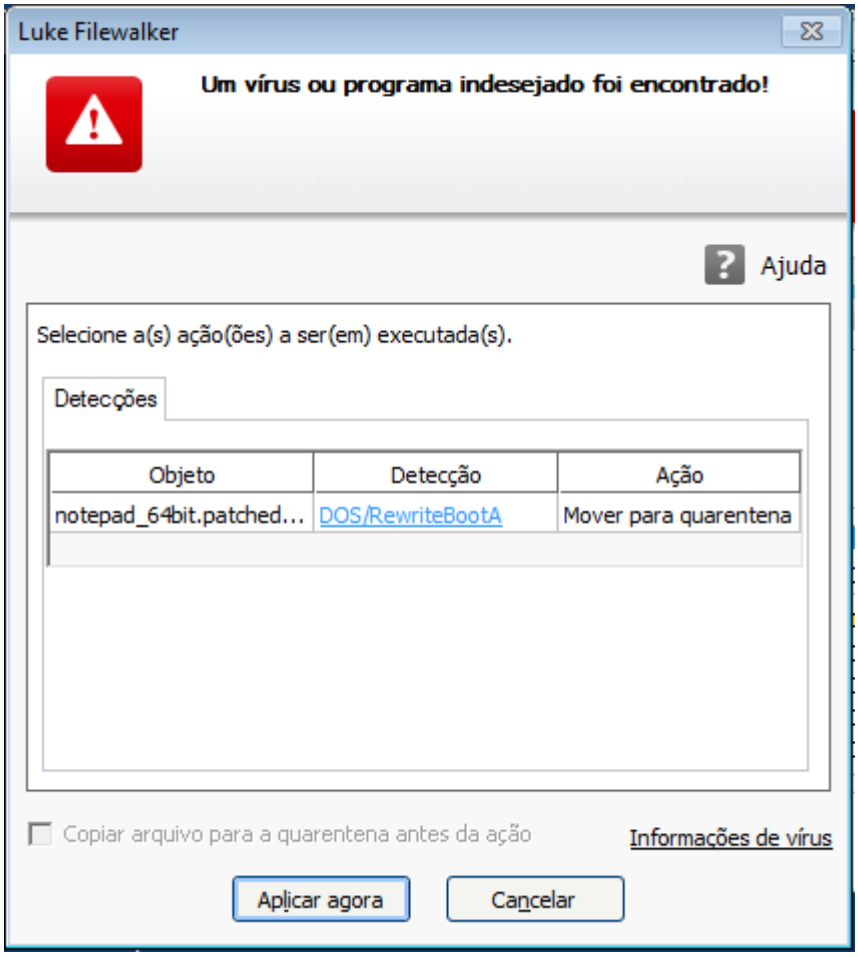
- consulte o Capítulo Scanner: Modo de ação interativa
- consulte o Capítulo Real-Time Protection
- consulte o Capítulo Web Protection

5.2 Modo de ação interativa

Se você tiver selecionado o modo *Interativo* como o modo de ação, quando um vírus é detectado, receberá um alerta contendo uma lista de arquivos afetados, quando a varredura for concluída (consulte a seção de configuração Scanner > Varredura > Ação para detecção).
Você pode usar o menu sensível ao contexto para selecionar uma ação a ser executada para os diversos arquivos afetados. Você pode executar as ações padrão para todos os arquivos infectados ou cancelar o Scanner.

Nota
Se relatório for ativado, o Scanner insere cada detecção no Arquivo de relatório.

5.2.1 Alerta



5.2.2 Detecção, Erros, Avisos

Informações detalhadas, opções de ação para vírus detectados e mensagens serão exibidas nas guias **Detecção**, **Erros** e **Avisos**:

- **Detecção:**
  - *Objeto:* Nome de arquivo do arquivo afetado
  - *Detecção:* nome do vírus ou programa indesejado detectado
  - *Ação:* ação selecionada com a qual o arquivo afetado deve ser manipulado
    Você pode escolher outras ações para lidar com o malware no menu contextual associado à ação exibida.
- **Erro:** mensagens sobre os erros que ocorreram durante a varredura
- **Alertas:** alertas relacionados aos vírus que foram detectados

> **Nota**
> As seguintes informações são exibidas na dica de ferramenta do objeto: nome

do arquivo ou afetado e caminho completo, nome do vírus e ação que deve ser executada com o botão **Aplicar agora**.

Nota
A ação padrão do Scanner é exibida como a ação a ser executada. A ação padrão do Scanner para manipular os arquivos afetados é mover os arquivos relevantes para a quarentena.

5.2.3 Ações do menu contextual

Nota
Se a detecção for um acesso heurístico (HEUR/), uma ferramenta de compactação de tempo de execução incomum (PCK/) ou um arquivo com uma extensão de arquivo oculta (HEUR-DBLEXT/), no modo interativo somente as opções Mover para quarentena e Ignorar estarão disponíveis. No modo automático a detecção é movida automaticamente para Quarentena.
. Essa restrição impede que os arquivos detectados, que podem ser um alarme falso, sejam removidos (excluídos) diretamente do computador. O arquivo pode ser recuperado a qualquer momento com a ajuda do Gerenciador de Quarentena.

Reparar

Se essa opção for ativada, o Scanner reparará o arquivo afetado.

Nota
A opção **Reparar** somente poderá ser ativada se for possível reparar o arquivo detectado.

Quarentena

Se essa opção for ativada, o Scanner move o arquivo para a quarentena. O arquivo pode ser recuperado do gerenciador de quarentena se tiver um valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira. Dependendo do arquivo, outras opções de seleção podem estar disponíveis no Gerenciador de quarentena.

Excluir

Se essa opção for ativada, o arquivo será excluído.

Renomear

Se essa opção for ativada, o Scanner renomeará o arquivo. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

Ignorar

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

Sempre Ignorar

Opção de ação para detecções do Real-Time Protection: nenhuma outra ação é executada pelo Real-Time Protection. O acesso ao arquivo é permitido. Todo acesso posterior a esse arquivo é permitido e nenhuma outra notificação será fornecida até o computador ser reiniciado ou o arquivo de definição de vírus ser atualizado.

Aviso
Se você ignorar as opções ou selecionar **Sempre ignorar**, os arquivos afetados permanecem ativos no computador! Isso pode causar danos graves à estação de trabalho!

5.2.4 Recursos especiais quando setores de inicialização infectados, rootkits e malware ativo são detectados

As opções de ação estão disponíveis para reparar setores de inicialização infectados quando forem detectados:

Reparar setor de inicialização de 722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB

Essas opções estão disponíveis para unidades de disquete.

Download do CD de resgate

Essa opção o levará ao site da Avira, onde você pode baixar uma ferramenta especial para detectar e remover vírus do setor de inicialização.

Se você executar ações nos processos em execução, os processos em questão serão finalizados antes de as ações serem executadas.

5.2.5 Botões e links

Botão / link	Descrição
Aplicar agora	As ações selecionadas são executadas para manipular todos os arquivos afetados.
Cancelar	O Scanner é fechado sem nenhuma outra ação. Os arquivos afetados não são alterados no sistema do seu computador.
	Esta página da ajuda on-line é aberta por meio deste botão ou link.

Aviso
Execute a ação *Cancelar* somente em casos excepcionais. Os arquivos afetados permanecem ativos na estação de trabalhos após o cancelamento! Isso pode causar danos graves à estação de trabalho!

5.2.6 Recursos especiais quando malware for detectado enquanto Web Protection estiver inativo

Se você desativou o Web Protection, o Scanner relata malware ativo que detectou por meio de um slide-up durante a varredura do sistema. Antes de reparar o sistema é possível criar um ponto de restauração.

✓ Primeiro é necessário ativar o System Restore no sistema Windows.

- Clique em **Detalhes** no slide up.
  - ↪ A janela *O sistema está sendo verificado* é exibida.
- Ative **Criar ponto de restauração do sistema antes do reparo**.
- Clique em **Aplicar**.
  - ↪ Um ponto de restauração do sistema foi criado. Agora você pode executar uma restauração do sistema usando o Painel de controle do Windows se necessário.

5.3 Real-Time Protection

Se vírus forem detectados pelo Real-Time Protection, o acesso ao arquivo será negado e uma notificação de desktop será exibida

Notificação

As informações a seguir são exibidas na notificação:

- Data e hora da detecção
- Caminho e nome do arquivo afetado
- Nome do malware

> **Nota**
> Quando o modo de partida padrão do Real-Time Protection (Partida normal) foi escolhido e o processo de logon na partida for executado com rapidez, os programas configurados para iniciar automaticamente na partida poderão não ser verificados porque poderão estar ativos e em execução antes de o Real-Time Protection ter iniciado completamente.

No modo interativo existem as seguintes opções:

Remover

O arquivo afetado é transferido para o componente Scanner e é excluído pelo Scanner. Nenhuma mensagem adicional é exibida.

Detalhes

O arquivo afetado é transferido para o componente Scanner. O Scanner abre uma janela que contém a notificação da detecção e diversas opções de gerenciamento do arquivo afetado.

> **Nota**
> Veja as informações sobre gerenciamento de vírus em Detecção > Scanner.

> **Nota**
> A ação *Quarentena* é pré-selecionada por padrão na notificação do Scanner. Outras ações podem ser selecionadas em um menu contextual.

Fechar

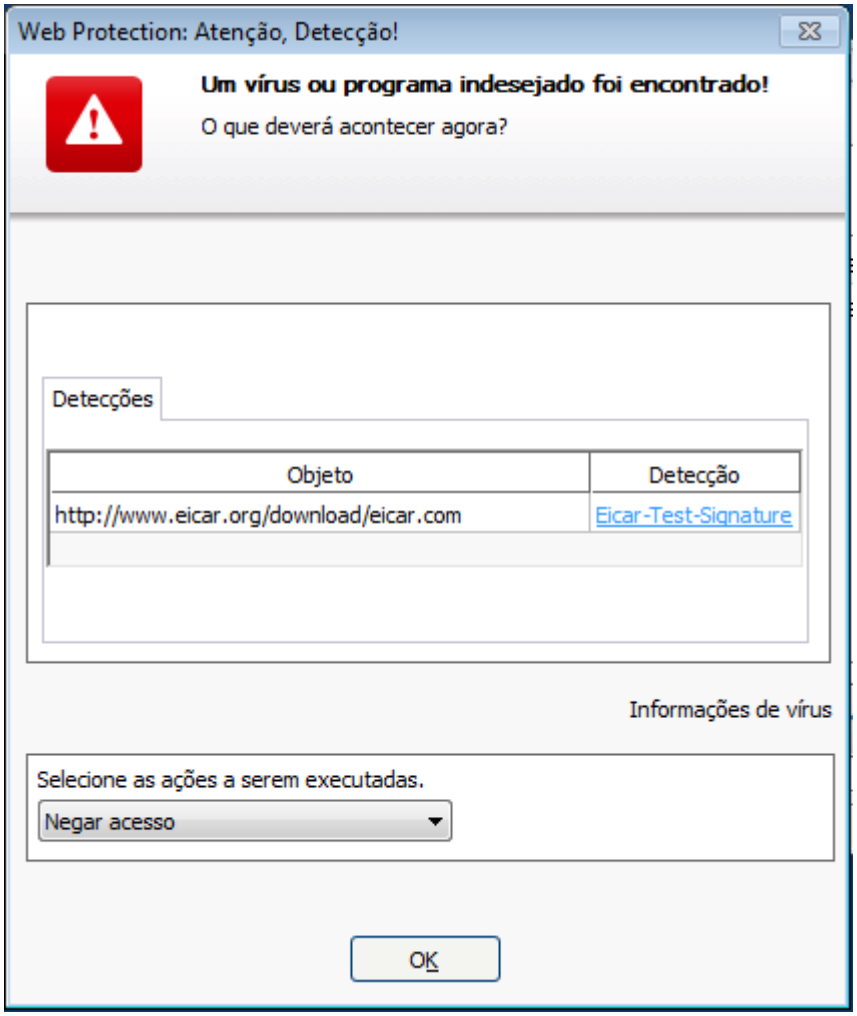
A mensagem é fechada. O gerenciamento de vírus é finalizado.

5.4 Web Protection

Se vírus forem detectados pelo Web Protection, você receberá um alerta se tiver selecionado o modo *interativo* (consulte a seção de configuração Web Protection >

Verificar > Ação na detecção). No modo interativo, você pode escolher o que deve ser feito com os dados enviados pelo servidor da Web na caixa de diálogo.

Alerta



Detecção, Erros, Avisos

Mensagens e informações detalhadas relacionadas aos vírus detectados são exibidas nas guias **Detecção**, **Erros** e **Avisos**:

- **Detecção:** URL e o nome do vírus ou programa indesejado detectado
- **Erro:** mensagens sobre os erros que ocorreram durante a verificação do Web Protection scan
- **Alertas:** avisos relacionados aos vírus que foram detectados

Ações possíveis

> **Nota**
> Se a detecção for um acesso heurístico (HEUR/), uma ferramenta de

compactação de tempo de execução incomum (PCK/) ou um arquivo com uma extensão de arquivo oculta (HEUR-DBLEXT/), no modo interativo somente as opções Mover para quarentena e Ignorar estarão disponíveis.
Essa restrição impede que os arquivos detectados, que podem ser um alarme falso, sejam removidos (excluídos) diretamente do computador. O arquivo pode ser recuperado a qualquer momento com a ajuda do Gerenciador de quarentena.

Negar acesso

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos não são enviados para o navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador. O Web Protection registra a detecção no arquivo de relatório se a função de registro estiver ativada.

Mover para quarentena

No caso um vírus ou malware ser detectado, o site solicitado do servidor da web e/ou os dados e arquivos transferidos são movidos para a quarentena. O arquivo afetado pode ser recuperado do Gerenciador de quarentena se tiver valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

Ignorar

O site solicitado do servidor da web e/ou os dados e arquivos que foram transferidos são encaminhados pelo Web Protection para o navegador.

Aviso
Isso pode permitir o acesso de vírus e programas indesejados ao sistema do computador. Selecione a opção **Ignorar** somente em casos excepcionais.

Botões e links

Botão / link	Descrição
Informações de vírus	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
Ajuda	Esta página da ajuda on-line é aberta por meio deste botão ou link.

6. Scanner

6.1 Scanner

Com o componente Scanner, você pode realizar varreduras direcionadas (sob demanda) em busca de vírus e programas indesejados. As seguintes opções estão disponíveis para varredura de arquivos infectados:

- **Varredura do Sistema via Menu Contextual**
  A varredura do sistema por meio do menu contextual (botão direito do mouse - entrada **Varredura de arquivos selecionados com o Avira**) é recomendada se, por exemplo, você deseja efetuar a varredura de arquivos e diretórios individuais. Uma outra vantagem é que não é necessário iniciar primeiro o Centro de Controle para uma varredura do sistema por meio do menu contextual.
- **Varredura do Sistema por meio de Arrastar e Soltar**
  Quando um arquivo ou diretório é arrastado na janela do programa do Centro de Controle, o Scanner efetua a varredura do arquivo ou diretório e todos os subdiretórios que ele contém. Esse procedimento é recomendado se você desejar efetuar a varredura de arquivos e diretórios individuais que foram salvos, por exemplo, em sua área de trabalho.
- **Varredura do Sistema Através de Perfis**
  Este procedimento é recomendado se você deseja efetuar a varredura de regularmente determinados diretórios e unidades (por exemplo, seu diretório de trabalho ou unidades nas quais você armazena novos arquivos regularmente). Você não precisa selecionar esses diretórios e unidades novamente em cada nova varredura, basta selecionar o perfil relevante.
- **Varredura do sistema via Agendamento**
  O Agendamento permite realizar verificações controladas pelo tempo.

Processos especiais são necessários ao efetuar a varredura de em busca de rootkits e vírus de setor de inicialização e ao efetuar a varredura de os processos ativos. As seguintes opções estão disponíveis:

- Varredura de rootkits por meio do perfil de varredura **Varredura de rootkits e malware ativo**
- Varredura de processos ativos através do perfil de varredura **Processos ativos**
- Varredura de vírus do setor de inicialização através do comando de menu **Varredura dos registros de inicialização...** no menu **Extras**

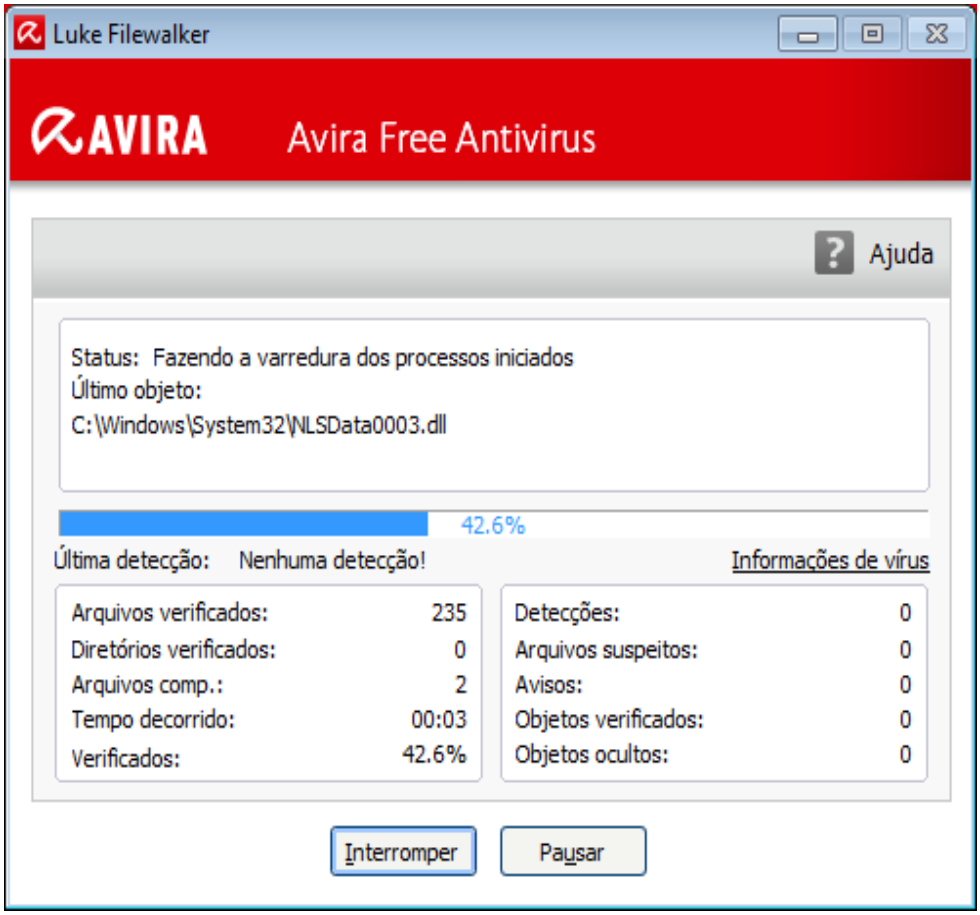
6.2 Luke Filewalker

Durante uma verificação do sistema, a janela de status **Luke Filewalker** aparece, a qual fornece informações exatas sobre o status da varredura.

Se a opção **interativa** estiver selecionada na configuração do System Scanner no grupo **Ação na Detecção**, será perguntado o que deve ser feito com um vírus ou programa indesejado detectado. Se a opção **automático** estiver selecionada, quaisquer detecções serão mostradas no Relatório do Scanner.

Quando a verificação for concluída, seu resultado (estatísticas), alertas e mensagens de erro serão exibidos em uma nova caixa de diálogo.

6.2.1 Luke Filewalker: Janela de Status da Verificação



Informações exibidas

Status: Há diferentes mensagens de status:

- *O programa será inicializado*
- *A pesquisa de objetos ocultos está em execução!*
- *Verificando os processos iniciados*
- *Verificando arquivo*
- *Inicializar arquivamento*
- *Liberar memória*
- *Arquivo está sendo descompactado*

- *Verificando setores de inicialização*
- *Verificando setores de inicialização mestres*
- *Verificando o registro*
- *O programa será encerrado!*
- *A verificação foi concluída*

Último Objeto: Nome e caminho do arquivo que está sendo verificado atualmente ou que foi verificado mais recentemente

Última Deteção: Há várias mensagens para a última detecção:

- *Nenhuma detecção!*
- Nome do vírus ou programa indesejado detectado mais recentemente

Arquivos Verificados: Número de arquivos verificados

Diretórios Verificados: Número de diretórios verificados

Arquivos Mortos Verificados: Número de arquivos mortos verificados

Tempo Utilizado: Duração da verificação do sistema

Verificado: Porcentagem da verificação já concluída

Detecções: Número de vírus e programas indesejados detectados

Arquivos Suspeitos: Número de arquivos relatados pela heurística

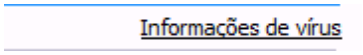
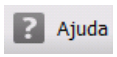
Avisos: Número de alertas sobre vírus detectados

Objetos Verificados: Número de objetos verificados durante a verificação de rootkits

Objetos Ocultos: Número total de objetos ocultos detectados

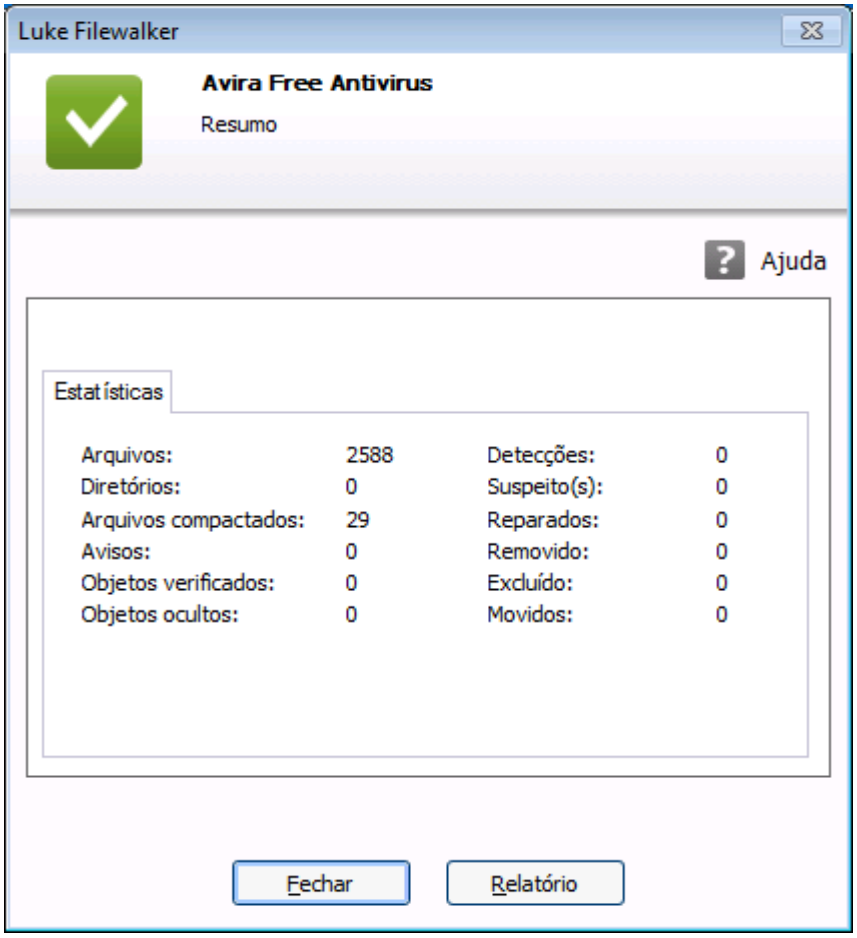
Observação
Os rootkits têm a capacidade de ocultar processos e objetos, tais como entradas de registro ou arquivos. No entanto, nem todo objeto oculto é necessariamente prova da existência de um rootkit. Os objetos ocultos também podem ser objetos inofensivos. Se uma verificação detectar objetos ocultos, mas não emitir um alerta de detecção de vírus, você deverá usar o relatório para determinar qual objeto é referido e obter mais informações sobre o objeto detectado.

