bitdefender

antivirus 2010

Guia de usuário

BitDefender Antivírus 2010
Guia de usuário

Publicado 2009.08.07

Nota Legal


bitdefender

Índice

Acordo de Licença de Software para Usuários Finais

SE VOCÊ NÃO CONCORDA COM ESTES TERMOS E CONDIÇÕES, NÃO INSTALE O SOFTWARE. AO SELECIONAR "EU ACEITO", "OK", "CONTINUE", "SIM" OU INSTALANDO OU USANDO O SOFTWARE DE QUALQUER MANEIRA, VOCÊ ESTÁ INDICANDO O COMPLETO CONHECIMENTO E ACEITAÇÃO DOS TERMOS DESTE ACORDO.

REGISTRO DO PRODUTO. Ao aceitar este acordo, você aceitará em registrar o Seu Software usando "My account (Minha conta)", como condição para o uso de seu software (recebendo atualizações) e Seu direito a Manutenção. Este controle assegurará que o software funcione somente em computadores com licenças validadas e que o usuário receba assim, serviços de Manutenção. O registro requer um número de série do produto e um endereço de e-mail válidos para renovações ou outros comunicados.

Estes termos abrangem as Soluções e Serviços BitDefender para usuários individuais licenciados, incluindo documentação relacionada, updates (atualizações da base de vírus) e upgrades (mudanças de versão) das aplicações que lhe foram entregues como parte da licença adquirida ou qualquer acordo de serviço tal como definido na documentação ou em qualquer cópia desses itens.

Este Acordo da Licença é um acordo legal entre você (seja um indivíduo ou representante legal) e a BITDEFENDER para uso do produto de software BITDEFENDER acima identificado, o qual inclui software de computador e serviços e poderá incluir meios associados, materiais impressos, e documentação "online" ou electrónica (daqui em diante designado por "BitDefender"), todos os quais estão protegidos pelos pelas leis internacionais dos direitos de autor e tratados internacionais. Ao instalar, copiar, ou usar de outra forma o BitDefender, estará a concordar com os termos deste acordo.

se você não concorda com os termos deste acôrdo, não instale ou use o BitDefender.

Licença BitDefender. O BitDefender está protegido pelas leis dos direitos de autor e pelos tratados internacionais sobre direitos de autor, como também por outras leis e tratados intelectuais de propriedade. O BitDefender é licenciado, não é vendido.

CONCESSÃO DE LICENÇA. Pela presente, a BITDEFENDER concede-lhe a si, e apenas a si a seguinte licença não-exclusiva, limitada, não-transmissível e passível de royalties para utilizar o BitDefender.

SOFTWARE APLICAÇÃO. Pode instalar e usar BitDefender, em tantos computadores quantos os abrangidos pelo número total de licenças de usuários. Pode fazer uma cópia adicional para efeitos de back-up (cópia de segurança).

LICENÇA DE USUÁRIO DE COMPUTADOR INDIVIDUAL. Esta licença aplica-se ao software BitDefender que pode ser instalado num único computador que não providencie serviços de rede. O primeiro usuário pode instalar este software num

único computador e fazer uma cópia adicional num dispositivo distinto para efeitos de backup. O número de usuários permitidos corresponde ao número de usuários abrangidos pela licença.

TERMOS DE LICENÇA. A Licença aqui outorgada começa na data da aquisição do BitDefender e expira no final do período para o qual a licença foi adquirida.

EXPIRAÇÂO. O produto deixará de executar as suas funções imediatamente após a expiração da licença.

UPGRADES. Se o BitDefender estiver marcado como um upgrade (mudança de versão), tem de estar corretamente licenciado para usar um produto identificado pela BITDEFENDER como sendo elegível para o upgrade para poder usar o BitDefender. O BitDefender marcado como upgrade substitui e/ou suplementa o produto que forma as bases para a sua elegibilidade de upgrade. Pode utilizar o produto resultante do upgrade apenas nos termos deste Acordo de Licença. Se o BitDefender for um upgrade de um componente de um pacote de programas de software que licenciou como um único produto, o BitDefender pode ser usado e transferido apenas como uma parte desse único pacote de produtos, e não pode ser separado para uso por mais do que o número total de usuários licenciados. Os termos e condições desta licença substituem quaisquer acordos prévios que possam ter existido entre si e a BITDEFENDER com respeito ao produto original ou ao upgrade resultante.

COPYRIGHT. Todos os direitos, títulos e interesses no e para o BitDefender e todos os direitos de autor em e no BitDefender (incluindo mas não limitado a qualquer imagem, fotografias, acessos, animações, vídeo, som, música, texto, e "applets" incorporadas no BitDefender), os materiais impressos que o acompanham, e quaisquer cópias do BitDefender são propriedade da BITDEFENDER. O BitDefender está protegido pelos direitos de autor e pelos tratados internacionais. Assim sendo, tem de tratar o BitDefender como qualquer outro material com direitos de autor. Não pode copiar os materiais impressos que acompanham o BitDefender. Tem de produzir e incluir todos os avisos de direitos de autor na sua forma original em todas as cópias criadas independentemente dos meios ou formas, nos quais o BitDefender existe. Não pode sub-licenciar, alugar, vender, fazer leasing ou partilhar a licença BitDefender. Não pode inverter a engenharia, recompilar, desmontar, criar trabalhos derivados, modificar, traduzir, ou fazer qualquer tentativa para descobrir a fonte do código do BitDefender.

GARANTIA LIMITADA. A BITDEFENDER garante que os meios, nos quais o BitDefender é distribuído, são livres de defeitos por um período de trinta dias desde a data de entrega do BitDefender a si. A única solução para uma quebra desta garantia será que a BITDEFENDER, em sua opção, poderá substituir o meio defeituoso após o recebimento do produto danificado, ou reembolsar-lhe o dinheiro que pagou pelo BitDefender. A BITDEFENDER não garante que o BitDefender não seja interrompido ou livre de erros, ou que os erros sejam corrigidos. A BITDEFENDER não garante que BitDefender vá de encontro às suas expectativas.

EXCETO TAL COMO EXPRESSAMENTE EXPOSTO NESTE ACORDO, BITDEFENDER RENUNCIA TODAS AS OUTRAS GARANTIAS, TANTO EXPRESSAS COMO IMPLÍCITAS, COM RESPEITO AOS PRODUTOS, MELHORIAS, MANUTENÇÃO OU SUPORTE RELACIONADOS COM ESTE ACORDO, OU QUAISQUER OUTROS MATERIAIS (TANGÍVEIS OU INTANGÍVEIS) OU SERVIÇOS FORNECIDOS POR ELE. A BITDEFENDER EXPRESSA AQUI A SUA RENÚNCIA A TODAS AS OUTRAS GARANTIAS, TANTO ESPRESSAS COMO IMPLÍCITAS, INCLUÍNDO AS GARANTIAS IMPLÍCITAS DE MERCADO, FEITAS PARA UM PROPÓSITO EM PARTICULAR, OU NÃO INTERFERÊNCIA, EXATIDÃO DOS DADOS, EXATIDÃO DO CONTEÚDO INFORMATIVO, INTEGRAÇÃO DE SISTEMAS, NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS AO FILTRAR, DESATIVAR OU REMOVER O SOFTWARE DE TERCEIROS, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTOS, PUBLICIDADE OU SEMELHANTE, QUER SURJAM POR ESTATUTO, LEI, NO CURSO DE TRANSAÇÕES, POR COSTUME E HÁBITO, OU USO COMERCIAL.

RENÚNCIA DE DANOS. Qualquer pessoa que use, teste, ou avalie o BitDefender será responsável por todo o risco, pela qualidade e desempenho do BitDefender. A BitDefender não será responsável, sob nenhuma circunstância, de qualquer dano de qualquer tipo, incluindo, sem limitação, danos diretos ou indiretos provenientes do uso, desempenho, ou entrega do BitDefender, mesmo que a BitDefender tenha sido avisada da existência ou possibilidade de tais danos. ALGUNS ESTADOS NÃO PERMITEM A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE DE INCIDENTES OU DANOS CONSEQUENTES, POR ISSO A LIMITAÇÃO ACIMA INDICADA PODERÁ NÃO SE APLICAR A SI. EM NENHUM CASO O RISCO DA BITDEFENDER PODERÁ EXCEDER O PREÇO QUE PAGOU PELO BITDEFENDER. As renúncias e limitações, estabelecidas acima, aplicar-se-ão independentemente se aceita usar, avaliar ou testar o BitDefender.

ALGUNS ESTADOS NÃO PERMITEM A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE POR DANOS INCIDENTAIS OU ACIDENTAIS CONSEQUENTES DO USO OU TESTE DAS SOLUÇÕES BITDEFENDER, PORTANTO A LIMITAÇÃO ACIMA OU EXCLUSÃO PODERÁ NÃO SE APLICAR A VOCÊ.

SOB NENHUMA CIRCUNSTÂNCIA A RESPONSABILIDADE DA BITDEFENDER EXCEDERÁ O PREÇO PAGO POR VOCÊ PELO PRODUTO BITDEFENDER. As renúncias e limitações citadas daqui em diante e acima serão aplicadas independentemente se você aceitar usar, avaliar ou testar alguma solução da BitDefender.

AVISO IMPORTANTE AOS USUÁRIOS. ESTE SOFTWARE PODE CONTER ERROS, E NÃO É INDICADA SUA UTILIZAÇÃO EM NENHUM MEIO QUE REQUEIRA UM ALTO GRAU DE RISCO E QUE NECESSITE ALTA ESTABILIDADE. ESTE PRODUTO DE SOFTWARE NÃO ESTÁ DESTINADO A SETORES DAS ÁREAS DE AVIAÇÃO, CENTRAIS NUCLEARES, SISTEMAS DE TELECOMUNICAÇÕES, ARMAS, OU SISTEMAS RELACIONADOS COM A SEGURANÇA DIRETA OU INDIRETA DA VIDA. TÃO POUCO ESTÁ INDICADO PARA APLICAÇÕES OU INSTALAÇÕES ONDE UM ERRO DE FUNCIONAMENTO PODERIA PROVOCAR A MORTE, DANOS FÍSICOS OU DANOS CONTRA A PROPRIEDADE.

PERMISSÃO PARA COMUNICADOS ELETRÔNICOS. BitDefender poderá ter que lhe enviar comunicados legais ou outros comunicados a respeito dos serviços de assinatura e Manutenção do Software ou a respeito de nosso uso de informação que você nos forneceu ("Comunicados"). A BitDefender enviará comunicados através de notas inseridas nos produtos, ou através do primeiro e-mail do usuário que registrou seu endereço de e-mail, ou colocar comunicados no website da BitDefender. Ao aceitar este Acordo, você consente em receber todos os comunicados através e somente destes meios eletrônicos e reconhece e demonstra que você pode acessar a comunicados via sites na internet.

TECNOLOGIA DE RECOLHIMENTO DE DADOS - A BitDefender informa que em certos programas ou produtos pode utilizar tecnologias de recolhimento de dados para coletar informações técnicas (incluindo arquivos suspeitos), para melhorar os produtos, para fornecer serviços relacionados, para adaptá-los e evitar a utilização ilegal ou sem licença do produto ou os danos resultantes de produtos malware. Você aceita que a BitDefender pode usar essas informações como parte dos serviços prestados em relação ao produto e para prevenir e parar a execução de programas malware no seu computador.

Você reconhece e aceita que o BitDefender pode fornecer atualizações ou complementos para o programa ou produto são automaticamente baixados para o seu computador.

Ao aceitar este acordo, você concorda em fazer o upload dos arquivos executáveis para o objetivo de serem analisados pelos servidores da BitDefender. Da mesma forma, para fins de contratação e utilização do programa, você pode ter que fornecer à BitDefender alguns dados pessoais. A BitDefender informa que irá tratar os seus dados pessoais em conformidade com a atual legislação aplicável e conforme estabelecido em sua Política de Privacidade.

RECOLHIMENTO DE DADOS. O acesso ao site pelo usuário e a aquisição de produtos e serviços e a utilização de ferramentas ou de conteúdo através do site implica o tratamento de dados pessoais. Em conformidade com a legislação que rege o processamento de dados pessoais e serviços da sociedade da informação e do comércio eletrônico é de extrema importância para a BitDefender. Às vezes, para acessar produtos, serviços, conteúdo ou ferramentas, você terá em alguns casos, a necessidade de fornecer certos detalhes pessoais. A BitDefender garante que tais dados serão tratados confidencialmente e em conformidade com a legislação relativa à proteção dos dados pessoais e da sociedade da informação e comércio eletrônico.

BitDefender cumpre com a legislação aplicável para proteção de dados e efetuou os procedimentos técnicos e administrativos necessários para garantir a segurança de seus dados pessoais que ele coletar.

Você declara que todos os dados que você fornecer serão verdadeiros e precisos e se compromete a informar a BitDefender de quaisquer alterações a esses dados. Você tem o direito de se opor ao tratamento de qualquer de seus dados que não

são essenciais para a execução do acordo e para a sua utilização para outros fins que não a manutenção da relação contratual.

No caso de você fornecer os detalhes de um terceiro, a BitDefender não deve ser responsabilizada pelo cumprimento dos princípios da informação e consentimento, e deve portanto ser você quem garante ter previamente informado e obtido o consentimento do proprietário dos dados, com a consideração de ter comunicado tais dados.

A BitDefender e suas afiliadas e parceiros irão enviar apenas informações de marketing por e-mail ou outros meios eletrônicos para os usuários que tenham dado o seu consentimento expresso para receber comunicações relativas a produtos ou serviços ou boletins informativos da BitDefender.

A política de privacidade da BitDefender garante-lhe o direito de acesso, retificação, eliminação e opor-se ao tratamento de dados através de notificação à BitDefender via e-mail: juridic@bitdefender.com.

GERAL. Este acordo será regido pelas leis da Roménia e pela regulamentação e tratados internacionais de direitos de autor. A jurisdição e foro exclusivo em caso de qualquer disputa que surja devido aos Termos desta Licença serão os tribunais da Roménia.

Em caso de não-validade de qualquer parte deste Acordo, a não-validade não afeta a validade das restantes partes deste Acordo.

BitDefender e os seus respectivos logotipos são marca registrada de BITDEFENDER. Todas as outras marcas registradas usadas no produto ou em materiais associados são propriedade de seus respectivos donos.

A licença cessará imediatamente e sem aviso se se encontrar a violar qualquer um dos pontos destes termos e condições. Não terá direito a um reembolso por parte de BITDEFENDER ou qualquer um dos revendedores de BitDefender como resultado da cessação da licença. Os termos e condições respeitantes à confidencialidade e restrições em uso manter-se-ão em vigor mesmo após a cessação da licença.

A BITDEFENDER poderá rever estes Termos a qualquer altura e os termos revistos serão automaticamente aplicáveis às versões correspondentes do Software distribuído com os termos revistos. Se qualquer parte destes Termos for encontrada como sendo desnecessária ou inaplicável, essa parte não afetará a validade dos restantes Termos, que permanecerão válidos e aplicáveis.

Em caso de controvérsia ou inconsistência entre as traduções destes Termos e outras línguas, a versão em Inglês emitida pela BITDEFENDER prevalecerá sobre todas as outras.

Contato BITDEFENDER, 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucareste, Romênia, Tel No: 40-21-206.34.70 Fax: 40-21-264.17.99, e-mail address: office@bitdefender.com.

Prefácio

Este guia é direcionado para todos os usuários que escolheram o **BitDefender Antivírus 2010** como a solução de segurança em seus computadores pessoais. A informação apresentada neste livro é aplicada não somente para usuários avançados de computação, mas também para qualquer pessoa que esteja apta a trabalhar com o sistema Windows.

Este livro irá descrever para você BitDefender Antivírus 2010, e irá guiá-lo através do processo de instalação, irá mostrar-lhe como configurá-lo. Você vai descobrir como usar o BitDefender Antivirus 2010, como atualizar, testar e personalizá-lo. Você vai aprender como obter o melhor do BitDefender.

Desejamos a você uma agradável e útil leitura.

1. Convenções usadas neste livro

1.1. Convenções tipográficas

Vários estilos de texto são usados no livro para aperfeiçoar a leitura. Seu aspecto e significado são apresentados na tabela abaixo.

Aparência	Descrição
`sample syntax`	Exemplos de sintaxe são impressos em caracteres do tipo `monospaced`.
http://www.bitdefender.com	As referências URL apontam para algum local externo, em servidores http ou ftp.
vendas@bitdefender.com.br	Mensagens de e-mail são inseridas no texto para informação sobre contato.
“Prefácio” (p. xiv)	Esta é uma referência interna, a algum lugar dentro do documento.
`filename`	Arquivos e pastas são impressos em caracteres do tipo `monospaced`.
option	Todas as opções do produtos são impressas em **negrito**.
`sample code listing`	Listas de código são impressos em caracteres do tipo `monospaced`.

1.2. Avisos

Os avisos estão em notas de texto, graficamente marcados, chamando a sua atenção para informação adicional relacionado ao parágrafo atual.

Nota
A nota é apenas uma breve observação. As notas providenciam informação valiosa, assim como uma função específica ou uma referência sobre um tópico relacionado.

Importante
Este requer sua atenção e não é recomendado deixar escapar. Normalmente providencia informação não crítica mas significante.

Atenção
Esta é uma informação crítica e deve ser tratada com cautela. Nada ruim acontecerá se você seguir as indicações. Você deve ler e entender tal informação, ela descreve algo de extreme risco.

2. Estrutura do Livro

O livro consiste de inúmeras partes contendo importantes tópicos Mais adiante, um glossário irá esclarecer alguns termos técnicos.

Instalação e Remoção. Instruções para instalar, passo a passo, o BitDefender num computador pessoal. Iniciando com os pré-quisitos para uma instalação com sucesso. Você será guiado através de todo o processo de instalação. Finalmente, o procedimento de remoção é descrito no caso de precisar desinstalar o BitDefender.

Introdução. Contém toda a informação que você precisa para começar com o BitDefender. Você é apresentado com a interface do BitDefender e como corrigir problemas, configurar definições básicas e registrar o seu produto.

Modo Intermediário. Apresenta a interface Modo Intermediário do BitDefender.

Modo Avançado. Uma apresentação detalhada da interface Modo Avançado do BitDefender. É-lhe ensinado como configurar e usar todos os módulos do BitDefender de forma a proteger eficientemente o seu computador contra todo o tipo de ameças de malware (vírus, spyware, rootkits e por aí fora).

Integração com o Windows e Programas de terceiros. Mostra como usar as opções do BitDefender no menu contextual do Windows e as barras de ferramentas integradas do BitDefender nos programas de terceiros suportados.

Como proceder. Fornece procedimentos para efetuar rapidamente as tarefas mais comuns no Bitdefender

Resolução de Problemas e Obtendo Ajuda. Onde procurar e onde perguntar por ajuda caso algo aconteça fora do esperado.

CD de Resgate BitDefender. Descrição do CD de Resgate BitDefender. Ajuda-o a compreender e a usar as características existentes neste CD de arranque.

Glossário. O Glossário tenta explicar alguns termos técnicos e incomuns que você pode encontrar nas páginas deste documento.

3. Convite a Comentários

Nós convidamos você a nos ajudar a melhorar o livro. Nós testamos e verificamos todas as informações na nossa habilidade. Por favor nos escreva sobre qualquer falha que você encontrar neste livro ou como você pensa que ele possa ser melhorado, para nos ajudar a providenciar a melhor documentação possível.

Mande-nos um e-mail para documentation@bitdefender.com.

Importante

Por favor escreva toda a sua documentação e e-mails em inglês de forma a que possamos dar-lhes seguimento de forma eficiente.

Instalação e Remoção

1. Requisitos de Sistema

Você pode instalar o BitDefender Antivírus 2010 apenas nos computadores com os seguintes sistemas operacionais:

- Windows XP (32/64 bit) com Service Pack 2 ou maior
- Windows Vista (32/64 bit) ou Windows Vista com Service Pack 1 ou maior
- Windows 7 (32/64 bit)

Antes da instalação, certifique-se que o seu computador cumpre com os requisitos mínimos de hardware e software.

Nota

Para ficar a saber que sistemo operativo o seu computador contém e a informação de hardware do mesmo, clique com o botão direito do mouse no ícone **Meu Computador** no Ambiente de Trabalho e depois selecione **Propriedades** do menu.

1.1. Requisitos Mínimos de Sistema

- 450 MB de espaço disponível em disco rígido
- Processador de 800 MHz
- Memória RAM:
  - 512 MB para Windows XP
  - 1 GB para Windows Vista e Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponível no kit de instalação)

1.2. Requerimentos Recomendados de Sistema

- 600 MB de espaço disponível em disco rígido
- Intel CORE Duo (1.66 GHz) ou processador equivalente
- Memória RAM:
  - 1 GB para Windows XP e Windows 7
  - 1.5 GB para Windows Vista
- Internet Explorer 7.0 (ou superior)
- .NET Framework 1.1 (disponível no kit de instalação)

1.3. Aplicativos Suportados

A proteção antiphising está disponível apenas para:

- Internet Explorer 6.0 (ou superior)
- Mozilla Firefox 2.5
- Yahoo! Messenger 8.5
- Windows Live Messenger 8

Criptografia para Instant Messaging (IM) está disponível para:

- Yahoo! Messenger 8.5
- Windows Live Messenger 8

2. Preparando para a Instalação

Antes de instalar o BitDefender Antivírus 2010, complete estes preparativos para assegurar que a instalação irá ocorrer suavemente:

- Assegure que o computador onde deseja instalar o BitDefender tenha os requerimentos mínimos de sistema. Se o computador não encontrar todos os requerimentos mínimos do sistema, o BitDefender não será instalado ou se instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade. Para uma lista completa de requerimentos de sistema, por favor consulte em "*Requisitos de Sistema*" (p. 2).
- Efetue logon no computador utilizando uma conta de Administrador.
- Remova qualquer outro software de segurança do seu computador. Rodando dois programas de segurança simultaneamente pode afetar o funcionamento deles e causar maiores problemas com o sistema. O Windows Defender será desabilitado por padrão antes da instalação iniciar.

3. Instalar BitDefender

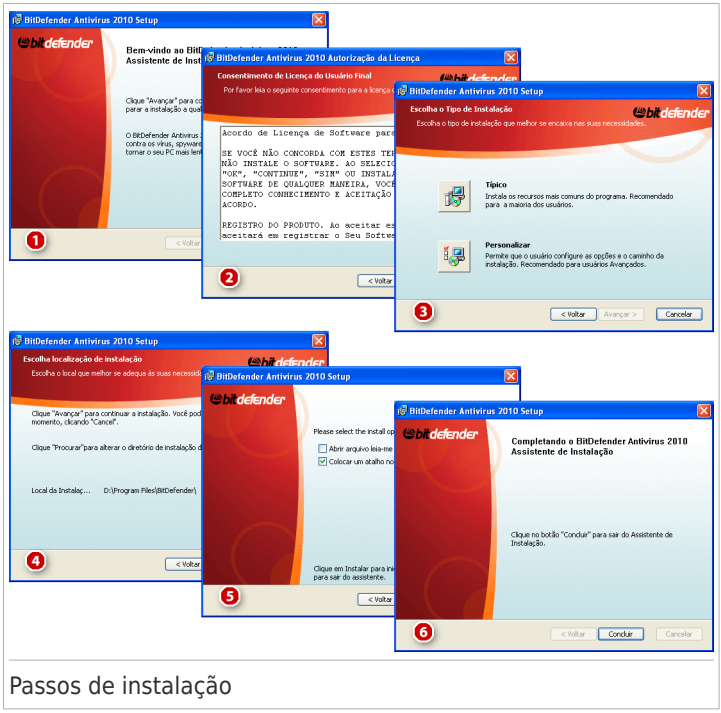
Você pode instalar o BitDefender de um CD de instalação ou usando um arquivo que fez o download do site da BitDefender ou de sites autorizados. (Por exemplo o site de um parceiro da BitDefender ou uma loja online). Você pode fazer o download do arquio de instalação do site da BitDefender no endereço a seguir: http://www.bitdefender.com/site/Downloads/.

Para instalar o BitDefender de um CD, insira o CD no drive. Uma tela de boas vindas deverá ser exibida em alguns instantes. Siga as instruções para iniciar a instalação.

Se a tela não aparecer, siga este caminho `Products\Antivirus\install\en\` do diretório raiz do CD e de um duplo clique em `runsetup.exe`.

Para instalar o BitDefender usando o arquivo de instalação que foi feito o download no seu computador, localize o arquivo e de um duplo clique sobre ele.

O instalador primeiro irá checar seu sistema para validar a instalação. Se a instalação estiver validada, o assistente de instalação irá aparecer. A seguinte imagem mostra os passos do assistente de instalação.



Passos de instalação

Siga estes passos para instalar o BitDefender Antivírus 2010:

1. Clique em **Próximo**. Você pode cancelar a instalação a qualquer momento se quiser clicando em **Cancelar**.

   O BitDefender Antivírus 2010 alertará você caso haja algum outro antivírus instalado no seu computador. Clique em **Remover** para começar a desinstalação do produto. Se deseja continuar sem remover os produtos detectados, clique em **Próximo**.

   Atenção
   É altamente recomendável que desinstale qualquer outro antivírus detectado antes de instalar BitDefender. Usar dois ou mais produtos antivírus ao mesmo tempo num computador pode bloquear totalmente o seu sistema.

2. Leia os termos do Acordo de Licença e clique em **Eu aceito**.

   Importante
   Se você não concordar com estes termos, clique em **Cancelar**. O processo de instalação será abandonado e você sairá da configuração.

3. Selecione o tipo de instalação a ser executada.

   - **Típica** - to install the program immediately, using the default installation options. Se escolher esta opção, pule o passo 6.
   - **Personalizada** - para configurar as opções da instalação e então instalar o programa. Esta opção permite que você troque o caminho da instalação.

4. Por padrão, o BitDefender Antivírus 2010 será instalado em `C:\Arquivos de Programas\BitDefender\BitDefender 2010`. Se você deseja selecionar outra pasta, clique **Procurar** e na janela que aparecerá, selecione a pasta que você deseja que o BitDefender seja instalado.

   Clique em **Próximo**.

5. Selecione as opções que tem a ver com o processo de instalação. Algumas delas serão selecionadas por padrão:

   - **Abra o arquivo leiame** - para abrir o arquivo leiame no final da instalação.
   - **Coloque um atalho na área de trabalho** - para colocar um atalho para o BitDefender Antivirus 2010 na área de trabalho de seu computador no final da instalação.
   - **Ejectar o CD quando a instalação terminar** - para obter que o CD seja ejetado no final da instalação esta opção aparece quando instala o produto a partir do CD.

- **Desabilitar o Caching de DNS** - para desabilitar o cashing de DNS (Domain Name System). O serviço DNS Client pode ser utilizado por aplicativos maliciosos para enviar informações pela estação de trabalho sem o seu consentimento.
- **Desligar o Windows Defender** - para desligar o Windows Defender; esta opção apenas surge no Windows Vista.

Clique em **Instalar** para começar a instalação do produto. Se aina não estiver instalado, o BitDefender instalará em primeiro lugar o .NET Framework 1.1.

6. Espere até que a instalação termine. Clique em **Finalizar**. Você será solicitada a reiniciar seu sistema para que o assistente complete o processo de instalação. Nós recomendamos que você o faça o mais rápido possível.

Importante

Após completar a instalação e reiniciar o computador, aparecerá um assistente de registo e um assistente de configuração . Complete os passos destes assistentes para registar e configurar o seu BitDefender Antivírus 2010 e criar uma conta BitDefender.

Se você aceitou as definições padrão do caminho da instalação, poderá ver em `Arquivos de Programas` uma nova pasta com o nome `BitDefender` que contém a subpasta `BitDefender 20010`.

3.1. Assistente de Registro

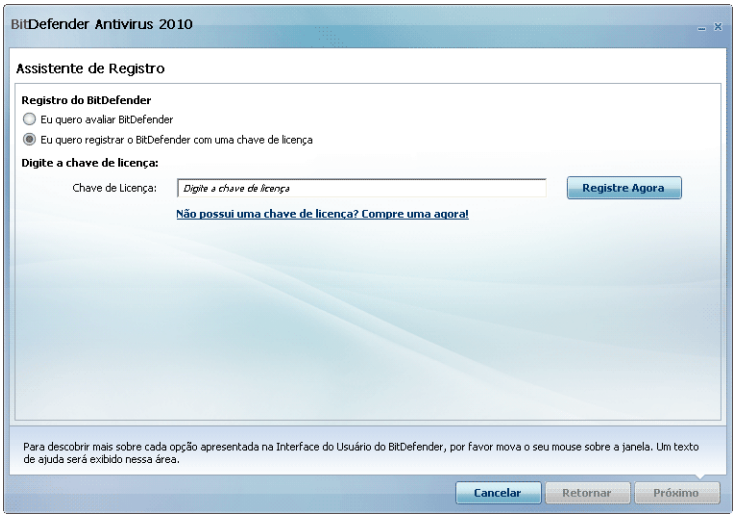
A primeira vez que iniciar o seu computador após a instalação um assistente de registo irá aparecer. O assistente ajuda-o a registar o seu BitDefender e a configurar uma conta BitDefender.

Você PRECISA criar uma conta BitDefender para poder receber as atualizações de virus da BitDefender. A conta BitDefender também lhe dá acesso a suporte técnico gratuito e promoções e ofertas especiais. Se perder a sua chave de licença BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Nota

Se você não quer seguir este assistente, clique em **Cancelar**. Pode abrir o assistente de registo a qualquer altura que deseje ao clicar no link **Registar** , localizado na parte de baixo do interface do usuário.

3.1.1. Passo 1/2 - Registar o BitDefender Antivirus 2010



Registro

BitDefender Antivirus 2010 vem com um período de teste de 30 dias. Para continuar avaliando este produto, selecione **Eu quero avaliar o BitDefender** e clique **Próximo**.

Para registrar o BitDefender Antivírus 2010:

1. Selecione **Eu quero avaliar o BitDefender com uma chave de licença**.
2. Insira a chave de licença no campo de edição.

Nota

Pode encontrar a sua chave de licença:

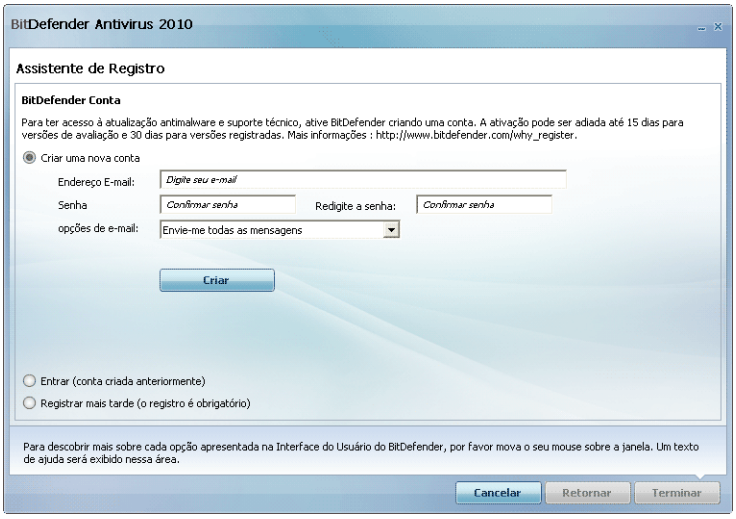
- Na bolsa do CD.
- ou no cartão de registo do produto.
- no e-mail da sua compra on-line.

Se não possuir uma chave de licença BitDefender, clique no link que lhe facultamos para ir até à loja on-line do BitDefender e adquirir uma.

3. Clique **Registrar Agora**.
4. Clique em **Próximo**.

Se uma chave de licença válida do BitDefender for detectada no seu sistema, você pode continuar usando esta chave clicando em **Próximo**.

3.1.2. Passo 2/2 - Criar uma conta BitDefender



Criar uma Conta

Se não deseja criar uma conta BitDefender neste momento, selecione **Registrar mais tarde** e clique em **Terminar**. De outra forma, actue de acordo com a sua presente situação:

- "Não tenho uma conta BitDefender" (p. 9)
- "Já tenho uma conta BitDefender" (p. 10)

Importante

Você deve criar uma conta dentro de 15 dias após instalar o BitDefender (Se você registrar com uma chave de licença, o prazo limitie é extendido para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus.

Não tenho uma conta BitDefender

Para criar uma conta BitDefender com sucesso, siga estes passos:

1. Selecione **Criar uma nova conta**.
2. Digite as informações necessárias nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   - **E-mail** - insira o seu endereço de e-mail.

- **Senha** - insira uma Senha para a sua conta BitDefender. A senha deve ter entre 6 e 16 caracteres de tamanho.
- **Re-insira a senha** - insira novamente a senha previamente definida.

Nota
Uma vez que a conta é ativada, você pode usar o endereço de e-mail fornecido e senha para fazer o log in na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Selecione uma das opções disponíveis do menu:
   - **Enviar todas as mensagens**
   - **Enviem-me apenas mensagens referentes ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique **Criar**.
5. Clique **Finalizar** para completar o assistente.
6. **Ative sua conta.** Antes de ser capaz de usar a sua conta, você deve ativá-la. Verifique seu e-mail e siga as instruções no e-mail enviado a você pelo serviço de registro da BitDefender.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Neste caso, forneça a senha de sua conta e clique em **Entrar**. Clique **Finalizar** para completar o assistente.

Se você já tiver uma conta ativa, mas o BitDefender não a detectou, siga estes passos para registrar o produto para aquela conta:

1. Selecione **Entrar (na conta criada previamente)**.
2. Digite o endereço de email e senha da sua conta nos campos correspondentes.

Nota
Se não se lembra da sua senha, clique em **Esqueceu a sua senha?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Selecione uma das opções disponíveis do menu:
   - **Enviar todas as mensagens**
   - **Enviem-me apenas mensagens referentes ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Entrar**.

5. Clique **Finalizar** para completar o assistente.

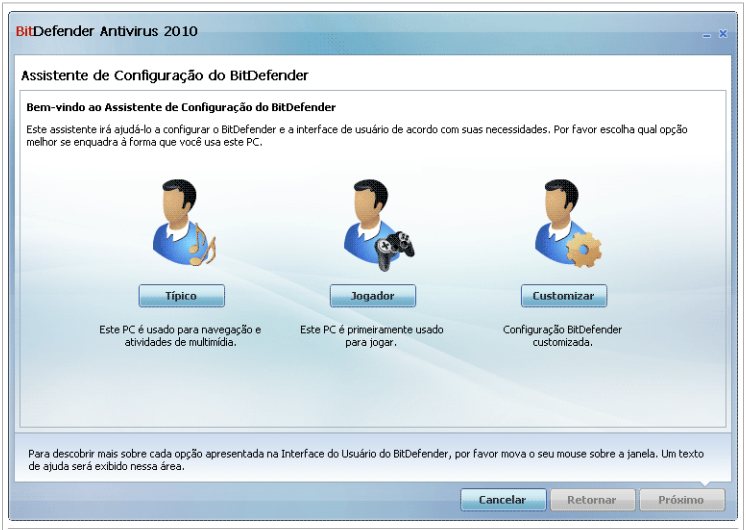
3.2. Assistente de Configuração

Um vez completado o asssitente de registo, aparecerá o assistente de configuração. Este assistente ajuda você a configurar as principais configurações do BitDefender e a interface do usuário, para que ele atenda suas necessidades melhor. No final do assistente, você pode atualizar os arquivos do produto, assinaturas malware, analisar os arquivos de sistemas e aplicações para assegurar que eles não estejam infectados.

O assistente consiste em simples e poucos passos. O número de passos depende das escolhas que você fizer. Todos os passos são apresentados aqui, mas você será notificado quando suas escolhas afetarem aquele número.

Completar este assistente não é obrigatório; no entanto, nós recomendamos que o faça para poupar seu tempo e assegurar a segurança do seu sistema mesmo antes do BitDefender Antivírus ser instalado. Se você não quer seguir este assistente, clique em **Cancelar**. BitDefender irá notificá-lo sobre os componentes que necessita de configurar quando abrir o interface do usuário.

3.2.1. Passo 1 - Selecionar o Perfil de Uso



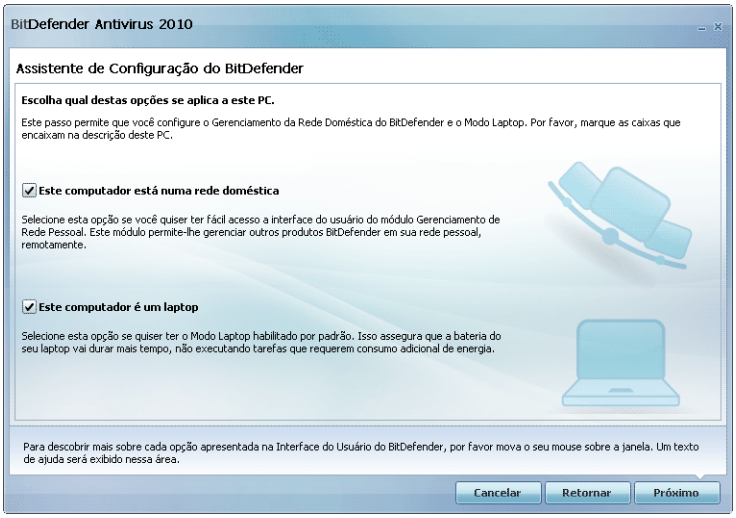
Perfis de Utilização

Clique no botão que melhor descreve as atividades realizadas no computador (o perfil de utilização).

Opção	Descrição
Típica	Clique aqui se este PC é usado principalmente para navegação e atividades multimídia.
Gamer	Clique aqui, se este PC é basicamente usado para jogar.
Personalizada	Clique aqui se você deseja configurar todos os principais recursos do BitDefender.

Você pode reiniciar mais tarde o perfil de uso a partir da interface do produto.

3.2.2. Passo 2 - Descreva o Computador



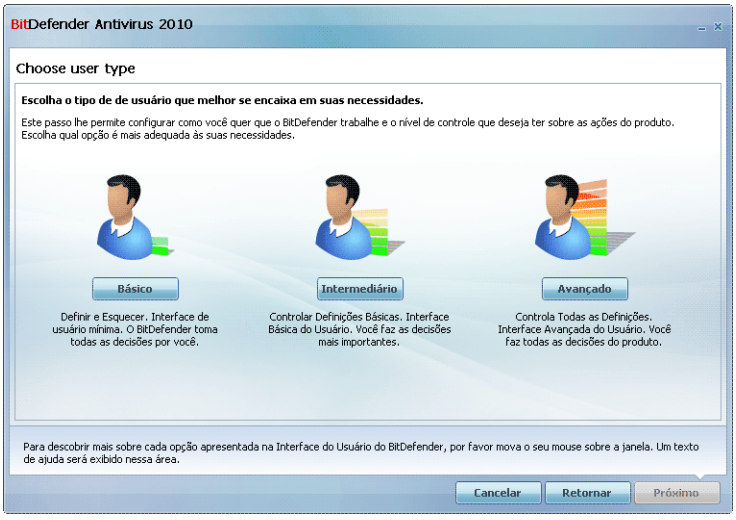
Descrição do Computador

Selecione a opção que se aplica a seu computador:

- **Este computador está numa rede doméstica.** Selecione esta opção se você deseja gerenciar remotamente (de um outro computador) o produto BtDefender que você instalou neste computador. Um passo adicional do assistente permitirá você configurar o módulo de Gerenciamento da Rede Doméstica.
- **Este computador é um laptop.** Selecione esta opção se você deseja ter habilitado o Modo LapTop como padrão. Equanto em Modo Laptop, varreduras agendadas não serão executadas, como elas necessitam de mais recursos do sistema e alto consumo de energia.

Clique em **Seguinte** para continuar.

3.2.3. Passo 3 - Selecione a Interface de Usuário



Modos de Visualização da Interface do usuário

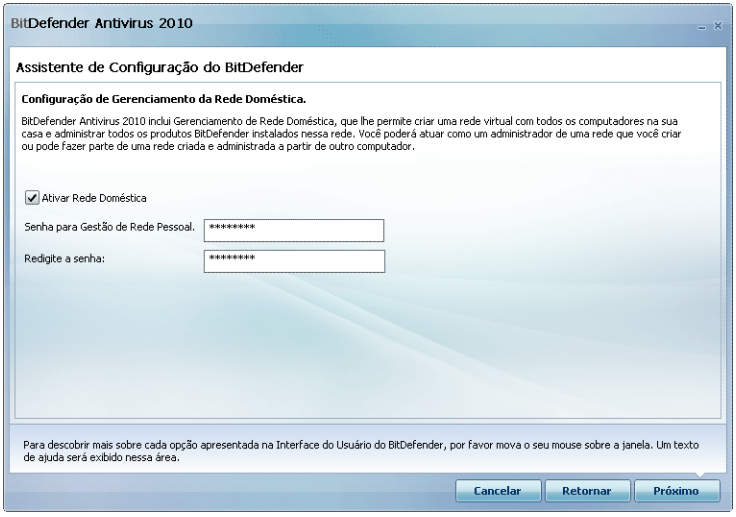
Clique aqui no botão que melhor descreve seus conhecimentos de computador para selecionar um modo de visualização da interface de usuário apropriada ao seu perfil. Você pode optar por ver a interface do usuário em qualquer dos três modos, dependendo do seu nível de conhecimento de computadores e de sua experiência anterior com o BitDefender.

Modo	Descrição
Mode Iniciante	Apropriado para iniciantes em computadores e pessoas que querem o BitDefender para proteger seu computador e dados sem serem incomodados. Este modo é simples de usar e requer mínima interação. Tudo que você tem que fazer é corrigir os problemas atuais quando indicado pelo BitDefender. Uma guia intuitivo passo-a-passo lhe auxilia na resolução dos problemas. Além disso, você pode efetuar tarefas comuns, tal como atualizar as vacinas antivírus da BitDefender e arquivos de produtos, ou analisar o computador.

Modo	Descrição
Modo Intermediário	Destinado a usuários com conhecimentos médios de informática, este modo estende o que você pode fazer no Modo Iniciante. Você pode corrigir os problemas separadamente e escolher quais problemas monitorar. Além disso, você pode gerenciar remotamente os produtos BitDefender instalados nos computadores de sua casa.
Modo Avançado	Destinado para os usuários mais técnicos, este modo permite configurar completamente cada funcionalidade do BitDefender. Voce também pode usar todas as tarefas disponíveis para proteger seu computador e dados.

3.2.4. Passo 4 - Configurar a Rede BitDefender

Nota
Este passo aparece somente se você especificou que o computador está conectado a uma rede doméstica no passo 2.



Configuração da Rede BitDefender

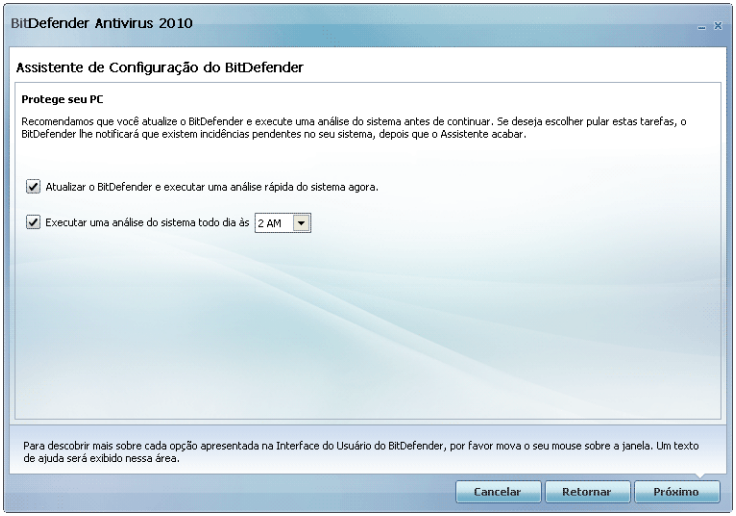
BitDefender permite-lhe criar uma rede virtual com os computadores do seu lar e a administrar os produtos BitDefender instalados nessa rede.

Se você deseja que este computador faça parte da Rede Doméstica do BitDefender, siga estes passos:

1. Selecione **Habilitar Rede Doméstica**.
2. Insira a mesma senha administrativa em cada um dos campos de edição. A senha permite ao administrador gerir os produtos BitDefender noutro computador.

Clique em **Seguinte** para continuar.

3.2.5. Passo 5 - Selecione as Tarefas a Executar



Seleção das Tarefas

Configure o BitDefender para executar importantes tarefas para a segurança de seu computador. As seguintes opções estão disponíveis:

- **Atualize o BitDefender e execute uma análise rápida do sistema agora** - durante o próximo passo, as vacinas contra vírus e os arquivos do produto do BitDefender serão atualizados para proteger seu computador contra as ameaças mais recentes. Também, imediatamente após a atualização finalizar, o BitDefender analisará os arquivos das pastas do `Windows` e `Arquivos de Programas` para certificar-se que eles não estão infectados. Estas pastas contêm arquivos do sistema operacional e de aplicativos instalados e estes são geralmente, os primeiros a serem infectados.
- **Execute uma Análise de Sistema todo dia às 2 AM** - configura o BitDefender para executar uma análise padrão de seu computador todo os dias `as 2 AM. Para

mudar a hora em que a análise é executada, clique o menu e selecione o tempo de início desejado. Se o computador for desligado na hora agendada da análise, esta será executada na próxima vez em que você reiniciar o computador.