Botões e links

Botão / Link	Descrição
	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
	Esta página da ajuda online é aberta por meio deste botão ou link.
Parar	O processo de verificação é interrompido.
Pausar	A verificação será interrompida e poderá ser retomada ao clicar no botão **Continuar**.
Continuar	A verificação interrompida continuará.
Finalizar	O System Scanner é fechado.

Relatório	O arquivo do relatório da verificação será mostrado.

6.2.2 Luke Filewalker: Estatísticas de Verificação



Informações exibidas: Estatísticas

Arquivos: Número de arquivos verificados

Diretórios: Número de diretórios verificados

Arquivo Morto: Número de arquivos mortos verificados

Avisos: Número de alertas sobre vírus detectados

Objetos Pesquisados: Número de objetos verificados durante a verificação de rootkits

Objetos Ocultos: Número de objetos ocultos detectados (rootkits)

Detecções: Número de vírus e programas indesejados detectados

Suspeito: Número de arquivos relatados pela heurística

Reparado: Número de arquivos reparados

Apagado: Número de arquivos substituídos

Excluído: Número de arquivos excluídos

Movido: Número de arquivos que são movidos para quarentena

Botões e links

Botão / Link	Descrição
	Esta página da ajuda online é aberta por meio deste botão ou link.
Fechar	A janela de resumo é fechada.
Relatório	O arquivo do relatório da verificação será mostrado.

7. Centro de Controle

7.1 Visão geral do Centro de controle

O Centro de controle é um centro de informações, configuração e gerenciamento. Além das seções que podem ser selecionadas individualmente, existem diversas opções que podem ser acessadas na barra de menus.Além das seções que podem ser selecionadas individualmente, existem diversas opções que podem ser acessadas na barra de menus.

Barra de menus

Todas as funções do Centro de Controle estão contidas na barra de menus.

Arquivo

- Sair (Alt + F4)

Exibir

- Status
- Proteção do PC
  - Scanner
  - Real-Time Protection
- Proteção na Internet
  - FireWall
  - Web Protection
- Proteção Móvel
  - Avira Free Android Security
- Administração
  - Quarentena
  - Agendamento
  - Relatórios
  - Eventos
- Atualizar (F5)

Extras

- Varredura dos registros de inicialização...
- Lista de detecções...
- Configuração (F8)

Atualização

- Iniciar atualização...
- Atualização manual...

Ajuda

- Sumário
- Leia-me
- Ajude-me
- Fórum
- Fazer download do manual
- Gerenciamento de licenças
- Indicar produto
- Enviar feedback
- Mostrar notificador novamente
- Sobre o Avira Free Antivirus

> **Nota**
> A navegação do teclado pode ser ativada na barra de menus com a ajuda da tecla [ALT]. Se a navegação estiver ativada, você poderá percorrer o menu com as teclas de seta. Com a tecla Voltar, você ativa o item de menu ativo.

Seções de navegação

Na barra de navegação esquerda são encontradas as seguintes seções:

- **Status**

PROTEÇÃO DO PC

- Scanner
- Real-Time Protection

PROTEÇÃO NA INTERNET

- FireWall
- Web Protection

PROTEÇÃO PARA CRIANÇAS

PROTEÇÃO MÓVEL

- Avira Free Android Security

ADMINISTRAÇÃO

- Quarentena
- Agendamento
- Relatórios
- Eventos

Descrição da navegação

- **Status**: Clicar na barra **Status** fornece uma visão geral da funcionalidade do produto e do desempenho (consulte Status).
  - A seção **Status** permite ver rapidamente quais módulos estão ativos e fornece informações sobre a última atualização realizada.
- *PROTEÇÃO DO PC*: Nesta seção você localizará os componentes para verificar os arquivos em seu sistema do computador em busca de vírus e malwares.
  - A seção Scanner permite configurar e iniciar facilmente uma varredura por demanda. Perfis predefinidos ativa uma varredura com opções padrão já adaptadas. Do mesmo modo, é possível adaptar a varredura de vírus e programas indesejados de acordo com seus requisitos pessoais com a ajuda da seleção manual (será salva).
  - A seção Real-Time Protection exibe informações sobre arquivos verificados, assim como outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".
- *PROTEÇÃO NA INTERNET*: Nesta seção você localizará os componentes para proteger seu sistema do computador contra vírus e malwares da Internet e contra acesso à rede não autorizado.
  - A seção FireWall permite configurar as configurações básicas do FireWall. Além disso, são exibidos a taxa de transferência de dados atual e todos os aplicativos ativos que usam uma conexão de rede.
  - A seção Web Protection apresenta informações sobre URLs verificados e vírus detetados e outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite o acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".
- *PROTEÇÃO PARA CRIANÇAS*: Nesta seção você localizará os componentes para assegurar uma experência na Internet segura para seus filhos.
- *PROTEÇÃO MÓVEL*: Desta seção você será redirecionado ao acesso on-line para dispositivos Android.
  - Avira Free Android Security gerencia todos os dispositivos baseados em Android.
- *ADMINISTRAÇÃO*: Nesta seção você localizará ferramentas para isolar e gerenciar arquivos suspeitos ou infectados e para planejar tarefas recorrentes.

- A seção Quarentena contém o conhecido gerenciador de quarentena. Este é o ponto central para os arquivos já colocados na quarentena ou para os arquivos suspeitos que deseja colocar na quarentena. Também é possível enviar um arquivo selecionado para o Avira Malware Research Center por e-mail.
- A seção Agendamento permite configurar trabalhos programados de varredura e atualização, bem como trabalhos de backup, e adaptar ou excluir os trabalhos existentes.
- A seção Relatórios permite visualizar os resultados de ações executadas.
- A seção Eventos permite visualizar os eventos gerados por determinados módulos do programa.

Botões e links

Os botões e links a seguir pode estar disponíveis.

Botão / link	Atalho	Descrição
Configuração		Esse botão ou link é usado para acessar o diálogo de configuração correspondente da seção.
	F1	Esse botão ou link abre o tópico da ajuda on-line correspondente da seção.

7.2 Arquivo

7.2.1 Sair

O item de menu **Sair** no menu **Arquivo** fecha o Centro de Controle.

7.3 Exibir

7.3.1 Status

A tela inicial do Centro de controle, a seção **Status**, permite ver com uma visão rápida se o sistema do computador está protegido e quais módulos do Avira estão ativos. A janela **Status** também fornece informações sobre a última atualização realizada. Você também pode ver se possui uma licença válida.

- Proteção do PC: Proteção em Tempo Real, Última varredura, Última atualização, Atualização
- Proteção na Internet : Web Protection, FireWall,

Nota
O Controle de Conta de Usuário vai pedir a você permissão para habilitar ou desabilitar a Real-Time Protection e Web Protection nos sistemas operacionais a partir do Windows Vista.

Proteção do PC

As informações sobre o status atual do serviço e das funções de proteção que protegem o computador localmente contra vírus e malware da Internet estão exibidas nessa seção.

Real-Time Protection

As informações sobre o status atual do Real-Time Protection são exibidas nesse campo.

É possível ativar ou desativar o Real-Time Protection clicando no botão **ON/OFF**. Outras opções do Real-Time Protection podem ser acessadas clicando em **Real-Time Protection** na barra de navegação. Inicialmente você recebe informações sobre o último malware e arquivos infectados encontrados. Clique em **Configuração** para definir outras configurações.

- **Configuração**: Acesse a Configuração para definir as configurações dos componentes do Real-Time Protection.

As seguintes possibilidades estão disponíveis:

Ícone	Status	Opção	Descrição
	*Ativado*	**Desativar**	O serviço Real-Time Protection está ativo, ou seja, o sistema é monitorado continuamente quanto a vírus e programas indesejados. **Nota** É possível desabilitar o serviço Real-Time Protection. No entanto, observe que se o Real-Time Protection for desativado você não estará mais protegido contra vírus e programas indesejados. Todos os arquivos podem passar despercebidos pelo sistema e causar danos.

	*Desativado*	**Ativar**	O serviço Real-Time Protection está desativado, ou seja, o serviço está carregado, mas não está ativo. **Aviso** Não é realizada nenhuma varredura quanto a vírus e programas indesejados. Todos os arquivos podem passar despercebidos pelo sistema. Você não está protegido contra vírus e programas indesejados. **Nota** Para ficar protegido contra vírus e programas indesejados, clique no botão **LIGA/DESLIGA** ao lado do **Real-Time Protection** na área *Proteção do PC*.

	*Serviço interrompido*	**Iniciar serviço**	O serviço Real-Time Protection está interrompido. **Aviso** Não é realizada nenhuma varredura quanto a vírus e programas indesejados. Todos os arquivos podem passar despercebidos pelo sistema. Você não está protegido contra vírus e programas indesejados. **Nota** Para ficar protegido contra vírus e programas indesejados, clique no botão **LIGA/DESLIGA** ao lado do **Real-Time Protection** na área *Proteção do PC*. O estado atual deve ser exibido em verde, o que significa **Ativado**.

	Desconhecido	**Ajuda**	Esse status é exibido quando ocorre um erro desconhecido. Nesse caso, entre em contato com o nosso Suporte.

Última varredura

As informações sobre a última varredura do sistema executada são exibidas nesse campo. Quando uma varredura do sistema completa é executada, todos os discos rígidos no computador são verificados totalmente. São empregados todos os processos de varredura, com exceção da varredura da integridade dos arquivos do sistema: varredura padrão dos arquivos, varredura do registro e dos setores de inicialização, varredura dos rootkits etc.

Os seguintes detalhes são exibidos:

- Data da última varredura completa do sistema

As seguintes possibilidades estão disponíveis:

Varredura do sistema	Opção	Descrição
Não executado	**Verificar sistema**	Nenhuma verificação completa do sistema foi executada desde a instalação. **Aviso** O status do sistema é não verificado. Vírus ou programas indesejados talvez sejam encontrados em seu computador. **Nota** Para verificar o computador, clique no link **Verificar sistema**.
Data da última varredura do sistema, por exemplo, *18/09/2011*	**Verificar sistema**	Você executou uma varredura completa do sistema na data especificada. **Nota** Recomendamos que use o trabalho de varredura padrão *Varredura completa do sistema*. Use o Agendamento para ativar o trabalho **Varredura completa do sistema**.
Desconhecido	**Ajuda**	Esse status é exibido quando ocorre um erro desconhecido. Nesse caso, entre em contato com o nosso Suporte.

Última atualização

As informações sobre o status atual da última atualização realizada são exibidas aqui.

Os seguintes detalhes são exibidos:

- Data da última atualização
  - Clique no botão **Abrir configuração** para definir outras configurações de atualização automática.

As seguintes possibilidades estão disponíveis:

Ícone	Status	Opção	Descrição
	*Data da última atualização, por exemplo, 18/07/2011*	**Iniciar atualização**	O programa foi atualizado nas últimas 24 horas. **Nota** Você pode atualizar o produto Avira para a versão mais recente com o botão **Iniciar atualização**.
	*Data da última atualização, por exemplo, 18/07/2011*	**Iniciar atualização**	Já se passaram 24 horas desde a atualização, mas você ainda está no ciclo de lembretes de atualização escolhido. Isso depende das definições da configuração. **Nota** Você pode atualizar o produto Avira para a versão mais recente com o botão **Iniciar atualização**.

	*Não executado*	**Iniciar atualização**	Desde a instalação, nenhuma atualização foi realizada -ou- O ciclo de lembretes de atualização foi excedido (consulte Configuração) e nenhuma atualização foi realizada -ou- O arquivo de definição de vírus é mais antigo que o ciclo de lembretes de atualização selecionado (consulte Configuração). **Nota** Você pode atualizar o produto Avira para a versão mais recente com o botão **Iniciar atualização**.
		Não disponível	Se a licença tiver expirado, nenhuma atualização pode ser realizada.

Atualizar

Neste campo, você pode adquirir a versão paga do produto Avira.

Proteção na Internet

As informações sobre o status atual do serviço que protegem o computador contra vírus e malwares da Internet são exibidos nessa seção.

- **FireWall**: O serviço monitora os canais de comunicação de entrada e saída do computador.
- **Web Protection**: O serviço verifica os dados que são transmitidos e carregados no navegador enquanto você navega na Internet (monitoramento das portas 80, 8080, 3128).

Outras opções para esses processos podem ser acessadas em um menu contextual clicando no ícone de configuração ao lado do botão **LIGA/DESLIGA**.

- **Configurar**: acesse Configuração para definir as configurações do componente do processo.

As seguintes possibilidades estão disponíveis: *Serviços*

Ícone	Status	Status do processo	Opção	Significado
	*OK*	*Ativado*	**Desativar**	Todos os serviços para Proteção na Internet estão ativos. **Nota** É possível desativar um serviço clicando no botão **LIGA/DESLIGA** . No entanto, você não estará mais totalmente protegido contra vírus e malwares assim que o serviço for desativado.
	*Restrito*	*Desativado*	**Ativar**	Um serviço está desativado, ou seja, o serviço foi iniciado, mas não está ativo. **Aviso** O seu sistema de computador não está sendo totalmente monitorado. Vírus e programas indesejados talvez acessem seu computador. **Nota** Para ativar o serviço, clique no botão **LIGA/DESLIGA**.

	Aviso	*Serviço interrompido*	**Iniciar serviço**	Um serviço foi interrompido **Aviso** O seu sistema de computador não está sendo totalmente monitorado. Vírus e programas indesejados talvez acessem seu computador. **Nota** Clique no botão **LIGA/DESLIGA** para iniciar o serviço e o seu sistema de computador passar a ser monitorado. O serviço é iniciado e ativado.
		Desconhecido	**Ajuda**	Esse status é exibido quando ocorre um erro desconhecido. Nesse caso, entre em contato com o nosso Suporte.

7.3.2 Scanner

A seção **Scanner** permite configurar e iniciar facilmente uma varredura do sistema. Perfis predefinidos permitem uma varredura do sistema com opções padrão já adaptadas. Da mesma maneira é possível adaptar a varredura do sistema quanto a vírus e programas indesejados para os seus requisitos pessoais com ajuda de seleção.

A exibição e a manipulação dos perfis editáveis são semelhantes às do Windows Explorer. Cada pasta do diretório principal corresponde a um perfil. Pastas a serem verificados são selecionados ou podem ser selecionados com uma marca de varredura na frente da pasta a ser verificado.

- Para alterar as unidades, clique duas vezes na letra da unidade desejada.
- Para selecionar unidades, pode clicar na caixa na frente do ícone da unidade.
- Você pode navegar pela estrutura de menus com a ajuda da barra de rolagem e das setas de rolagem.

Perfis predefinidos

Os perfis de varredura predefinidos estão disponíveis se necessários.

Nota
Esses perfis são somente leitura e não podem ser alterados ou excluídos. Para adaptar um perfil a suas necessidades, selecione a pasta Seleção manual.

Nota
As opções de varredura para os perfis predefinidos podem ser definidas em Configuração > Scanner > Varredura > Arquivos. É possível adaptar essas configurações a suas necessidades.

Unidades locais

Todas as unidades locais do sistema são verificadas quanto a vírus ou programas indesejados.

Discos rígidos locais

Todos os discos rígidos locais do sistema são verificados quanto a vírus ou programas indesejados.

Unidades removíveis

Todas as unidades removíveis disponíveis do sistema são verificadas quanto a vírus ou programas indesejados.

Diretório do sistema Windows

O diretório do sistema Windows do sistema é verificado quanto a vírus ou programas indesejados.

Varredura completa do sistema

Todos os discos rígidos locais do computador são verificados quanto a vírus ou programas indesejados. Durante a varredura, são usados todos os processos de varredura, com exceção da verificação de integridade dos arquivos do sistema: varredura padrão dos arquivos, varredura do registro e dos setores de inicialização, varredura dos rootkits, etc. (consulte Scanner > Visão geral). Os processos de varredura são realizados independentemente da definição do scanner na configuração em Scanner > Varredura: outras configurações.

Varredura rápida do sistema

As pastas mais importantes do sistema (diretórios *Windows*, *Programs*, *Documents and Settings\Local User*, *Documents and Settings\All Users*) são verificadas quanto a vírus e programas indesejados.

Meus documentos

O local padrão de "*Meus documentos*" do usuário conectado é verificado quanto a vírus e programas indesejados.

Nota
No Windows, "*Meus documentos*" é um diretório no perfil do usuário que é usado como o local padrão para documentos que precisam ser salvos. A configuração padrão do diretório é *C:\Documents and Settings\[nome do usuário]\My Documents*.

Processos ativos

Todos os processos atuais são verificados quanto a vírus ou programas indesejados.

Verificar rootkits e malware ativo

O computador não é verificado quanto a rootkits e programa de malware ativos (em execução). Todos os processos em execução são verificados.

Nota
No modo interativo existem várias maneiras de reagir a uma detecção. No modo automático a detecção é registrada no arquivo de relatório.

Nota
A varredura de rootkit não está disponível para o Windows XP de 64 bits !

7.3.3 Seleção manual

Selecione esta unidade para adaptar a varredura às suas necessidades individuais.

7.3.4 Real-Time Protection

A seção **Real-Time Protection** exibe informações sobre arquivos verificados, assim como outros dados estatísticos e permite acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".

Nota
Se o serviço Real-Time Protection não for iniciado, o botão ao lado do módulo é exibido na cor amarela. Porém, o arquivo de relatório do Real-Time Protection pode ser exibido.

Barra de ferramentas

Ícone	Descrição
	**Exibir arquivo de relatório** O arquivo de relatório do Real-Time Protection é exibido.

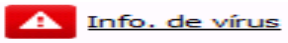
Informações exibidas

Último arquivo encontrado

Mostra o nome e o local do último arquivo encontrado pelo Real-Time Protection.

Ultimo vírus ou programa indesejado encontrado

Fornece o nome do último vírus ou programa indesejado encontrado.

Ícone/link	Descrição
	Clique no ícone ou link para exibir informações detalhadas sobre o vírus ou programa indesejado se houver uma conexão com a Internet.

Último arquivo verificado

Mostra o nome e o caminho do último arquivo verificado pelo Real-Time Protection.

Estatística

Número de arquivos

Mostra o número de arquivos verificados até o momento.

Número de detecções

Mostra o número de vírus e programas indesejados encontrados até o momento.

Número de arquivos suspeitos

Exibe o número de arquivos registrados pela heurística.

Número de arquivos excluídos

Mostra o número de arquivos excluídos até o momento.

Número de arquivos reparados

Mostra o número de arquivos reparados até o momento.

Número de arquivos movidos

Mostra o número de arquivos movidos até o momento.

Número de arquivos renomeados

Mostra o número de arquivos renomeados até o momento.

7.3.5 FireWall

Firewall do Windows (Windows 7 ou superior)

Avira gerencia o Firewall do Windows a partir do Centro de Controle e Configuração.

A seção do FireWall permite verificar o estado do Firewall do Windows e restaurar as configurações recomendadas clicando no botão **Corrigir problema**.

7.3.6 Web Protection

A seção **Web Protection** mostra informações sobre URLs verificadas, além de outros dados estatísticos que podem ser redefinidos a qualquer momento e e permitem acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o pressionamento de um botão".

Barra de ferramentas

Ícone	Descrição
	**Mostrar arquivo de relatório** O arquivo de relatório do Web Protection é exibido.

Informações exibidas

Último URL relatado

Exibe o último URL detectado pelo Web Protection.

Último vírus ou programa indesejado detectado

Fornece o nome do último vírus ou programa indesejado encontrado.

Ícone/link	Descrição
Info. de vírus	Clique no ícone ou link para exibir informações detalhadas sobre o vírus ou programa indesejado se houver uma conexão com a Internet.

Último URL verificado

Mostra o nome e o caminho do último URL verificado pelo Web Protection.

Estatística

Número de URLs

Mostra o número de URLs verificados até o momento.

Número de detecções

Mostra o número de vírus e programas indesejados encontrados até o momento.

Número de URLs bloqueados

Mostra o número de URLs bloqueados anteriormente.

Número de URLs ignorados

Mostra o número de URLs ignorados anteriormente.

7.3.7 Avira Free Android Security

O aplicativo Avira Free Android Security não está focado somente em medidas antirroubo que ajudam a recuperar o dispositivo remoto se você perdê-lo ou, pior ainda, se ele for roubado. O aplicativo permite bloquear chamadas de entrada e SMS. O Avira Free Android Security protege telefones celulares e smartphones que executam o sistema operacional Android.

O Avira Free Android Security consiste em dois componentes:

- o próprio aplicativo, instalado no dispositivo Android
- o Console da web Avira Android para registro e controle de recursos

Avira Free Android Security é um aplicativo gratuito que não precisa de licença. Todas as principais marcas são suportadas pelo Avira Free Android Security como Samsung, HTC, LG e Motorola.

Mais informações podem ser encontradas no nosso site:

http://www.avira.com/android

7.3.8 Quarentena

O **Gerenciador de quarentena** gerencia os objetos afetados. O produto Avira pode mover os objetos afetados para o diretório de quarentena em um formato especial. Não podem ser executados ou abertos.

> **Nota**
> Para mover objetos para o Gerenciador de quarentena, selecione a opção relevante para a quarentena em **Configuração** em **Scanner** - **Varredura > Ação na detecção** se estiver trabalhando em **modo automático**.
> Como alternativa, pode selecionar a opção de quarentena relevante no **modo interativo**.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**F2**	**Verificar novamente o(s) objeto(s)** Um objeto selecionado é verificado novamente em busca de vírus e programas indesejados. As configurações da varredura sob demanda são usadas para isso.
	**Retornar**	**Propriedades** Abre uma caixa de diálogo com informações mais detalhadas sobre o objeto selecionado. **Nota** Informações detalhadas podem ser obtidas também clicando duas vezes em um objeto.

  (Windows Vista)	**F3**	**Restaurar objeto(s)** Um objeto selecionado é restaurado. Em seguida, o objeto é colocado no seu local original. **Aviso** Danos graves no sistema devido a vírus e programas indesejados! Se arquivos forem restaurados: certifique-se de que somente arquivos que puderam ser limpos em outra varredura sejam restaurados. **Nota** No Windows Vista é necessário ter direitos de administrador para restaurar objetos.
	**F6**	**Restaurar objeto(s) para...** Um objeto selecionado pode ser restaurado em um local escolhido por você. Se essa opção for selecionada, a caixa de diálogo "Salvar como" será exibida; nessa caixa é possível selecionar o local do armazenamento. **Aviso** Danos graves no sistema devido a vírus e programas indesejados! Se arquivos forem restaurados: certifique-se de que somente arquivos que puderam ser limpos em outra varredura sejam restaurados.

	**Ins**	**Adicionar arquivo para quarentena** Se um arquivo for considerado suspeito, pode ser adicionado manualmente ao Gerenciador de quarentena com essa opção. Se um arquivo for considerado suspeito, pode ser adicionado ao Gerenciador de quarentena Avira com a opção Enviar objeto para investigação.
	**F4**	**Enviar objeto(s)** O objeto é carregado em um servidor da Web do Avira Malware Research Center para ser investigado pelo Avira Malware Research Center. Quando você clica no botão **Enviar objeto**, uma caixa de diálogo é aberta com um formulário para inserir seus dados de contato. Insira todos os dados necessários. Selecione um tipo: **Arquivo Suspeito** ou **Falso-Positivo** . Clique em **OK** para enviar o arquivo suspeito. **Observação** O tamanho dos arquivos carregados é limitado a 20 MB descompactados ou 8 MB compactados. **Nota** Você pode carregar somente um arquivo por vez.
	**Del**	**Excluir objeto(s)** Um objeto selecionado é excluído do Gerenciador de quarentena. O objeto não pode ser restaurado.
	**F7**	**Exportar todas as propriedades** As propriedades do objeto em quarentena realçado são exportadas em um arquivo de texto.
	**F10**	**Abrir diretório de quarentena** Abre o diretório INFECTADO.