Nota

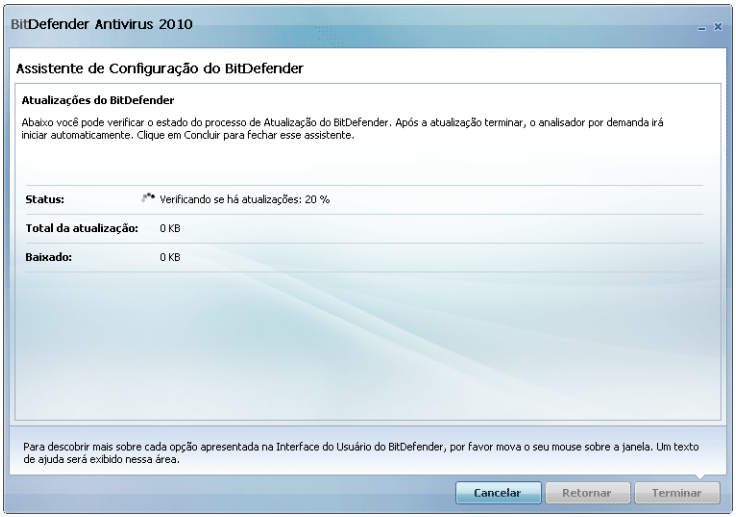
Se mais tarde você desejar mudar a data em que análise foi programada para ser executada, siga estes passos:

1. Abra o BitDefender e troque a interface de usuário para Modo Avançado.
2. Clique em **Antivírus** no menu do lado esquerdo.
3. Clique na aba **Análise Vírus Scan**.
4. Clique com o botão direito do mouse a tarefa **Análise de Sistema** e selecione **Agendar**. Uma nova janela irá aparecer.
5. Altere a frequência e a hora de início como desejar.
6. Clique em **OK** para salvar as alterações.

Recomendamos que tenha estas opções ativas antes de avançar para o próximo passo de forma a assegurar a segurança do seu sistema. Clique em **Seguinte** para continuar.

Se você desmarcar a primeira caixa, não haverá tarefas a serem executadas no último passo do assistente. Clique **Finalizar** para completar o assistente.

3.2.6. Passo 6 - Finalizar



Estado das Tarefas

Aguarde o BitDefender atualizar suas vacinas antimalware e o mecanismo de análise. Assim que a atualização estiver completa, uma rápida análise do sistema será iniciada. A análise será executada silenciosamente no computador, enquanto você o utiliza. Você pode notar o o ícone de andamento na área de notificação. Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da análise.

Clique **Finalizar** para completar o assistente. Você não precisa aguardar o término da análise.

Nota

A análise levará alguns minutos. Quando estiver finalizada, abra a janela de análise e verifique os resultados desta ação, para ver se o sistema está limpo. Se vírus foram detectados durante a análise, você pode abrir o BitDefender imediatamente e executar uma análise completa do sistema.

4. Atualização de versão

Você pode fazer o upgrade do BitDefender Anivirus 2010 se você estiver usando o BitDefender Antivirus 2010 beta, ou as versões 2008 ou 2009.

Há duas formas de executar o upgrade:

- Instalar o BitDefender Antivirus 2010 encima da antiga versão.
- Remover a versão antiga, então reinicie o computador e instale a nova versão descrita no capítulo "*Instalar BitDefender*" (p. 5). Nenhuma configuração do produto será salva. Use este método de upgrade se o outro falhar.

5. Remover ou Reparar o BitDefender

Se você deseja reparar ou remover o BitDefender Antivírus 2010, siga o caminho através do menu Iniciar do Windows: **Iniciar → Programas → BitDefender 2010 → Reparar ou Remover**.

Você terá que confirmar a opção clicando em **Próximo**. Uma nova janela aparecerá e você pode selecionar:

- **Reparar** - para reinstalar todos os componentes do programa instalados pelo passo anterior.

  Se escolher reparar o BitDefender, surgirá uma nova janela. Clique em **Reparar** para dar início ao processo de reparação.

  Reinicie o computador quando for solicitado, e depois clique em **Instalar** para reinstalar o BitDefender Antivírus 2010.

  Uma vez terminado o processo de intalação, surgirá uma nova janela. Clique em **Finalizar**.

- **Remover** - para remover todos os componentes instalados.

  Nota
  Recomendamos que escolha **Desinstalar** para uma reinstalação limpa.

  Se escolher desinstalar BitDefender, surgirá uma nova janela.

  Importante

  Apenas Windows Vista! Ao remover BitDefender, deixará de estar protegido contra as ameaças de malware, tais como vírus e spyware. Se deseja que o Windows Defender seja ativado após a desinstalação do BitDefender, selecione a respectiva caixa de seleção.

  Clique em **Desinstalar** para dar início à desinstalação do BitDefender Antivirus 2010 do seu computador.

  Durante o processo de desinstalação será solicitado o seu feedback. Por favor clique em **OK** para responder a um inquérito online que consiste apenas de cinco pequenas perguntas. Se não pretender responder ao inquérito clique em **Cancelar**.

  Uma vez terminada a desinstalação, surgirá uma nova janela. Clique em **Finalizar**.

  Nota
  Quando o processo de desinstalação tiver terminado, recomendamos que elimine a pasta `BitDefender` dos `Programas`.

Introdução

6. Sumário

Uma vez instalado o BitDefender o seu computador fica protegido. Se você ainda não completou o Assistente de configuração, você deve abrir o BitDefender o mais rápido possível e corrigir os problemas existentes. Você pode ter que configurar componentes específicos do BitDefender ou tomar ações preventivas para proteger seu computador e seus dados. Se você desejar, pode configurar o BitDefender para não lhe alertar sobre problemas específicos.

Se você ainda não registrou o produto (incluindo a criação da conta BitDefender), lembre-se de fazê-lo antes do término do período de experiência. Você deve criar uma conta dentro de 15 dias após instalar o BitDefender (Se você registrar com uma chave de licença, o prazo limitie é extendido para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus. Para mais informações sobre o processo de registro, por favor consulte a seção "*Registro e Minha Conta*" (p. 46).

6.1. Abrindo o BitDefender

Para acessar a interface principal do BitDefender Antivírus 2010, utilize o menu Iniciar do Windows, seguindo o caminho **Iniciar → Programas → BitDefender 2010 → BitDefender Antivírus 2010** ou mais rápido, dando um duplo clique no ícone do BitDefender na Área de notificação.

6.2. Modos de Visualização da Interface do usuário

O BitDefender Antivírus 2010 vai de encontro às necessidades tanto de iniciantes como de pessoas mais técnicas. Sua interface gráfica do usuário foi desenhada para facilitar o uso de ambos.

Você pode optar por ver a interface do usuário em qualquer dos três modos, dependendo do seu nível de conhecimento de computadores e de sua experiência anterior com o BitDefender.

Modo	Descrição
Mode Iniciante	Apropriado para iniciantes em computadores e pessoas que querem o BitDefender para proteger seu computador e dados sem serem incomodados. Este modo é simples de usar e requer mínima interação. Tudo que você tem que fazer é corrigir os problemas atuais quando indicado pelo BitDefender. Uma guia intuitivo passo-a-passo lhe auxilia na resolução dos problemas. Além disso, você pode efetuar tarefas comuns, tal como atualizar as vacinas antivírus da

Modo	Descrição
	BitDefender e arquivos de produtos, ou analisar o computador.
Modo Intermediário	Destinado a usuários com conhecimentos médios de informática, este modo estende o que você pode fazer no Modo Iniciante. Você pode corrigir os problemas separadamente e escolher quais problemas monitorar. Além disso, você pode gerenciar remotamente os produtos BitDefender instalados nos computadores de sua casa.
Modo Avançado	Destinado para os usuários mais técnicos, este modo permite configurar completamente cada funcionalidade do BitDefender. Voce também pode usar todas as tarefas disponíveis para proteger seu computador e dados.

O modo de interface de usuário esta selecionado no assistente de configuração. Este assistente aparece após o assistente de registro, a primeira vez que você liga o computador após instalar o produto. Se você cancelar o assistente de registro ou assistente de configuração, o modo de interface de usuário se tornará padrão para Modo Intermediário.

Para o mudar o modo de interface de usuário, siga estes passos:

1. Abra o BitDefender.
2. Clique no botão **Configurações** no canto superior direito da janela.
3. Na categoria de Configurações da Interface do Usuário, clique na seta no botão e selecione o modo desejado a partir do menu.
4. Clique**OK** para salvar e aplicar as alterações.

6.2.1. Modo Básico

Se você é usuário básico do computador, mostrando a interface de usuário básico pode ser a escolha mais adequada para você. Este modo é simples de usar e requer interação mínima do usuário.

Modo Básico

Esta janela é organizada em três seções principais:

- **Statius de Segurança** informa quais problemas afetam a segurança do seu computador e ajuda a corrigi-los. Clicando **Corrigir todos erros**, um assistente irá ajuda-lo facilmente a remover qualquer ameaça ao seu computador e seus dados. Para informação detalhada, por favor consulte "*Reparando Incidências*" (p. 36).
- **Proteja seu PC** é onde você pode achar as tarefas necessárias para proteger seu computador e dados. As tarefas disponíveis que você pode executar são diferentes, dependendo do perfil de uso selecionado.
  - O botão **Analisar Agora** inicia uma análise padrão de seu sistema à procura de vírus, spywares e outros malwares. O assistente de varredura irá aparecer e guiar você através do processo de varredura. Para informações detalhadas sobre esse assistente, por favor consulte a seção "*Assistente do analisador Antivírus*" (p. 51).
  - O botão **Atualizar Agora** lhe ajuda a atualizar as vacinas contra vírus e arquivos de produtos da BitDefender. Uma nova janela aparecerá, onde você pode ver o status da atualização. Se algumas atualizações forem detectadas, estas serão automaticamente baixadas e instaladas em seu computador.
  - Quando o perfil **Típico** é selecionado, o botão **Checar Vulnerabilidades** inicia um assistente que lhe ajuda a encontrar e consertar vulnerabilidades do sistema, tais como softwares desatualizados ou atualizações perdidas do Windows. Para

informação mais detalhada, por favor vá para a seção "*Assistente de Verificação de Vulnerabilidades*" (p. 63).

- Quando o perfil **Jogador** é selecionado, o botão **Ligar/Desligar Modo Jogo** permite habilitar/desabilitar o Modo Jogo. O Modo de Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema.

- **Proteja Seu PC** é onde você pode encontrar tarefas adicionais para proteger seu computador e dados.
  - **Análise Minuciosa** inicia uma varredura de seu sistema para todos os tipos de malware.
  - **Análise dos Meus Documentos** analisa à procura de vírus e outros malwares os seus diretórios mais utilizados: `Meus Documentos` e `Área de Trabalho`. Isto irá garantir a segurança dos seus documentos, um trabalho seguro e aplicações limpas executadas durante a inicialização.
  - **Análise de Autologon** analisa os itens que são executados ao iniciar o Windows.

No canto superior direito da janela, você pode ver o botão **Configurações**. Ele abre uma janela onde você pode mudar o modo de interface do usuário e ativar ou desativar as principais definições do BitDefender. Para informação detalhada, por favor consulte em "*Definindo Configurações Básicas*" (p. 39).

No canto inferior direito da janela, você pode encontrar diversos links úteis.

Link	Descrição
Comprar/Renovar	Abre uma página web onde você pode comprar uma chave de licença para o seu produto BitDefender Antivírus 2010.
Registro	Permite-lhe inserir uma nova licença ou ver a atual e o status do seu registo.
Ajuda & Suporte	Dá acesso a um arquivo de ajuda que mostra como utilizar o BitDefender.

6.2.2. Modo Intermediário

Destinado a usuários com conhecimento médio de informática, o Modo Intermediário é uma interface simples que lhe dá acesso a todos os módulos em um nível básico. Você terá que acompanhar as advertências e alertas críticos e corrigir problemas indesejáveis.

Modo Intermediário

A janela de modo intermediário consiste em 5 guias. A tabela a seguir descreve brevemente cada guia. Para informações detalhadas, por favor consulte a "Modo Intermediário" (p. 70) parte deste guia.

Barra	Descrição
Painel	Exibe o status de segurança de seu sistema e deixa que você reinicie o perfil de uso.
Antivírus	Exibe o status do módulo Antivirus que lhe ajuda a manter o seu BitDefender atualizado e o seu computador livre de vírus.
Antiphishing	Mostra a situação dos módulos que o protege contra phishing (roubo de informações pessoais) enquanto você está online.
Vulnerabilidade	Mostra o status do módulo de Vulnerabilidades que o ajuda a manter atualizados os softwares cruciais para seu PC. Aqui você pode facilmente corrigir qualquer vulnerabilidade que pode afetar a segurança de seu computador.
Rede	Mosta a estrutura da rede pessoal BitDefender. Aqui você pode executar várias ações para configurar e gerenciar os produtos BitDefender instalados em sua rede doméstica. Dessa forma, você pode gerenciar a segurança de sua rede doméstica de um único computador.

No canto superior direito da janela, você pode ver o botão **Configurações**. Ele abre uma janela onde você pode mudar o modo de interface do usuário e ativar ou desativar as principais definições do BitDefender. Para informação detalhada, por favor consulte em "*Definindo Configurações Básicas*" (p. 39).

No canto inferior direito da janela, você pode encontrar diversos links úteis.

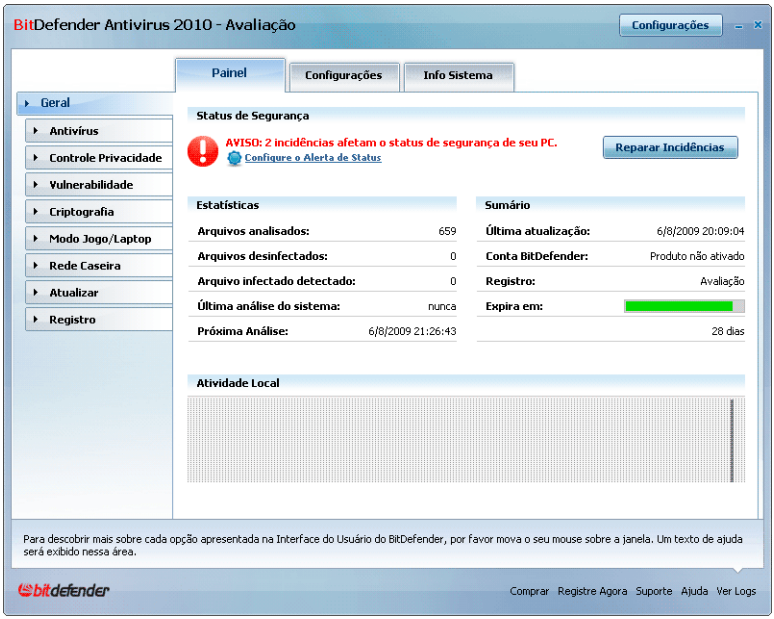
Link	Descrição
Comprar/Renovar	Abre uma página web onde você pode comprar uma chave de licença para o seu produto BitDefender Antivírus 2010.
Registar	Permite-lhe inserir uma nova licença ou ver a atual e o status do seu registo.
Suporte	Permite o contato com a equipa de suporte BitDefender.
Ajuda	Dá acesso a um arquivo de ajuda que mostra como utilizar o BitDefender.
Visualizar Relatórios	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

6.2.3. Modo Avançado

O Modo avançado lhe dá acesso específico a cada componente do BitDefender, onde você pode configurar o BitDefender em detalhes.

Nota

O Modo Avançado é designado para usuários com maior conhecimento de computadores, que sabem o tipo de ameaças que um computador está exposto e como programas de segurança trabalham.



Modo Avançado

Do lado esquerdo da janela existe um menu que contém todos os módulos de segurança. Cada módulo possui uma ou mais abas onde você pode configurar as definições de segurança correspondentes ou executar tarefas administrativas ou de segurança. A tabela a seguir descreve brevemente cada módulo. Para informações detalhadas, por favor consulte a "Modo Avançado" (p. 92) parte deste guia.

Módulo	Descrição
Geral	Permite-lhe accessar às definições gerais ou ver o painel e a info detalhada do sistema.
Antivírus	Permite-lhe configurar o escudo de vírus e as operações de análise em detalhe, definir exceções e configurar o módulo de quarentena.
Controle de Privacidade	Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.
Vulnerabilidade	Permite-lhe manter atualizados os softwares cruciais para o seu PC.

Módulo	Descrição
Criptografia	Permite-lhe criptografar as comunicações via Yahoo! MSN e Windows Live (MSN) Messenger.
Modo de Jogo/Portátil	Permite-lhe adiar as tarefas agendadas BitDefender enquanto o seu portátil está a funcionar a bateria e também elimina alertas e pop-ups enquanto está a jogar.
Rede	Permite-lhe configurar e gerir vários computadores do seu lar.
Atualização	Permite-lhe obter informação das últimas atualizações, atualizar o produto e configurar o processo de atualização em detalhe.
Registro	Permite você registrar o BitDefender Antivirus 2010, para criar a chave de licença ou para criar a conta BitDefender.

No canto superior direito da janela, você pode ver o botão **Configurações**. Ele abre uma janela onde você pode mudar o modo de interface do usuário e ativar ou desativar as principais definições do BitDefender. Para informação detalhada, por favor consulte em "*Definindo Configurações Básicas*" (p. 39).

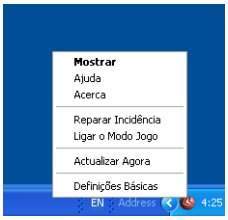
No canto inferior direito da janela, você pode encontrar diversos links úteis.

Link	Descrição
Comprar/Renovar	Abre uma página web onde você pode comprar uma chave de licença para o seu produto BitDefender Antivírus 2010.
Registar	Permite-lhe inserir uma nova licença ou ver a atual e o status do seu registo.
Suporte	Permite o contato com a equipa de suporte BitDefender.
Ajuda	Dá acesso a um arquivo de ajuda que mostra como utilizar o BitDefender.
Visualizar Relatórios	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

6.3. Ícone da Área de Notificação

Para gerenciar todo o produto mais rapidamente, você pode usar o ícone do BitDefender na área de notificação. Se fizer um duplo-clique neste ícone, o BitDefender irá abrir. Clicando com o botão direito do mouse sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do BitDefender.

- **Mostrar** - abre a interface principal do BitDefender.
- **Help** - abre o arquivo de ajuda, o qual explica em detalhes como configurar e suar o BitDefender Antivirus 2010.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.



Ícone da área de notificação

- **Corrigir todos os problemas** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, não há problemas a serem corrigidos. Para informação detalhada, por favor consulte "*Reparando Incidências*" (p. 36).
- **Alternar o Modo Jogo ligado/desligado** - ativa/desativa o Modo Jogo.
- **Atualizar agora** - realiza uma atualização imediata. Uma nova janela aparecerá, onde você pode ver o status da atualização.
- **Configurações Básicas** - abre uma janela onde você pode trocar o modo de interface de usuário e habilitar ou desabilitar as principais configurações do produto. Para mais informações, por favor consulte em "*Definindo Configurações Básicas*" (p. 39).

O ícone da área de notificação do BitDefender lhe informa quando problemas afetam seu computador ou como o produto é operado, ao mostrar um símbolo especial, como segue:

Triângulo vermelho com um ponto de exclamação: Problemas críticos afetam a segurança de seu sistema. Eles requerem sua atenção imediata e devem ser corrigidos assim que possível.

Triângulo amarelo com um ponto de exclamação: Problemas não críticos afetam a segurança de seu sistema. Você deve verificar e corrigí-los quando tiver tempo.

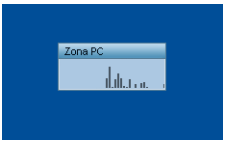
Letter G: The product operates in Game Mode.

Se o BitDefender não estiver funcionando, o ícone na área de notificação estará cinza . Isso geralmente ocorre quando a chave de licença expirou. Isso pode ocorrer também quando os serviços do BitDefender não estão respondendo ou quando outros erros afetam a operação normal do BitDefender.

6.4. Barra de Atividade da Análise

A **Barra de atividade de verificação** é uma visualização gráfica da atividade de verificação em seu sistema. Esta pequena janela esta disponível por padrão apenas noModo Avançado.

As barras cinzentas (a **zona PC**) mostram o número de arquivos analisados por segundo, numa escala de 0 a 50.

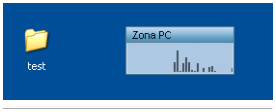


Barra de Atividade da Análise

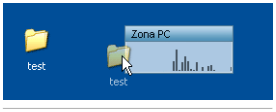
Nota
A Barra de Atividade da Análise irá avisá-lo quando a proteção em tempo-real está desativada ao mostrar-lhe uma cruz vermelha sobre a **Zona de Arquivos**).

6.4.1. Analisa Arquivos e Diretórios

Você pode utilizar a barra de atividade da Análise para rapidamente analisar arquivos e diretórios. Arraste o arquivo ou pasta que você quer verificado e solte-o sobre a **Barra de Atividade**, como nas imagens abaixo.



Arraste o arquivo



Solte o arquivo

O assistente de varredura irá aparecer e guiar você através do processo de varredura. Para informações detalhadas sobre esse assistente, por favor consulte a seção "*Assistente do analisador Antivírus*" (p. 51).

Opções de detecção. As opções de análise são pré-configuradas para obter os melhores resultados em detecção. Se arquivos infectados forem detectados, o BitDefender irá tentar os desinfectar (remover o código malware). Se a desinfecção falhar, o wizard do analisador Antivírus irá permitir que você especifique outras ações a serem tomadas nos arquivos infectados. As opções de análise são padrão e você não pode as alterar.

6.4.2. Desabilitar/Restaurar a Barra de Atividade da Análise

Quando você não quiser mais a visualização gráfica, basta clicar nela com o botão direito e escolher **Ocultar**. Para restaurar a barra de atividade da Análise, siga os seguintes passos:

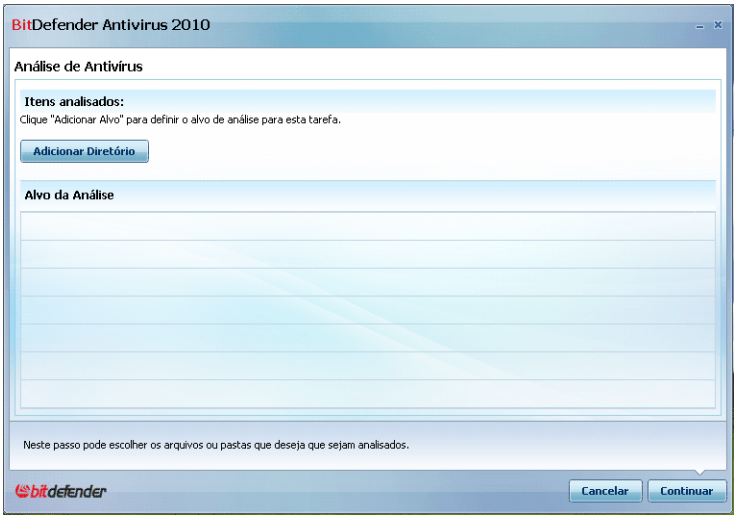
1. Abra o BitDefender.

2. Clique no botão **Configurações** no canto superior direito da janela.
3. Na categoria de Configurações Gerais, marque a opção correspondente a**Barra de Atividade de Análise**.
4. Clique**OK** para salvar e aplicar as alterações.

6.5. Análise Manual BitDefender

A análise Manual do BitDefender permite que você especifique o diretório ou a partição do disco rígido sem a necessidade de criar uma tarefa de análise. Essa característica foi designada para ser utilizada quando o Windows está sendo executado no Modo de Segurança. Se seu sistema está infectado com um vírus resistente, você pode tentar removê-lo iniciando o Windows em Modo de Segurança e analisar cada partição do disco utilizando a Análise Manual do BitDefender.

Para acessar o manual de varredura BitDefender, use o menu iniciar do Windows, pelo caminho a seguir**Iniciar → Programas → BitDefender 2010 → Manual de varredura BitDefender** A seguinte análise irá aparecer:



Análise Manual BitDefender

Clique **Adicionar Pasta**, selecione o destino que você deseja analisar e clique **OK**. Se você quiser analisar multiplas pastas, repita esta ação para cada localidade adicional.

O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela. Clique no botão

Remover Todos Caminhos para remover todas as localizações que foram adicionadas à lista.

Quando você terminar de selecionar os locais, clique **Continuar**. O assistente de varredura irá aparecer e guiar você através do processo de varredura. Para informações detalhadas sobre esse assistente, por favor consulte a seção "*Assistente do analisador Antivírus*" (p. 51).

Opções de detecção. As opções de análise são pré-configuradas para obter os melhores resultados em detecção. Se arquivos infectados forem detectados, o BitDefender irá tentar os desinfectar (remover o código malware). Se a desinfecção falhar, o wizard do analisador Antivírus irá permitir que você especifique outras ações a serem tomadas nos arquivos infectados. As opções de análise são padrão e você não pode as alterar.

O que é Modo de Segurança?
O Modo de Segurança é um modo especial de iniciar o Windows, utilizado principalmente para resolver problemas afetando a operação normal do sistema. Esses problemas variam de conflitos em drivers até vírus que não permitem que o Windows inicie normalmente. No Modo de Segurança, o Windows carrega apenas o mínimo de componentes e drivers básicos do sistema operacional. Apenas poucos aplicativos trabalham no Modo de Segurança. É por essa razão que a maioria dos vírus estão inativos e podem ser facilmente removidos, quando utilizamos o Windows em Modo de Segurança.
Para iniciar o Windows no Modo de Segurança, reinicie seu computador e aperte a tecla F8 até aparecer o menu Opções Avançadas do Windows. Você pode escolher várias opções de inicialização no Modo de Segurança. Você pode desejar escolher a opção **Modo de Segurança com Rede** para poder acessar a internet.

Nota

Para mais informações sobre o Modo de Segurança, visite a página de Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**). Você também pode encontrar informações úteis ao pesquisar na internet.

6.6. Modo Jogo e Modo Laptop

Algumas atividades do computador, como jogos ou apresentações, requerem melhor resposta do sistema e performace e sem interrupções. Quando seu laptop esta operando funcionando com a bateria, o melhor é que operações desnecessárias, que consomem energia, sejam adiadas até que o laptop esteja ligado a uma rede de energia.

Para se adaptar a estas situações particulares, o Antivirus BitDefender 2010 inclui dois modos especiais de operação:

- Modo Jogo
- Modo Laptop

6.6.1. Modo de Jogo

O Modo de Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema. Quando liga o Modo de Jogo, as seguintes definições são aplicadas:

- Minimiza o tempo de processador & consumo de memória
- Adia análises e atualizações & automáticas
- Elimina todos os alertas e pop-ups
- Analisar apenas os arquivos mais importantes

Enquanto no Modo de Jogo, pode ver a letraG sobre o  icone do BitDefender.

Usar o Modo de Jogo

Por padrão, o BitDefender entra automaticamente em Modo Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender, ou quando uma aplicativo vai para tela cheia. O BitDefender retornará automaticamente ao modo de operação normal quando você fechar o jogo ou quando o aplicativo detectado sair da tela cheia.

Se você quiser ativar o Modo Jogo manualmente, use um dos métodos a seguir:

- Clique com o botão-direito do mouse no ícone do BitDefender que está na área de notificação e selecione **Ligar Modo de Jogo**.
- Aperte `Ctrl+Shift+Alt+G` (A tecla atalho por padrão).

Importante
Não se esqueça de desligar o Modo de Jogo quando terminar. Para fazer isto, use os mesmos processos que usou para o ligar.

Mudar a Hotkey do Modo de Jogo

Se deseja mudar a hotkey, siga estes passos:

1. Abra o BitDefender e troque a interface de usuário para Modo Avançado.
2. Clique em **Modo de Jogo/Portátil** no menu do lado esquerdo.
3. Clique na barra **Modo de Jogo**
4. Clique no botão **Configuração Avançada** .
5. Por baixo da opção **Usar HotKey** , defina a hotkey desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

Por exemplo, de deseja usar a hotkey `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir `D`.

Nota
Ao remover a marca da caixa ao lado de **Usar tecla de atalho** irá desativar a tecla de atalho.

6. Clique em **OK** para salvar as alterações.

6.6.2. Modo Laptop

O Modo Portátil foi especialmente desenhado para os usuários de laptops. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o laptop estiver a funcionar a bateria. Equanto em Modo Laptop, varreduras agendadas não serão executadas, como elas necessitam de mais recursos do sistema e alto consumo de energia.

O BitDefender detecta quando o seu portátil está a funcionar a bateria e automaticamente entra em Modo de Portátil. De igual forma, O BitDefender sai automaticamente do Modo de Portátil quando detecta que o seu portátil já não está a funcionar a bateria.

Para usar o Modo Laptop, você deve especificar noassistente de configuração que você esta usando um laptop. Se você não selecionou a opção apropriada quando estava configurando o assistente, você pode habilitar o Modo Laptop depois com segue:

1. Abra o BitDefender.
2. Clique no botão **Configurações** no canto superior direito da janela.
3. Na categoria de Configurações Gerais, marque a opção correspondente a**Detecção de Modo Laptop**.
4. Clique**OK** para salvar e aplicar as alterações.

6.7. Detecção Automática de Dispositivo

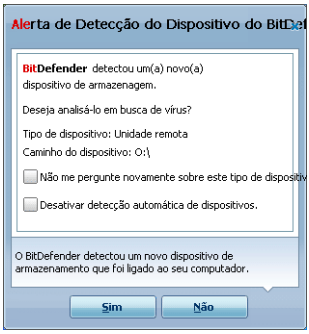
O BitDefender detecta automaticamente quando você conectar um dispositivo de armazenamento removível em seu computador e se oferece para o análisar antes de você acessar seus arquivos. Isto é recomendado, a fim de evitar vírus e outros malwares de infectarem seu computador.

Os dispositivos detectados se enquadram em uma destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pen drives e HDs externos.
- Diretórios de rede mapeados (remotos)

Quando um tal dispositivo é detectado, uma janela de alerta é mostrada.

Para analisar um dispositivo de armazenamento, apenas clique em **Sim**. O assistente de varredura irá aparecer e guiar você através do processo de varredura. Para informações detalhadas sobre esse assistente, por favor consulte a seção "*Assistente do analisador Antivírus*" (p. 51).



Alerta Detecta Dispositivo

Se você não deseja analisar o dispositivo, você deve clicar em **Não**. Neste caso, você pode encontrar uma destas opções úteis:

- **Não perguntar novamente sobre este tipo de dispositivo** - O BitDefender deixará de perguntar se deseja analisar dispositivos de armazenamento deste tipo quando forem conectados ao seu computador.
- **Desativar a detecção automática de dispositivos** - Você não será mais questionado sobre a verificação de novos dispositivos de armazenamento quando forem conectados ao computador.

Se você acidentalmente desativou o dispositivo automático de detecção e pretende ativá-lo, ou se você deseja configurar suas definições, siga estas etapas:

1. Abra o BitDefender e troque a interface de usuário para Modo Avançado.
2. Vá em **Antivírus>Análise de Vírus**.
3. Na lista de tarefas de análise, localize a tarefa **Detecção de Dispositivos**.
4. Clique com o botão direito na tarefa e selecione **Abrir**. Uma nova janela irá aparecer.
5. Na aba **Visão Geral**, configure as opções de análise conforme necessário. For more information, please refer to "*Configurar Definições da Análise*" (p. 117).
6. Na guia **Detecção**, escolha que tipos de dispositivos de armazenamento serão detectados.
7. Clique**OK** para salvar e aplicar as alterações.

7. Reparando Incidências

O BitDefender utiliza um sistema de rastreio de problemas para detectar e lhe informar sobre os problemas que podem afetar a segurança do seu computador e dados. Por padrão, ele irá monitorar apenas uma série de problemas que são considerados muito importantes. De qualquer forma você pode configurar ele conforme suas necessidades, escolhendo quais problemas em específico você deseja ser notificado.

É dessa forma que os problemas pendentes são notificados:

- Um símbolo especial é mostrado sobre o ícone do BitDefender na área de notificação para indicar um problema pendente.

  Triângulo vermelho com um ponto de exclamação: Problemas críticos afetam a segurança de seu sistema. Eles requerem sua atenção imediata e devem ser corrigidos assim que possível.
  Triângulo amarelo com um ponto de exclamação: Problemas não críticos afetam a segurança de seu sistema. Você deve verificar e corrigí-los quando tiver tempo.

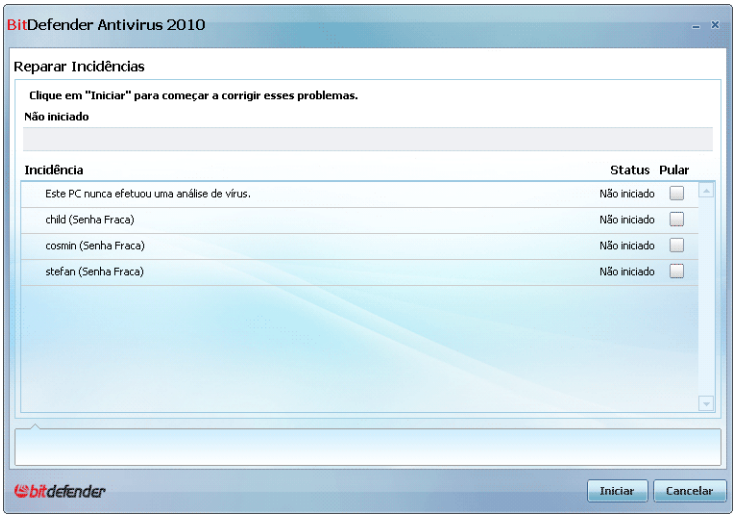
  Também, se você mover o cursor do mouse sobre o ícone, um pop-up irá confirmar a existência de problemas pendentes.

- Quando você abre o BitDefender, a área do Status de Segurança irá indicar o número de problemas afetando o seu sistema.
  - No modo Intermediário, o status de segurança é mostrado na aba **Painel**.
  - No Modo Avançado, vá em **Geral>Painel** para verificar o status de segurança.

7.1. Assistente de Correção de todos os Problemas

O modo mais fácil de se corrigir os problemas existentes é seguir o passo a passo do assistente **Corrigir Todos os Problemas**. O assistente lhe ajuda a facilmente remover qualquer ameaça em seu computador e segurança dos dados. Para abrir o assistente, faça qualquer um dos seguintes:

- CLique com o botão direito do mouse no ícone do BitDefender na área de notificação e selecione **Corrigir Todos os Problemas**.
- Abra o BitDefender. Dependendo do modo da interface do usuário, prossiga a seguir:
  - No modo Básico, clique em **Corrigir Todos os Problemas**.
  - No Modo Intermediário, vá para a aba **Painel** e clique em **Corrigir Todos os Problemas**.
  - No Modo Avançado, vá para **Geral>Painel** e clique em **Corrigir Todos os Problemas**.



Assistente de Correção de todos os Problemas

O assistente mostra uma lista das vulnerabilidades de segurança existentes em seu computador.

Todas ocorrências atuais estão selecionadas para serem corrigidas. Se existe uma ocorrência que você não quer que seja corrigida, selecione o campo correspondente a ela. Se você fizer isto, o status irá mudar para **Pular**.

Nota
Se você não quiser ser notificado sobre ocorrências específicas, você deve configurar o sistema de monitoramento de acordo, como descrito na seção seguinte.

Para corrigir as ocorrências selecionadas, clique **Iniciar**. Algumas ocorrências são corrigidas imediatamente. Para outras, um assistente ajudará a corrigir

As questões que este assistente ajuda você a corrigir podem ser agrupadas em cinco categorias principais:

- **Configurações de segurança desativadas.** Tais problemas são corrigidos imediatamente, ao permitir as respectivas definições de segurança.
- **Tarefas preventivas de segurança que você precisa executar.** Um exemplo deste tipo de tarefa é analisar o seu computador. É recomendado que você analise o seu computador pelo menos uma vez por semana. O BitDefender irá automaticamente fazer isso para você na maioria dos casos. No entanto, se você alterou o calendário de análise ou se a agenda não for concluída, você será notificado sobre este assunto.

Ao fixar tais problemas, um assistente ajuda-o a concluir com êxito a tarefa.

- **Vulnerabilidades do sistema.** O BitDefender verifica automaticamente o seu sistema por vulnerabilidades e alerta você sobre elas. As vulnerabilidades do sistema incluem o seguinte:
  - Senhas fracas para contas de usuário do Windows.
  - software desatualizado no seu computador.
  - Falta de atualizações do Windows.
  - A Atualização automática do Windows está desativada

  Quando esses problemas forem corrigidos, o assistente de análise de vulnerabilidades é iniciado. Este assistente lhe auxilia a corrigir as vulnerabilidades detectadas no sistema. Para informação mais detalhada, por favor vá para a seção "*Assistente de Verificação de Vulnerabilidades*" (p. 63).

7.2. Configurando o Rastreio de Problemas

O sistema de rastreamento de problemas é pre-configurado para monitorar e alertar você a respeito dos problemas mais importantes que possam afetar a segurança de seu compuatador e dados. Problemas adicionais podem ser monitorados, baseado nas escolhas feitas por você no assistente de configuração (onde você configura seu perfil de uso). Além dos problemas monitorados por padrão, existem várias outros problemas que você pode ser informado.

Você pode configurar o sistema de rastreio para melhor servir as suas necessidades de segurança, escolhendo quais problemas específicos a ser informado. Você pode fazer isso tanto no Modo Intermediário ou no Modo Avançado.

- No Modo Intermediário, o sistema de rastreamento é configurado de locais separados. Siga esses passos:
  1. Vá até a guia **Antivirus**, **Antiphishing** ou **Vulnerabilidade**.
  2. Clique **Configurar Status de Varredura**.
  3. Marque a caixa de seleção correspondente ao item que você deseja que seja monitorado.

  Para informações detalhadas, por favor consulte a "Modo Intermediário" (p. 70) parte deste guia.
- No Modo Avançado, o sistema de monitoramento pode ser configurado de uma posição central. Siga esses passos:
  1. Vá em **Geral>Painel**.
  2. Clique **Configurar Status de Varredura**.
  3. Marque a caixa de seleção correspondente ao item que você deseja que seja monitorado.

  Para informação detalhada,por favor consulte o capítulo"*Painel*" (p. 93).

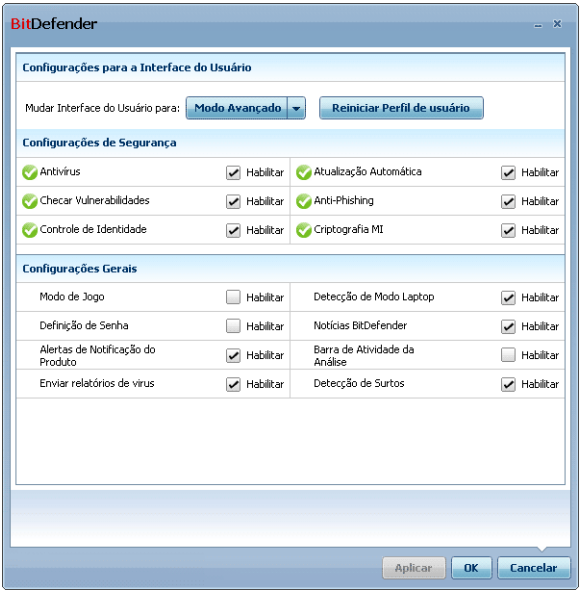
8. Definindo Configurações Básicas

Você pode definir as principais configurações (incluindo trocar o modo de interface de usuário) a partir da janela de configurações básicas. Para abri-la, siga qualquer um dos passos a seguir:

- Abra o BitDefender e clique no botão **Configurações** no canto superior direito da janela.
- CLique com o botão direito do mouse no ícone do BitDefender naárea de notificação e selecione **Definições Básicas**.

Nota

Para configurar em detalhes as definições do produto, use o Modo Avançado de interface. Para informações detalhadas, por favor consulte a “Modo Avançado” (p. 92) parte deste guia.



Definições Básicas

As definições são organizadas em três categorias:

- Definições da Interface de Usuário
- Definições de Segurança
- Definições Gerais

Para aplicar e salvar as alterações que você, cliqueOK. Para fechar a janela sem salvar as alterações clique **Cancel**.

8.1. Configurações para a Interface do Usuário

Nesta área, você pode alternar o modo de visualização da interface do usuário e redefinir o perfil de utilização.

Alternando o modo de visualização da interface de usuário. Conforme descrito nesta seção "*Modos de Visualização da Interface do usuário*" (p. 21), existem três modos para mostrar a interface de usuário. Cada modo de interface de usuário é designado para uma categoria específica de usuários, baseado em suas habilidades em computação. Desta forma, a interface de usuário abrange todos tipos de usuários, desde pessoas iniciantes até pessoas técnicas.

O primeiro botão mostra o modo atual de visualização da interface do usuário. Para alterar o modo de Interface do Usuário, clique na seta no botão e selecione o modo desejado a partir do menu.

Modo	Descrição
Modo Iniciante	Apropriado para iniciantes em computadores e pessoas que querem o BitDefender para proteger seu computador e dados sem serem incomodados. Este modo é simples de usar e requer mínima interação. Tudo que você tem que fazer é corrigir os problemas atuais quando indicado pelo BitDefender. Uma guia intuitivo passo-a-passo lhe auxilia na resolução dos problemas. Além disso, você pode efetuar tarefas comuns, tal como atualizar as vacinas antivírus da BitDefender e arquivos de produtos, ou analisar o computador.
Modo Intermediário	Destinado a usuários com conhecimentos médios de informática, este modo estende o que você pode fazer no Modo Iniciante. Você pode corrigir os problemas separadamente e escolher quais problemas monitorar. Além disso, você pode gerenciar remotamente os produtos BitDefender instalados nos computadores de sua casa.
Modo Avançado	Destinado para os usuários mais técnicos, este modo permite configurar completamente cada funcionalidade do BitDefender. Voce também pode usar todas as tarefas disponíveis para proteger seu computador e dados.

Redefinindo o perfil de utilização. O perfil de utilização reflete as principais atividades realizadas no computador. Dependendo do perfil de utilização, a interface do produto está organizada para permitir um acesso fácil à suas tarefas preferidas.

Para reconfigurar o perfil de utilização, clique em **Redefinir o Perfil de Utilização** e siga o assistente de configuração.

8.2. Configurações de Segurança

Nesta área, você poder habilitar ou desabilitar definições do produto que abrangem aspectos de segurança do seu computador e dados. O estado atual de uma definição é indicado usando um destes ícones.

Círculo vermelho com uma marca de verificação: A definição esta habilitada.
Círculo vermelho com uma marca de exclamação: A definição esta desabilitada.

Para habilitar / desabilitar uma definição marque / desmarque a opção **Habilitar**.

Atenção

Tenha cuidado ao desabilitar a proteção de Antivírus em tempo real ou a atualização automática. Desativando esses recursos pode comprometer a segurança do seu computador. Se você realmente precisa desativá-los, lembre-se de reativá-los o mais rápido possível.

A lista inteira de definições e suas descrições são apresentadas no quadro a seguir:

Definição	Descrição
Antivírus	A proteção de arquivos em Tempo-real lhe assegura que todos os arquivos sejam analisados ao ser acessados por você, ou por um aplicativo executado neste sistema.
Atualização Automática	Atualização automática garante que o produto BitDefender e as assinaturas mais recente sejam descarregadas e instaladas automaticamente, periodicamente.
Análise de Vulnerabilidade	A Verificação Automática de Vulnerabilidades assegura que o software crucial no seu PC está atualizado.
Antiphishing	Antiphishing detecta e alerta você em tempo real se uma página tenta roubar suas informações pessoais.
Controle de Identidade	Controle de Identidade ajuda a previnir que seus dados pessoais sejam enviados para internet sem o seu consentimento. Ele bloqueia qualquer mensagem instantânea, e-mail ou meios de transmitir dados que

Definição	Descrição
	você definiu como sendo privados para receptores não autorizados (endereços).
Criptografia MI	A criptografia MI (Mensagens Instantâneas) protege as suas conversas via Yahoo! Messenger e Windows Live Messenger desde que os seus contatos de MI utilizem programas BitDefender e MI compatíveis.

O estado de algumas dessas definições podem ser monitoradas pelo sistema de monitoramento de problemas do BitDefender. Se você desativar uma configuração monitorada, o BitDefender irá indicar que se trata de um problema que precisa de correção.

Se você não quer que uma configuração monitorada que você desabilitou seja exibida como problema, você deve configurar o sistema de monitoramento de problemas de acordo. Você pode fazer isto tanto no Modo Intermediário quanto no Modo Avançado.

- No Modo Intermediário, o sistema de monitoramento pode ser configurado de diferentes locais, baseado nas categorias de definições. Para informações detalhadas, por favor consulte a "Modo Intermediário" (p. 70) parte deste guia.
- No Modo Avançado, o sistema de monitoramento pode ser configurado de uma posição central. Siga esses passos:
  1. Vá em **Geral>Painel**.
  2. Clique **Configurar Status de Varredura**.
  3. Marque a caixa de seleção correspondente ao item que você deseja que não seja monitorado.

  Para informação detalhada,por favor consulte o capítulo"*Painel*" (p. 93).

8.3. Configurações Gerais

Nesta área, você pode habilitar ou desabilitar as definições que afetam o comportamento do produto e a experiência do usuário. O estado atual de uma definição é indicado usando um destes ícones.

Círculo vermelho com uma marca de verificação: A definição esta habilitada.
Círculo vermelho com uma marca de exclamação: A definição esta desabilitada.

Para habilitar / desabilitar uma definição marque / desmarque a opção **Habilitar**.