Nota
Você tem a opção de executar ações em vários objetos realçados.
Para realçar vários objetos (objetos nas colunas), mantenha pressionada a

tecla ctrl ou a tecla shift enquanto seleciona os objetos no gerenciador de quarentena. Pressione **Ctrl + A** para selecionar todos os objetos exibidos. Quando a ação **Exibir propriedades** é executada, não é possível selecionar vários objetos. Não é possível fazer várias seleções com a ação **Enviar objeto**, pois apenas um arquivo pode ser carregado por vez.

Tabela

Status

Um objeto colocado em quarentena pode ter diferentes status:

Ícone	Descrição
	Nenhum vírus ou programa indesejado foi encontrado, o objeto está "limpo".
	Um vírus ou programa indesejado foi encontrado.
	Se um arquivo suspeito tiver sido adicionado ao Gerenciador de quarentena com a opção Adicionar arquivo, ele terá esse ícone de aviso.

Tipo

Designação	Descrição
Arquivo	O objeto detectado é um arquivo.

Detecção

Mostra o nome do malware encontrado.
Os resultados heurísticos são identificados com a abreviação HEUR/.

Origem

Mostra o caminho em que o objeto foi encontrado.

Data/Hora

Mostra a data e hora da detecção.

Informações detalhadas

Nome do arquivo

Caminho completo e nome do arquivo do objeto.

Objeto em quarentena

Nome do arquivo do objeto em quarentena.

Restaurado

SIM/ NÃO

SIM: o objeto selecionado foi restaurado.

NÃO:o objeto selecionado não foi restaurado.

Carregado para Avira

SIM/ NÃO

SIM: o objeto já foi carregado para um servidor da web do Avira Malware Research Center

para ser investigado pelo Avira Malware Research Center.

SIM: o objeto já foi carregado para um servidor da web do Avira Malware Research Center

para ser investigado pelo Avira Malware Research Center.

Sistema operacional

Windows XP: O malware foi identificado por um produto Avira de desktop.

Mecanismo de varredura

Número de versão do mecanismo de varredura

Arquivo de definição de vírus

Número de versão do arquivo de definição de vírus

Detecção

Nome do malware detectado.

Data/Hora

Data e hora da detecção

7.3.9 Agendamento

O **Agendamento** dá a opção de criar trabalhos de atualização e verificação programados e adaptar ou excluir trabalhos existentes.

Por padrão, o seguinte trabalho é criado após a instalação:

- Verificar trabalho **Verificação rápida do sistema** (ativado por padrão): Uma verificação rápida do sistema semanalmente é executada automaticamente. Durante a verificação rápida do sistema, somente pastas e arquivos importantes do computador

são verificados quanto a vírus ou programas indesejados. . O trabalho **Verificação rápida do sistema** pode ser modificado, mas é recomendável criar outros trabalhos de verificação que reflitam melhor suas necessidades.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**Ins**	**Inserir novo trabalho** Cria um novo trabalho. Um assistente o conduz pelas configurações necessárias.
	**Voltar**	**Propriedades** Abre uma caixa de diálogo com mais informações sobre o trabalho selecionado.
	**F2**	**Editar trabalho** Abre o assistente para criar e alterar um trabalho.
	**Del**	**Excluir trabalho** Exclui os trabalhos selecionados da lista.
		**Exibir arquivo de relatório** O arquivo de relatório do Agendamento é exibido.
	**F3**	**Iniciar trabalho** Inicia um trabalho marcado na lista.
	F4	**Interromper trabalho** Interrompe um trabalho iniciado e marcado.

Tabela

Tipo de trabalho

Ícone	Descrição
	O trabalho é um trabalho de atualização.
	O trabalho é um trabalho de verificação.

Nome

Nome do trabalho.

Ação

Indica se o trabalho é uma **verificação** ou uma **atualização**.

Frequência

Indica com que frequência e quando o trabalho é iniciado.

Modo de exibição

Os seguintes modos de exibição estão disponíveis:

Invisível: o trabalho é realizado em segundo plano e não é visível. Isso se aplica aos trabalhos de verificação e de atualização.

Minimizar: a janela do trabalho exibe somente uma barra de andamento.

Maximizar: a janela do trabalho fica completamente visível.

Ativado

O trabalho é ativado quando você ativa a caixa de seleção.

> **Nota**
> Se a frequência do trabalho tiver sido definida como Imediato, o trabalho será iniciado assim que for ativado. Isso possibilita reiniciar o trabalho, se necessário.

Status

Exibe o status do trabalho:

Pronto: o trabalho está pronto para execução.

Em execução: o trabalho foi iniciado e está sendo executado.

Criar trabalhos com o Agendamento

o assistente de planejamento oferece suporte no planejamento, na configuração e na criação

- uma verificação programada de vírus e programas indesejados
- uma atualização programada via Internet

Para os dois tipos de trabalho é necessário inserir

- o nome e a descrição do trabalho
- quando o trabalho deve ser iniciado
- com que frequência o trabalho deverá ser realizado
- o modo de exibição do trabalho

Frequência do trabalho

Frequência do trabalho	Descrição
Imediatamente	O trabalho é iniciado imediatamente após o término do assistente de planejamento.
Diariamente	O trabalho é iniciado todos os dias em uma determinada hora, por exemplo, 22:00.
Semanalmente	O trabalho é iniciado semanalmente em um determinado dia ou em vários dias da semana em uma determinada hora, por exemplo, terça-feira e sexta-feira às 16:26.
Intervalo	O trabalho é realizado em intervalos específicos, por exemplo, a cada 24 horas.
Única	O trabalho é realizado uma única vez em um horário definido, por exemplo, no dia 10.04.04 às 10:04.

Hora inicial do trabalho

Você pode definir um dia da semana, data, hora ou intervalo para o horário de início do trabalho. Essa opção não será exibida se você tiver inserido **Imediatamente** como o horário de início.

Dependendo do tipo de trabalho, existem diversas opções adicionais

Repetir o trabalho se o tempo já tiver expirado

São realizados trabalhos passados que não puderam ser realizados no horário determinado, por exemplo, porque o computador estava desligado.
Essa opção pode ser selecionada tanto com um trabalho de atualização quanto com um trabalho de verificação que deve ser realizado diariamente, semanalmente, em intervalos ou uma única vez.

Desligar o computador se o trabalho tiver sido concluído

O computador é encerrado quando o trabalho é concluído. Os trabalhos de verificação podem ser exibidos minimizados e maximizados.

Nota
Com um trabalho de verificação é possível selecionar perfis predefinidos.

7.3.10 Relatórios

A seção **Relatórios** permite acessar os resultados das ações executadas pelo programa.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**Voltar**	**Exibir relatório** Abre uma janela na qual é exibido o resultado da ação selecionada. Por exemplo, o resultado de uma verificação.
	**F3**	**Exibir arquivo de relatório** Exibe o arquivo do relatório selecionado.
	**F4**	**Imprimir o arquivo de relatório** Abre a caixa de diálogo de impressão do Windows para imprimir o arquivo de relatório.
	**Del**	**Excluir relatório(s)** Exclui o relatório selecionado e o arquivo de relatório relevante.

Tabela

Status

Ícone	Descrição
	**Verificar ação**: concluído com êxito sem detectar vírus.
	**Verificar ação**: vírus detectado ou falha de conclusão.
	**Atualização da ação**: concluído com êxito.
	**Atualização da ação**: não concluído com êxito.

- **Ação**

  Mostra a ação executada.
- **Resultado**

  Mostra o resultado da ação.
- **Data/Hora**

  Mostra a data e a hora em que o relatório foi criado.

Conteúdo de um relatório de uma verificação

- *Data da verificação:*

  Data da verificação.
- *Hora inicial da verificação:*

  Hora inicial da verificação em hh:mm.
- *Tempo de verificação necessário:*

  A duração da verificação em formato mm:ss.
- *Status da verificação:*

  Mostra se a verificação foi concluída.
- *Última detecção:*

  Nome do último vírus ou programa indesejado encontrado.
- *Diretórios verificados:*

  Número total de diretórios verificados.
- *Arquivos verificados:*

  Número total de arquivos verificados.
- *Arquivos verificados:*

  Número de arquivos verificados.
- *Objetos ocultos:*

Número total de objetos ocultos detectados

- *Detecções:*

  Número total de vírus e programas indesejados detectados.

- *Suspeito:*

  Número de arquivos suspeitos.

- *Avisos:*

  Número de alertas sobre vírus detectados.

- *Informações:*

  Número de itens informativos emitidos, por exemplo, mais informações que podem surgir durante uma verificação.

- *Reparados:*

  Número total de arquivos reparados

- *Quarentena:*

  Número total de arquivos colocados em quarentena.

- *Renomeados:*

  Número total de arquivos renomeados.

- *Excluídos:*

  Número total de arquivos excluídos.

- *Apagados:*

  Número total de arquivos substituídos.

Nota
Os rootkits têm a capacidade de ocultar processos e objetos como entradas do registro ou arquivos. No entanto, nem todo objeto oculto é necessariamente prova da existência de um rootkit. Objetos ocultos também podem ser objetos inofensivos. Se uma verificação detectar objetos ocultos mas não emitir um alerta de detecção de vírus, o relatório deverá ser usado para determinar qual é o objeto de referência e obter mais informações sobre o objeto detectado.

7.3.11 Eventos

Eventos que foram gerados por vários componentes do programa serão exibidos em **Eventos**.

Os eventos são armazenados em um banco de dados. Você pode limitar o tamanho do banco de dados de eventos ou desativar a restrição de tamanho do banco de dados (consulte). Somente os eventos dos últimos 30 dias são salvos na configuração padrão. A exibição do evento é atualizada automaticamente quando a seção **Eventos** é selecionada.

Nota
A exibição não é atualizada automaticamente quando a seção for selecionada se houver mais de 20.000 eventos armazenados no banco de dados de eventos. Nesse caso, pressione **F5** para atualizar o visualizador de eventos.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**Retornar**	**Mostrar evento selecionado** Abre uma janela na qual é exibido o resultado da ação selecionada. Por exemplo, o resultado de uma varredura.
	**F3**	**Exportar evento(s) selecionado(s)** Exporta eventos selecionados.
	**Del**	**Excluir evento(s) selecionado(s)** Exclui o evento selecionado.

Nota
Você tem a opção de executar ações em vários eventos selecionados. Para selecionar diversos eventos, mantenha pressionada a tecla **Ctrl** ou a tecla **Shift** (seleciona eventos consecutivos) à medida que seleciona os eventos desejados. Para selecionar todos os eventos exibidos, pressione **Ctrl + A**.
No caso da ação **Mostra evento selecionado**, não é possível executar a ação em várias seleções de objetos.

Módulos

Os eventos dos módulos a seguir (aqui em ordem alfabética) podem ser exibidos pelo visualizador de eventos:

Nome do módulo
Serviço de ajuda
Real-Time Protection

Agendamento
Scanner
Atualizador
Web Protection

Marcando a caixa **Tudo** você pode exibir os eventos de todos os módulos disponíveis. Para exibir somente os eventos de um módulo específico, marque a caixa ao lado do módulo necessário.

Filtro

A classificação de eventos a seguir pode ser exibida pelo visualizador de eventos.

Ícone	Descrição
	Informações
	Aviso
	Erro
	Detecção

Marcando a caixa **Filtrar**  , você pode exibir todos os eventos. Para exibir somente determinados eventos, marque a caixa ao lado do evento desejado.

Tabela

A lista de eventos contém as seguintes informações:

- **Ícone**

  O ícone da classificação do evento.
- **Tipo**

  Uma classificação da gravidade do evento: *Informaçãon*, *Aviso*, *Erro*, *Detecção*.
- **Módulo**

  O módulo que registrou o evento. Por exemplo, o módulo do Real-Time Protection que fez uma detecção.

- **Ação**

  Descrição do evento do respectivo módulo.

- **Data/Hora**

  A data e a hora local em que o evento ocorreu.

7.3.12 Atualizar

Atualiza a visualização da seção aberta.

7.4 Extras

7.4.1 Varredura de registros de inicialização

Você também pode verificar os setores de inicialização das unidades da estação de trabalho com uma verificação do sistema. É recomendável, por exemplo, quando uma verificação do sistema detectar um vírus e você deseja assegurar que os setores de inicialização não estão afetados.

É possível selecionar mais de um setor de inicialização mantendo a tecla Shift pressionada e selecionando as unidades necessárias com o mouse.

> **Nota**
> os setores de inicialização podem ser verificados automaticamente com uma verificação do sistema (consulte Varrer registros de inicialização selecionados).

> **Nota**
> No Windows Vista, é necessário ter direitos de administrador para verificar os setores de inicialização.

7.4.2 Lista de detecções

Esta função faz uma lista dos nomes dos vírus e programas indesejados reconhecidos pelo produto Avira. Existe uma função integrada conveniente de pesquisa de nomes.

Pesquisar na lista de detecções

insira uma palavra ou sequência de caracteres de pesquisa na caixa *Pesquisar:* .

Pesquisar sequência de caracteres dentro de um nome

Você pode inserir uma sequência consecutiva de letras ou caracteres aqui no teclado e o marcador se moverá até o primeiro ponto na lista de nomes que inclui essa

sequência – até mesmo no meio de um nome (por exemplo: "raxa" localiza "Abraxas").

Pesquisar a partir do primeiro caractere de um nome

Você pode inserir a primeira letra e os caracteres seguintes aqui no teclado e o marcador percorre a lista de nomes em ordem alfabética (por exemplo: "Ra" localiza "Rabbit").

Se o nome ou a sequência de caracteres procurado estiver disponível, a posição encontrada é marcada na lista.

Pesquisar para frente

Inicia a pesquisa para frente em ordem alfabética.

Pesquisar para trás

Inicia a pesquisa para trás em ordem alfabética.

Primeira correspondência

Percorre a lista até a primeira entrada encontrada.

Entradas da lista de detecções

Essa opção exibe uma lista de nomes de vírus ou programas indesejados que podem ser reconhecidos. A maioria das entradas dessa lista também pode ser removida com o produto Avira. Elas são listadas em ordem alfabética (primeiro caracteres especiais e números e, em seguida, as letras). Use a barra de rolagem para percorrer a lista para cima ou para baixo.

7.4.3 Configuração

O item de menu **Configuração** no menu **Extras** abre a Configuração.

7.5 Atualização

7.5.1 Iniciar atualização...

O item de menu **Iniciar atualização** no menu **Atualizar** inicia uma atualização imediata. O arquivo de definição de vírus e o mecanismo de varredura são atualizados.

7.5.2 Atualização manual...

O item de menu **Atualização manual...** no menu **Atualizar** abre uma caixa de diálogo para selecionar e carregar um pacote de atualização do VDF/mecanismo de pesquisa. O pacote de atualização pode ser baixado do site do fabricante e contém o arquivo de definição de vírus e o mecanismo de pesquisa atuais:
http://www.avira.com/pt-br

Observação
No Windows Vista, você precisa ter direitos de administrador para efetuar uma atualização manual.

7.6 Ajuda

7.6.1 Tópicos

O item de menu **Tópicos** no menu **Ajuda** abre a lista de sumário da ajuda on-line.

7.6.2 Ajude-me

Quando houver uma conexão de Internet ativa, o item **Ajude-me** no menu **Ajuda** abre a página Suporte relevante do produto no site da Avira. Ali você pode ler respostas a perguntas frequentes, consultar a base de conhecimentos e entrar em contato com o Suporte Avira.Ali você pode ler respostas a perguntas frequentes, consultar a base de conhecimentos e entrar em contato com o Suporte Avira.

7.6.3 Fórum

Quando houver uma conexão ativa com a Internet, o comando de menu **Fórum** no menu **Ajuda** abre uma página da web que oferece acesso ao Fórum Avira.

7.6.4 Fazer download do manual

Quando houver uma conexão de Internet ativa, o comando de menu **Fazer download do manual** no menu **Ajuda** abre a página de download do produto Avira. Ali você encontrará o link para download da versão atual do manual do produto Avira.

7.6.5 Gerenciamento de licenças

O item de menu **Gerenciamento de licenças** no menu **Ajuda** abre o assistente de licença. Esse assistente ajuda a licenciar ou ativar o produto Avira com facilidade.

Ativar Produto

Ative esta opção se você já tiver um código de ativação e ainda não ativou o produto Avira. Durante a ativação do produto, você é registrado como cliente e o produto Avira é ativado com a sua licença. Você recebeu o código de ativação por e-mail ou ele estava impresso na embalagem do produto.

Nota
A ativação do programa pode ser executada repetidamente com um código de ativação válido, caso isso seja solicitado por uma nova instalação do sistema.

Nota
Para ativação o programa use o protocolo HTTP e a porta 80 (comunicação com a web), além do protocolo de criptografia SSL e a porta 443 para se comunicar com os servidores da Avira. Se estiver usando um firewall, certifique-se de que as conexões necessárias e/ou os dados de entrada ou de saída não estão bloqueados pelo firewall.

Nota
Você tem a opção de ativar uma atualização de produto para um produto da família de produtos de desktop Avira (consulte Informações do produto > Licenciamento e atualização). Insira o código de atualização do produto que deseja atualizar na caixa de entrada **Código de ativação**. Se houver uma atualização disponível, o produto é instalado automaticamente.

Comprar/estender licença

Essa opção é exibida se a sua licença ainda estiver válida, estiver vencida ou você tiver apenas uma licença de avaliação. Use essa opção para estender a licença do produto ou comprar uma licença de versão completa. Isso requer uma conexão ativa com a Internet. Selecione a opção **Comprar/estender licença** e clique em **Avançar**. O navegador da web abrirá e o conduzirá à loja on-line onde você poderá comprar uma licença.

Arquivo de licença válido

Você pode carregar um arquivo de licença válido seguindo o link do **arquivo de licença**.

Durante a ativação do produto com um código de ativação válida, a chave de licença é gerada, salva no diretório do programa do produto Avira e carregada. Use esta opção se você já ativou um produto.

Configurações de proxy...

Uma caixa de diálogo será exibida quando você clicar nesse botão. Se e quando necessário, é possível definir aqui que você deseja estabelecer conexão com a Internet para ativar o produto por meio de um servidor proxy.

7.6.6 Produto recomendado

Se houver uma conexão ativa com a Internet, o item **Produto recomendado** no menu **Ajuda** abre um site para clientes Avira. Use essa página para recomendar o produto Avira e aproveitar os descontos da Avira.

7.6.7 Enviar feedback

Quando houver uma conexão ativa com a Internet, o comando de menu **Enviar feedback** no menu **Ajuda** abre uma página de feedback para produtos Avira. Ali você encontrará um formulário de avaliação do produto que pode enviar para a Avira com suas avaliações da qualidade do produto e outras sugestões.

7.6.8 Mostrar notificador novamente

O comando de menu **Mostrar notificador novamente** no menu **Ajuda** permite acessar o notificador do por novo produto Avira. O notificador mantém você informado sobre as ofertas de proteção contra malware mais recentes.

7.6.9 Sobre Avira Free Antivirus

- **Geral**

  Endereços e informações do produto Avira.
- **Informações da versão**

  Informações da versão dos arquivos no pacote do produto Avira.
- **Informações da licença**

  Dados da licença da licença atual e links para a loja on-line (comprar ou estender uma licença).

> **Nota**
> Os dados da licença podem ser salvos no cache. Clique com o botão direito na área *Dados da licença*. Um menu contextual é aberto. No menu contextual, clique no comando de menu **Copiar para área de transferência**. Seus dados de licença são salvos na área de transferência e podem ser adicionados a emails, formulários ou documentos através do comando **Adicionar** do Windows.

8. Proteção Móvel

Avira não só protege o seu computador de malware e vírus, mas também protege de perda e roubo o seu smartphone que opera com o sistema operacional Android. Com o Avira Free Android Security você também pode bloquear chamadas ou SMS indesejados. Basta adicionar números de telefone do Registro de chamadas, Registro de SMS e da lista de contatos à lista negra, ou criar manualmente um contato que pretende bloquear.

Mais informações podem ser encontradas no nosso site:

http://www.avira.com/android

9. Configuração

9.1 Configuração

- Visão geral das opções de configuração
- Botões

Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:

- **Scanner**: configuração de uma varredura do sistema (sob demanda)
  - Opções de varredura
  - Resolução de na detecções
  - Opções de varredura do arquivo
  - Exceções de varredura do sistema
  - Heurística de varredura do sistema
  - Configuração da função de registro
- **Real-Time Protection**: configuração de uma varredura em tempo real (durante o acesso)
  - Opções de varredura
  - Resolução de na detecções
  - Mais ações
  - Exceções de varredura durante o acesso
  - Heurística de varredura durante o acesso
  - Configuração da função de registro
- **Atualização**: Configuração das configurações de atualização, configuração de atualizações de produtos
  - Fazer download através do servidor Web
  - Configurações de proxy
- **Web Protection**: Configuração da Web Protection
  - Opções de varredura, ativação e desativação da Web Protection
  - Resolução de na detecções
  - Acesso bloqueado: Tipos de arquivo e tipos MIME indesejados
  - Exceções de varredura da Web Protection: URLs, tipos de arquivo, tipos MIME
  - Heurística de Web Protection
  - Configuração da função de registro
- **Geral**:
  - Categorias de ameaça para o Scanner e o Real-Time Protection

- Filtro de aplicativos: bloquear ou permitir aplicativos
- Proteção com senha para acesso ao Centro de controle e à Configuração
- Segurança: bloquear função autostart, exibição completa do status de varredura do sistema, proteção do produto, proteger arquivo hosts do Windows
- WMI: Ativar o suporte a WMI
- Configuração do registro de eventos
- Configuração das funções de registro
- Configuração dos diretórios usados

Botões

Botão	Descrição
Valores padrão	Todas as opções da configuração são restauradas aos valores padrão. Todas as correções e entradas personalizadas são perdidas quando as configurações padrão são restauradas.
OK	Todas as configurações feitas são salvas. A configuração é fechada. O Controle de Conta de Usuário vai pedir a você permissão para aplicar as alterações em sistemas operacionais a partir do Windows Vista.
Cancelar	A configuração é fechada sem salvar as definições.
Aplicar	Todas as configurações feitas são salvas. O Controle de Conta de Usuário vai pedir a você permissão para aplicar as alterações em sistemas operacionais a partir do Windows Vista.

9.2 Scanner

A seção **System Scanner** é responsável pela configuração da verificação sob demanda.

9.2.1 Varredura

É possível definir o comportamento da rotina de varredura por demanda. Se você selecionar alguns diretórios a serem verificados sob demanda, dependendo da configuração, o Scanner verificará:

- com uma determinada prioridade de varredura,
- também os setores de inicialização e a memória principal,
- alguns ou todos os arquivos do diretório.

Arquivos

O Scanner pode usar um filtro para varredura de somente os arquivos com uma determinada extensão (tipo).

Todos os arquivos

Se essa opção for ativada, todos os arquivos serão verificados em busca de vírus ou programas indesejados, independentemente do conteúdo e da extensão. O filtro não é usado.