A lista inteira de definições e suas descrições são apresentadas no quadro a seguir:

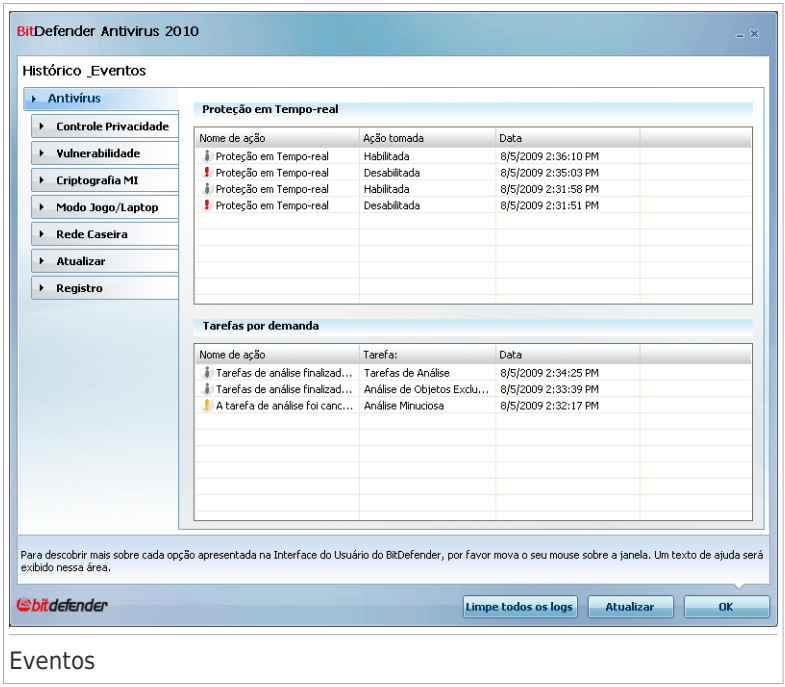
Definição	Descrição
Modo de Jogo	O Modo de Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema durante os jogos.
Modo de Detecção de Laptop	O Modo de Portátil modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no tempo de vida da bateria do seu portátil.
Senha de Configuração	Isto assegura que as definições do BitDefender só podem ser modificadas pela pessoa que conhece esta senha. Quando você habilitar esse modo, você será questionado a configurar a senha de definições. Digite a senha desejada em ambos os campos e clique em **OK** para definir a senha.
Notícias BitDefender	Ao ativar esta opção, você receberá notícias importantes sobre a empresa BitDefender, sobre as atualizações do produto ou sobre novas ameaças de segurança.
Notificações de Alerta do Produto	Ao ativar esta opção, você receberá alertas de informação.
Barra de Atividade de Análise	A barra de Atividade da análise é uma pequena e transparente janela que indica o progresso da atividade de análise do BitDefender. Para mais informações, por favor consulte a seção *"Barra de Atividade da Análise" (p. 29)*.
Enviar Relatórios de Vírus	Ao ativar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.
Detecção de Surtos	Ao ativar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

9. Histórico & Eventos

O link**Ver Logs** na parte inferior da janela principal do BitDefender abre uma outra janela com o histórico & eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança. Por exemplo, você pode facilmente verificar se a atualização foi executada com sucesso, se foi encontrado algum malware no seu computador.

Nota

O link só está acessível no Modo Intermediário ou no Modo Avançado.



Eventos

De forma a ajudá-lo a filtrar o histórico dos & eventos BitDefender, as seguintes categorias são apresentadas do lado esquerdo:

- **Antivírus**
- **Controle Privacidade**
- **Vulnerabilidade**
- **Criptografia IM**
- **Modo de Jogo/Portátil**

- **Rede Doméstica**
- **Atualização**
- **Registro**
- **Log de Internet**

Uma lista de eventos está disponível para cada categoria. Cada evento vem com a seguinte informação: uma breve descrição, a ação que o BitDefender tomou e quando aconteceu, e a data e hora em que ocorreu. Se deseja saber mais informação acerca de um evento em particular da lista, faça duplo clique sobre esse evento.

Clique em **Limpar todos os Logs** se deseja remover antigos logs ou **Atualizar** para se certificar que os logs mais recentes são mostrados.

10. Registro e Minha Conta

BitDefender Antivirus 2010 vem com um período de teste de 30 dias. Durante o período experimental, o produto é totalmente funcional e você pode testá-lo para ver se ele atende às suas expectativas. Observe que, após 15 dias de avaliação, o produto deixará de ser atualizado, a menos que você crie uma conta BitDefender. Criar uma conta BitDefender é uma parte obrigatória do processo de registro.

Antes do término do período experimental, você deve registrar o produto, a fim de manter o computador protegido. O processo de registro é composto por dois passos:

1. **Ativação do produto (registro de uma conta BitDefender).** Você deve criar uma conta BitDefender para receber atualizações e para ter acesso ao suporte técnico gratuito. Se você já possui uma conta na BitDefender, registre o seu produto BitDefender à essa conta. O BitDefender vai lhe notificar que você precisa ativar seu produto e isso irá lhe ajudar a solucionar esse problema.

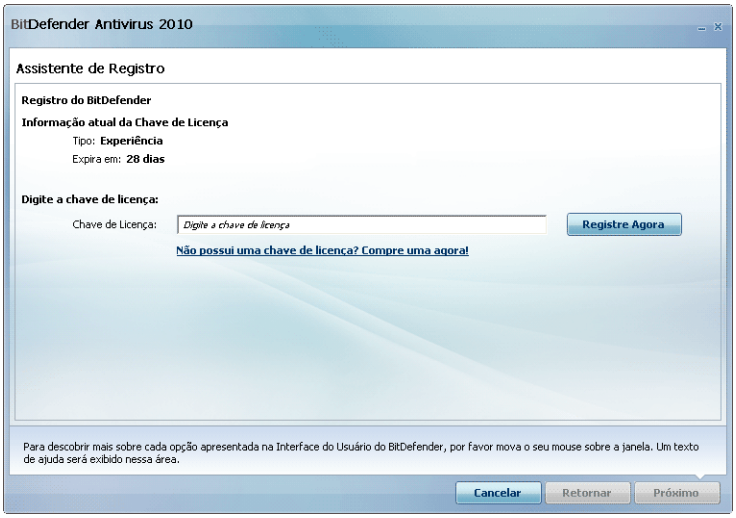
   Importante

   Você deve criar uma conta dentro de 15 dias após instalar o BitDefender (Se você registrar com uma chave de licença, o prazo limitie é extendido para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus.

2. **Registro com uma chave de licença.** A chave de licença especifica quanto tempo você tem direito a utilizar o produto. Logo que a chave da licença expirar, o BitDefender para de executar as suas funções e proteger o seu computador. Você deve registrar o produto com uma chave de licença quando o período de experiência termina. Você deve comprar uma chave de licença ou renovar sua licença poucos dias antes do prazo que a chave de licença atual expira.

10.1. Registrando o BitDefender Antivírus 2010

Se você quiser registrar o produto com uma chave de licença ou alterar a atual, clique no link **Registrar Agora**, localizado na parte inferior da janela do BitDefender. A janela de registro do produto irá aparecer.



Registro

Você pode ver o estado do registo do BitDefender, a chave de licença atual e quantos dias faltam para a licença expirar.

Para registrar o BitDefender Antivírus 2010:

1. Insira a chave de licença no campo de edição.

   Nota
   Pode encontrar a sua chave de licença:
   - Na bolsa do CD.
   - ou no cartão de registo do produto.
   - no e-mail da sua compra on-line.

   Se não possuir uma chave de licença BitDefender, clique no link que lhe facultamos para ir até à loja on-line do BitDefender e adquirir uma.

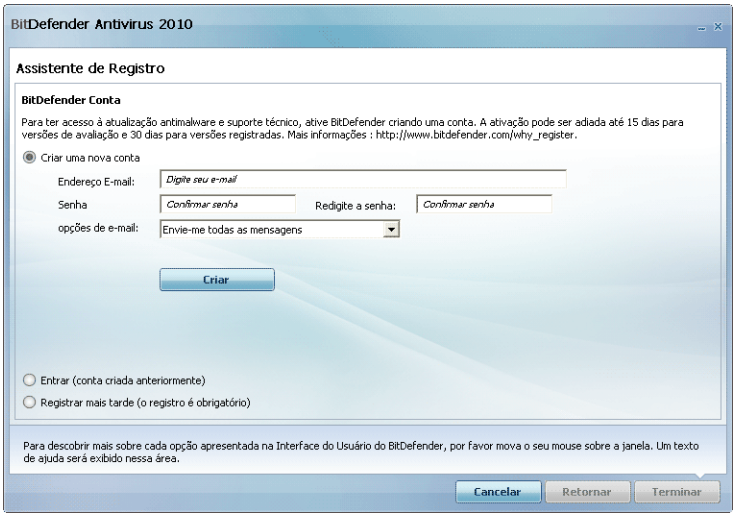
2. Clique **Registrar Agora**.
3. Clique em **Finalizar**.

10.2. Ativando o BitDefender

Para ativar o BitDefender, você tem que criar ou acessar uma conta BitDefender. Se você não registrar uma conta BitDefender durante o assistente de registro inicial, você pode fazer isto da seguinte forma:

- No modo Básico, clique em **Corrigir Todos os Problemas**. O assistente irá ajudá-lo a corrigir todas os problemas pendentes, incluindo a ativação do produto.
- No modo Intermediário, vá para a aba **Segurança** e clique o botão **Consertar** correspondente ao problema relacionado à ativação do produto.
- No Modo Avançado, vá para **Registro** e clique o botão **Ativar Produto**.

A janela de registro da conta abrirá. Aqui é onde você pode criar ou entrar numa conta BitDefender para ativar seu produto.



Criar uma Conta

Se não deseja criar uma conta BitDefender neste momento, selecione **Registrar mais tarde** e clique em **Terminar**. De outra forma, actue de acordo com a sua presente situação:

- “Não tenho uma conta BitDefender” (p. 48)
- “Já tenho uma conta BitDefender” (p. 49)

Importante

Você deve criar uma conta dentro de 15 dias após instalar o BitDefender (Se você registrar com uma chave de licença, o prazo limitie é extendido para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus.

Não tenho uma conta BitDefender

Para criar uma conta BitDefender com sucesso, siga estes passos:

1. Selecione **Criar uma nova conta**.
2. Digite as informações necessárias nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   - **E-mail** - insira o seu endereço de e-mail.
   - **Senha** - insira uma Senha para a sua conta BitDefender. A senha deve ter entre 6 e 16 caracteres de tamanho.
   - **Re-insira a senha** - insira novamente a senha previamente definida.

   Nota
   Uma vez que a conta é ativada, você pode usar o endereço de e-mail fornecido e senha para fazer o log in na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Selecione uma das opções disponíveis do menu:
   - **Enviar todas as mensagens**
   - **Enviem-me apenas mensagens referentes ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique **Criar**.
5. Clique **Finalizar** para completar o assistente.
6. **Ative sua conta.** Antes de ser capaz de usar a sua conta, você deve ativá-la. Verifique seu e-mail e siga as instruções no e-mail enviado a você pelo serviço de registro da BitDefender.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Neste caso, forneça a senha de sua conta e clique em **Entrar**. Clique **Finalizar** para completar o assistente.

Se você já tiver uma conta ativa, mas o BitDefender não a detectou, siga estes passos para registrar o produto para aquela conta:

1. Selecione **Entrar (na conta criada previamente)**.
2. Digite o endereço de email e senha da sua conta nos campos correspondentes.

   Nota
   Se não se lembra da sua senha, clique em **Esqueceu a sua senha?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Selecione uma das opções disponíveis do menu:
   - **Enviar todas as mensagens**
   - **Enviem-me apenas mensagens referentes ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Entrar**.
5. Clique **Finalizar** para completar o assistente.

10.3. Comprando Chaves de licença

Se o período experimental, vai acabar em breve, você deve comprar uma chave de licença e registrar o seu produto. Abra o BitDefender e clique no link **Comprar/Renovar**, localizado na parte de baixo da janela. O link leva você a uma página web onde você pode comprar uma chave de licença para o seu BitDefender.

10.4. Renovando sua licença

Como um cliente BitDefender, você é elegível a um desconto na renovação da licença do seu BitDefender. Você também pode atualizar o seu produto para a versão atual a um desconto especial ou gratuito.

Se a sua chave de licença atual estiver para expirar, você deve renovar sua licença. Abra o BitDefender e clique no link **Comprar/Renovar**, localizado na parte de baixo da janela. O link leva você a uma página web onde você pode renovar sua licença.

11. Assistentes

Com a finalidade de fazer o BitDefender muito fácil de usar, vários assistentes ajudam você a realizar específicas tarefas de segurança ou configurar definições mais complexas do produto. Este capítulo descreve os assistentes que devem aparecer quando você corrigir as ocorrências ou realizar tarefas específicas com o BitDefender. Outros assistentes de configuração são descritos separadamente na parte “Modo Avançado” (p. 92) .

11.1. Assistente do analisador Antivírus

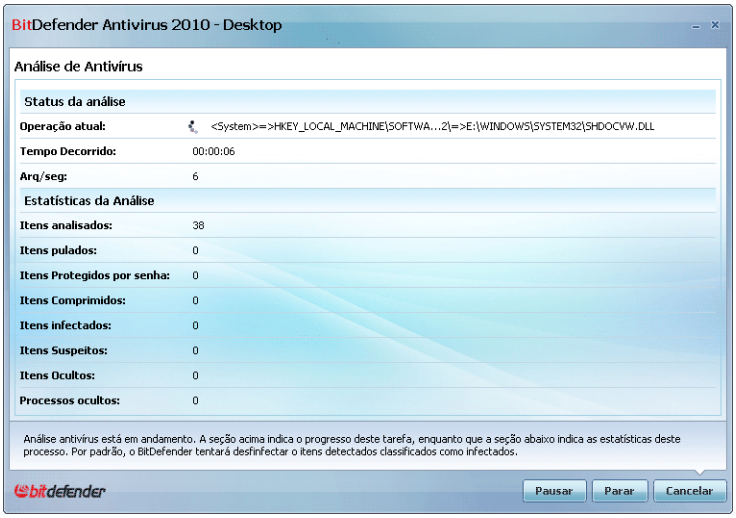
A qualquer momento que você iniciar uma análise por demanda (por exemplo, clique com o botão direito do mouse numa pasta e selecione **Analisar com o BitDefender**), O assistente de Análise do BitDefender Antivirus aparecerá. Siga o processo guiado de três passos para completar o processo de análise.

Nota

Se o assistente de análise não aparecer, a análise pode estar configurada para executar silenciosamente no computador, enquanto você o utiliza. Você pode visualizar o ícone Progresso da análise na área de notificação. Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da análise.

11.1.1. Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Espere que o BitDefender termine a análise.

Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Arquivos comprimidos protegidos por senha. Se o BitDefender detecta um arquivo protegido por senha durante a análise e a ação padrão está configurada para **Perguntar a senha**, você será questionado a fornecer a senha. Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha. As seguintes opções estão disponíveis:

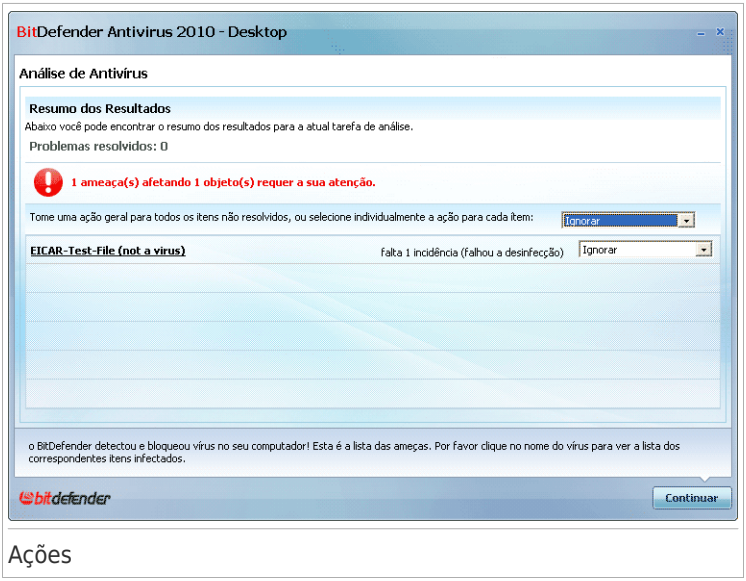
- **Desejo digitar a senha para esse objeto.** Se você deseja que o BitDefender analise o arquivo, selecione essa opção e digite a senha. Se você não sabe a senha, escolha uma das outras opções.
- **Não desejo digitar uma senha para esse objeto.** Selecione essa opção para pular a análise desse arquivo.
- **Não desejo digitar a senha para qualquer objeto (pular todos os objetos protegidos por senha).** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha. O BitDefender não será capaz de os analisar, porém um registro será mantido no relatório da análise.

Clique em **OK** para continuar.

Parando ou suspendendo a análise. Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá diretamente para o último passo do assistente. Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

11.1.2. Passo 2/3 - Selecionar as ações

Quando a análise é completada, surge uma nova janela, onde pode ver os resultados da análise.



Ações

Pode ver o número de incidências que afectam o seu sistema.

Os objectos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objectos infectados.

Você pode escolher uma ação geral a ser executada para todos os problemas ou escolher ações separadas para cada grupo de problemas.

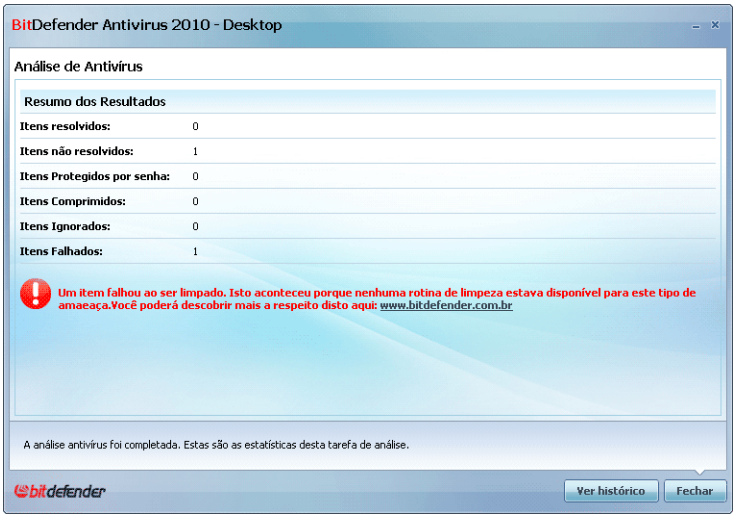
Uma ou várias das seguintes opções podem aparecer no menu:

Ação	Descrição
Não Tomar Ação	Nenhuma ação será tomada em arquivos detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.
Desinfetar	Remove o código malware dos arquivos infectados.
Apagar	Apaga os arquivos detectados.
Mover para a quarentena	Move os arquivos detectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Renomear arquivos	Altera o nome de arquivos escondidos ao adicionar `.bd.ren` ao nome. Como resultado, você será capaz de pesquisar e encontrar esses arquivos em seu computador, caso existam. Por favor verifique se esses arquivos escondidos não são arquivos que você escondeu intencionalmente do Windows. Eles são arquivos escondidos por programas especiais, conhecidos como rootkits. Os Rootkits não são maliciosos por natureza. Porém são comumente utilizados para criar vírus e spywares não detectados por programas normais de Antivírus.

Clique em **Continuar** para aplicar as acções especificadas.

11.1.3. Passo 3/3 - Ver Resultados

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela.



Sumário

Pode ver o sumário dos resultados. Se você deseja obter informação abrangente sobre o processo de análise, clique em **Ver Relatório** para visualizar o relatório da análise.

Importante
Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado.

Clique em **Fechar** para fechar a janela.

BitDefender Não Pode Resolver Algumas Incidências

Na maioria dos casos o BitDefender desinfecta com sucesso o arquivo infectado ou isola a infecção. No entanto, existem incidências que não puderam ser resolvidas.

Nesse caso, recomendamos que contacte o Suporte Técnico BitDefender em www.bitdefender.com.br. Os nossos membros do suporte ajudá-lo-ão a resolver as incidências que esteja a experimentar.

BitDefender Detectou Arquivos Suspeitos

Arquivos suspeitos são arquivos detectados pela análise heurística e que poderão estar infectados com malware cuja a vacinas de detecção ainda não foi disponibilizada.

Se foram detectados arquivos suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender. Clique **OK** para enviar estes arquivos para análise no Laboratório do BitDefender.

11.2. Assistente de Análise Customizado

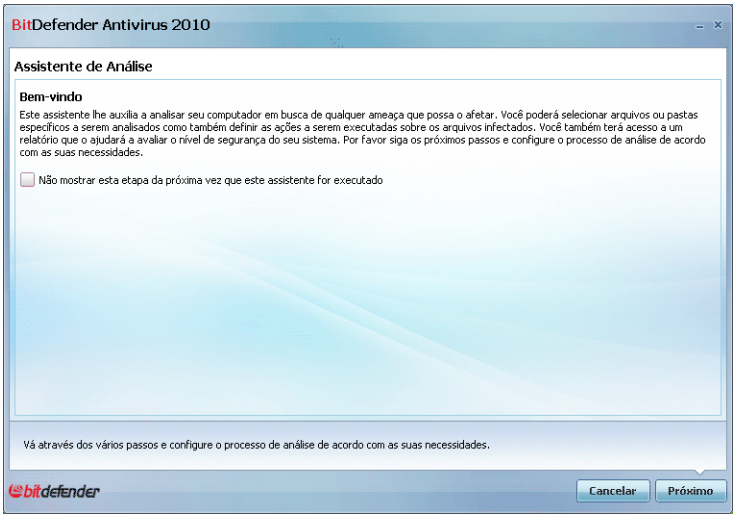
O Assistente de Análise Customizado permite criar e executar uma análise customizável e opcionalmente salvar como uma Tarefa Rápida, ao usar o BitDefender em modo intermediário.

Para executar uma tarefa de análise customizável utilizando o Assistente de Análise Customizado, você deve seguir esses passos:

1. No Modo Intermediário, vá para a aba **Segurança**.
2. Na área **Tarefas Rápidas**, clique na seta no botão **Análise do Sistema** e selecione **Análise Customizada**.
3. Siga o processo guiado de seis passos para completar o processo de análise.

11.2.1. Passo 1/6 - Janela de Boas-vindas

Essa é uma janela de boas vindas.



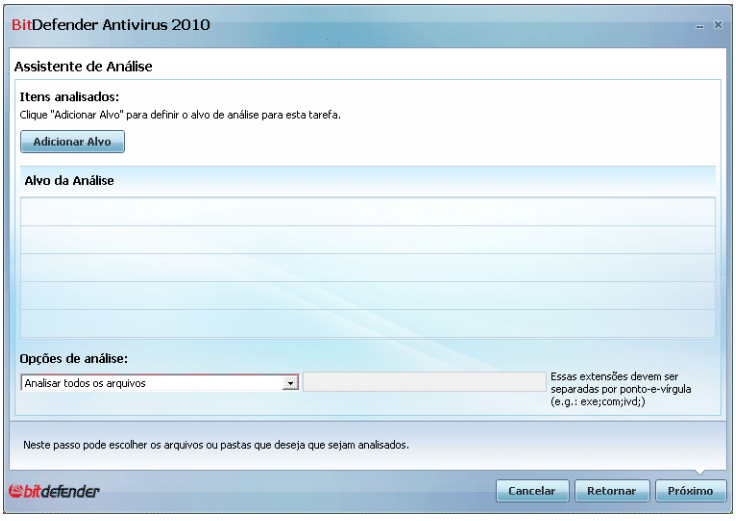
Janela de Boas-Vindas

Se você desejar ignorar essa janela ao executar esse assistente no futuro, selecione a caixa de seleção **Nça mostrar esse passo na próxima vez que o assistente for executado**.

Clique em **Próximo**.

11.2.2. Passo 2/6 - Selecionar Alvo

Aqui você pode especificar os arquivos ou diretórios para serem analisados assim como as opções de análise.



Selecione o Alvo

Clique em **Adicionar Alvo**, selecione os arquivos ou pastas que deseja analisar e clique em **OK**. Os caminhos para os locais selecionados irão aparecer na coluna **Alvo de Anáise**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela. Clique no botão **Remover Todos** para remover todos os locais que foram adicionados à lista.