> **Nota**
> Se **Todos os arquivos** for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

Usar extensões inteligentes

Se essa opção for ativada, a seleção dos arquivos verificados em busca de vírus ou programas indesejados será escolhida automaticamente pelo programa. Isso significa que o programa Avira decide se os arquivos são verificados ou não com base em seu conteúdo. Esse procedimento é um pouco mais lento do que Usar lista de extensão de arquivo, porém é mais seguro visto que não é apenas a extensão que é verificada. Essa opção é ativada como configuração padrão e é recomendada.

> **Nota**
> Se **Usar extensões inteligentes** for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

Usar lista de extensão de arquivo

Se essa opção for ativada, somente os arquivos com a extensão especificada serão verificados. Todos os tipos de arquivo que podem conter vírus e programas indesejados são predefinidos. A lista pode ser editada manualmente através do botão "**Extensões de arquivo**".

> **Nota**
> Se essa opção for ativada e todas as entradas tiverem sido excluídas da lista com as extensões, aparecerá a mensagem "*Sem extensões*" no botão **Extensões de arquivo**.

Extensões de arquivo

Quando esse botão é pressionado, uma caixa de diálogo é aberta na qual são exibidas todas as extensões que são verificadas no modo "**Usar lista de extensões de arquivos"**. Entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

Nota
Observe que a lista padrão pode variar de acordo com a versão.

Configurações adicionais

Varrer registros de inicialização selecionados

Se essa opção for ativada, o Scanner verificará somente os setores de inicialização das unidades selecionadas para a varredura do sistema. Essa opção é ativada como a configuração padrão.

Varrer registros mestres de inicialização

Se essa opção for ativada, o Scanner verificará os setores de inicialização principais dos discos rígidos usados no sistema.

Ignorar arquivos off-line

Se essa opção for ativada, a varredura direta ignorará os arquivos off-line por completo durante uma varredura. Isso significa que esses arquivos não são verificados em busca de vírus e programas indesejados. Os arquivos off-line são arquivos que foram movidos fisicamente pelo chamado HSMS (Hierarchical Storage Management System, Sistema de gerenciamento de armazenamento hierárquico), por exemplo, do disco rígido para uma fita. Essa opção é ativada como a configuração padrão.

Varredura da integridade dos arquivos de sistema

Quando essa opção está ativada, os arquivos mais importantes do sistema Windows são submetidos a uma varredura particularmente segura das alterações realizadas por malwares durante cada varredura sob demanda. Se um arquivo corrigido for detectado, será registrado como suspeito. Essa função consome muita memória do computador. É por esse motivo que a opção é desativada como configuração padrão.

Nota
Essa opção está disponível somente no Windows Vista e superior.

Nota
Essa opção não deverá ser usada se você estiver usando ferramentas de terceiros que modificam arquivos do sistema e adaptam a tela de inicialização aos seus próprios requisitos. O Skinpacks, o TuneUp Utilities e o Vista Customization são exemplos dessas ferramentas.

Varredura otimizada

Quando essa opção está ativada, a capacidade do processador é utilizada de modo ideal durante uma varredura do Scanner. Por razões de desempenho, a varredura utilizada é realizada somente no nível padrão.

Nota
Essa opção está disponível somente em sistemas com vários processadores.

Seguir links simbólicos

Se essa opção for ativada, o Scanner realizará uma varredura que segue todos os links simbólicos no perfil de varredura ou diretório selecionado e verifica os arquivos vinculados em busca de vírus e malwares.

Nota
A opção não inclui nenhum atalho, mas faz referência exclusivamente a links simbólicos (gerados por mklink.exe) ou pontos de junção (gerados por junction.exe) que são transparentes no sistema de arquivos.

Procurar rootkits antes da varredura

Se essa opção for ativado e uma varredura for iniciada, o Scanner verificará o diretório do sistema Windows em busca de rootkits ativos em um atalho conhecido. Esse processo não verifica seu computador em busca de rootkits ativos de modo tão abrangente quanto o perfil de varredura "**Varredura de rootkits**", mas sua execução é significativamente mais rápida. Essa opção altera somente as configurações de perfis criados por você.

Nota
A varredura de rootkit não está disponível para o Windows XP de 64 bits

Fazer a varredura do registro

Se essa opção for ativada, o registro será verificado quanto a referências de malware. Essa opção altera somente as configurações de perfis criados por você.

Ignorar arquivos e caminhos nas unidades de rede

Se essa opção for ativada, as unidades de rede conectadas ao computador serão excluídas da varredura sob demanda. Essa opção é recomendada quando os servidores ou outras estações de trabalho são protegidos com software antivírus. Essa opção é desativada como a configuração padrão.

Processo da varredura

Permitir interrupção da varredura

Se essa opção for ativada, a varredura em busca de vírus ou programas indesejados poderá ser encerrada a qualquer momento com o botão "**Parar"** na janela Luke Filewalker. Se essa configuração for desativada, o botão **Parar** na janela Luke Filewalker terá um fundo cinza. Desse modo, o encerramento prematuro de um processo de varredura não é permitido! Essa opção é ativada como a configuração padrão.

Prioridade scanner

Com a varredura sob demanda, o Scanner diferencia os níveis de prioridade. Isso será útil somente se vários processos estiverem em execução simultaneamente na estação de trabalho. A seleção afeta a velocidade da varredura.

Baixo

O Scanner terá apenas o tempo de processador alocado pelo sistema operacional se nenhum outro processo exigir o tempo de computação, isto é, contanto que apenas o Scanner esteja em execução, a velocidade será máxima. Em suma, trabalhar com outros programas é ideal: o computador responderá mais rapidamente se outros programas exigirem o tempo de computação enquanto o Scanner continua em execução em segundo plano.

Normal

O Scanner é executado com prioridade normal. O sistema operacional aloca a mesma quantidade de tempo de processador para todos os processos. Essa opção é ativada como configuração padrão e é recomendada. Em algumas circunstâncias, o trabalho com outros aplicativos pode ser afetado.

Alto

O Scanner tem a prioridade mais alta. O trabalho simultâneo com outros aplicativos é quase impossível. No entanto, o Scanner conclui sua varredura em velocidade máxima.

Resolução de na detecções

Você pode definir as ações a serem realizadas pelo System Scanner quando um vírus ou programa indesejado for detectado.

Interativo

Se essa opção for ativada, os resultados da verificação do System Scanner serão exibidos em uma caixa de diálogo. Ao realizar uma verificação com o System Scanner, um alerta será emitido com uma lista dos arquivos afetados no final da verificação. Você pode usar o menu sensível ao contexto para selecionar uma ação a ser executada para os diversos arquivos afetados. Você pode executar as ações padrão para todos os arquivos infectados ou cancelar o Scanner.

Nota
A ação **Quarentena** é pré-selecionada por padrão na notificação do System Scanner. Outras ações podem ser selecionadas em um menu contextual.

, onde o arquivo poderá ser restaurado se tiver valor informativo. Você também pode enviar a cópia de backup para o Centro de pesquisa de malware da Avira para novas investigações.

Ação primária

Ação primária é a ação realizada quando o System Scanner encontra um vírus ou programa indesejado. Se a opção "" for selecionada mas o arquivo afetado não puder ser reparado, a ação selecionada em "" será realizada.

Nota
A opção só poderá ser selecionada se a configuração tiver sido selecionada em .

Reparar

Se essa opção for ativada, o System Scanner reparará os arquivos afetados automaticamente. Se o System Scanner não conseguir reparar um arquivo afetado, realizará a ação selecionada em .

Nota
Um reparo automático é recomendado, mas o System Scanner modificará os arquivos na estação de trabalho.

Renomear

Se essa opção for ativada, o System Scanner renomeará o arquivo. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

Quarentena

Se essa opção for ativada, o System Scanner moverá o arquivo para a quarentena. Esses arquivos podem ser reparados posteriormente ou, se necessário, enviados para o Centro de pesquisa de malware da Avira.

Excluir

Se essa opção for ativada, o arquivo é excluído.

Ignorar

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

Aviso
O arquivo afetado permanece ativo em sua estação de trabalho! Isso pode causar danos graves à estação de trabalho!

Ação secundária

A opção " so poderá ser selecionada se a configuração tiver sido selecionada em ". Com essa opção, agora é possível decidir o que deve ser feito com o arquivo afetado caso não seja possível repará-lo.

Renomear

Se essa opção for ativada, o System Scanner renomeará o arquivo. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

Quarentena

Se essa opção for ativada, o System Scanner moverá o arquivo para a . Esses arquivos podem ser reparados posteriormente ou, se necessário, enviados para o Centro de pesquisa de malware da Avira.

Excluir

Se essa opção for ativada, o arquivo é excluído.

Ignorar

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

Aviso
O arquivo afetado permanece ativo em sua estação de trabalho! Isso pode causar danos graves à estação de trabalho!

Nota
Se você tiver selecionado **Excluir**

Arquivos

Ao verificar os arquivos, o System Scanner utiliza uma verificação recursiva: Arquivamentos em arquivamentos também são descompactados e verificados quanto a vírus e programas indesejados. Os arquivos são verificados, descompactados e verificados novamente.

Varrer arquivos compactados

Se essa opção for ativada, os arquivos compactados selecionados na lista serão verificados. Essa opção é ativada como a configuração padrão.

Todos os tipos de arquivo

Se essa opção for ativada, todos os tipos de arquivo da lista de arquivos compactados serão selecionados e verificados.

Extensões inteligentes

Se essa opção for ativada, o System Scanner detectará se um arquivo está em um formato compactado (arquivo compactado), mesmo que a extensão seja diferente das extensões normais, e fará a verificação do arquivo compactado. No entanto, para isso, é necessário abrir cada arquivo, o que diminui a velocidade da verificação. Exemplo: e um arquivo *.zip tiver a extensão *.xyz, o System Scanner também descompactará e verificará esse arquivo. Essa opção é ativada como a configuração padrão.

Nota
Somente os tipos de arquivo marcados na lista são suportados.

Limitar profundidade da recursão

A descompactação e a verificação de arquivos compactados recursivos podem consumir muito tempo e muitos recursos do computador. Se essa opção for ativada, a profundidade da verificação de arquivos com vários níveis de compactação será limitada a um determinado número de níveis de compactação (profundidade máxima de recursão). Isso economiza tempo e recursos do computador.

Nota
Para encontrar um vírus ou programa indesejado em um arquivo, o System Scanner deve fazer a verificação até o nível de recursão em que o vírus ou programa indesejado está localizado.

Profundidade máxima da recursão

Para inserir a recursividade máxima, a opção Profundidade máxima de recursão deve ser ativada.
Você pode inserir a profundidade de recursão solicitada diretamente ou usando a tecla de seta para a direita no campo de entrada. Os valores permitidos estão entre 1 e 99. O valor padrão é 20, que é recomendado.

Valores padrão

O botão restaura os valores predefinidos para verificar os arquivos compactados.

Arquivos

Nessa área de exibição, é possível definir os arquivos compactados que devem ser verificados pelo System Scanner. Para isso, você deve selecionar as entradas relevantes.

Exceções

Objetos do arquivo devem ser ignorados do Scanner

A lista dessa janela contém arquivos e caminhos que não devem ser incluídos pelo Scanner na varredura em busca de vírus ou programas indesejados.

Insira o mínimo de exceções possível aqui e somente os arquivos que, por algum motivo, não devem ser incluídos em uma varredura normal. Recomendamos que você sempre verifique esses arquivos quanto à presença de vírus ou programas indesejados antes que eles sejam incluídos nessa lista!

Nota
As entradas da lista devem ter no máximo 6000 caracteres no total.

Aviso
Esses arquivos não são incluídos no processo de varredura!

Nota
Os arquivos incluídos nessa lista são registrados no arquivo de relatório. Verifique o arquivo de relatório periodicamente para observar se há algum arquivo não verificado, pois a causa que fez você excluir um arquivo aqui talvez não exista mais. Nesse caso, remova o nome desse arquivo dessa lista novamente.

Caixa de entrada

Nessa caixa de entrada, é possível inserir o nome do objeto de arquivo que não é incluído na varredura sob demanda. Nenhum objeto de arquivo é inserido como configuração padrão.

O botão abre uma janela na qual é possível selecionar o arquivo ou caminho desejado.
Quando um nome de arquivo com seu caminho completo é inserido, somente o arquivo em questão não é verificado quanto à presença de infecção. Caso tenha inserido um nome de arquivo sem um caminho, todos os arquivos com esse nome (independentemente do caminho ou da unidade) não serão verificados.

Adicionar

Com esse botão você pode adicionar o objeto de arquivo inserido na caixa de entrada à janela de exibição.

Excluir

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de varredura.

Os produtos Avira contêm uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

Heurística para vírus de macro

Heurística para vírus de macro

O seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja, você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

Seu programa Avira contém uma heurística muito poderosa na forma da tecnologia Avira AHeAD, que também pode detectar (novos) malwares desconhecidos. Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser agressiva. Essa opção é ativada como a configuração padrão.

Nível de detecção baixo

Se essa opção for ativada, serão detectados ligeiramente menos malwares conhecidos; o risco de alertas falsos é baixo nesse caso.

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

9.2.2 Relatório

O System Scanner tem uma função de relatório abrangente. Com ela, você obtém informações precisas sobre os resultados de uma verificação sob demanda. O arquivo de relatório contém todas as entradas do sistema, bem como alertas e mensagens da verificação sob demanda.

Nota
Para ser capaz de definir as ações que o System Scanner realizou, quando vírus ou programas indesejados foram detectados, você deve ativar o arquivo de relatório na configuração .

Relatório

Desativado

Se essa opção for ativada, o System Scanner não registrará as ações e os resultados da verificação sob demanda.

Padrão

Padrão:quando essa opção é ativada, o System Scanner registra os nomes dos arquivos relacionados e seu caminho. Além disso, a configuração da verificação atual, as informações de versão e as informações sobre o usuário licenciado são gravadas no arquivo de relatório.

Estendido

Quando essa opção é ativada, o System Scanner registra alertas e dicas além das informações padrão.

Concluído

Quando essa opção está ativada, o System Scanner também registra todos os arquivos verificados. Além disso, todos os arquivos envolvidos, bem como os alertas e as dicas, são incluídos no arquivo de relatório.

Nota
Se precisar enviar um arquivo de relatório a qualquer momento (para solucionar problemas), crie esse arquivo nesse modo.

9.3 Real-Time Protection

A seção **Real-Time Protection** da configuração é responsável pela configuração da varredura durante o acesso.

9.3.1 Varredura

Em geral, você quer monitorar seu sistema constantemente. Para este fim, use o Real-Time Protection (= Scanner de acesso). Com ele, você pode executar a varredura de todos os arquivos que são copiados ou abertos no computador imediatamente em busca de vírus e programas indesejados.

Arquivos

O Real-Time Protection pode usar um filtro para verificar somente os arquivos com uma determinada extensão (tipo).

Todos os arquivos

Se essa opção for ativada, todos os arquivos serão verificados em busca de vírus ou programas indesejados, independentemente do conteúdo e da extensão.

> **Nota**
> Se **Todos os arquivos** for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

Usar extensões inteligentes

Se essa opção for ativada, a seleção dos arquivos verificados em busca de vírus ou programas indesejados será escolhida automaticamente pelo programa. Desse modo, o decidirá se os arquivos devem ou não ser verificados com base em seu conteúdo. Esse procedimento é um pouco mais lento do que **Usar lista de extensão de arquivo**, porém é mais seguro visto que não é apenas a extensão que é verificada.

> **Nota**
> Se **Usarextensões inteligentes** for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

Usar lista de extensão de arquivo

Se essa opção for ativada, somente os arquivos com a extensão especificada serão verificados. Todos os tipos de arquivo que podem conter vírus e programas indesejados são predefinidos. A lista pode ser editada manualmente através do botão "**Extensões de arquivo"**. Essa opção é ativada como configuração padrão e é recomendada.

Nota
Se essa opção for ativada e todas as entradas tiverem sido excluídas da lista com as extensões, aparecerá a mensagem "Sem extensões" no botão **Extensões de arquivo**.

Extensões de arquivo

Quando esse botão é pressionado, uma caixa de diálogo é aberta na qual são exibidas todas as extensões que são verificadas no modo "**Usar lista de extensões de arquivos"**. Entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

Nota
A lista de extensões pode variar de acordo com a versão.

Unidades

Monitorar unidades de rede

Se essa opção for ativada, os arquivos das unidades de rede (unidades mapeadas), como volumes de servidor e unidades pontuais, serão verificados.

Nota
Para não prejudicar muito o desempenho do computador, a opção **Monitorar unidades de rede** deve ser ativada somente em casos excepcionais.

Aviso
Se essa opção for desativada, as unidades de rede **não** serão monitoradas. Elas não estarão mais protegidas contra vírus ou programas indesejados!

Nota
Quando os arquivos são executados em unidades de rede, eles são verificados pelo Real-Time Protection, independentemente da configuração da opção **Monitorar unidades de rede**. Em alguns casos, os arquivos das unidades de rede são verificados quando são abertos, mesmo que a opção **Monitoriar unidades de rede** esteja desativada. Motivo: esses arquivos são acessados com os direitos “Executar arquivo”. Se desejar excluir esses arquivos ou, ou até mesmo os arquivos executados nas unidades de rede, da varredura feita pelo Real-Tim Protection, insira os arquivos na lista de objetos de arquivo a serem excluídos (consulte: Real-Time Protection > Varredura > Exceções).

Ativar armazenamento em cache

Se essa opção for ativada, os arquivos monitorados nas unidades de rede serão disponibilizados no cache do Real-Time Protection. O monitoramento das unidades de rede sem a função de armazenamento em cache é mais segura, mas não executa tão bem o monitoramento das unidades de rede com armazenamento em cache.

Arquivos

Varrer arquivos compactados

Se essa opção for ativada, os arquivos compactados serão verificados. Os arquivos compactados são verificados, descompactados e verificados novamente. Essa opção é desativada por padrão. A varredura do arquivo compactado é restrita pela profundidade de recursão, pelo número de arquivos a serem verificados e pelo tamanho do arquivo compactado. É possível definir a profundidade de recursão máxima, o número de arquivos a serem verificados e o tamanho máximo do arquivo compactado.

Nota
Essa opção é desativada por padrão, pois o processo consome muita memória do computador. Geralmente, é recomendado verificar os arquivos compactados com uma varredura sob demanda.

Profundidade máxima de recursão

Ao verificar os arquivos, o Real-Time Protection utiliza uma varredura recursiva: Arquivos em arquivos também são descompactados e verificados quanto a vírus e programas indesejados. É possível definir a profundidade de recursão. O valor padrão e recomendado para a profundidade recursiva é 1: todos os arquivos que estão diretamente localizados no arquivo principal são verificados.

Número máximo de arquivos

Ao verificar os arquivos compactados, é possível limitar a varredura a um número máximo de arquivo. O valor padrão e recomendado para o número máximo de arquivos a serem verificados é 10.

Tamanho máximo (KB)

Ao verificar os arquivos compactados, é possível limitar a varredura a um tamanho máximo de arquivo a ser descompactado. O valor padrão de 1000 KB é recomendado.

Resolução de na detecções

Usar registro de eventos

Se essa opção é ativada, uma entrada é adicionada ao registro de eventos do Windows para cada detecção. Os eventos podem ser chamados no visualizador de eventos do Windows. Essa opção é ativada como a configuração padrão.

Exceções

Com essas opções é possível configurar objetos de exceção para o Real-Time Protection (varredura durante o acesso). Os objetos relevantes não são incluídos na varredura durante o acesso. O Real-Time Protection pode ignorar os acessos do arquivo a esses objetos na varredura durante o acesso através da lista de processos a serem omitidos. Isso é útil, por exemplo, com soluções de backup ou bancos de dados.

Observe o seguinte ao especificar processos e objetos de arquivo a serem omitidos: A lista é processada de cima para baixo. Quanto maior a lista, mais tempo será necessário para processar a lista para cada acesso. Desse modo, mantenha a lista o menor possível.

Processos a serem omitidos pelo Real-Time Protection

Todos os acessos de processos dessa lista são excluídos do monitoramento pelo Real-Time Protection.

Caixa de entrada

Neste campo, insira o nome do processo que deve ser ignorado pela varredura em tempo real. Nenhum processo é inserido como configuração padrão.

O caminho e o nome de arquivo do processo especificados deverão ter no máximo 255 caracteres. Você pode inserir até 128 processos. As entradas da lista devem ter no máximo 6000 caracteres no total.

Ao inserir o processo, símbolos Unicode são aceitos. Portanto, você pode inserir o processo ou nomes de diretórios que contenham símbolos especiais.

As informações da unidade devem ser inseridas da seguinte maneira: `[Letra da unidade]:\`

O símbolo de dois pontos (:) só é usado para especificar unidades.

Ao especificar o processo, você pode usar os curingas * (qualquer número de caracteres) e ? (um único caractere).

```
C:\Arquivos de programas\Application\application.exe
C:\Arquivos de programas\Application\applicatio?.exe
C:\Arquivos de programas\Application\applic*.exe
C:\Arquivos de programas\Application\*.exe
```

Para evitar o processo de exclusão globalmente do monitoramento pelo Real-Time Protection, as especificações que compreendem exclusivamente os seguintes caracteres são inválidas: * (asterisco), ? (ponto de interrogação), / (barra), \ (barra invertida), . (ponto), : (dois pontos).

Você tem a opção de excluir processos do monitoramento pelo Real-Time Protection sem detalhes completos do caminho. Por exemplo: `application.exe`

Porém, isso só se aplica a processos em que os arquivos executáveis estão localizados em unidades de disco rígido.

Detalhes completos do caminho em que os arquivos executáveis estão localizados em unidades conectadas, por exemplo, unidades de rede. Observe as informações gerais sobre a notação de Exceções em unidades de rede conectadas.

Não especifique quaisquer exceções para processos em que os arquivos executáveis estão localizados em unidades dinâmicas. Unidades dinâmicas são utilizadas para discos removíveis, como CDs, DVDs ou pen drives.

Aviso
Todos os acessos de arquivo feitos pelos processos registrados na lista são excluídos da varredura quanto a vírus e programas indesejados!

O botão abre uma janela na qual é possível selecionar um arquivo executável.

Processos

O botão "**Processos**" abre a janela "**Seleção de processos**" na qual são exibidos os processos em execução.

Adicionar

Com esse botão, você pode adicionar o processo inserido na caixa de entrada à janela de exibição.

Excluir

Com esse botão, é possível excluir um processo selecionado na janela de exibição.

Objetos de arquivo a serem omitidos pelo Real-Time Protection

Todos os acessos a objetos dessa lista são excluídos do monitoramento pelo Real-Time Protection.

Caixa de entrada

Nessa caixa, é possível inserir o nome do objeto de arquivo que não é incluído na varredura durante o acesso. Nenhum objeto de arquivo é inserido como configuração padrão.

As entradas da lista devem ter no máximo 6000 caracteres no total.

Ao especificar os objetos de arquivo a serem omitidos, você pode usar os curingas* (qualquer número de caracteres) e ? (um único caractere): Extensões de arquivo individuais também podem ser excluídas (inclusive curingas):

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

Nomes de diretório devem terminar com uma barra invertida \ .

Se um diretório for excluído, todos os subdiretórios também são excluídos automaticamente.

Para cada unidade, é possível especificar no máximo 20 exceções inserindo o caminho completo (começando com a letra da unidade). Por exemplo:

```
Por exemplo, C:\Arquivos de programas\Application\Nome.log
```

Podem existir no máximo 64 exceções sem um caminho completo. Por exemplo:

```
*.log
\computer1\C\directory1
```

No caso das unidades dinâmicas que são montadas como um diretório em outra unidade, o alias do sistema operacional da unidade integrada na lista de exceções deve ser usado, por exemplo:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

No entanto, se você usar o ponto de montagem propriamente dito, por exemplo, `C:\DynDrive`, a unidade dinâmica será verificada. Você pode determinar o alias do sistema operacional a ser usado no arquivo de relatório do Real-Time Protection.