Quando você terminar de selecionar os locais, defina as **Opções de Análise**. As seguintes estão disponíveis:

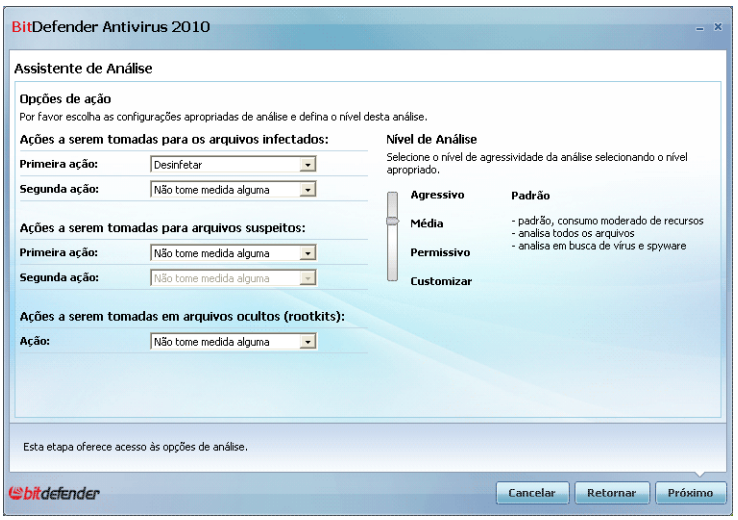
Opção	Descrição
Verificar todos os arquivos	Selecione esta opção para analisar todos os arquivos nos diretórios selecionados.
Analisar apenas os arquivos com extensões de aplicativos	Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`;

Opção	Descrição
	.ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
Analisar apenas as extensões definidas pelo usuário	Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";".

Clique em **Próximo**.

11.2.3. Passo 3/6 - Selecionar as ações

Aqui você pode especificar as definições e o nível de análise.



Selecionar as Ações

- Selecione as ações a serem tomadas sobre arquivos infectados e suspeitos detectados. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Ação	Nenhuma ação será tomada em arquivos infectados. Esses arquivos aparecerão no arquivo de relatório.
Desinfetar arquivos	Remover o código de malware dos arquivos infectados detectados.
Apagar arquivos	Apaga o arquivo infectado imediatamente, sem avisar.
Mover arquivos para a quarentena	Move os arquivos infectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

- Selecionar a ação a ser tomada sobre os arquivos (rootkits) ocultos. As seguintes opções estão disponíveis:

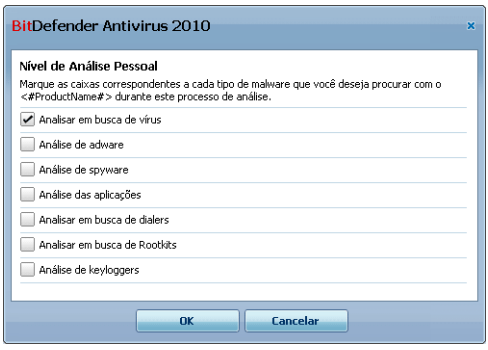
Ação	Descrição
Não Tomar Ação	Nenhuma ação será levada a cabo sobre os arquivos ocultos. Estes arquivos aparecerão no arquivo de relatório.
Renomear	Altera o nome de arquivos escondidos ao adicionar `.bd.ren` ao nome. Como resultado, você será capaz de pesquisar e encontrar esses arquivos em seu computador, caso existam.

- Configura a agressividade do analisador. Há 3 modos para se escolher. Movimente o cursor pela escala para definir o nível de proteção apropriado:

Nível de Análise	Descrição
Permissivo	Apenas arquivos de programas são analisados e apenas para vírus. O nível de consumo de recursos é baixo.
Por Padrão	O nível de consumo de recursos é moderado. Todos os arquivos são analisados por vírus e spyware.
Agressivo	Todos os arquivos (incluindo arquivos comprimidos) são analisados a procura de vírus e spyware. Arquivos ocultos e processos são incluídos na análise. O nível de consumo de recursos é maior.

Os usuários avançados podem tirar vantagem das definições de análise que o BitDefender oferece. O analisador pode ser configurado para procurar apenas por ameaças de malware. Isso pode reduzir drasticamente o tempo de análise e diminuir o tempo de resposta de seu computador durante uma análise.

Arraste o ponteiro para selecionar **Padrão** e depois clique no botão **Nível Padrão**. A seguinte análise irá aparecer:



Nível de Análise Pessoal

Especifique o tipo de malware que você deseja que o BitDefender analise, selecionando as opções apropriadas:

Opção	Descrição
Analisar em busca de vírus	Analisa em busca de vírus. O BitDefender também detecta corpos incompletos de vírus, removendo assim qualquer possível ameaça de segurança que possa vir a afetar o seu sistema.
Analisar em busca de adware	Analisa em busca de ameaças de adware. Estes arquivos serão tratados como arquivos infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa.
Analisar em busca de spyware	Analisa em busca de ameaças de spyware. Estes arquivos serão tratados como arquivos infectados.
Analisar aplicações	Analisar aplicações legítimas que podem ser usadas como ferramenta de espionagem, para ocultar aplicações maliciosas ou outras intenções maliciosas.

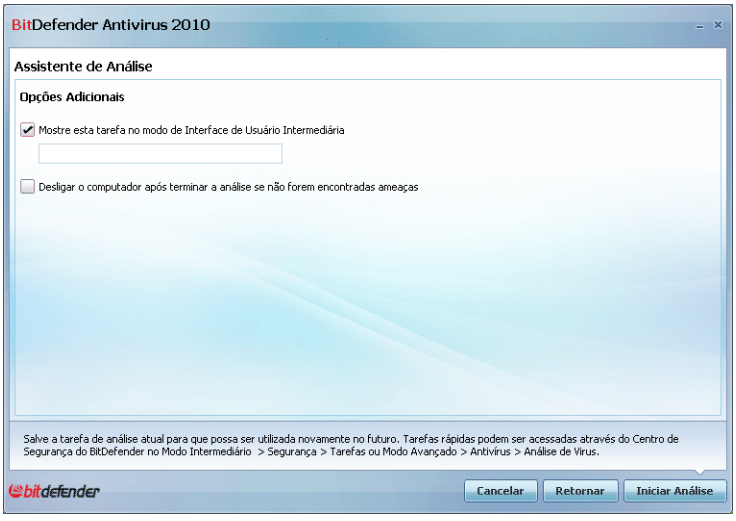
Opção	Descrição
Analisa em busca de dialers	Analisa aplicativos conectando-se a números de alto custo. Estes arquivos serão tratados como arquivos infectados. O software que inclua componentes de conexão deste tipo poderá deixar de funcionar se esta opção estiver ativa.
Analisar em busca de Rootkits	Analisa em busca de objectos ocultos (arquivos e processos), conhecidos por rootkits.
Analisar em busca de keyloggers	Analisar a procura de aplicativos maliciosos que gravam as teclas digitadas..

Clique em **OK** para fechar a janela.

Clique em **Próximo**.

11.2.4. Passo 4/6 - Configurações Adicionais

Antes da análise começar, opções adicionais estão disponíveis:



Configurações Adicionais

- Para salvar a tarefa padronizada que você está criando, para futuro uso, marque a caixa de seleção **Mostrar essa tarefa na interface Modo Intermediário** e escolha um nome para a tarefa no campo de edição mostrado.

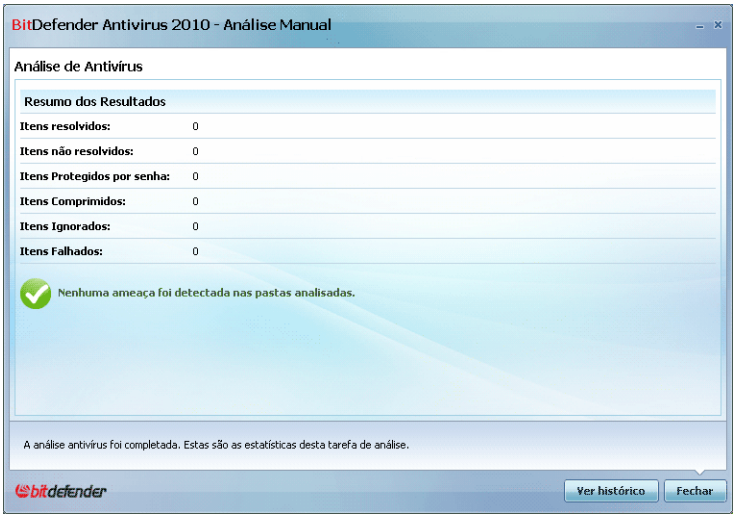
A tarefa será adicionada à lista de Tarefas Rápidas já disponíveis na aba segurança e também irá aparecer no **Modo Avançado > Antivírus > Análise de Vírus**.

- Para desligar o computador após o processo de análise ser completado, selecione a caixa de seleção **Desligar o computador após o processo de análise finalizar se nenhuma ameaça foi detectada**.

Clique em **Próximo**.

11.2.5. Passo 5/6 - Analisando

O BitDefender iniciará a análise dos objetos selecionados:



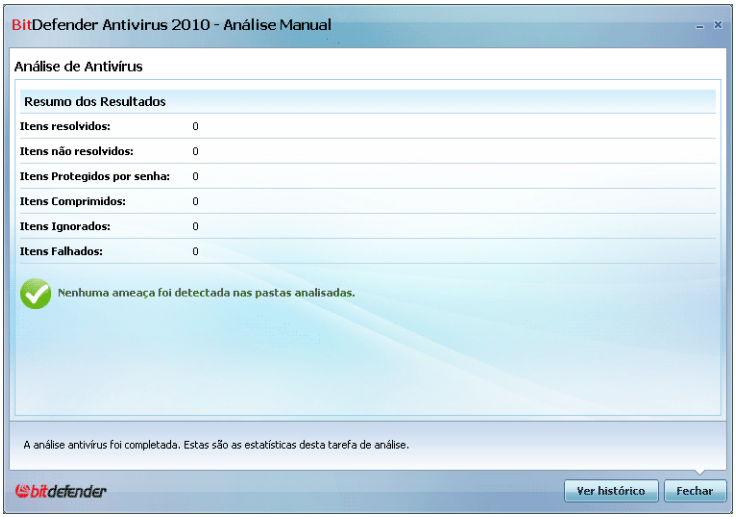
Analisar

Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma. Você pode clicar no ícone de progresso da análise na área de notificação para abrir a janela de análise e ver o progresso.

11.2.6. Passo 6/6 - Ver Resultados

Quando o BitDefender completa o processo de análise, o resultado aparecerá numa nova janela:



Sumário

Você pode ver o resumo dos resultados. Se você deseja obter informação detalhada do processo de análise, clique em **Visualizar Relatório** para visualizar o relatório da análise.

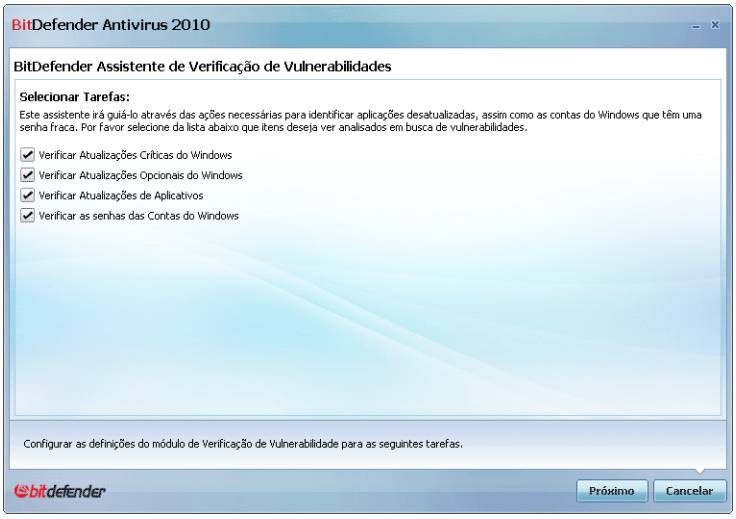
Importante
Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado.

Clique em **Fechar** para fechar a janela.

11.3. Assistente de Verificação de Vulnerabilidades

Este assistente verifica o sistema à procura de vulnerabilidades e ajuda a consertá-las.

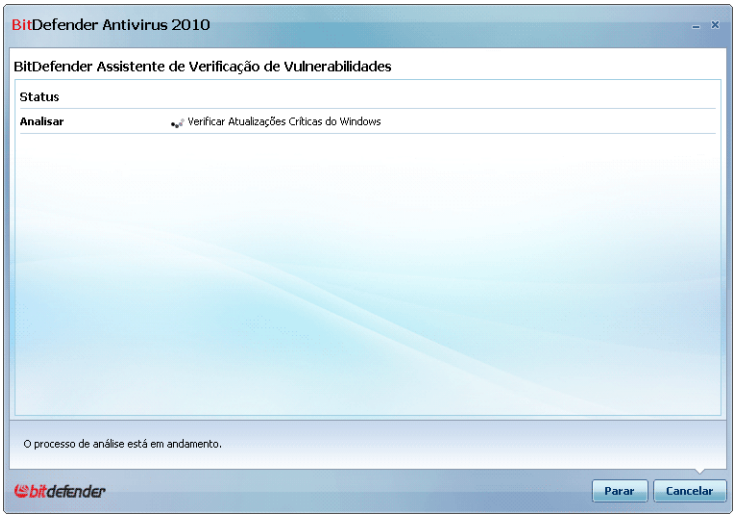
11.3.1. Passo 1/6 - Seleccionar Vulnerabilidades a Verificar



Vulnerabilidades

Clique em **Seguinte** para analisar o sistema em busca das vulnerabilidades seleccionadas.

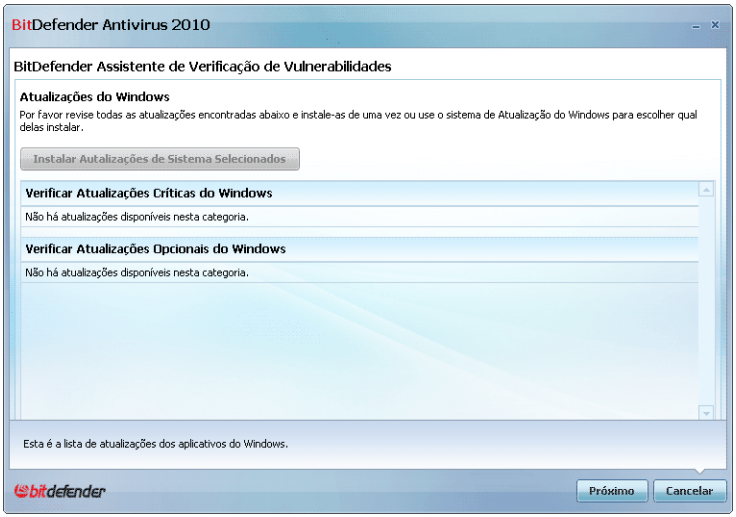
11.3.2. Passo 2/6 - Analisar em Busca de Vulnerabilidades



Checar Vulnerabilidades

Espere que o BitDefender termine a análise de vulnerabilidades.

11.3.3. Passo 3/6 - Atualizar o Windows

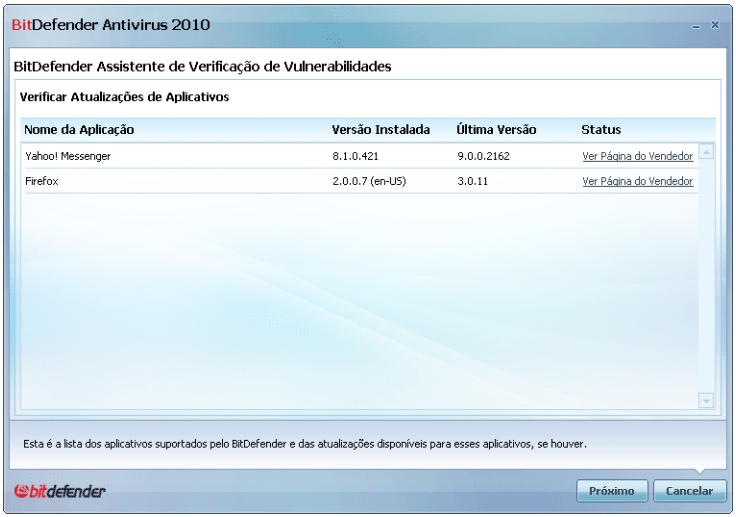


Atualizações do Windows

Pode ver a lista das atualizações criticas e não-criticas do Windows que não se encontram atualmente instaladas no seu computador. Clique em **Instalar Todas Atualizações do Sistema** para instalar todas as atualizações disponíveis.

Clique em **Próximo**.

11.3.4. Passo 4/6 - Atualizar Aplicativos

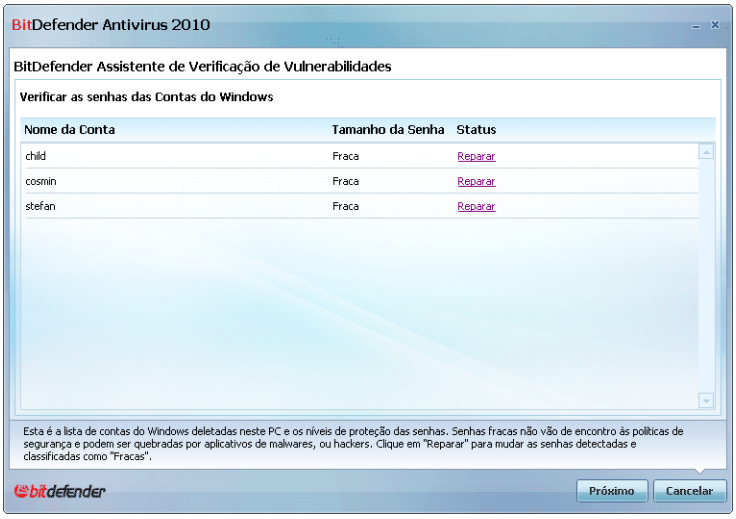


Aplicações

Você pode ver a lista de todos os aplicativos verificados pelo BitDefender e se estes estão ou não atualizados. Se o aplicativo não estiver atualizado, clique no link fornecido para baixar a versão mais recente.

Clique em **Próximo**.

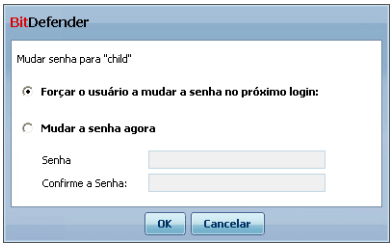
11.3.5. Passo 5/6 - Alterar senhas fracas



Senhas do usuário

Pode ver a lista dos usuários de contas Windows configurados no seu computador e o nível de proteção que as suas senhas garantem. Uma senha pode ser **forte** (difícil de se adivinhar) ou **fraca** (fácil de se quebrar através de pessoas mal intencionadas com softwares específicos).

Clique em **Reparar** para modificar as palavras-passe fracas. Uma nova janela irá aparecer.



Mudar a senha

Seleccionar o método para reparar esta incidência:

- **Forçar o usuário a mudar a senha no próximo login:** O BitDefender avisará o usuário que tem de alterar a senha da próxima vez que ele entrar no Windows.
- **Mudar a senha do usuário.** Deve inserir a nova senha nos campos editáveis. Não se esqueça de informar o usuário sobre a alteração da senha.

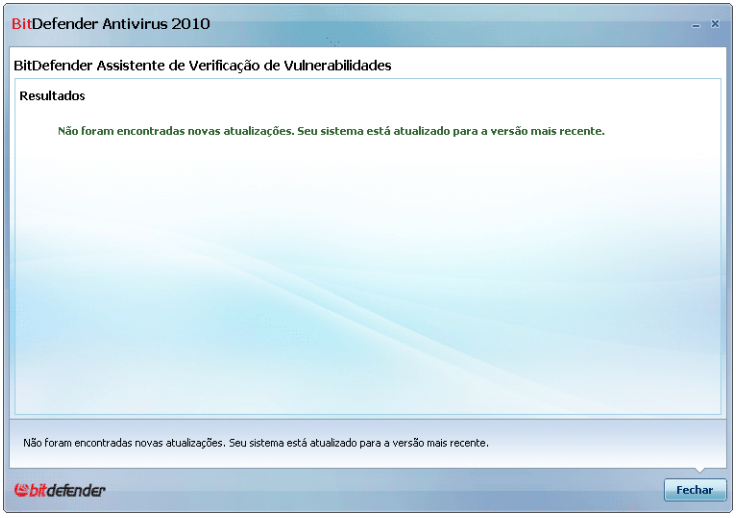
Nota

Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @). Você pode pesquisar na internet sobre mais informações e dicas para criar senhas seguras.

Clique em **OK** para alterar a senha.

Clique em **Próximo**.

11.3.6. Passo 6/6 - Ver Resultados



Resultados

Clique em **Fechar**.

Modo Intermediário

12. Painel

A aba Painel fornece informações referentes ao status de segurança de seu computador e permite que você corrija os problemas pendentes.

Painel

O painel consiste das seguintes seções:

- **Estado** - Indica o número de problemas que afetam o seu computador e ajuda você a resolvê-los. Se há algum problema pendente, você verá um **círculo vermelho com um ponto de exclamação** e o botão **Corrigir todos os Problemas**. Clique no botão para iniciar o assistente Corrigir todos os Problemas.
- **Detalhe do Estado** - Indica o estado de cada módulo principal utilizando sentenças explícitas e um dos seguintes ícones:

  Círculo vermelho com uma marca de verificação: Nenhum problema afeta o estado de segurança. Seu computador e dados estão protegidos.

  Círculo cinza com um ponto de exclamação: A atividade dos componentes desse módulo não é monitorada. Nenhuma informação está disponível referente ao seu estado de segurança. Podem haver problemas específicos relacionados à esse módulo.

  Círculo vermelho com uma marca de exclamação: Há incidências que afetam a segurança do seu sistema. Problemas críticos requerem sua atenção

imediata. Problemas não críticos também devem ser verificados o mais rápido possível.

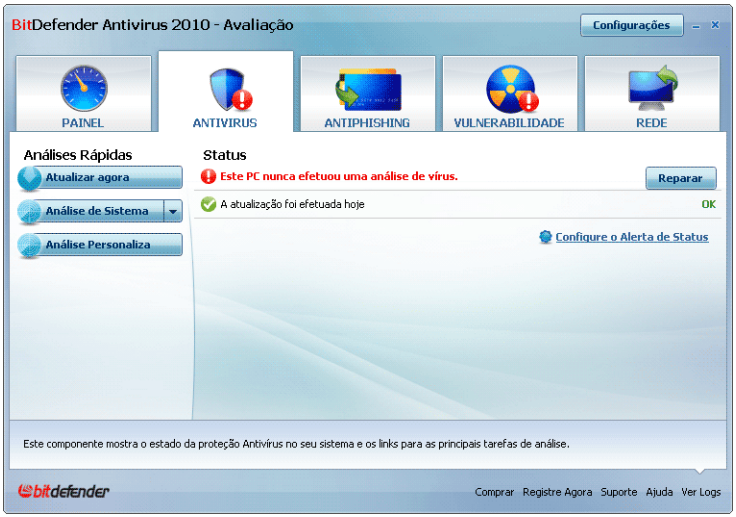
Clique no nome de um módulo para ver mais detalhes sobre seu estado e para configurar o rastreamento de estado de seus componentes.

- **Perfil de Utilização** - Indica o perfil de utilização que está atualmente selecionado e oferece um link para uma atividade relevante para aquele perfil:
  - Quando o perfil **Típico** é selecionado, o botão **Analisar Agora** permite a você executar uma Análise do Sistema utilizando o Assistente de Análise Antivírus. O sistema inteiro será analisado, exceto os arquivos comprimidos. Na configuração padrão, ele analisa a procura de todos os tipos de malware além de rootkits.
  - Quando o perfil **Jogador** é selecionado, o botão **Ligar/Desligar Modo Jogo** permite habilitar/desabilitar o Modo Jogo. O Modo de Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema.
  - Quando o perfil **Padronizado** é selecionado, o botão **Atualizar Agora** inicia uma atualização imediata. Uma nova janela aparecerá, onde você pode ver o status da atualização.

  Se você deseja alternar para um perfil diferente, ou editar aquele que você está usando, clique o perfil e siga o assistente de configuração wizard.

13. Antivírus

O BitDefender traz consigo um módulo Antivírus que o ajuda a manter o seu BitDefender atualizado e o seu computador livre de vírus. Para entrar no módulo Antivírus, clique na barra **Antivírus**.



Antivírus

O módulo Antivírus consiste de duas secções:

- **Área de Status** - Exibe o status atual de todos os componentes de segurança monitorados e permite que você escolha quais destes componentes deve ser monitorado.
- **Tarefas Rápidas** - Aqui é onde você pode encontrar links para as mais importantes tarefas de segurança: Atualizar Agora, Análise dos Meus Documentos, Análise do Sistema, Análise Minuciosa e Análise Personalizada do Sistema.

13.1. Área de Estado

A área de estado é onde você pode ver a lista completa de componentes do módulo de segurança e seu estado atual. Ao monitorar cada módulo de segurança, o BitDefender irá permitir a você saber não somente quando você configurar as definições que podem afetar a segurança do seu computador, mas também quando você esquecer de executar tarefas importantes.

O estado atual de um componente é indicado utilizando sentenças explícitas e um dos seguintes ícones:

Círculo vermelho com uma marca de verificação: Nenhum problema afeta o componente.

Círculo vermelho com uma marca de exclamação: Problemas afetam o computador.

As sentenças descrevendo problemas estão escritas em vermelho. Apenas clique no botão **Corrigir** correspondente a sentença para corrigir o problema apontado. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

13.1.1. Configurando o Alerta de Status

Para selecionar os componentes que o BitDefender deve monitorar, clique em **Configure o Alerta de Status** e selecione a caixa de seleção **Habilitar alertas** correspondente às funções que você deseja que sejam rastreadas.

Importante

Para se assegurar que o seu sistema esteja totalmente protegido por favor habilite o rastreamento para todos os componentes e corrija todos os problemas apontados.

O estado dos seguintes componentes de segurança podem ser rastreados pelo BitDefender:

- **Antivírus** - O BitDefender monitora o estado dos dois componentes da funcionalidade Antivírus: Proteção em tempo-real e análise por demanda.

  Os problemas mais comuns apontados para esse componente estão listados na seguinte tabela.

Incidência	Descrição
A proteção em tempo-real está desativada	Os arquivos não são analisados conforme são acessados por você ou por um aplicativo em execução no sistema.
Esse PC nunca foi analisado a procura de vírus	Uma análise por demanda nunca foi executada para verificar se os arquivos armazenados no seu computador estão livres de malware.
A última análise do sistema que você iniciou foi abortada antes de ser finalizada	Uma análise completa dos sistema foi iniciada mas não foi completada.
O Antivírus está em um estado crítico	A proteção em tempo-real está desabilitada e uma análise do sistema está atrasada.

- **Atualização** - O BitDefender monitora se as assinaturas de malware estão atualizadas.

  Os problemas mais comuns apontados para esse componente estão listados na seguinte tabela.

Incidência	Descrição
A Atualização Automática está desativada	As assinaturas de malware do seu BitDefender não estão sendo automaticamente atualizas em uma base regular.
A atualização não foi executada a x dias	As assinaturas de malware do seu BitDefender estão desatualizadas.

13.2. Análises Rápidas

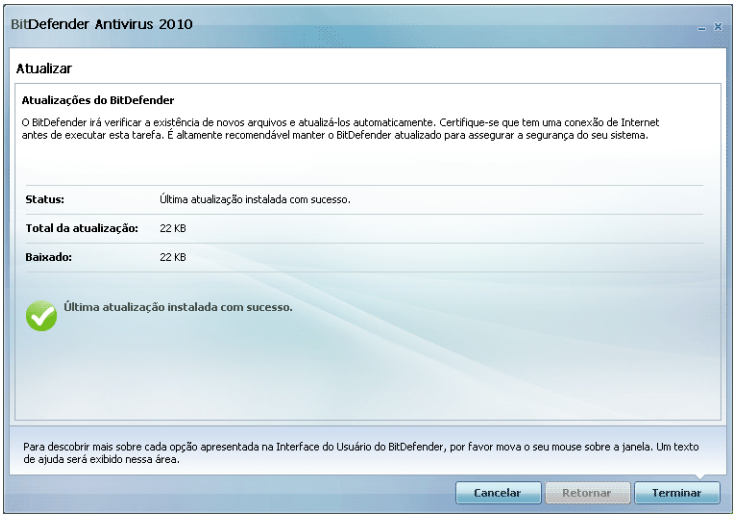
Aqui você pode encontrar links para as mais importantes tarefas de segurança:

- **Atualizar agora** - realiza uma atualização imediata.
- **Análise do Sistema** - começa uma análise completa do seu sistema (menos os arquivos comprimidos). Para tarefas adicionais de análise por demanda, clique em nesse botão e selecione uma tarefa diferente de análise: Análise de Meus Documentos ou Análise Minuciosa.
- **Análise Padronizada** - inicia um assistente que permite criar e executar uma tarefa de análise padronizada.

13.2.1. Atualizando o BitDefender

Novo malware é achado e identificado todos os dias. É por isso que é muito importante manter o BitDefender atualizado com as últimas assinaturas de malware.

Como padrão, O BitDefender verifica se há atualizações, quando você liga o computador e depois disto, o faz **de hora em hora**. No entanto, se você deseja atualizar o BitDefender, clique em **Atualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Atualizando o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

O processo de atualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Se deseja fechar esta janela, clique em **Cancelar**. No entanto, isso não irá parar o processo de actualização.

Nota
Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o BitDefender a pedido do usuário.

Reinicie o computador se necessário. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador: Clique em **Reiniciar** para reiniciar o seu sistema imediatamente.

Se deseja reiniciar o seu sistema mais tarde, clique apenas em **OK**. Nós recomendamos que você reinicie o computador o mais rápido possível.

13.2.2. A analisar com BitDefender

Para analisar o seu computador em busca de malware, execute uma tarefa de análise em particular, clicando no respectivo botão ou selecionando-a do menu. A

seguinte tabela aprsenta todas as tarefas disponíveis, com uma descrição de cada uma delas:

Tarefa	Descrição
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração padrão, ele analisa todos os tipos de malware além de rootkits.
Analisar o diretório Meus Documentos	Use esta tarefa para analisar pastas de usuários atuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto assegurará a segurança dos seus documentos, um espaço de trabalho seguro e aplicações limpas que se executam durante o iniciar do windows.
Análise Minuciosa	Analisa todo o sistema. Na configuração padrão, analisa em busca de todo tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Pessoal	Use esta tarefa para escolher arquivos ou pastas específicos a serem analisados.

Nota

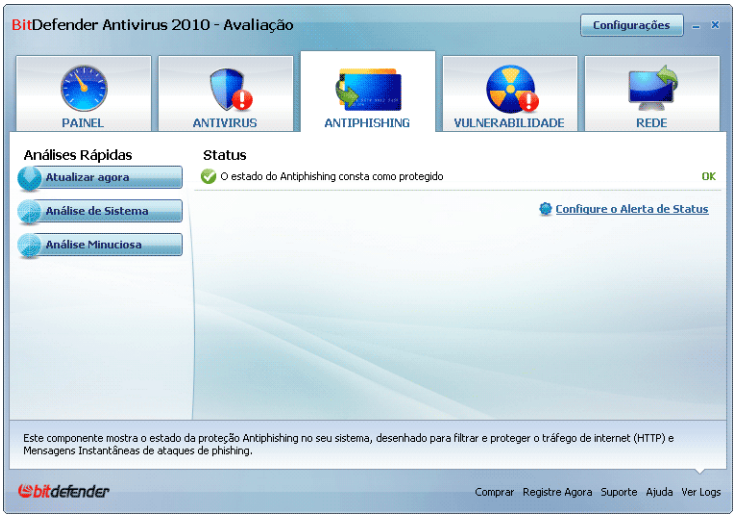
Um vez que as tarefas **Análise Minuciosa** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inativo.

Quando você executa uma Análise do Sistema, Análise Minuciosa ou Análise dos Meus Documentos, o assistente de análise por Antivírus irá aparecer. Siga o processo guiado de três passos para completar o processo de análise. Para informações detalhadas sobre esse assistente, por favor consulte a seção *"Assistente do analisador Antivírus"* (p. 51).

Quando você executar uma Análise Padronizada, o assistente de Análise Padronizada irá lhe guiar através do processo de análise. Siga o procedimento de seis passos para analisar arquivos ou diretórios específicos. Para informações detalhadas sobre esse assistente, por favor consulte a seção *"Assistente de Análise Customizado"* (p. 56).

14. Anti-Phishing

O BitDefender vem com um módulo Antiphishing que assegura que todas as páginas web que você acessa via Internet Explorer ou Firefox são seguras. Para entrar no módulo de Antiphishing, clique na barra **Antiphishing**.



Anti-Phishing

O módulo de Antiphishing é composto por duas secções:

- **Área de Status** - Exibe o status atual do módulo antiphising e permite que você ative / desative o rastreamento das atividades deste módulo.
- **Tarefas Rápidas** - Aqui é onde você pode encontrar links para importantes tarefas de segurança: Atualizar Agora, Análise do Sistema e Análise Minuciosa.

14.1. Área de Estado

O estado atual de um componente é indicado utilizando sentenças explícitas e um dos seguintes ícones:

Círculo vermelho com uma marca de verificação: Nenhum problema afeta o componente.

Círculo vermelho com uma marca de exclamação: Problemas afetam o computador.

As sentenças descrevendo problemas estão escritas em vermelho. Apenas clique no botão **Corrigir** correspondente a sentença para corrigir o problema apontado.

A incidência mais comum informada por este módulo é **O Antiphishing esta desabilitado**. Isso significa que o Antiphishing não está ativado para nenhum dos seguintes aplicativos suportados: Internet Explorer, Mozilla Firefox, Yahoo! Messenger ou Windows Live Messenger.

14.2. Análises Rápidas

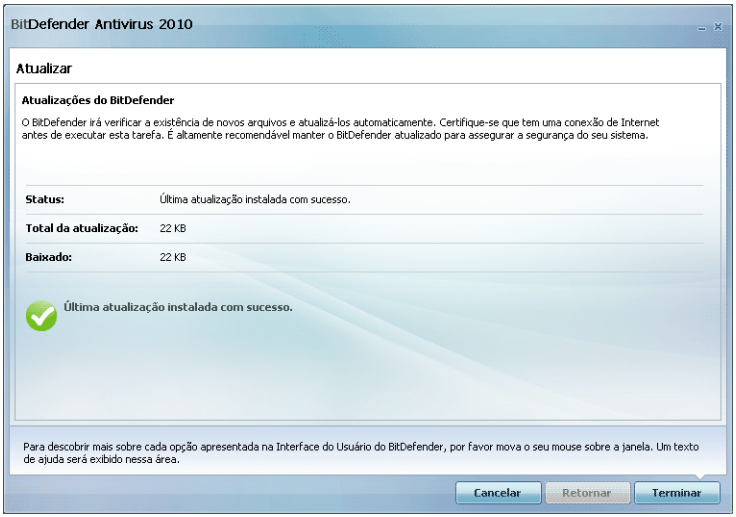
Aqui você pode encontrar links para as mais importantes tarefas de segurança:

- **Atualizar agora** - realiza uma atualização imediata.
- **Análise do Sistema** - inicia uma análise completa no seu computador (menos arquivos comprimidos).
- **Análise Minuciosa** - Inicia uma análise minuciosa no seu computador (incluindo arquivos comprimidos).

14.2.1. Atualizando o BitDefender

Novo malware é achado e identificado todos os dias. É por isso que é muito importante manter o BitDefender atualizado com as últimas assinaturas de malware.

Como padrão, O BitDefender verifica se há atualizações, quando você liga o computador e depois disto, o faz **de hora em hora**. No entanto, se você deseja atualizar o BitDefender, clique em **Atualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Atualizando o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

O processo de atualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Se deseja fechar esta janela, clique em **Cancelar**. No entanto, isso não irá parar o processo de actualização.

Nota
Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o BitDefender a pedido do usuário.

Reinicie o computador se necessário. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador: Clique em **Reiniciar** para reiniciar o seu sistema imediatamente.

Se deseja reiniciar o seu sistema mais tarde, clique apenas em **OK**. Nós recomendamos que você reinicie o computador o mais rápido possível.

14.2.2. A analisar com BitDefender

Para analisar o seu computador em busca de malware, execute uma tarefa de análise em particular, clicando no respectivo botão ou selecionando-a do menu. A

seguinte tabela aprsenta todas as tarefas disponíveis, com uma descrição de cada uma delas:

Tarefa	Descrição
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração padrão, ele analisa todos os tipos de malware além de rootkits.
Análise Minuciosa	Analisa todo o sistema. Na configuração padrão, analisa em busca de todo tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Nota

Um vez que as tarefas **Análise Minuciosa** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inativo.

Quando você executa uma Análise do Sistema ou Análise Minuciosa o assistente de análise por Antivírus irá aparecer. Siga o processo guiado de três passos para completar o processo de análise. Para informações detalhadas sobre esse assistente, por favor consulte a seção "*Assistente do analisador Antivírus*" (p. 51).

15. Vulnerabilidade

O BitDefender traz consigo um módulo de Vulnerabilidade que ajuda-o a manter o software mais crucial do seu PC sempre atualizado. Para monitorar e corrigir as Vulnerabilidade do seu sistema, clique na aba **Vulnerabilidade**.

Vulnerabilidade

O módulo de Vulnerabilidade é composto por duas secções:

- **Área de Status** - Exibe o status do módulo de Verificação de Vulnerabilidade e permite que você ative/desative o rastreamento das atividades deste módulo.
- **Tarefas Rápidas** - Aqui é onde você pode encontrar um link para o assistente de Verificação de Vulnerabilidade.

15.1. Área de Estado

O estado atual de um componente é indicado utilizando sentenças explícitas e um dos seguintes ícones:

Círculo vermelho com uma marca de verificação: Nenhum problema afeta o componente.

Círculo vermelho com uma marca de exclamação: Problemas afetam o computador.

As sentenças descrevendo problemas estão escritas em vermelho. Clique apenas o botão **Consertar** ou **Instalar** relativo a uma sentença para consertar a incidência relatada.

Os problemas mais comuns apontados para esse componente estão listados na seguinte tabela.

Status	Descrição
A Verificação de Vulnerabilidades está desativada	O BitDefender não verifica por vulnerabilidades potenciais de atualizações do Windows faltantes, atualização de aplicativos ou senhas fracas.
Múltiplas vulnerabilidades foram detectadas	O BitDefender encontrou atualizações faltantes do Windows/aplicativos e/ou senhas fracas.
Actualizações Criticas da Microsoft	Atualizações Críticas da Microsoft estão disponíveis mas não foram instaladas.
Outras Actualizações da Microsoft	As atualizações não críticas da Microsoft estão disponíveis mas não foram instaladas.
A Atualização Automática do Windows está desativada	As atualizações de segurança do Windows não estão sendo automaticamente instaladas logo que disponíveis.
`Aplicativo` (desatualizado)	Uma nova versão do `Aplicativo` está disponível mas não instalado.
`Usuário` (Senha Fraca)	A senha de um usuário é fácil de quebrar por pessoas maliciosas com programas especializados.

15.2. Análises Rápidas

Há apenas uma tarefa disponível:

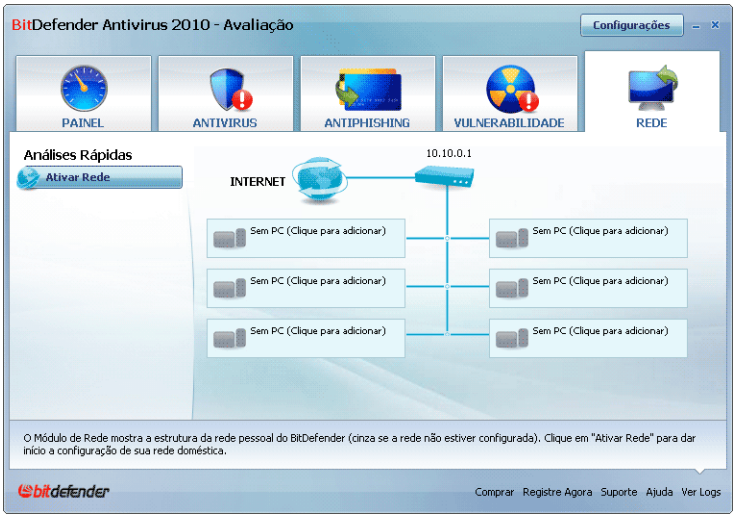
- **Análise de Vulnerabilidade** - inicia um assistente que verifica se há vulnerabilidades no seu sistema e ajuda você a resolvê-los.

A análise de Vulnerabilidade monitoriza as atualizações do Microsoft Windows, do Microsoft Windows Office e as senhas das contas Microsoft Windows para assegurar que o seu SO está atualizado e não se encontra vulnerável à quebra de senhas.

Para verificar o seu computador por vulnerabilidades, clique em **Análise de Vulnerabilidade** e siga o "*Assistente de Verificação de Vulnerabilidades*" (p. 63).

16. Rede

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador. Para entrar no Módulo de Rede, clique na aba **Rede**.



Rede

Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

1. Adira à rede pessoal do BitDefender no seu computador. Aderir à rede consiste em configurar uma senha administrativa para o gestor da rede pessoal.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a senha).
3. Volte para o seu computador e adicione os computadores que deseja gerir.

16.1. Análises Rápidas

Inicialmente só um botão está disponível.

- **Ativar Rede** - permite-lhe definir a senha de rede, e em seguida criar e entrar na rede.

Após aderir à rede, mais botões irão surgir.

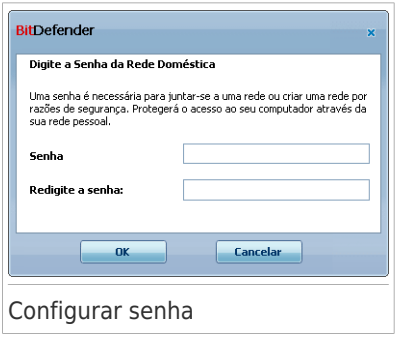
- **Desativar a Rede** - permite-lhe sair da rede.
- **Adicionar Computador** - permite que você adicione computadores à sua rede.

- **Analisar Todos** - permite-lhe analisar ao mesmo tempo todos os computadores geridos.
- **Atualizar Todos** - permite-lhe atualizar ao mesmo tempo todos os computadores geridos.
- **Registar Todos** - permite-lhe registar ao mesmo tempo todos os computadores geridos.

16.1.1. Aderir à Rede BitDefender

Para aderir à rede pessoal BitDefender, siga os seguintes passos:

1. Clique em **Ativar Rede**. Será notificado para configurar a senha de gestão de rede pessoal.



Configurar senha

2. Insira a mesma senha em cada um dos campos editáveis.
3. Clique em **OK**.

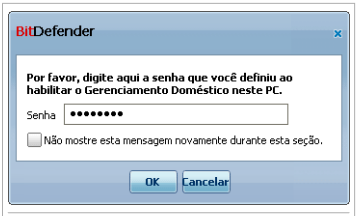
Pode ver o nome do computador a aparecer no mapa de rede.

16.1.2. Adicionar Computadores à Rede BitDefender

Antes que possa adicionar um computador à rede doméstica BitDefender, deve de configurar a sua senha de gestão de rede pessoal no respectivo computador.

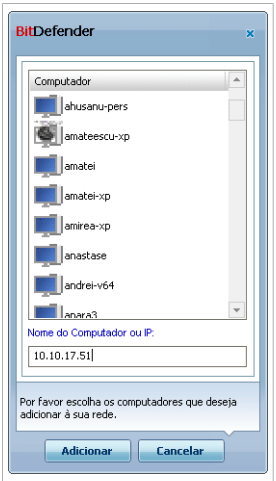
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

1. Clique em **Adicionar Computador**. Será notificado para inserir a sua senha de gestão de rede pessoal local.



Inserir senha

2. Insira a senha de gestão rede pessoal e clique em **OK**. Uma nova janela irá aparecer.



Adicionar Computador

Pode ver a lista dos computadores na rede. O significado do ícone é o seguinte:

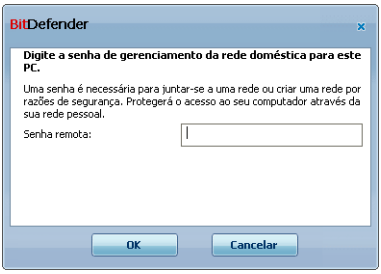
Indica um computador on-line sem produtos BitDefender instalados.

Indica um computador on-line com o BitDefender instalado.

Indica um computador offline com o BitDefender instalado.

3. Faça uma das coisas seguintes:
   - Selecione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.

4. Clicando **Adicionar**. Será notificado para inserir a sua senha de gestão de rede pessoal do respectivo computador.



Autenticar

5. Insira a senha de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**. Se forneceu a senha correta, a nome do computador selecionado aparecerá no mapa de rede.

Nota
Pode adicionar até cinco computadores neste mapa de rede.

16.1.3. Gerir a Rede BitDefender

Uma vez que tenha criado com sucesso a sua rede pessoal BitDefender pode gerir todos os produtos BitDefender a partir de um único computador.

Mapa de Rede

Se mover o curso do seu mouse sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afetar a segurança do sistema, o estado de registo do BitDefender).

Se você clicar com o botão direito do mouse sobre o nome de um computador no mapa de rede, você pode ver todas as tarefas administrativas que você pode executar no computador remoto.

- **Remover o PC da rede doméstica**

  Permite que você remova o PC da rede doméstica.

- **Registar o BitDefender neste computador**

  Permite que você registre o BitDefender neste computador digitando uma licença.

- **Definir uma senha para as definições em um PC remoto**

  Permite você criar uma senha para restringir o acesso às configurações do BitDefender neste PC.

- **Executar uma tarefa de análise por demanda**

  Permite você executar uma análise por demanda num computador remoto. Você pode executar qualquer das seguintes tarefas de análise: Analisar Meus Documentos, Análise de Sistema ou Análise Minuciosa do Sistema.

- **Reparar todas as incidências neste computador**

Permite que você corriga ocorrências que estão afetando a segurança deste computador seguindo o assistente Corrigir Todas Ocorrências.

- **Ver Histórico/Eventos**

  Permite que você acesse o módulo **História&Eventos** do produto BitDefender instalado neste computador.