O botão abre uma janela na qual é possível selecionar o objeto de arquivo a ser excluído.

Adicionar

Com esse botão você pode adicionar o objeto de arquivo inserido na caixa de entrada à janela de exibição.

Excluir

Com esse botão, é possível excluir um objeto de arquivo selecionado da janela de exibição.

Observe as informações ao especificar exceções:

Para excluir também os objetos quando forem acessados com nomes curtos de arquivo DOS (convenção de nome DOS 8.3), o nome curto relevante do arquivo deve ser inserido na lista.

Um nome de arquivo que contém caracteres curinga não pode terminar com uma barra invertida. Por exemplo:
`C:\Arquivos de programas\Application\applic*.exe\`
Essa entrada não é válida e não é tratada como uma exceção!

Observe o seguinte com relação às **exceções em unidades de rede conectadas**: se você usar a letra da unidade de rede conectada, os arquivos e as pastas especificados NÃO são excluídos da varredura do Real-Time Protection. Se o caminho UNC na lista de

exceções for diferente do caminho UNC usado para conectar com a unidade de rede (especificação do endereço IP na lista de exceções – especificação do nome do computador para conexão com a unidade de rede), os arquivos e pastas especificados NÃO serão excluídos pela varredura do Real-Time Protection. Localize o caminho UNC relevante no arquivo de relatório do Real-Time Protection:
`\\<Nome do computador>\<Ativar>\` - OU - `\\<endereço IP>\<Ativar>\`

Você pode localizar o caminho que o Real-Time Protection utiliza para verificar os arquivos infectados no arquivo de relatório do Real-Time Protection. Indique exatamente o mesmo caminho na lista de exceções. Proceda da seguinte maneira: configure a função de protocolo do Real-Time Protection para **Completar** na configuração em Real-Time Protection > Relatório. Agora acesse os arquivos, as pastas, as unidades montadas ou as unidades de rede conectadas com o Real-Time Protection ativado. Agora você pode ler o caminho a ser usado no arquivo de relatório do Real-Time Protection. O arquivo de relatório pode ser acessado no Centro de controle em Proteção local > Real-Time Protection.

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de varredura.

Os produtos Avira contêm uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

Heurística para vírus de macro

Heurística para vírus de macro

O seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja, você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

Seu programa Avira contém uma heurística muito poderosa na forma da tecnologia Avira AHeAD, que também pode detectar (novos) malwares desconhecidos. Se essa

opção for ativada, você poderá definir até que ponto essa heurística deve ser agressiva. Essa opção é ativada como a configuração padrão.

Nível de detecção baixo

Se essa opção for ativada, serão detectados ligeiramente menos malwares conhecidos; o risco de alertas falsos é baixo nesse caso.

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

9.3.2 Relatório

O Real-Time Protection inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção.

Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

Desativado

Se essa opção for ativada, o Real-Time Protection não criará um registro.
É recomendado desativar a função de registro somente em casos excepcionais, por exemplo, se você executar avaliações com vários vírus ou programas indesejados.

Padrão

Se essa opção for ativada, o Real-Time Protection registrará informações importantes (sobre detecções, alertas e erros) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como a configuração padrão.

Estendido

Se essa opção for ativada, o Real-Time Protection registrará informações menos importantes no arquivo de relatório também.

Concluído

Se essa opção for ativada, o Real-Time Protection registrará todas as informações disponíveis no arquivo de relatório, incluindo o tamanho e o tipo de arquivo, a data, etc.

Limitar arquivo de relatório

Limitar tamanho para n MB

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho. Os valores permitidos devem estar entre 1 e 100 MB. São permitidos aproximadamente 50 KB de espaço extra ao limitar o tamanho do arquivo de relatório para minimizar o uso dos recursos do sistema. Se o tamanho do arquivo de registro ultrapassar o tamanho indicado em mais de 50 KB, as entradas antigas serão excluídas até que o tamanho indicado menos 50 KB seja atingido.

Fazer backup do relatório

Se essa opção for ativada, o backup do arquivo de relatório será feito antes de sua redução.

Gravar configuração no relatório

Se essa opção for ativada, a configuração da varredura durante o acesso será registrada no arquivo de relatório.

Nota
Se você não especificou nenhuma restrição no arquivo de relatório, será criado automaticamente um novo arquivo de relatório quando o mesmo atingir 100MB. É criado um backup do antigo arquivo de relatório. São salvos até três backups dos antigos arquivos de relatório. Os backups mais antigos são excluídos primeiro.

9.4 Atualização

Na seção **Atualizar** é possível configurar o recebimento automático de atualizações. Você pode especificar vários intervalos de atualização.

Atualização automática

Todos os n dia(s) / hora(s) / minuto(s)

Nesta caixa é possível especificar o intervalo em que a atualização automática é realizada. Para alterar o intervalo de atualização, realce uma das opções de tempo na caixa e altere-a usando a tecla de seta à direita da caixa de entrada.

Repetir o trabalho se o tempo já tiver expirado

ISe essa opção for ativada, serão realizados os trabalhos de atualização antigos que não foram realizados na hora especificada, por exemplo, porque o computador estava desligado.

9.4.1 Servidor da web

Servidor da web

A atualização pode ser realizada diretamente através de um servidor da web na Internet.

Conexão do servidor da web

Usar conexão já existente (rede)

Essa configuração é exibida quando a conexão é usada por meio de uma rede.

Usar a conexão a seguir

Essa configuração é exibida se você definir sua conexão individualmente.

O Atualizador detecta automaticamente as opções de conexão que estão disponíveis. As opções de conexão que não estão disponíveis aparecem desativadas e não podem ser ativadas. Uma conexão discada pode ser estabelecida manualmente, por exemplo, através de uma entrada do catálogo de telefones do Windows.Uma conexão discada pode ser estabelecida manualmente, por exemplo, através de uma entrada do catálogo de telefones do Windows.

Usuário

Insira o nome de usuário da conta selecionada.

Senha

Insira a senha dessa conta. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*).

Nota
Caso tenha esquecido o nome de usuário ou a senha de uma conta da Internet existente, entre em contato com seu provedor de serviços de Internet.

Nota
A discagem automática do atualizador através das chamadas ferramentas de discagem (por exemplo, SmartSurfer, Oleco etc.) não está disponível no momento.

Encerrar uma conexão discada que foi configurada para a atualização

Se essa opção for ativada, a conexão discada feita para a atualização é interrompida automaticamente mais uma vez assim que o download tiver sido concluído com êxito.

Nota
Essa opção está disponível somente no Windows XP. Nos sistemas operacionais mais novos a conexão discada aberta para a atualização é sempre finalizada assim que o download for realizado.

Configurações de proxy

Servidor proxy

Não use um servidor proxy

Se essa opção for ativada, sua conexão com o servidor da web não é estabelecida por meio de um servidor proxy.

Usar configurações do sistema proxy

Quando a opção está ativada, as configurações atuais do sistema Windows são usadas para a conexão com o servidor da web através de um servidor proxy. Configure as definições do sistema Windows para usar um servidor proxy em **Painel de controle > Opções da internet > Conexões > Configurações da LAN**. Também é possível acessar as opções da Internet no menu **Extras** no Internet Explorer.

Aviso
Se estiver sendo usado um servidor proxy que precisa de autêntica, insira todos os dados solicitados na opção **Usar este servidor proxy**. A opção **Usar configurações do sistema proxy** pode ser usada somente para servidores proxy sem autenticação.

Usar este servidor proxy

Se a conexão com o servidor da web for configurada através de um servidor proxy, você pode inserir as informações relevantes aqui.

Endereço

Insira o URL ou o endereço IP do servidor proxy que deseja usar para conectar com o servidor da web.

Porta

Insira o número da porta do servidor proxy que deseja usar para conectar com o servidor da web.

Nome de logon

Insira um nome de usuário para conectar no servidor proxy.

Senha de logon

Insira a senha relevante para fazer login no servidor proxy aqui. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*).

Exemplos:

Endereço: `proxy.domain.com` Porta: `8080`

Endereço: `192.168.1.100` Porta: `3128`

9.5 FireWall

9.5.1 Configurar o FireWall

Avira Free Antivirus permite gerenciar o Firewall do Windows:

- Firewall do Windows

9.5.2 Firewall do Windows

A seção **FireWall** em **Configuração > Proteção na Internet** é responsável pela configuração do Firewall do Windows, a partir do Windows 7.

Perfis de rede

Perfis de rede

O Firewall do Windows bloqueia o acesso não autorizado a programas e aplicativos do seu computador com base em três perfis de localização de rede:

- Rede privada: para redes domésticas ou de escritório
- Rede pública: para redes de locais públicos
- Rede de domínio: para redes com um controlador de domínio

Você pode gerenciar esses perfis a partir da configuração do seu produto Avira em **Proteção na Internet > Firewall do Windows > Perfis de rede**.

Para obter mais informações sobre esses perfis de rede, visite o site oficial da Microsoft.

Atenção
O Firewall do Windows aplica as mesmas regras a todas as rede que pertencem ao mesmo local de rede, ou seja, se você permitir que um programa ou aplicativo seja executado, também será concedido acesso a esse programa ou aplicativo também em todas as redes que têm o mesmo perfil.

Rede privada

Configurações de rede privada

As configurações de rede privada gerenciam o acesso que outros computadores ou dispositivos na sua rede doméstica ou do escritório têm ao seu computador. Como padrão, essas configurações permitem que os usuários da rede privada vejam o seu computador e tenham acesso a ele.

Ativar

Se essa opção estiver ativada, o Firewall do Windows está ativado e em funcionamento através do produto Avira.

Bloquear todas as conexões de entrada

Se esta opção estiver ativada, o Firewall do Windows rejeitará todas as tentativas não solicitadas de conexão ao seu computador, inclusive conexões de entrada de aplicativos permitidos.

Notifique-me quando um novo aplicativo for bloqueado

Se esta opção estiver ativada, você receberá uma notificação sempre que o Firewall do Windows bloquear um novo programa ou aplicativo.

Desativar (não recomendada)

Se esta opção estiver ativada, o Firewall do Windows estará desativado. Essa opção não é recomendada, porque expõe o seu computador a riscos.

Rede pública

Configurações de rede pública

As configurações de rede pública gerenciam o acesso que outros computadores ou dispositivos em redes de locais públicos têm ao seu computador. Como padrão, essas configurações não permitem que os usuários da rede pública vejam o seu computador ou tenham acesso a ele.

Ativar

Se essa opção estiver ativada, o Firewall do Windows está ativado e funcionamento através do produto Avira.

Bloquear todas as conexões de entrada

Se esta opção estiver ativada, o Firewall do Windows rejeitará todas as tentativas não solicitadas de conexão ao seu computador, inclusive conexões de entrada de aplicativos permitidos.

Notifique-me quando um novo aplicativo for bloqueado

Se esta opção estiver ativada, você receberá uma notificação todas as vezes que o Firewall do Windows bloquear um novo programa ou aplicativo.

Desativar (não recomendada)

Se esta opção estiver ativada, o Firewall do Windows estará desativado. Essa opção não é recomendada porque expõe o seu computador a riscos.

Rede de domínio

Configurações de rede de domínio

As configurações de rede de domínio gerenciam o acesso que outros computadores ou dispositivos têm ao seu computador em uma rede que é autenticada através de um controlador de domínio. Como padrão, essas configurações permitem que usuários autenticados do domínio vejam e acessem o seu computador.

Ativar

Se essa opção estiver ativada, o Firewall do Windows está ativado e em funcionamento através do produto Avira.

Bloquear todas as conexões de entrada

Se esta opção estiver ativada, o Firewall do Windows rejeitará todas as tentativas não solicitadas de conexão ao seu computador, inclusive conexões de entrada de aplicativos permitidos.

Notifique-me quando um novo aplicativo for bloqueado

Se esta opção estiver ativada, você receberá uma notificação todas as vezes que o Firewall do Windows bloquear um novo programa ou aplicativo.

Desativar (não recomendada)

Se esta opção estiver ativada, o Firewall do Windows estará desativado. Essa opção não é recomendada porque expõe o seu computador a riscos.

Nota
Esta opção apenas está disponível se o seu computador estiver conectado a uma rede com um controlador de domínio.

Regras de aplicativo

Se você clicar no link sob **Firewall do Windows > Regras de aplicativo**, você será redirecionado ao menu **Aplicativos e recursos permitidos** da configuração do Firewall do Windows.

Configurações avançadas

Se você clicar no link sob **Firewall do Windows > Configurações avançadas**, você será redirecionado ao menu **Firewall do Windows com Segurança Avançada** da configuração do Firewall do Windows.

9.6 Web Protection

A seção **Proteção para a Web** em **Configuração > Proteção para a internet** é responsável pela configuração da Proteção para a Web.

9.6.1 Varredura

A Proteção para a Web protege você contra vírus ou malwares que atingem seu computador a partir de páginas da Web carregadas em seu navegador a partir da Internet. A opção **Verificar** pode ser usada para definir o comportamento do componente da Proteção para a Web.

Varredura

Ativar suporte para IPv6

Se essa opção for ativada, a versão 6 do Internet Protocol será suportada pela Web Protection. Esta opção não está disponível para novas instalações ou instalações alteradas em Windows 8.

Proteção da unidade

A proteção da unidade permite que você defina configurações para bloquear I-Frames, também conhecidos como quadros internos. I-Frames são elementos HTML, isto é, elementos de páginas da Internet que delimitam uma área de uma página da Web. Os I-Frames podem ser usados para carregar e exibir conteúdos da Web diferentes - normalmente outros URLs - como documentos independentes em uma subjanela do navegador. Na maioria das vezes, os I-Frames são usados para anúncios em banner. Em alguns casos, os I-Frames são usados para ocultar malwares. Nesses casos, a área do I-Frame fica total ou parcialmente invisível no navegador. A opção **Bloquear I-frames suspeitos** permite verificar e bloquear o carregamento de I-Frames.

Bloquear I-frames suspeitos

Se essa opção for ativada, os I-Frames das páginas da Web solicitadas serão verificados de acordo com determinados critérios. Se houver I-Frames suspeitos em uma página da Web solicitada, o I-Frame será bloqueado. Uma mensagem de erro será exibida na janela do I-Frame.

Resolução de na detecções

Você pode definir as ações a serem realizadas pela Proteção para a Web quando um vírus ou programa indesejado for detectado.

Interativo

Se essa opção for ativada, uma caixa de diálogo aparecerá quando um vírus ou programa indesejado for detectado durante uma verificação sob demanda, na qual

você poderá especificar o que deve ser feito com o arquivo afetado. Essa opção é ativada como a configuração padrão.

Mostrar barra de andamento

Se essa opção for ativada, uma notificação será exibida na área de trabalho com uma barra de andamento de download se o download de um conteúdo do site ultrapassar o tempo limite de 20 segundos.Esta notificação foi criada especialmente para fazer download de sites com volumes maiores de dados: se estiver navegando com a Proteção para a Web, o conteúdo do site não será baixado de modo incremental no navegador, pois ele será verificado quanto à presença de vírus e malware antes de ser exibido no navegador. Essa opção é desativada como a configuração padrão.

Clique aqui para obter mais informações.

Automático

Se esta opção for ativada, não aparecerá nenhuma caixa de diálogo em caso de vírus. A Proteção para a Web reage de acordo com as configurações pré-definidas nesta seção como ação primária e secundária.

Ação primária

Ação primária é a ação realizada quando a Proteção para a Web encontra um vírus ou programa indesejado.

Negar acesso

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos não são enviados para seu navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador. A Proteção para a Web registrará a detecção no arquivo de relatório se a função de registro estiver ativada.

Mover para quarentena

Caso um vírus ou malware seja detectado, o site solicitado do servidor Web e/ou os dados e arquivos transferidos serão movidos para a quarentena. O arquivo afetado pode ser recuperado do Gerenciador de quarentena se tiver um valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

Ignorar

O site solicitado do servidor Web e/ou os dados e arquivos que foram transferidos são encaminhados pela Proteção para a Web para seu navegador. O acesso ao arquivo é permitido e o arquivo é ignorado.

Aviso
O arquivo afetado permanece ativo em sua estação de trabalho! Isso pode causar danos graves à estação de trabalho!

Solicitações bloqueadas

Em **Solicitações bloqueadas** é possível especificar os tipos de arquivo e os tipos MIME (tipos de conteúdo para os dados transferidos) a serem bloqueados pela Proteção para a Web. A Proteção para a Web impede a transferência de dados da Internet para seu computador. pecialista.

A Proteção para a Web bloqueia os seguintes tipos de arquivos / Os tipos MIME

Todos os tipos de arquivo e tipos MIME (tipos de conteúdo para os dados transferidos) na lista são bloqueados pela Proteção para a Web.

Caixa de entrada

Nessa caixa, insira os nomes dos tipos MIME e dos tipos de arquivo que devem ser bloqueados pela Proteção para a Web. Para tipos de arquivo, insira a extensão, por exemplo, **.htm**. Para tipos MIME, indique o tipo de mídia e, quando aplicável, o subtipo. As duas instruções são separadas uma da outra por uma única barra, por exemplo, **video/mpeg** ou **audio/x-wav**.

Nota
No entanto, os arquivos que já estão armazenados em seu computador como arquivos de Internet temporários e bloqueados pela Web Protection podem ser baixados localmente da Internet pelo navegador do computador. Arquivos de Internet temporários são arquivos salvos em seu computador pelo navegador para que os sites possam ser acessados mais rapidamente.

Nota
A lista de tipos de arquivo e MIME bloqueados será ignorada se os tipos forem inseridos na lista de tipos de arquivo e MIME excluídos em Proteção para a Web > Verificar > Exceções.

Nota
Nenhum caractere curinga (* para qualquer número de caracteres ou ?para um único caractere) pode ser usado ao inserir os tipos de arquivo e os tipos MIME.

Tipos MIME: exemplos para tipos de mídia:

- `text` = para arquivos de texto
- `image` = para arquivos gráficos
- `video` = para arquivos de vídeo
- `audio` = para arquivos de som
- `application` = para arquivos vinculados a um programa específico

Exemplos de tipos de arquivo e MIME excluídos

- `application/octet-stream` = os arquivos de tipo MIME application/octet-stream (arquivos executáveis *.bin, *.exe, *.com, *dll, *.class) são bloqueados pela Proteção para a Web.
- `application/olescript` = os arquivos de tipo MIME application/olescript (arquivos de script ActiveX *.axs) são bloqueados pela Proteção para a Web.
- `.exe` = todos os arquivos com a extensão .exe (arquivos executáveis) são bloqueados pela Proteção para a Web.
- `.msi` = todos os arquivos com a extensão .msi (arquivos do Windows Installer) são bloqueados pela Proteção para a Web.

Adicionar

O botão permite copiar os tipos MIME e de arquivo do campo de entrada na janela de exibição.

Excluir

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

Exceções

Essas opções permitem definir exceções com base nos tipos MIME (tipos de conteúdo para os dados transferidos) e nos tipos de arquivo para URLs (endereços da Internet) para a verificação realizada pela Proteção para a Web. Os tipos MIME e os URLs especificados são ignorados pela Proteção para a Web, isto é, os dados não são verificados em busca de vírus e malwares quando são transferidos para seu computador.

Tipos MIME ignorados pela Proteção para a Web

Nesse campo, é possível selecionar os tipos MIME (tipos de conteúdo para os dados transferidos) a serem ignorados pela Proteção para a Web durante a verificação.

Tipos de arquivo/tipos MIME ignorados pelo Web Protection (definido pelo usuário)

Todos os tipos MIME (tipos de conteúdo para os dados transferidos) na lista são ignorados pela Proteção para a Web durante a verificação.

Caixa de entrada

Nessa caixa, é possível inserir o nome dos tipos MIME e dos tipos de arquivo a serem ignorados pela Proteção para a Web durante a verificação. Para tipos de arquivo, insira a extensão, por exemplo, **.htm**. Para tipos MIME, indique o tipo de mídia e, quando aplicável, o subtipo. As duas instruções são separadas uma da outra por uma única barra, por exemplo, **video/mpeg** ou **audio/x-wav**.

Nota
Nenhum caractere curinga (* para qualquer número de caracteres ou ?para um único caractere) pode ser usado ao inserir os tipos de arquivo e os tipos MIME.

Aviso
É feito o download de todos os tipos de arquivo e tipos de conteúdo na lista de exclusão no navegador da Internet sem nenhuma verificação das solicitações bloqueadas (Lista de tipos de arquivos e MIME a serem bloqueados na Proteção para a Web > Verificar > Solicitações bloqueadas) ou pela Proteção para a Web: Para todas as entradas na lista de exclusão, as entradas na lista de arquivo e tipos MIME a serem bloqueados são ignorados. Nenhuma verificação quanto a vírus e malwares é realizada.

Tipos MIME: exemplos para tipos de mídia:

- `text` = para arquivos de texto
- `image` = para arquivos gráficos
- `video` = para arquivos de vídeo
- `audio` = para arquivos de som
- `application` = para arquivos vinculados a um programa específico

Exemplos de tipos de arquivo e MIME excluídos:

- `audio/` = Todos os arquivos de tipo de mídia de áudio são excluídos das verificações da Proteção para a Web
- `video/quicktime` = Todos os arquivos de vídeo do subtipo Quicktime (*.qt, *.mov) são excluídos das verificações da Proteção para a Web
- `.pdf` = Todos os arquivos Adobe PDF são excluídos das verificações da Proteção para a Web.

Adicionar

O botão permite copiar os tipos MIME e de arquivo do campo de entrada na janela de exibição.

Excluir

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

URLs ignoradas pela Proteção da Web

Todos os URLs dessa lista são excluídos das verificações da Proteção para a Web.

Caixa de entrada

Nessa caixa, é possível inserir os URLs (endereços da Internet) a serem excluídos das verificações da Proteção para a Web, por exemplo, `www.domainname.com`. Você pode especificar as partes do URL, usando pontos principais ou seguir para indicar o nível de domínio: `.domainname.com` para todas as páginas e todos os subdomínios do domínio. Indique os sites com domínio de nível superior (`.com` ou `.net`) com um ponto a seguir: `domainname.`Se você indicar uma string sem um ponto no início ou no final, a string será interpretada como um domínio de nível superior, como `net`, para todos os domínios NET (`www.domain.net`).

Nota
Você também pode usar o caractere curinga * para qualquer número de caracteres ao especificar os URLs. Você também pode usar pontos principais ou a seguir em combinação com curingas para indicar o nível de domínio:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (válido mas não recomendado)
Especificações sem pontos, como *`name`*, são interpretadas como parte de um domínio de nível superior e não são recomendadas.

Aviso
É feito o download de todos os sites na lista de URLs excluídos no navegador da Internet sem nenhuma verificação pela Proteção para a Web: Nenhuma verificação quanto a vírus e malwares é realizada. Desse modo, somente URLs confiáveis devem ser excluídos das verificações da Proteção para a Web.

Adicionar

O botão permite copiar o URL inserido no campo de entrada (endereço da Internet) na janela do visualizador.

Excluir

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

Exemplos: URLs ignorados

- `www.avira.com` -OU- `www.avira.com/*`
  = Todos os URLs com o domínio `www.avira.com` são excluídos das verificações da Proteção para a Web: *www.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*, etc. Os URLs com o domínio `www.avira.de` não são excluídos das verificações da Proteção para a Web.
- `avira.com` -OU- `*.avira.com`
  = Todos os URLs com o domínio de segundo nível e de nível superior `avira.com`

são excluídos das verificações da Proteção para a Web: A especificação implica todos os subdomínios existentes para `.avira.com`: *www.avira.com*, *forum.avira.com*, etc.

- `avira.` -OU- `*.avira.*`
  = Todos os URLs com o domínio de segundo nível `avira` são excluídos das verificações da Proteção para a Web: A especificação implica todos os domínios de nível superior ou subdomínios para `.avira`: *www.avira.com*, *www.avira.de*, *forum.avira.com*, etc.
- `.*domain*.*`
  Todos os URLs contendo um domínio de segundo nível com a string `domain` são excluídos das verificações da Proteção para a Web: *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -OU- `*.net`
  = Todos os URLs com o domínio de nível superior `net` são excluídos das verificações da Proteção para a Web: *www.name1.net*, *www.name2.net*, etc.

Aviso
Insira o URLs que deseja excluir da verificação da Proteção para a Web o mais precisamente possível. Evite especificar um domínio de nível superior inteiro ou partes de um domínio de segundo nível, pois as páginas da Internet que distribuem malwares e programas indesejados serão excluídas da verificação da Proteção para a Web através das especificações globais em exclusões. É recomendado especificar pelo menos o domínio de segundo nível completo e o domínio de nível superior: `domainname.com`

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de varredura.

Os produtos Avira contêm uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

Heurística para vírus de macro

O seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja,

você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

Seu programa Avira contém uma heurística muito poderosa na forma da tecnologia Avira AHeAD, que também pode detectar (novos) malwares desconhecidos. Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser agressiva. Essa opção é ativada como a configuração padrão.

Nível de detecção baixo

Se essa opção for ativada, serão detectados ligeiramente menos malwares conhecidos; o risco de alertas falsos é baixo nesse caso.

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

9.6.2 Relatório

A Web Protection inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção.

Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

Desativado

Se essa opção for ativada, a Web Protection não criará um registro.
É recomendado desativar a função de registro somente em casos excepcionais, por exemplo, se você executar avaliações com vários vírus ou programas indesejados.

Padrão

Se essa opção for ativada, a Web Protection registrará informações importantes (sobre detecções, alertas e erros) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

Avançado

Se essa opção for ativada, a Web Protection registrará informações menos importantes no arquivo de relatório também.

Concluído

Se essa opção for ativada, a Web Protection registrará todas as informações disponíveis no arquivo de relatório, incluindo o tamanho e o tipo de arquivo, a data, etc.

Limitar arquivo de relatório

Limitar tamanho para n MB

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho; possíveis valores: Os valores permitidos estão entre 1 e 100 MB. São permitidos aproximadamente 50 KB de espaço extra ao limitar o tamanho do arquivo de relatório para minimizar o uso dos recursos do sistema. Se o tamanho do arquivo de registro ultrapassar o tamanho indicado em mais de 50 KB, as entradas antigas serão excluídas até que o tamanho indicado tenha sido reduzido em 20%.

Gravar configuração no arquivo de relatório

Se essa opção for ativada, a configuração da verificação durante o acesso será registrada no arquivo de relatório.

Nota
Se você não especificou nenhuma restrição no arquivo de relatório, entradas antigas serão automaticamente excluídas quando o arquivo de relatório atingir 100MB. As entradas serão excluídas até que o tamanho do arquivo de relatório atinja 80 MB.

9.7 Geral

9.7.1 Categorias de ameaça

Seleção das categorias de ameaça estendidas

O produto Avira protege você contra vírus de computador. Além disso, você pode fazer a verificação de acordo com as categorias de ameaça estendidas a seguir.

- Adware
- Adware/Spyware
- Aplicativos
- Clientes Backdoor
- Discador
- Arquivos com Extensão Dupla
- Software fraudulento
- Jogos

- Piadas
- Phishing
- Programas que violam o domínio privado
- Compactadores de tempo de execução incomuns

Ao clicar na caixa relevante o tipo selecionado é ativado (marca de seleção definida) ou desativado (sem marca de seleção).

Selecionar tudo

Se essa opção for ativada, todos os tipos são ativados.

Valores padrão

Esse botão restaura os valores padrão predefinidos.

> **Nota**
> Se um tipo for desativado, os arquivos reconhecidos como sendo do tipo de programa relevante não são mais indicados. Nenhuma entrada é feita no arquivo de relatório.

9.7.2 Senha

Você pode proteger o produto Avira em diferentes áreas com uma senha. Se uma senha foi criada, ela será solicitada toda vez que desejar abrir a área protegida.

Senha

Digitar senha

Insira a senha solicitada aqui. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*). A senha pode ter no máximo 20 caracteres. Depois que a senha for criada, o programa nega acesso se uma senha incorreta for inserida. Uma caixa vazia significa "Sem senha".

Confirmação

Confirme a senha inserida acima inserindo-a aqui novamente. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*).

> **Nota**
> A senha diferencia maiúsculas e minúsculas!

Áreas protegidas por senha

O produto Avira pode proteger áreas individuais com uma senha. Ao clicar na caixa relevante, a solicitação de senha pode ser desativada ou reativada para áreas individuais conforme necessário.

Área protegida por senha	Função
Centro de controle	Se essa opção for ativada, a senha predefinida é necessária para iniciar o Centro de Controle.
Ativar / desativar o Real-Time Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar ou desativar o Avira Real-Time Protection.
Ativar / desativar o Web Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o Web Protection.
Quarentena	Se essa opção for ativada, todas as áreas possíveis do gerenciador de quarentena protegidas por senha serão ativadas. Ao clicar na caixa relevante, a solicitação da senha poderá ser desativada ou reativada para áreas individuais.
Restaurar objetos afetados	Se essa opção for ativada, a senha predefinida será necessária para restaurar um objeto.
Nova varredura dos objetos afetados	Se essa opção for ativada, a senha predefinida será necessária para verificar novamente um objeto.
Propriedades do objeto afetado	Se essa opção for ativada, a senha predefinida é necessária para exibir as propriedades de um objeto.
Excluir objetos afetados	Se essa opção for ativada, a senha predefinida é necessária para excluir um objeto.

Enviar e-mail para a Avira	Se essa opção for ativada, uma senha predefinida é necessária para enviar um objeto para o Centro de pesquisa de malware da Avira para análise.
Configuração	Se essa opção for ativada, a configuração do programa somente poderá ser feita depois que a senha predefinida for inserida.
Instalação / desinstalação	Se essa opção for ativada, a senha predefinida é necessária para a instalação ou desinstalação do programa.

9.7.3 Segurança

Execução automática

Bloquear função de execução automática

Se essa opção estiver ativada, a execução da função Execução automática do Windows é bloqueada em todas as unidades conectadas, incluindo pendrives, unidades de CD e DVD e unidades de rede. Com a função de execução automática do Windows, os arquivos em mídias de dados ou unidades de rede são lidos imediatamente no carregamento ou na conexão e, assim, podem ser iniciados e copiados automaticamente. No entanto, essa funcionalidade tem um alto risco de segurança, pois malwares e programas indesejados podem ser instalados durante o início automático. A função Execução automática é particularmente crítica para pendrives, pois os dados de um pendrive podem ser alterados a qualquer momento.

Excluir CDs e DVDs

Quando esta opção estiver ativada, a função Execução automática é permitida em unidades de CD e DVD.

Aviso
Desative a função Início automático para unidades de CD e DVD somente se tiver certeza de que está usando mídias de dados confiáveis.

Proteção do sistema

Proteger arquivos host do Windows contra alterações

Se essa opção for configurada para ativada, os arquivos hosts do Windows são protegidos contra gravação. A manipulação não é mais possível. Por exemplo, o malware não pode redirecioná-lo para sites indesejados. Essa opção é ativada como a configuração padrão.

Proteção do produto

Nota
As opções de proteção do produto não estão disponíveis se o Real-Time Protection não foi instalado usando a opção de instalação definida pelo usuário.

Proteger os processos de encerramento indesejado

Se essa opção for ativada, todos os processos do programa serão protegidos contra encerramento indesejado acionado por vírus e malwares ou contra encerramento “não controlado” acionado pelo usuário, por exemplo, através do Gerenciador de tarefas. Essa opção é ativada como a configuração padrão.

Proteção de processo avançada

Se essa opção for ativada, todos os processos do programa serão protegidos com opções avançadas contra encerramento indesejado. A proteção de processo consome uma quantidade significativamente maior de recursos do computador do que a proteção simples do processo. A opção é ativada como configuração padrão. Para desativar essa opção é necessário reiniciar o computador.

Nota
A proteção por senha não está disponível para Windows XP 64 bits !

Aviso
Se a proteção do processo for ativada, poderão ocorrer problemas de interação com outros produtos de software. Nesses casos, desative a proteção do processo.

Proteger os arquivos e as entradas do registro contra manipulação

Se essa opção for ativada, todas as entradas do registro do programa e todos os arquivos do programa (arquivos binários e de configuração) serão protegidos contra manipulação. A proteção contra manipulação impede o acesso de gravação, exclusão e, em alguns casos, de leitura às entradas do registro ou aos arquivos de programa por usuários ou programas externos. Para ativar essa opção, é necessário reiniciar o computador.

Aviso
Observe que se essa opção for desativa, o reparo de computadores infectado com tipos específicos de malware poderá falhar.

Nota
Quando essa opção estiver ativada, as alterações podem ser feitas somente na configuração, incluindo alterações nas solicitações de varredura ou atualização, por meio da interface do usuário.

Nota
A proteção de arquivos e entradas de registro não está disponível para Windows XP 64 bits !

9.7.4 WMI

Suporte para Instrumentação de gerenciamento do Windows

A Instrumentação de gerenciamento do Windows é uma técnica de administração básica do Windows que usa linguagens de script e programação para permitir o acesso de leitura e gravação, local e remoto, às configurações dos sistemas Windows. Seu produto Avira oferece suporte a WMI e fornece dados (informações de status, dados estatísticos, relatórios, solicitações planejadas etc.) bem como eventos e por meio de uma interface. A WMI oferece a opção de baixar dados operacionais do programa

Ativar suporte para WMI

Quando essa opção está ativada, é possível baixar dados operacionais do programa via WMI.

9.7.5 Eventos

Limitar tamanho do banco de dados de eventos

Limitar o tamanho ao máximo de n entradas

Se essa opção for ativada, o número máximo de eventos indicados no banco de dados de eventos pode ser limitado a um tamanho determinado; valores possíveis: 100 a 10000 e entradas. Se o número de entradas inseridas foi excedido, as entradas mais antigas são excluídas.

Excluir todos os eventos mais antigos que n dia(s)

Se essa opção for ativada, os eventos listados no banco de dados de eventos serão excluídos depois de um determinado período; valores possíveis: 1 a 90 de dias. Essa opção é ativada como a configuração padrão, com um valor de 30 dias.

Sem limite

Quando essa opção é ativada, o tamanho do banco de dados de eventos não é limitado. No entanto, são exibidas no máximo 20.000 entradas na interface do programa em Eventos.

9.7.6 Relatórios

Limitar relatórios

Limitar número para no máx. n partes

Quando essa opção é ativada, o número máximo de relatórios pode ser limitado a um valor específico. São permitidos valores entre 1 e 300. Se o número especificado for ultrapassado, o relatório mais antigo no momento é excluído.

Excluir todos os relatórios mais antigos que n dia(s)

Se essa opção for ativada, os relatórios são excluídos automaticamente depois de um número de dias específico. Os valores permitidos são: 1 a 90 dias. Essa opção é ativada como a configuração padrão, com um valor de 30 dias.

Sem limite

Se essa opção for ativada, o número de relatórios não é restringido.

9.7.7 Diretórios

Caminho temporário

Usar configurações padrão do sistema

Se essa opção for ativada, as configurações do sistema são usadas para manipular arquivos temporários.

Nota
Você pode ver onde o sistema salva os arquivos temporários - por exemplo, com o Windows XP - em: **Iniciar > Configurações > Painel de Controle > Sistema > Cartão de índice** "**Avançado**" Botão "**Variáveis ambientais**". As variáveis temporárias (`TEMP`, `TMP`) do usuário registrado atualmente e das variáveis de sistema (`TEMP`, `TMP`) são mostradas aqui com seus valores relevantes.

Use o seguinte diretório

Se essa opção for ativada, o caminho exibido na caixa de entrada é usado.

Caixa de entrada

Nesta caixa de entrada, insira o caminho em que o programa armazenará seus arquivos temporários.

O botão abre uma janela na qual é possível selecionar o caminho temporário desejado.

Padrão

O botão restaura o diretório predefinido para o caminho temporário.

9.7.8 Alertas acústicos

Quando um vírus ou malware é detectado pelo Scanner ou Real-Time Protection, um alerta acústico é emitido no modo de ação interativa. Agora você pode desativar ou ativar o alerta acústico e selecionar um arquivo WAVE alternativo como o alerta.

Nota
O modo de ação do System Scanner é definido na configuração em System Scanner > Verificar > Ação na detecção.

Nenhum aviso

Quando essa opção for ativada, nenhum alerta acústico será emitido quando um vírus for detectado pelo Scanner ou Real-Time Protection.

Usar os alto falantes do PC (apenas no modo interativo)

Se essa opção for ativada, há um alerta acústico com o sinal padrão quando um vírus for detectado pelo Scanner ou Real-Time Protection. O alerta acústico é emitido no alto-falante interno do computador.

Usar o arquivo WAVE a seguir (apenas no modo interativo)

Se essa opção for ativada, há um alerta acústico com o WAVE arquivo selecionado quando um vírus for detectado pelo Scanner ou Real-Time Protection. O arquivo WAVE selecionado é reproduzido em um alto falante externo conectado.

Arquivo WAVE

Nessa caixa de entrada é possível inserir o nome e o caminho associado ao arquivo de áudio escolhido. O sinal acústico padrão do programa é inserido como padrão.

O botão abre uma janela na qual é possível selecionar o arquivo desejado com a ajuda do explorador de arquivos.

Testar

Esse botão é usado para testar o arquivo WAVE selecionado.

9.7.9 Alertas

O produto Avira gera as chamadas telas deslizantes, notificações de área de trabalho para eventos específicos, que fornecem informações sobre sequências de programa bem sucedidas ou não, como as atualizações. Em **Alertas** é possível ativar ou desativar as notificações de eventos específicos.

Com as notificações de área de trabalho, você pode desativar a notificação diretamente na tela deslizante. É possível reativar a notificação na janela de configuração **Alertas**.

Atualização

Alertar, se a última atualização ocorreu há mais de n dia(s)

Nessa caixa você pode inserir o número máximo de dias que podem transcorrer desde a última atualização. Se esse número de dias tiver passado, um ícone vermelho é exibido para o status de atualização em **Status** no Centro de Controle.

Mostrar aviso se o arquivo de definição de vírus estiver desatualizado

Se essa opção for ativada, uma mensagem de alerta é exibida se o arquivo de definição de vírus não estiver desatualizado. Com a ajuda da opção de alerta, você pode configurar o intervalo de tempo para um alerta se a última atualização tiver mais que n dia(s).

Avisos / Notas com as situações a seguir

É usada conexão discada

Se essa opção for ativada, será emitido um alerta de notificação de área de trabalho se um discador criar uma conexão discada no computador através da rede telefônica ou ISDN. There is a danger that the connection may have been created by an unknown and unwanted dialer and that the connection may be chargeable (consulte Vírus e mais > Categorias de Ameaça: Discador).

Arquivos foram atualizados com sucesso

Se essa opção for ativada, você receberá uma notificação de área de trabalho toda vez que uma atualização for realizada com sucesso e os arquivos forem atualizados.

Atualização falhou

Se essa opção for ativada, você receberá uma notificação de área de trabalho toda vez que uma atualização falhar: não pôde ser criada conexão com o servidor de download ou os arquivos de atualização não puderam ser instalados.

Nenhuma atualização é necessária

Se essa opção for ativada, você receberá uma notificação de área de trabalho toda vez que uma atualização for iniciada, mas a instalação dos arquivos não for necessária porque o programa está atualizado.

10. Ícone de Bandeja

O ícone de bandeja na bandeja do sistema da barra de tarefas exibe o status do serviço do Real-Time Protection .

Ícone	Descrição
	O Avira Real-Time Protection é ativado
	O Avira Real-Time Protection é desativado

Entradas no menu contextual

- **Ativar Real-Time Protection**: Ativa ou desativa o Avira Real-Time Protection.
- **Ativar Web Protection**: Ativa ou desativa o Avira Web Protection.
  - **Ativar Firewall do Windows**: Ativa ou desativa o Firewall do Windows (esta funcionalidade está disponível a partir do Windows 8).
- **Iniciar Avira Free Antivirus**: Abre o Centro de Controle.
- **Configurar Avira Free Antivirus**: Abre a Configuração.
- **Minhas mensagens**: Abre um slide com as informações atuais sobre seu produto Avira.
- **Iniciar atualização** Inicia uma atualização.
- **Ajuda**: abre a ajuda online.
- **Sobre o Avira Free Antivirus**: Abre uma caixa de diálogo com informações sobre seu produto Avira: Informações do produto, Informações da versão, Informações de licença.
- **Avira na Internet**: Abre o portal da Web da Avira na Internet. Para isso, é necessário ter uma conexão ativa com a Internet.

11. Mensagens no Produto

11.1.1 Product Message Subscription Center

Você acessará o *Product Message Subscription Center* clicando em **Minhas configurações de comunicação** no menu contextual do Ícone de bandeja do Avira ou clicando no símbolo para **Configuração** na notificação suspensa **Minhas mensagens**.

- Você pode influenciar o fluxo de informações clicando no botão **ON/OFF** adequado.
- Clique em **Atualizar Perfil** para configurar seu perfil do sistema de mensagens pessoal.
  - ↪ Você recebe a mensagem de que seu perfil foi atualizado com êxito.

  Fique online clicando em um dos links.

11.1.2 Informações Atuais

A notificação suspensa *Minhas mensagens* é usada como um canal de comunicação. Ela fornece a você as últimas novidades de segurança na Internet, notícias sobre os produtos Avira (atualizações, versões mais avançadas e notificações de licenças) e informações de vírus.

Se não houver novas mensagens, você receberá a informação *Nenhuma nova mensagem disponível*. Clique em **OK** para fechar a notificação suspensa.

Se novas mensagens estiverem disponíveis, você terá as seguintes opções:

- Clique em **Lembrar-me mais tarde**, se desejar ler a mensagem posteriormente.
- Clique em **+ Ler mais**, para ler todos os detalhes da mensagem.
  - ↪ Dependendo do tipo de mensagem, você será direcionado à nossa home page ou uma nova janela se expandirá para fornecer as informações a você.
- Clique no símbolo **x** do título para fechar mensagens únicas.
- Clique no símbolo para **Configuração** no cabeçalho da notificação suspensa para criar seu perfil do sistema de mensagens pessoal.

12. FireWall

Avira Free Antivirus permite gerenciar o tráfego de dados de entrada e de saída dependendo das configurações do computador:

- Firewall do Windows

A partir do Windows 7, o Firewall do Windows é agora gerenciado com o produto Avira.

12.1 Firewall do Windows

A partir do Windows 7, Avira Free Antivirus dá a opção de gerenciar diretamente o Firewall do Windows por meio do Centro de Controle e Configuração Avira. As seguintes opções estão disponíveis para o Firewall do Windows:

ativar o Firewall do Windows por meio do Centro de Controle

A opção *FireWall* em **Status > Proteção na Internet** permite ativar ou desativar o Firewall do Windows clicando no botão **ON/OFF**.

verificar o estado do Firewall do Windows por meio do Centro de Controle

É possível verificar o estado do Firewall do Windows na seção **PROTEÇÃO NA INTERNET > FireWall** e restaurar as configurações recomendadas clicando no botão **Corrigir problema**.

13. Atualizações

13.1 Atualizações

A eficiência do software antivírus depende do quão atualizado está o programa, especialmente o ficheiro de definição de vírus e o motor de pesquisa. Para executar atualizações regulares, o componente Atualizador é integrado no seu produto Avira. O Atualizador assegura que o seu produto Avira está sempre atualizado e é capaz de lidar com novos vírus que surgem diariamente. O Atualizador atualiza os seguintes componentes:

- Ficheiro de definição de vírus:

  O ficheiro de definição de vírus contém os padrões de vírus dos programas prejudiciais utilizados pelo seu produto Avira para verificar a presença de vírus e malwares e reparar objetos infectados.

- Motor de pesquisa:

  O motor de pesquisa contém os métodos utilizados pelo seu produto Avira para verificar a existência de vírus e malwares.

- Ficheiros do programa (atualização do produto):

  Os pacotes de atualização do produto disponibilizam funções adicionais para os componentes individuais do programa.

Uma atualização verifica se o ficheiro de definição de vírus, o motor de pesquisa e o produto estão atualizados e, se necessário, implementa uma atualização. Depois da atualização do produto, talvez seja necessário reiniciar o sistema do computador. Se apenas o ficheiro de definição de vírus e o motor de pesquisa forem atualizados, o computador não precisará de ser reiniciado.

Quando uma atualização do produto requer um reinício, pode decidir continuar com a atualização ou ser lembrado mais tarde sobre esta. Se continuar a atualização do produto imediatamente, poderá escolher quando pretende que o reinício seja efetuado.

Se pretende ser lembrado sobre a atualização mais tarde, o ficheiro de definição de vírus e o motor de pesquisa serão atualizados de qualquer maneira mas a atualização do produto não será desempenhada.

Nota
A atualização do produto não será concluída até que seja efetuado um reinício.

Nota
Por motivos de segurança, o Atualizador verifica se o ficheiro *hosts* do Windows do seu computador foi alterado de modo a que, por exemplo, o URL de Atualização tenha sido manipulado por malware e esteja a desviar o

Atualizador para sites de transferências indesejados. Se o ficheiro hosts do Windows tiver sido manipulado, isso será mostrado no ficheiro de relatório do Atualizador.

Uma atualização é executada automaticamente no seguinte intervalo: 6 horas.

No Centro de Controlo, no **Agendamento**, pode criar trabalhos de atualização adicionais que são realizados pelo Atualizador nos intervalos especificados. Também pode iniciar uma atualização manualmente:

- no Centro de Controlo: no menu **Atualizar** e na secção **Estado**
- através do menu de contexto do ícone de bandeja

As atualizações podem ser obtidas na Internet através de um servidor da Web do fabricante. A ligação de rede existente é a ligação padrão com os servidores de transferência da Avira. Pode alterar esta configuração predefinida em Configuração > Atualização.

13.2 Atualizador

A janela Atualizador é aberta no início de uma atualização.

Observação
Para atualizar trabalhos criados no Agendamento, é possível definir o modo de exibição para a janela de atualização: Você pode selecionar **Ocultar**, **Minimizar** ou **Maximizar**.

Observação
Se estiver usando um programa no modo de tela inteira (por exemplo,. jogos) e o modo de exibição do atualizador estiver configurado como maximizado ou minimizado, o atualizador comutará para a área de trabalho. Para evitar isto, inicie o atualizador com o modo de exibição configurado como Ocultar. Nesse modo, você não receberá mais notificações sobre atualizações na janela de atualização.

Status: Mostra o andamento do atualizador.

Tempo decorrido: O tempo que decorreu desde o início do download.

Tempo restante: Tempo até o fim do download.

Velocidade do download: A velocidade do download.

Transmitido: Bytes já baixados.

Restantes: Bytes que faltam baixar.

Botões e links

Botão / link	Descrição
Ajuda	Esta página da ajuda on-line é aberta por meio deste botão ou link.
Reduzir	A janela de exibição do atualizador aparecerá em tamanho reduzido.
Ampliar	A janela de exibição do atualizador voltará ao tamanho original.
Anular	O procedimento de atualização será cancelado. O atualizador será fechado.
Fechar	O procedimento de atualização foi concluído. A janela de exibição será fechada.
Relatório	O arquivo de relatório da atualização é exibido.

14. Perguntas Frequentes, Dicas

Este capítulo contém informações importantes sobre solução de problemas e dicas adicionais sobre como usar seu produto Avira.

- consulte o Capítulo Ajuda no caso de um problema
- consulte o Capítulo Atalhos
- consulte o Capítulo Windows Security Center (Windows XP) ou Windows Action Center (no Windows 7)

14.1 Ajuda caso ocorra um problema

Aqui você encontrará informações sobre causas e soluções de possíveis problemas.

- A mensagem de erro *Falha de conexão ao baixar o arquivo*... é exibida ao tentar iniciar uma atualização.
- Vírus e malwares não podem ser movidos nem excluídos.
- O status do ícone de bandeja está desativado.
- O computador fica extremamente lento quando faço backup dos dados.
- Meu firewall relata o Avira Real-Time Protection imediatamente após a ativação.
- O Webchat não está operacional: As mensagens de bate-papo não são exibidas; os dados estão sendo carregados no navegador.

A mensagem de erro *Falha de conexão ao baixar o arquivo*... é exibida ao tentar iniciar uma atualização.

Motivo: sua conexão com a Internet não está ativa. Nenhuma conexão com o servidor da web na Internet pode, portanto, ser estabelecida.

- Teste se outros serviços da Internet, como WWW ou e-mail, funcionam. Em caso negativo, restabeleça a conexão com a Internet.

Motivo: não é possível conectar com o servidor proxy.

- Verifique se o logon do servidor proxy foi alterado e adapte-o à sua configuração se necessário.

Motivo: O arquivo *update.exe* não foi totalmente aprovado por seu firewall pessoal.

- Verifique se o arquivo *update.exe* foi totalmente aprovado por seu firewall pessoal.

Caso contrário:

- Verifique sua configurações na Configuração em Proteção do PC > Atualizar.

Vírus e malwares não podem ser movidos nem excluídos.

Motivo: O arquivo foi carregado pelo Windows e está ativo.

- Atualize seu produto Avira.
- Se você usar o sistema operacional Windows XP, desative a Restauração do Sistema.
- Inicie o computador no Modo de Segurança.
- Inicie a Configuração de seu produto Avira .
- Selecione **Scanner > Varredura > Arquivos compactados > Todos os tipos de arquivamento** e confirme a janela com **OK**.
- Inicie uma varredura de todas as unidades locais.
- Inicie o computador no Modo Normal.
- Realize uma varredura no Modo Normal.
- Se nenhum outro vírus ou malware for encontrado, ative a Restauração do Sistema se estiver disponível e for posasível utilizá-la.

O status do ícone de bandeja está desativado.

Motivo: o Avira Real-Time Protection está desativado.

- No Centro de Controle, clique em **Status** e ative o **Real-Time Protection** na área *Proteção do PC*.

-OU-

- Abra o menu de contexto com um clique no botão direito do mouse no Ícone da bandeja. Clique em **Ativar o Real-Time Protection**.

Motivo: o Avira Real-Time Protection está bloqueado por um firewall.

- Defina uma aprovação geral para o Avira Real-Time Protection na configuração do firewall. O Avira Real-Time Protection funciona somente com o endereço 127.0.0.1 (host local). Uma conexão com a Internet não está estabelecida.

Caso contrário:

- Verifique o tipo de partida do serviço Avira Real-Time Protection. Se necessário, ative o serviço na barra de tarefas, selecione **Iniciar > Configurações > Painel de controle**. Inicie o painel de configuração **Serviços** clicando duas vezes (no Windows XP o applet de serviços está localizado no subdiretório *Ferramentas Administrativas*). Localize a entrada *Avira Real-Time Protection*. `Automático` deve ser inserido como o tipo de inicialização e `Iniciado` como o status. Se necessário, inicie o serviço manualmente selecionando a linha relevante e o botão **Iniciar**. Se uma mensagem de erro for exibida, verifique a exibição do evento.

O computador fica extremamente lento quando faço backup dos dados.

Motivo: durante o procedimento de backup, o Avira Real-Time Protection verifica todos os arquivos que estão sendo usados pelo procedimento de backup.

- Selecione **Real-Time Protection > Varredura > Exceções** na Configuração e insira os nomes de processo do software de backup.

Meu firewall relata o Avira Real-Time Protection

Motivo: A comunicação com o Avira Real-Time Protection ocorre através do protocolo da Internet TCP/IP. Um firewall monitora todas as conexões através desse protocolo.

- Defina uma aprovação geral para o Avira Real-Time Protection. O Avira Real-Time Protection funciona somente com o endereço 127.0.0.1 (host local). Uma conexão com a Internet não está estabelecida.

> **Observação**
> Recomendamos que você instale as atualizações da Microsoft regularmente para preencher todas as lacunas de segurança.

O Webchat não está operacional: As mensagens de bate-papo não são exibidas; os dados estão sendo carregados no navegador.

Esse fenômeno pode ocorrer durante bate-papos que são baseados no protocolo HTTP com “transfer-encoding= chunked.

Motivo: O Web Protection verifica os dados enviados completamente em busca de vírus e programas indesejados primeiro, antes que os dados sejam carregados no navegador da web. Durante uma transferência de dados com ‘transfer-encoding: chunked’, o Web Protection não consegue determinar o tamanho da mensagem nem o volume de dados.

- Insira a configuração da URL dos bate-papos da web como uma exceção (consulte Configuração: **Web Protection > Varredura > Exceções**).

14.2 Atalhos

Os comandos de teclado - também chamados de atalhos - permitem navegar através do programa, recuperar módulos individuais e iniciar ações rapidamente.

A seguir há uma visão geral dos comandos do teclado disponíveis. Mais informações sobre a funcionalidade estão disponíveis no capítulo correspondente da ajuda.

14.2.1 Nas caixas de diálogo

Atalho	Descrição
Ctrl + Tab **Ctrl + Page down**	Navegação no Centro de Controle Ir para a próxima seção.
Ctrl + Shift + Tab **Ctrl + Page up**	Navegação no Centro de Controle Ir para seção anterior.
← ↑ → ↓	Navegação nas seções de configuração Primeiro, use o mouse para definir o foco em uma seção de configuração. Alternar entre as opções de uma lista suspensa marcada ou entre várias opções de um grupo de opções.
Tab	Altera para a opção ou grupo de opções seguinte.
Shift + Tab	Alterar para a opção ou o grupo de opções anterior.
Espaço	Ativar ou desativar uma caixa de seleção, se a opção ativa for uma caixa de seleção.
Alt + letra sublinhada	Selecionar a opção ou iniciar o comando.
Alt + ↓ **F4**	Abrir a lista suspensa selecionada.
Esc	Fechar a lista suspensa selecionada. Cancelar o comando e fechar diálogo.
Enter	Inicia o comando para a opção ou o botão ativo.

14.2.2 Na ajuda

Atalho	Descrição
Alt + Espaço	Exibir menu do sistema.
Alt + Tab	Alternar entre a ajuda e as outras janelas abertas.
Alt + F4	Fechar a ajuda.
Shift + F10	Exibir o menu contextual da ajuda.
Ctrl + Tab	Ir para a próxima seção na janela de navegação.
Ctrl + Shift + Tab	Ir para a seção anterior na janela de navegação.
Page up	Mudar para o assunto, que é exibido acima no conteúdo, no índice ou na lista de resultados de pesquisa.
Page down	Mudar para o assunto, que é exibido abaixo no conteúdo atual, no índice ou na lista de resultados de pesquisa.
Page up **Page down**	Navegar por um assunto.

14.2.3 No Centro de controle

Geral

Atalho	Descrição
F1	Exibir ajuda
Alt + F4	Fechar o Centro de controle
F5	Atualizar
F8	Abrir a configuração

F9	Iniciar atualização

Seção Verificar

Atalho	Descrição
F3	Iniciar verificação com o perfil selecionado
F4	Criar link na área de trabalho para o perfil selecionado

Seção Quarentena

Atalho	Descrição
F2	Verificar novamente o objeto
F3	Restaurar objeto
F4	Enviar objeto
F6	Restaurar objeto para...
Voltar	Propriedades
Ins	Adicionar arquivo
Del	Excluir objeto

Seção Agendamiento

Atalho	Descrição
F2	Editar trabalho
Voltar	Propriedades

Ins	Inserir novo trabalho
Del	Excluir trabalho

Seção Relatórios

Atalho	Descrição
F3	Exibir arquivo de relatório
F4	Imprimir arquivo de relatório
Voltar	Exibir relatório
Del	Excluir relatório(s)

Seção Eventos

Atalho	Descrição
F3	Exportar evento(s)
Voltar	Mostrar evento
Del	Excluir evento(s)

14.3 Central de Segurança do Windows

- Windows XP Service Pack 2 -

14.3.1 Geral

A Central de segurança do Windows verifica o status do computador com relação a importantes aspectos de segurança.

Se algum problema for detectado em um desses pontos importantes (por exemplo, um programa antivírus desatualizado), a Central de Segurança emitirá um alerta e fará recomendações sobre como proteger melhor seu computador.

14.3.2 A Central de Segurança do Windows e o produto da sua Avira

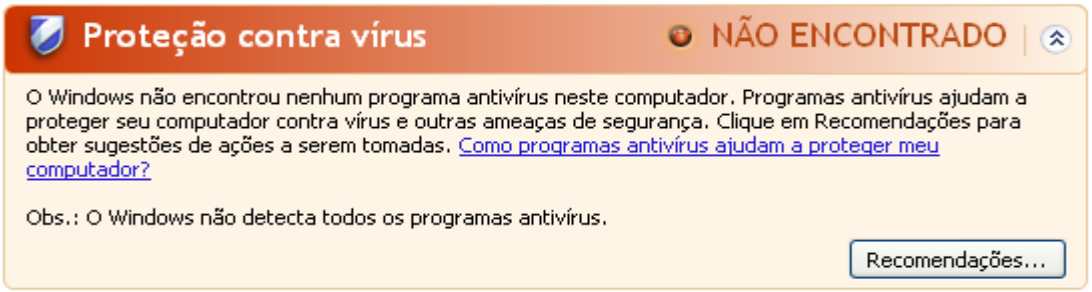
Software de proteção contra vírus/Proteção contra software malicioso

Você poderá receber as seguintes informações da Central de Segurança do Windows com relação à proteção contra vírus:

- Proteção contra vírus NÃO ENCONTRADA
- Proteção contra vírus DESATUALIZADA
- Proteção contra vírus ATIVADA
- Proteção contra vírus DESATIVADA
- Proteção contra vírus NÃO MONITORADA

Proteção contra vírus NÃO ENCONTRADA

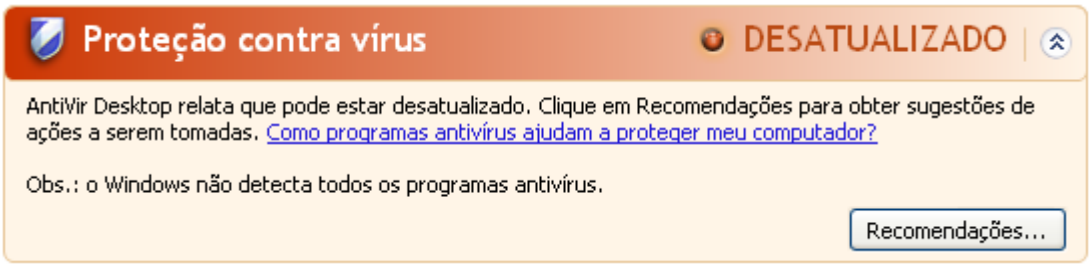
Essas informações aparecem quando a Central de segurança do Windows não encontra nenhum software antivírus em seu computador.



Observação
Instale seu produto Avira no seu computador para proteção contra vírus e outros programas indesejados!

Proteção contra vírus DESATUALIZADA

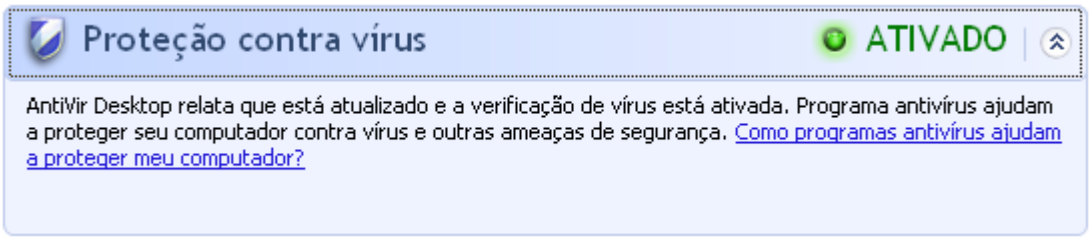
Se você já tiver instalado o Windows XP Service Pack 2 e então instalar o produto Avira, ou instalar o Windows XP Service Pack 2 em um sistema o qual o Avira já estiver instalado, você receberá a seguinte mensagem:



Observação
Para que o Centro de Segurança do Windows reconheça seu produto Avira como atualizado, deverá ser feita uma atualização após a instalação Atualize o sistema executando uma atualização.

Proteção contra vírus ATIVADA

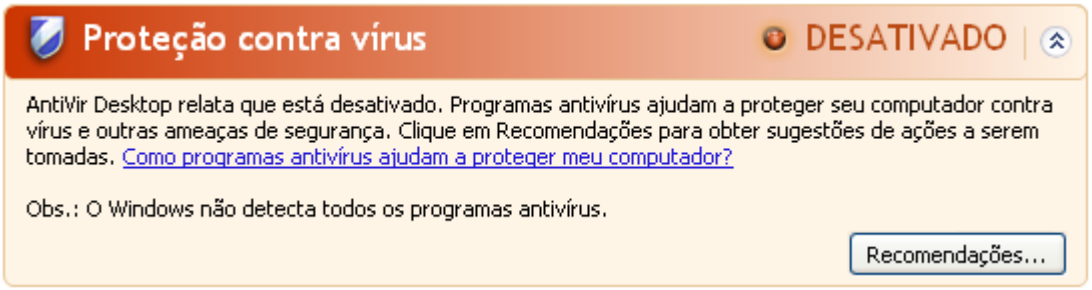
Após instalar seu produto Avira e efetuar a atualização subsequente, você receberá a seguinte mensagem:



O seu produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

Proteção contra vírus DESATIVADA

Você receberá a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.

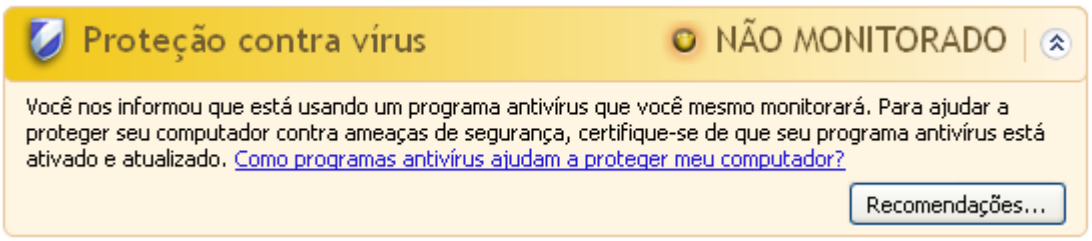


Observação
Você pode ativar ou desativar o Avira Real-Time Protection na seção de Status

da **Central de Controle**. Você também pode verificar que o Avira Real-Time Protection está ativado se o guarda-chuva vermelho em sua barra de tarefas estiver aberto.

Proteção contra vírus NÃO MONITORADA

Se a seguinte mensagem da Central de Segurança do Windows for exibida, você decidiu monitorar seu software antivírus por conta própria.



Observação
A Central de Segurança do Windows é suportada por seu produto Avira. Você pode ativar esta opção a qualquer momento por meio do botão **Recomendações**.

Observação
Mesmo se você tiver instalado o Windows XP Service Pack 2, ainda precisará de uma solução de proteção contra vírus. Embora o Windows monitore seu software antivírus, ele não contém nenhuma função antivírus. Desse modo, você não tem proteção contra vírus e outros malwares sem uma solução antivírus adicional!

14.4 Central de Ações do Windows

- Windows 7 e Windows 8 -

14.4.1 Geral

Nota:
A partir do Windows 7 a **Central de Segurança do Windows** foi renomeado para **Central de Ações do Windows**. Nesta seção você localizará o status de todas as opções de segurança.

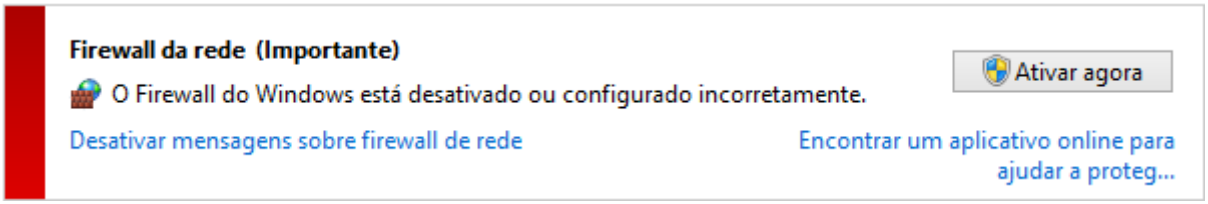
A Central de Ações do Windows verifica o status do computador com relação a importantes aspectos de segurança. Pode ser acessada diretamente clicando na bandeirinha na barra de tarefas ou em **Painel de Controle > Central de Ações**.

Se algum problema for detectado em um desses pontos importantes (por exemplo, um programa antivírus desatualizado), a Central de Ações emitirá um alerta e fará recomendações sobre como proteger melhor seu computador. Isto significa que, se tudo funcionar corretamente, não serão exibidas mensagens. O status de segurança do computador pode ser observado no **Central de Ações do Windows**, no item **Segurança**. A **Central de Ações do Windows** também oferece a opção de gerenciar os programas instalados e escolher entre eles (por exemplo, *Ver programas antispyware instalados*).

Você pode até mesmo desativar as mensagens de aviso em **Alterar Configurações da Central de Ações** (por exemplo, *Desativar mensagens sobre o spyware e a proteção relacionada*).

14.4.2 A Central de Ações do Windows e seu produto Avira

Firewall do Windows está desativado ou configurado incorretamente



- **Firewall do Windows**

  A partir do Windows 7, Avira Free Antivirus dá a opção de gerenciar diretamente o Firewall do Windows a partir do Centro de Controle e Configuração Avira.

Proteção contra vírus

Você poderá receber as seguintes informações da Central de Ações do Windows com relação à sua proteção contra vírus:

- O Avira Desktop relata que está atualizado e a verificação de vírus está ativada.
- O Avira Desktop relata que está ativado.
- O Avira Desktop relata que está desatualizado.
- O Windows não localizou software antivírus neste computador.
- O Avira Desktop expirou.

O Avira Desktop relata que está atualizado e a verificação de vírus está ativada

Após a instalação de seu produto Avira e uma atualização subsequente, você não receberá nenhuma mensagem da Central de Ações do Windows. Mas, se você acessar **Central de Ações > Segurança**, poderá ver: *O Avira Desktop relata que ele está*

atualizado e a verificação de vírus está ativada. Isso significa que o produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

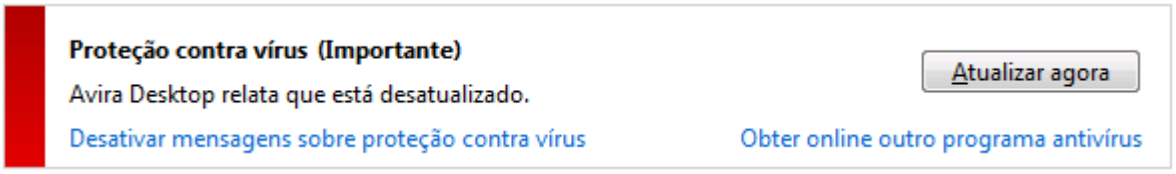
O Avira Desktop relata que está desativado

Você recebe a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.

Nota
O Avira Real-Time Protection pode ser ativado ou desativado na seção **Status** do **Centro de Controle Avira**. Você também pode verificar que o Avira Real-Time Protection está ativado com o guarda-chuva vermelho aberto na barra de tarefas. Também é possível ativar o produto Avira clicando no botão *Ativar agora* na mensagem da Central de Ações do Windows. Você receberá uma notificação solicitando sua permissão para executar o Avira. Clique em *Sim, eu confio no Editor e desejo executar este programa* e o Real-Time Protection será ativado novamente.

O Avira Desktop relata que está desatualizado

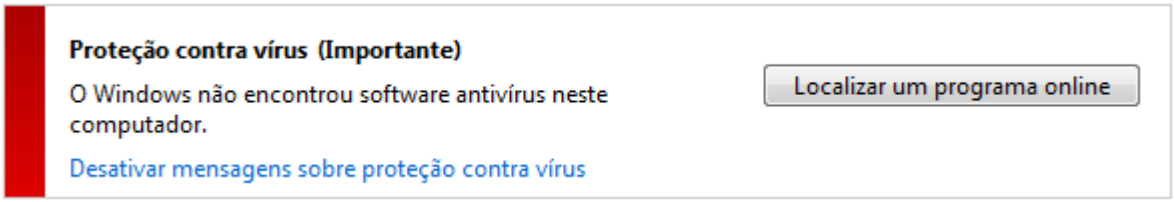
Se você acabou de instalar o Avira ou se por algum motivo o arquivo de definição de vírus, o mecanismo de varredura ou os arquivos de programa do produto Avira não foram atualizados automaticamente (por exemplo, se foi feita uma atualização de um sistema operacional Windows mais antigo, no qual o produto Avira já está instalado) você receberá a seguinte mensagem:



Observação
Para que a Central de Ações do Windows reconheça seu produto Avira como atualizado, uma atualização deverá ser executada após a instalação. Atualize seu Produto Avira executando uma atualização.

O Windows não localizou software antivírus neste computador

Essas informações da Central de Ações do Windows aparecem quando a Central de Ações do Windows não encontra nenhum software antivírus em seu computador.



Nota
Observe que esta opção não aparece no Windows 8, pois o Windows Defender agora também é a função de proteção de vírus predefinida.

Observação
Instale o produto Avira em seu computador para protegê-lo contra vírus e outros programas indesejados!

O Avira Desktop expirou

Essas informações da Central de Ações do Windows aparecem quando a licença do produto Avira expirou.
Se você clicar no botão **Renovar a assinatura** será redirecionado para um site da Avira, onde poderá comprar uma nova licença.

Nota
Observe que essa opção está disponível somente para o Windows 8.

Spyware e proteção contra software indesejado

Você poderá receber as seguintes informações da Central de Ações do Windows com relação à sua proteção contra spyware:

- O Avira Desktop relata que está ativado.
- O Windows Defender e o Avira Desktop relatam que estão desativados.
- O Avira Desktop relata que está desatualizado.
- O Windows Defender está desligado.

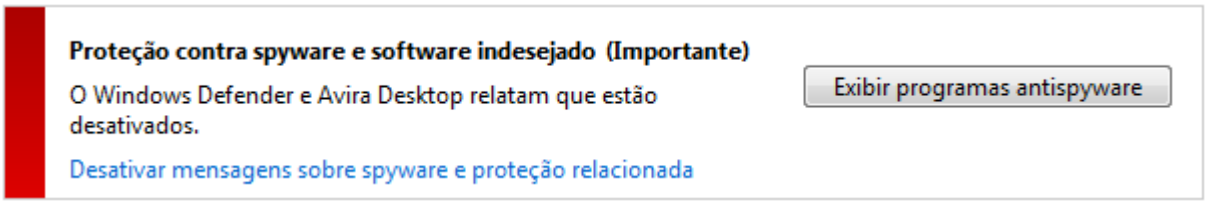
- O Windows Defender está desligado.

O Avira Desktop relata que está ativado

Após a instalação do produto Avira e uma atualização subsequente, você não receberá nenhuma mensagem da Central de Ações do Windows. Mas, se você acessar **Central de Ações > Segurança**, poderá ver: *O Avira Desktop relata que ele está ativado*. Isso significa que o produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

O Windows Defender e o Avira Desktop relatam que estão desativados

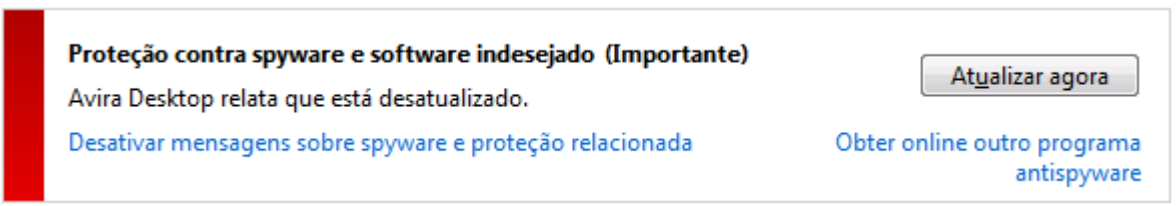
Você recebe a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.



Nota
O Avira Real-Time Protection pode ser ativado ou desativado na seção **Status** do **Centro de Controle Avira**. Você também pode verificar que o Avira Real-Time Protection está ativado com o guarda-chuva vermelho aberto na barra de tarefas. Também é possível ativar o produto Avira clicando no botão *Ativar agora* na mensagem da Central de Ações do Windows. Você receberá uma notificação solicitando sua permissão para executar o Avira. Clique em *Sim, eu confio no Editor e desejo executar este programa* e o Real-Time Protection será ativado novamente.

O Avira Desktop relata que está desatualizado

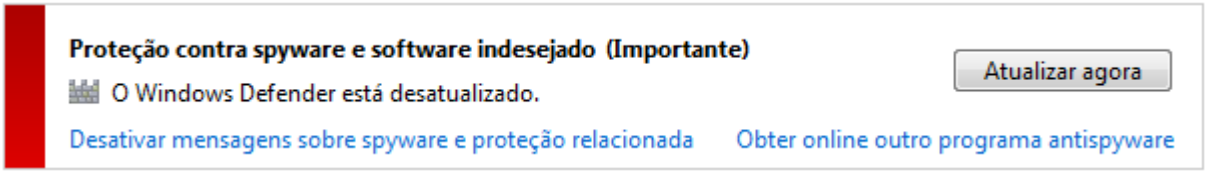
Se você acabou de instalar o Avira ou se por algum motivo o arquivo de definição de vírus, o mecanismo de varredura ou os arquivos de programa do produto Avira não foram atualizados automaticamente (por exemplo, se foi feita uma atualização de um sistema operacional Windows mais antigo, no qual o produto Avira já está instalado) você receberá a seguinte mensagem:



Observação
Para que a Central de Ações do Windows reconheça seu produto Avira como atualizado, uma atualização deverá ser executada após a instalação. Atualize seu Produto Avira executando uma atualização.

O Windows Defender está desatualizado

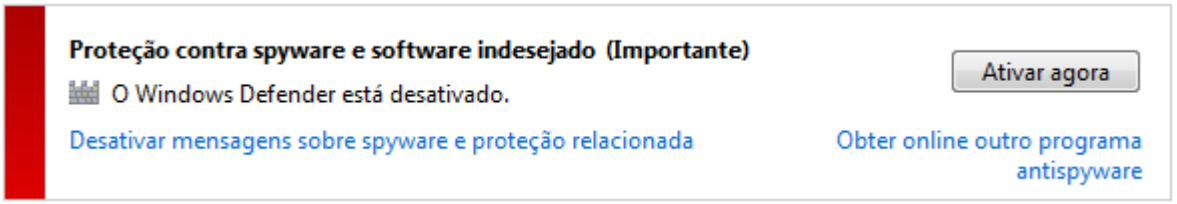
Você pode receber a mensagem a seguir se o Windows Defender estiver ativado. Se já tiver instalado o produto Avira, esta mensagem não deve ser exibida. Verifique se a instalação ocorreu corretamente.



Nota
O Windows Defender é a solução predefinida de proteção contra vírus e spyware do Windows.

O Windows Defender está desligado

Essas informações da Central de Ações do Windows aparecem quando a Central de Ações do Windows não encontrar nenhum outro software antivírus no computador além daquele que o sistema operacional integra por padrão: Windows Defender. Se você tiver algum software antivírus instalado anteriormente em seu computador, este aplicativo foi desativado. Se você já tiver instalado o produto Avira, esta mensagem não deverá ser exibida: O Avira deve ser detectado automaticamente. Verifique se a instalação ocorreu corretamente.



15. Vírus e mais

Avira Free Antivirus não somente detecta vírus e malware, como também protege de outras ameaças. Neste capítulo é possível obter uma visão geral dos diferentes tipos de malware e outras ameaças, descrevendo suas práticas, seus comportamentos e as surpresas desagradáveis que elas reservam para você.

Tópicos relacionados:

- Categorias de ameaça
- Vírus e outros malwares

15.1 Categorias de ameaça

Adware

Adware é um software que apresenta anúncios de banner ou janelas pop-up através de uma barra que aparece na tela do computador. Esses anúncios normalmente não podem ser removidos e, por isso, estão sempre visíveis. Os dados de conexão fornecem várias conclusões quanto ao comportamento de uso e são problemáticos em termos de segurança de dados.

Seu produto Avira detecta Adware. Se a opção **Adware** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar adware.

Adware/Spyware

Software que exibe propaganda ou software que envia dados pessoais do usuário para terceiros, geralmente sem seu conhecimento ou consentimento e, por esse motivo, pode ser indesejado.

Seu produto Avira reconhece "Adware/Spyware". Se a opção **Adware/Spyware** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar adware ou spyware.

Aplicativos

O termo APPL refere-se a um aplicativo que pode envolver um risco quando usado ou é de origem duvidosa.

Seu produto Avira reconhece "Aplicativo (APPL)". Se a opção **Aplicativo** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal comportamento.

Clientes backdoor

Para roubar dados ou manipular computadores, um programa de servidor backdoor é introduzido no sistema sem o conhecimento do usuário. Esse programa pode ser controlado por terceiros com o uso de um software de controle backdoor (cliente) via Internet ou por uma rede.

Seu produto Avira reconhece "Software de controle de backdoor". Se a opção **Software de controle de backdoor** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal software.

Discador

É necessário pagar por alguns serviços disponíveis na Internet. Eles são faturados na Alemanha através de discadores com os números 0190/0900 (ou através dos números 09x0 na Áustria e na Suíça; na Alemanha, o número está definido para mudar para 09x0 a médio prazo). Depois de serem instalados no computador, esses programas garantem uma conexão através de um número de taxa premium que pode ter tarifas muito variadas.

A comercialização de conteúdo on-line pela conta de telefone é legal e pode ser vantajosa para o usuário. Os discadores genuínos não deixam dúvidas de que estão sendo usados deliberada e intencionalmente pelo usuário. Eles são instalados somente no computador do usuário com o consentimento do usuário, que deve ser fornecido através de uma marcação ou solicitação totalmente sem ambiguidade e claramente visível. O processo de discagem dos discadores genuínos é exibido claramente. Além disso, os discadores genuínos mostram os custos incorridos de maneira exata e sem erros.

Infelizmente, também existem discadores que se instalam nos computadores sem serem percebidos de modo duvidoso ou até mesmo com a intenção de enganar o usuário. Por exemplo, eles substituem o link de comunicação de dados padrão do usuário da Internet no ISP (Internet Service Provider, Provedor de Serviço de Internet) e discam para um número 0190/0900 que geralmente acarreta custos altíssimos sempre que uma conexão é estabelecida. O usuário afetado provavelmente não perceberá até receber a próxima conta de telefone que um discador 0190/0900 indesejado em seu computador discou para um número de taxa premium em cada conexão, resultando em custos significativamente maiores.

Recomendamos que você entre em contato com a operadora de telefone para solicitar o bloqueio dessa faixa de números para que seja protegido imediatamente contra discadores indesejados (discadores 0190/0900).

Seu produto Avira pode detectar os discadores familiares por padrão.

Se a opção **Discadores** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se um discador for detectado. Agora você pode simplesmente excluir o discador 0190/0900 possivelmente indesejado. No entanto, se for um programa de discagem desejado, você poderá declará-lo como um arquivo excepcional e esse arquivo não será mais verificado no futuro.

Arquivos com extensão dupla

Arquivos executáveis que ocultam a extensão real do arquivo de uma maneira suspeita. Esse método de camuflagem normalmente é usado por malwares.

Seu produto Avira reconhece "Arquivos com extensão dupla". Se a opção **Arquivos com extensão dupla** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detetar tais arquivos.

Software fraudulento

Também conhecido como "scareware" ou "rogueware", ele é um software fraudulento que deseja que seu computador seja infectado por vírus ou malware. Este software se parece enganosamente com um software Antivírus profissional, mas seu objetivo é provocar incertezas ou assustar o usuário. Sua finalidade é fazer as vítimas se sentirem ameaçadas por um perigo iminente (irreal) e fazê-las pagar para eliminar esse perigo. Também há casos em que as vítimas são levadas a acreditar que foram atacadas e recebem instruções para executar uma ação que é, na verdade, o ataque real.

Seu produto Avira detecta scareware. Se a opção **Software Fraudulento** estiver ativada com um visto na configuração Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tais arquivos.

Jogos

Os jogos de computador são permitidos, mas não necessariamente no trabalho (talvez na hora do almoço). No entanto, com a variedade de jogos disponíveis para download na Internet, o Campo minado e o jogo da Paciência não são os únicos que fazem parte do dia a dia dos funcionários e dos usuários em geral. Você pode baixar diversos jogos pela Internet. Jogos por e-mail também se tornaram mais populares: inúmeras variações estão circulando, variando desde simples jogo de xadrez até "treinamentos de tropas" (incluindo combates de torpedo): Os movimentos correspondentes são enviados aos parceiros via programas de e-mail, os quais respondem.

Estudos mostram que o número de horas de trabalho dedicadas aos jogos de computador tem atingido proporções economicamente significativas. Portanto, não é surpreendente o fato de cada vez mais empresas procurarem meios para banir os jogos de computador do local de trabalho.

Seu produto Avira reconhece jogos de computador. Se a opção **Jogos** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar um jogo. Agora o jogo acabou literalmente porque você pode simplesmente excluí-lo.

Piadas

As piadas servem simplesmente para assustar alguém ou provocar o divertimento de todos sem causar danos. Quando um programa de piadas é carregado, o computador normalmente começa, em algum ponto, a reproduzir um som ou exibir algo incomum na

tela. A máquina de lavar na unidade de disco (DRAIN.COM) e o comedor de tela (BUGSRES.COM) são exemplos de piadas.

Mas tome cuidado! Todos os sintomas dos programas de piadas também podem se originar de um vírus ou cavalo de Tróia. Em último caso, os usuários terão um choque ou entrarão em pânico, o que pode causar danos reais.

Graças à extensão das rotinas de verificação e identificação, seu produto Avira pode detectar programas de piada e eliminá-los como programas indesejados se necessário. Se a opção **Piadas** estiver ativada com um visto na configuração em Categorias de ameaça, um alerta correspondente será emitido se um programa de piadas for detectado.

Phishing

Phishing, também conhecido como "brand spoofing" (falsificação de marca), é uma forma mais inteligente de roubo de dados, cujo objetivo são clientes ou possíveis clientes de provedores de serviços de Internet, bancos, serviços bancários on-line e autoridades de registros.
Ao enviar seu endereço de email pela Internet, preencher formulários on-line, acessar grupos de notícias ou sites, seus dados podem ser roubados por "rastreadores" da Internet e usados sem sua permissão para cometer fraudes e outros crimes.

Seu produto Avira reconhece "Phishing". Se a opção **Phishing** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal comportamento.

Programas que violam o domínio privado

Software que pode comprometer a segurança do seu sistema, iniciar atividades de programa indesejado, danificar sua privacidade ou espionar o comportamento do usuário e, portanto, pode ser indesejado.

Seu produto Avira detecta o software "Security Privacy Risk". Se a opção **Programas que violam o domínio privado** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal software.

Compactadores de tempo de execução incomuns

Arquivos que foram compactados com um compactador de tempo de execução incomum e que podem, portanto, ser classificados como possivelmente suspeitos.

Seu produto Avira reconhece "Compactadores de tempo de execução incomuns". Se a opção **Compactadores de tempo de execução incomuns** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tais compactadores.

15.2 Vírus e outros malwares

Adware

Adware é um software que apresenta anúncios de banner ou janelas pop-up através de uma barra que aparece na tela do computador. Esses anúncios normalmente não podem ser removidos e, por isso, estão sempre visíveis. Os dados de conexão fornecem várias conclusões quanto ao comportamento de uso e são problemáticos em termos de segurança de dados.

Backdoors

Um backdoor pode obter acesso a um computador enganando os mecanismos de segurança de acesso do computador.

Um programa que está sendo executado em segundo plano geralmente concede ao invasor direitos quase ilimitados. Os dados pessoais do usuário podem ser vistos com a ajuda de um backdoor. Mas são usados principalmente para instalar outros worms ou vírus de computador no sistema relevante.

Vírus de inicialização

O setor mestre ou de inicialização dos discos rígidos é infectado principalmente através de vírus do setor de inicialização. Eles substituem informações importantes necessárias para a execução do sistema. Uma das piores consequências: o sistema do computador não pode mais ser carregado...

Bot-Net

Um bot net é definido como uma rede remota de computadores (na Internet) que é composta por bots que se comunicam entre si. Um Bot-Net pode comprometer vários computadores invadidos por programas (mais conhecidos como worms, cavalos de Tróia) executados sob um comando e uma infraestrutura de controle comuns. Os Boot-Nets possuem várias finalidades, entre elas, ataques de negação de serviço, muitas vezes sem o conhecimento do usuário do PC afetado. O grande potencial dos Bot-Nets é que as redes podem alcançar a dimensão de milhares de computadores e a soma de suas larguras de banda sobrecarrega o acesso à Internet mais convencional.

Exploit

Um exploit (lacuna de segurança) é um programa de computador ou script que se aproveita de um bug, glitch ou de uma vulnerabilidade que leva ao escalamento de privilégios ou à negação de serviço em um sistema de computador. Por exemplo, um tipo de exploit são ataques a partir da Internet com a ajuda de pacotes de dados manipulados. Os programas podem ser infiltrados para obter acesso de nível mais alto.

Software fraudulento

Também conhecido como "scareware" ou "rogueware", ele é um software fraudulento que deseja que seu computador seja infectado por vírus ou malware. Este software se parece enganosamente com um software Antivírus profissional, mas seu objetivo é provocar incertezas ou assustar o usuário. Sua finalidade é fazer as vítimas se sentirem ameaçadas por um perigo iminente (irreal) e fazê-las pagar para eliminar esse perigo. Também há casos em que as vítimas são levadas a acreditar que foram atacadas e recebem instruções para executar uma ação que é, na verdade, o ataque real.

Hoaxes

Há muitos anos, os usuários da Internet e outros usuários de rede têm recebido alertas sobre vírus disseminados intencionalmente por email. Esses alertas são difundidos por email com a solicitação para que sejam enviados ao maior número possível de amigos e outros usuários para avisá-los do "perigo".

Honeypot

Honeypot é um serviço (programa ou servidor) que é instalado em uma rede. Sua função é monitorar uma rede e registrar ataques. Um usuário legítimo da rede não tem conhecimento desse serviço, por isso ele nunca é avisado. Se um invasor examinar os pontos de falhas na rede e usar os serviços oferecidos por um honeypot, ele será registrado e será acionado um alerta.

Vírus de macro

Os vírus de macro são pequenos programas escritos na linguagem de macro de um aplicativo (por exemplo, WordBasic no WinWord 6.0) que, em geral, só se propagam em documentos desse aplicativo. Por causa disso, eles também são chamados de vírus de documentos. Para se tornarem ativos, eles precisam que aplicativos correspondentes sejam ativados e que uma das macros infectadas seja executada. Diferentemente dos vírus "normais", os vírus de macro não atacam arquivos executáveis, mas atacam os documentos do aplicativo host correspondente.

Pharming

Pharming é uma manipulação do arquivo de host dos navegadores da Web para desviar as consultas para sites falsos. É mais um desenvolvimento do phishing clássico. Os vigaristas de pharming operam seus próprios farms de servidor enormes nos quais os sites falsos são armazenados. Pharming foi estabelecido como um termo geral para os diversos tipos de ataques de DNS. No caso da manipulação do arquivo de host, uma manipulação específica de um sistema é realizada com a ajuda de um cavalo de Tróia ou vírus. O resultado disso é que o sistema agora só poderá acessar sites falsos, mesmo se o endereço da Web correto for inserido.

Phishing

Phishing significa pescar os dados pessoais do usuário da Internet. Os praticantes de phishing geralmente enviam para suas vítimas cartas aparentemente oficiais, como emails, cujo objetivo é levá-los a revelar informações confidenciais para os criminosos em boa fé, especialmente nomes de usuário e senhas ou PINs e TANs de contas bancárias on-line. Com os detalhes de acesso roubados, os fraudadores podem assumir a identidade de suas vítimas e realizar transações em nome delas. Obviamente, os bancos e as seguradoras nunca pedem números de cartão de crédito, PINs, TANs ou outros detalhes de acesso por email, SMS ou telefone.

Vírus polimorfos

Os vírus polimorfos são verdadeiros mestres do disfarce. Eles alteram seus próprios códigos de programação e, por isso, são muito difíceis de detectar.

Vírus de programa

Um vírus de computador é um programa capaz de se anexar a outros programas depois de ser executado e causar uma infecção. Os vírus se multiplicam diferentemente de bombas lógicas e cavalos de Tróia. Ao contrário de um worm, um vírus sempre precisa de um programa como host, no qual ele deposita seu código infeccioso. Como regra, a execução do programa do host em si não é alterada.

Rootkits

Um rootkit é uma coleção de ferramentas de software que são instaladas após o sistema do computador ser invadido para dissimular logons do invasor, ocultar processos e registrar dados – em outras palavras: torná-los invisíveis. Eles tentam atualizar programas espiões já instalados e reinstalar spywares excluídos.

Vírus de script e worms

Esses vírus são extremamente fáceis de programar e, se a tecnologia necessária estiver à disposição, podem se difundir por email para o mundo inteiro em questão de horas.

Os vírus de script e worms usam uma das linguagens de script, como Javascript, VBScript e outras, para se infiltrar em novos scripts ou se propagar pela chamada de funções do sistema operacional. Isso acontece com frequência por email ou através da troca de arquivos (documentos).

Um worm é um programa que se multiplica, mas não infecta o host. Consequentemente, os worms não podem fazer parte das sequências de outros programas. Muitas vezes, só eles são capazes de se infiltrar em algum tipo de programa nocivo em sistemas com medidas de segurança restritivas.

Spyware

Spyware é o programa espião que intercepta ou assume o controle parcial da operação de um computador sem o consentimento informado do usuário. O spyware é criado para explorar computadores infectados para fins comerciais.

Cavalos de Tróia (abreviação: Tróias)

Os cavalos de Tróia são bastante comuns hoje em dia. Eles incluem programas que parecem ter uma determinada função, mas mostram sua verdadeira imagem depois de serem executados, quando carregam uma função diferente que, na maioria dos casos, é destrutiva. Os cavalos de Tróia não podem se multiplicar, o que os diferencia dos vírus e worms. A maioria tem um nome interessante (SEXO.EXE ou EXECUTE.EXE) com a intenção de induzir o usuário a iniciar o cavalo de Tróia. Logo depois da execução, eles se tornam ativos e podem, por exemplo, formatar o disco rígido. Um dropper é uma forma especial de cavalo de Tróia que "solta" vírus, isto é, incorpora vírus no sistema do computador.

Zumbi

Um computador zumbi é aquele infectado por programas de malware e que permite aos hackers invadirem as máquinas por controle remoto para fins ilegais. Sob comando, o computador afetado inicia, por exemplo, ataques DoS (Negação de Serviço) ou envia spam e emails de phishing.

16. Informações e Serviço

Este capítulo contém informações sobre Informações e Serviços do Avira.

- Endereço de Contato
- Suporte Técnico
- Arquivo Suspeito
- Relatando Falso-Positivos
- Seus comentários para mais segurança

16.1 Endereço de Contato

Se você tiver qualquer dúvida ou solicitação relacionada à gama de produtos Avira, teremos o prazer em ajudá-lo. Para obter nossos endereços de contato, consulte o Centro de controle em **Ajuda > Sobre o Avira Free Antivirus**.

16.2 Suporte Técnico

O suporte do Avira fornece assistência confiável para esclarecer suas dúvidas ou solucionar um problema técnico.

Todas as informações necessárias sobre nosso abrangente serviço de suporte podem ser obtidas em nosso site:

http://www.avira.com/pt-br/personal-support

Para que possamos fornecer ajuda rápida e confiável, tenha as seguintes informações em mãos:

- **Informações da versão**. Você pode localizar estas informações na interface do programa, no item de menu **Ajuda > Sobre o Avira Free Antivirus > Inormações da Versão**. Consulte Informações da Versão.
- **Versão do sistema operacional** e quaisquer Service Packs instalados.
- **Pacotes de software instalados**, por exemplo, software antivírus de outros fornecedores.
- **Mensagens exatas** do programa ou do arquivo de relatório.

16.3 Arquivo Suspeito

Arquivos suspeitos ou vírus que podem não ter sido detectados ou removidos ainda por nossos produtos podem ser enviados para nós. Fornecemos várias maneiras para fazer isso.

- Identifique o arquivo no gerenciador de quarentena do Centro de controle do Avira Server Security Console e selecione o item **Enviar arquivo** por meio do menu contextual ou do botão correspondente.
- Envie o arquivo requerido compactado (WinZIP, PKZip, Arj, etc.) no anexo de um email para o seguinte endereço:
  virus-personal-pt-br@avira.com
  Como alguns gateways de e-mail funcionam com software antivírus, você também deve fornecer ao(s) arquivo(s) uma senha (lembre-se de nos informar a senha).

16.4 Relatando Falso-Positivos

Se achar que o Avira Free Antivirus esteja relatando uma detecção em um arquivo que está mais provavelmente "limpo", envie o arquivo relevante compactado (WinZIP, PKZip, Arj, etc.) como um anexo de e-mail para o seguinte endereço:

virus-personal-pt-br@avira.com

Como alguns gateways de e-mail funcionam com software antivírus, você também deve fornecer ao(s) arquivo(s) uma senha (lembre-se de nos informar a senha).

16.5 Seus comentários para mais segurança

No Avira, a segurança de nossos clientes é superior. Por este motivo, nós não apenas temos uma equipe de especialistas interna que testa a qualidade e a segurança de cada solução Avira antes de o produto ser lançado. Também damos grande importância às indicações relacionadas a lacunas relevantes na segurança que poderiam se desenvolver e tratamos isso com seriedade.

Se você achar que detectou uma lacuna na segurança de um de nossos produtos, envie-nos um e-mail para os endereços a seguir:

vulnerabilities@avira.com

Avira

Edição Q4-2013.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Alemanha | Telefone: +49 7542-500 0
www.avira.com/pt-br