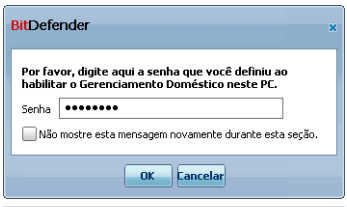
- **Atualizar Agora**

  Inicia o processo de atualização do produto BitDefender instalado neste computador.

- **Definir este computador como Servidor de Atualizações desta Rede**

  Permite que você defina este computador como um servidor de atualização para todos produtos BitDefender instalados nesta rede. Usando esta opção irá reduzir o tráfego de internet, porque apenas um computador na rede irá se conectar e fazer o download das atualizações.

Antes de executar uma tarefa num computador específico, voê será notificado para inserir a senha de gerenciamento de rede doméstica local.



Inserir senha

Insira a senha de gestão rede pessoal e clique em **OK**.

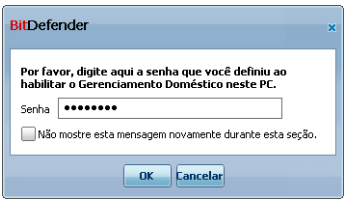
Nota

Se você planeja executar várias tarefas, você pode querer selecionar **Não mostrar essa mensagem novamente durante esta seção**. Ao selecionar esta opção, não será notificado novamente pela senha durante esta sessão.

16.1.4. Analisar Todos os Computadores

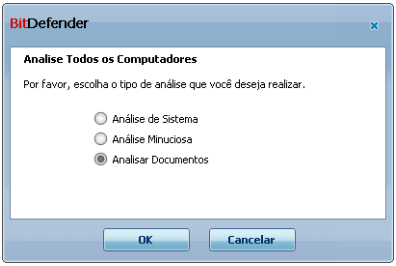
Para analisar todos os computadores geridos, siga estes passos:

1. Clique em **Analisar Todos**. Será notificado para inserir a sua senha de gestão de rede pessoal local.



Inserir senha

2. Selecione o tipo de análise.
   - **Análise do Sistema** - inicia uma análise completa no seu computador (menos arquivos comprimidos).
   - **Análise Minuciosa** - inicia uma análise minuciosa no seu computador (incluindo arquivos comprimidos).
   - **Analisar os Meus Documentos** - inicia uma análise rápida no diretório Documentos e Configurações.



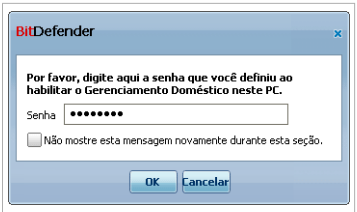
Seleccionar o Tipo de Análise

3. Clique em **OK**.

16.1.5. Atualizando Todos os Computadores

Para atualizar todos os computadores gerenciados, siga estes passos:

1. Clique em **Atualizar Todos**. Será notificado para inserir a sua senha de gestão de rede pessoal local.



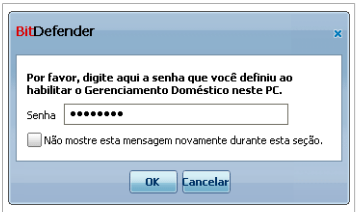
Inserir senha

2. Clique em **OK**.

16.1.6. Registar Todos os Computadores

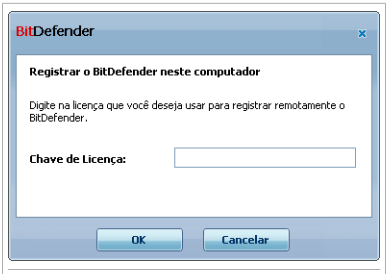
Para registar todos os computadores geridos, siga estes passos:

1. Clique em **Registar Todos**. Será notificado para inserir a sua senha de gestão de rede pessoal local.



Inserir senha

2. Insira a chave de licença que deseja usar para os registar.



Registar Todos

3. Clique em **OK**.

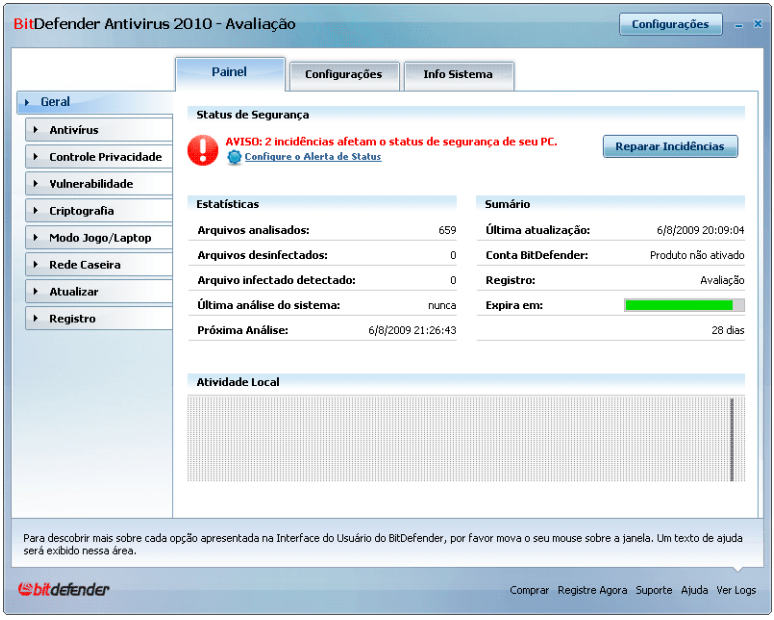
Modo Avançado

17. Geral

O módulo Geral dá-lhe informação sobre a atividade do BitDefender e do sistema. Aqui é onde pode modificar o comportamento global do BitDefender.

17.1. Painel

Para verificar se alguma ocorrência afeta seu computador, bem como estatística da atividade do produto e status do registro, vá até **Geral>Painel** no Modo Avançado.



Painel

O painel é composto de várias seções:

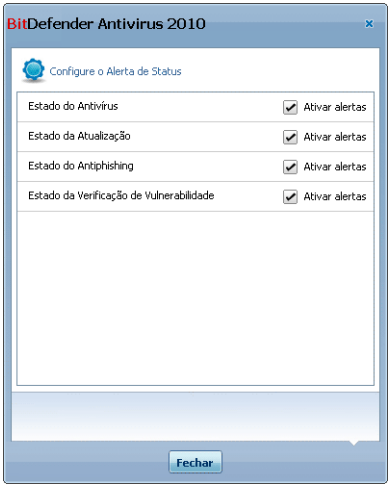
- **Estado Geral** - Lhe Informa sobre quaisquer problemas que afetam a segurança do seu computador.
- **Estatísticas** - Mostra informação importante com respeito à atividade do BitDefender.
- **Visão Geral** - Mostra o status da atualização, o estado da sua conta, e informação do seu registo e licença.

- **Atividade de Arquivo** - Indica a evolução dos números de objetos verificados pelo Antimalware do BitDefender. A barra de altura indica a intensidade do tráfego durante aquele intervalo de tempo.

17.1.1. Status Geral

Aqui é onde você pode encontrar o número de ocorrências que estão afetando a segurança do seu computador. Para remover todas ameaças, clique **Corrigir todas ocorrências**. Isto iniciará o assistente Corrigir Todas Ocorrências wizard.

Para configurar os módulos que serão monitorados pelo BitDefender Antivírus 2010, clique em **Configurar o Monitoramento de Status**. Uma nova janela irá aparecer:



Configure o Alerta de Status

Se você quiser que o BitDefender monitore um componente, selecione a caixa de seleção **Ativar alertas** para o componente. O estado dos seguintes componentes de segurança podem ser rastreados pelo BitDefender:

- **Antivírus** - O BitDefender monitora o estado dos dois componentes da funcionalidade Antivírus: Proteção em tempo-real e análise por demanda.

  Os problemas mais comuns apontados para esse componente estão listados na seguinte tabela.

Incidência	Descrição
A proteção em tempo-real está desativada	Os arquivos não são analisados conforme são acessados por você ou por um aplicativo em execução no sistema.
Você nunca analisou o seu computador em busca de malware	Uma análise por demanda nunca foi executada para verificar se os arquivos armazenados no seu computador estão livres de malware.
A última análise do sistema que você iniciou foi abortada antes de ser finalizada	Uma análise completa dos sistema foi iniciada mas não foi completada.
O Antivírus está em um estado crítico	A proteção em tempo-real está desabilitada e uma análise do sistema está atrasada.

- **Atualização** - O BitDefender monitora se as assinaturas de malware estão atualizadas.

  Os problemas mais comuns apontados para esse componente estão listados na seguinte tabela.

Incidência	Descrição
A Atualização Automática está desativada	As assinaturas de malware do seu BitDefender não estão sendo automaticamente atualizas em uma base regular.
A atualização não foi executada a x dias	As assinaturas de malware do seu BitDefender estão desatualizadas.

- **Antiphishing** - O BitDefender monitora o estado do recurso Antiphishing. Se ele não está ativado para todas as aplicações suportadas, a advertência **O Antiphishing está desativado** será mostrada.
- **Verificação de Vulnerabilidades** - O BitDefender mantém registro do recurso de Verificação de Vulnerabilidades. A Verificação de Vulnerabilidades permite-lhe saber se você precisa instalar qualquer atualização do Windows, a atualizações de aplicativos ou se você precisa reforçar alguma senha.

  Os problemas mais comuns apontados para esse componente estão listados na seguinte tabela.

Status	Descrição
A Verificação de Vulnerabilidades está desativada	O BitDefender não verifica por vulnerabilidades potenciais de atualizações do Windows faltantes, atualização de aplicativos ou senhas fracas.
Múltiplas vulnerabilidades foram detectadas	O BitDefender encontrou atualizações faltantes do Windows/aplicativos e/ou senhas fracas.
Actualizações Criticas da Microsoft	Atualizações Críticas da Microsoft estão disponíveis mas não foram instaladas.
Outras Actualizações da Microsoft	As atualizações não críticas da Microsoft estão disponíveis mas não foram instaladas.
A Atualização Automática do Windows está desativada	As atualizações de segurança do Windows não estão sendo automaticamente instaladas logo que disponíveis.
`Aplicativo` (desatualizado)	Uma nova versão do `Aplicativo` está disponível mas não instalado.
`Usuário` (Senha Fraca)	A senha de um usuário é fácil de quebrar por pessoas maliciosas com programas especializados.

Importante

Para se assegurar que o seu sistema esteja totalmente protegido por favor habilite o rastreamento para todos os componentes e corrija todos os problemas apontados.

17.1.2. Estatísticas

Se deseja dar uma espreitadela à atividade do BitDefender, um bom lugar para começar é a seção de Estatísticas. Pode ver os seguintes itens:

Item	Descrição
arquivos analisados	Indica o número de arquivos que foram analisados até ao momento da sua última análise.
arquivos desinfectados	Indica o número de arquivos que foram desinfectados até ao momento da sua última análise.
Arquivos Infectados detectados	Indica o número de arquivos infectados que foram encontrados no seu sistema durante a última análise.
Última Análise do Sistema	Indica quando o seu computador foi analisado pela última vez. Se o seu computador foi analisado a mais de uma semana, por favor analise seu computador o mais rápido possível. Para analisar o computador inteiro, vá em

Item	Descrição
	Antivírus, na aba Análise de Vírus, e execute a Análise Completa ou a Análise Minuciosa.
Próxima análise	Indica a próxima vez em que o computador será analisado.

17.1.3. Sumário

Aqui é onde você pode acompanhar o status da atualização, de sua conta, o registro e as informações da licença.

Item	Descrição
Última atualização	Indica quando o o seu produto BitDefender foi atualizado pela última vez. Faça atualizações regulares, a fim de ter um sistema totalmente protegido.
Conta na BitDefender	Indica o endereço de e-mail que pode usar para acessar à sua conta on-line para recuperar a sua chave de licença perdida e beneficiar do suporte BitDefender e de outros serviços personalizados. Você deve criar uma conta BitDefender para poder ativar o seu produto. Para saber mais informações sobre a conta BitDefender, por favor consulte em "*Registro e Minha Conta*" (p. 46).
Registro	Indica o seu tipo de licença e o seu estado. Para manter o seu sistema seguro tem de renovar ou efectuar o upgrade do BitDefender se a sua chave de licença tiver expirado.
Expira em	Indica o número de dias que faltam até que a sua chave de licença expire. Se a sua chave de licença expirar nos próximos dias, por favor registre o produto com uma nova chave de licença. Para comprar ou renovar uma chave, clique no link **Comprar/Renovar**, localizado na parte de baixo da janela.

17.2. Configurações

Para efetuar as configurações gerais do BitDefender e para gerenciar suas configurações, vá para **Configurações>Geral** no modo Avançado.

Configurações Gerais

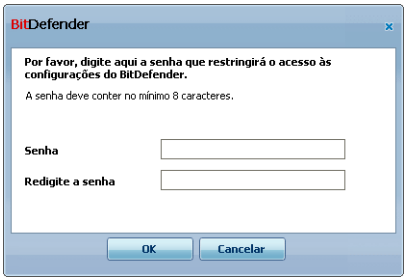
Aqui você pode ajustar o comportamento integral do BitDefender. Por padrão, o BitDefender é carregado na inicialização do Windows e então roda minimizado na área de notificação.

17.2.1. Configurações Gerais

- **Ativar proteção por senha** - ativa a inserção de uma senha para proteger a configuração do BitDefender.

  Nota
  Se você não é a única pessoa a usar esse computador com direitos de administrador, é recomendado que você proteja suas configurações do BitDefender com uma senha.

  Se você selecionar esta opção, a seguinta janela irá aparecer:



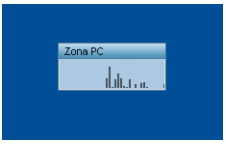
Confirmar senha

Insira a senha no campo **Senha** re-digite no campo **Redigite a senha** e clique em **OK**.

Uma vez que tenha definido a senha, será solicitado que a insira sempre que deseje alterar as configurações do BitDefender. Os outros administradores de sistema (se existirem) também terão de inserir a senha se desejarem alterar as configurações do BitDefender.

Importante
Se você esqueceu a senha, terá que reparar o produto para modificar a configuração do BitDefender.

- **Receber Notícias BitDefender (notificações de segurança)** - de tempos em tempos recebe notificações de segurança com relação a novas epidemias de vírus, enviadas pelo servidor BitDefender.
- **Mostrar pop-ups (notas na tela)** - mostrar janelas pop-up a respeito do status do produto. Você pode configurar o BitDefender para exibir pop-ups apenas quando a interface está no modo Iniciante / Intermediário ou Avançado.
- **Mostrar a barra de Atividade de Análise (na tela gráfica de atividade do produto)** - mostra a Barra de Atividade de Análise sempre que você se logar ao Windows. Limpe esta caixa se deseja que a barra de Atividade da Análise não seja mostrada daí em diante.



Barra de Atividade da Análise

Nota
Esta opção pode ser configurada apenas para a atual conta de usuário Windows. A barra de atividade da Análise só está disponível quando a interface está em Modo Avançado.

17.2.2. Configurações do Relatório de Vírus

- **Enviar relatórios de vírus** - envia a BitDefender relatórios com os vírus identificados em seu computador. Isso nos ajuda a manter controle de epidemias de vírus.

O relatório não contém dados confidenciais, tais como seu nome, endereço de IP ou outros, e não será usado para propósitos comerciais. A informação fornecida conterá apenas o nome do vírus e será usada somente para criar estatísticas.

- **Ativar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  O relatório não contém dados confidenciais, tais como seu nome, endereço de IP ou outros, e não será usado para propósitos comerciais. A informação fornecida conterá apenas o potencial vírus e será usada somente para detectar novos vírus.

17.3. Informação do Sistema

BitDefender permite-lhe visualizar, a partir de uma única localização, todas as configurações do sistema e as aplicações registadas para se executarem durante o iniciar do Windows. Desta forma, pode gerir a atividade da seu sistema e as aplicações instaladas nele como também identificar possíveis infecções.

Para obter a informação do sistema, vá para**Geral>Informação do Sistema** no Modo Avançado.

Informação do Sistema

A lista contém todos os itens carregados quando o sistema é iniciado como também os itens carregados por várias aplicações.

Três botões estão disponíveis:

- **Restaurar** - muda a atual associação de arquivos para padrão. Disponível apenas para as definições das **Associações de Arquivos**!
- **Ir Para** - abre uma janela onde o item selecionado é colocado (o **Registro** por exemplo).

Nota
Dependendo do item seleccionado o botão **Ir Para** poderá não aparecer.

- **Atualizar** - reabre a seção **Info Sistema**.

18. Antivírus

BitDefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora). A proteção que o BitDefender oferece está dividida em duas categorias:

- Proteção em Tempo-real - previne que novas ameaças de malware entrem no seu sistema. Por exemplo, BitDefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

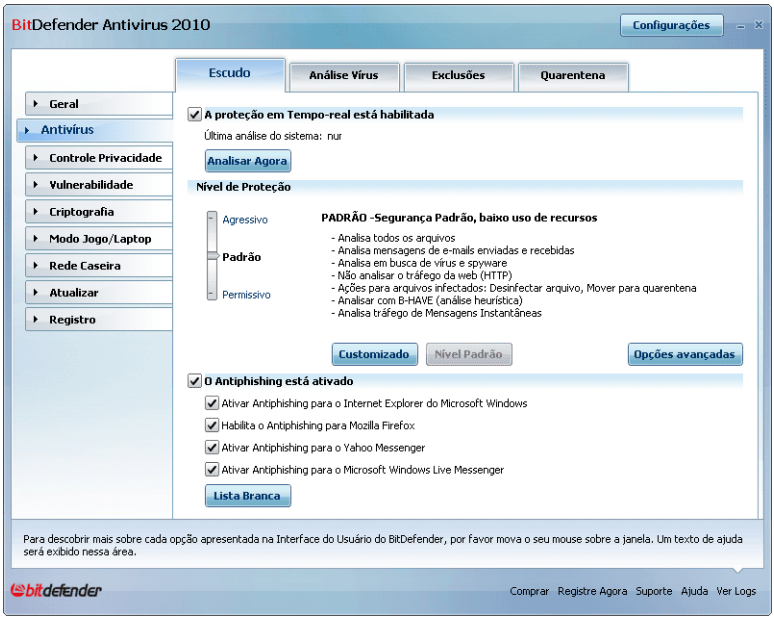
  Nota
  A proteção em Tempo-real, também referida como análise no acesso - os arquivos são analisados à medida que os usuários lhes acessem.

- Análise a-pedido - permite detectar e remover malware que já se encontra a residir no seu sistema. Esta é uma análise clássica iniciada pelo usuário – você escolhe qual a drive, pasta ou arquivo o BitDefender deverá analisar, e o mesmo é analisado – a-pedido. A tarefa de análise permite que crie rotinas personalizadas de análise e elas podem ser agendadas para serem executadas numa base regular.

18.1. Proteção em Tempo-real

O BitDefender providencia uma proteção contínua e em tempo-real, contra todo tipo de ameaças de malware ao analisar os arquivos acessados, e as comunicações feitas através de aplicaticos de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). O BitDefender Antiphishing impede que seja revelada informação pessoal enquanto explora a internet ao alertá-lo acerca das páginas web potencialmente phishing.

Para configurar a proteção em tempo-real e o BitDefender Antiphishing, clique em **Antivírus>Escudo** no Modo Avançado.



Proteção em Tempo-real

Você pode ver se a proteção em tempo-real está ativada ou desativada. Se deseja mudar o atual status da proteção em Tempo-real, limpe ou selecione a respectiva caixa de seleção.

Importante
Para prevenir que o seu computador seja infectado por vírus, mantenha ativa a **Proteção em Tempo-real**.

Para dar início a uma análise no sistema, clique em **Analisar Agora**.

18.1.1. Configurar Nível de Proteção

Pode escolher o nível de proteção que melhor se adapta às suas necessidades de segurança. Arraste o barra deslizante ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de proteção:

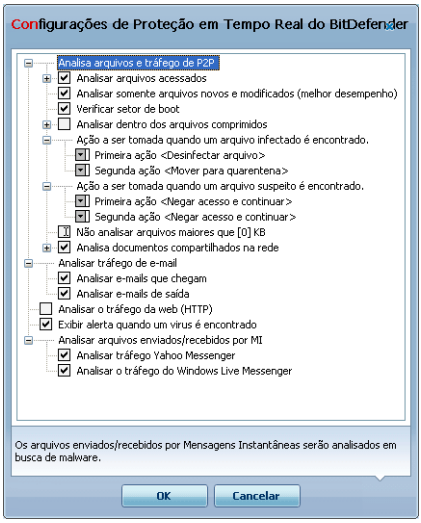
Nível de Proteção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Apenas programas e mensagens de e-mail são analisados em busca de vírus. Além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As ações executadas em arquivos infectados são as seguintes: limpar arquivo/mover para quarentena.
Por Padrão	Oferece segurança standard. O nível de consumo de recursos é baixo. Todos os arquivos e mensagens de e-mail de entrada&saída são analisados em busca de vírus e spyware. Além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As ações executadas em arquivos infectados são as seguintes: limpar arquivo/mover para quarentena.
Agressivo	Oferece uma segurança elevada. O nível de consumo de recursos é moderado. Todos os arquivos,mensagens de e-mail de entrada&saída e tráfego de web são analisados em busca de vírus e spyware. Além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As ações executadas em arquivos infectados são as seguintes: limpar arquivo/mover para quarentena.

Para aplicar as configurações padrão de proteção em tempo real clique em **Nível Padrão**.

18.1.2. Nível Personalizado de Proteção

Os usuários avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de arquivos, diretorios ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Você pode personalizar **Proteção em Tempo-real** ao clicar **Nível personalizado**. A seguinte janela aparecerá:



Configurações do Escudo

As opções de análise são organizadas como um menu expansível muito semelhante aos menus usados para explorar o Windows. Clique na caixa com "+" para abrir uma opção ou na caixa com "-" para fechar uma opção.

Nota

Você pode observar que algumas opções de verificação, embora tenham o sinal de "+", não podem ser abertas. A razão é que essas opções ainda não estão selecionadas. Você observará que, se você selecioná-las, elas poderão ser abertas.

- **Analisa arquivos acessados e transferência P2P** - para verificar os arquivos acessados e comunicação entre programas de mensagens instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Selecione também o tipo de arquivos a serem verificados.

Opção		Descrição
Analisar arquivos acedidos	**Verificar todos os arquivos**	Todos os arquivos acessados serão analisados, não importando o tipo.
	Analisar apenas os aplicativos	Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`;

Opção		Descrição
		.ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Verificar as extensões definidas pelo usuário	Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";".
	Analisar em busca de riskware	Analisar em busca de riskware. Os arquivos detectados serão tratados como arquivos infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa. Selecione **Não analisar discadores e aplicações** e/ou **Não analisar keyloggers** se você quiser excluir esses tipos de arquivos da análise.
Analisar apenas arquivos novos e alterados		Analisa apenas arquivos que não foram analisados antes ou que tenham sido alterados desde a última vez que foram analisados. Ao selecionar esta opção, você pode melhorar bastante a resposta do sistema com um impacto mínimo em segurança.
Verificar setores de boot		Para verificar o setor de boot do sistema.
Verificar dentro dos arquivos comprimidos		Arquivos de backup acessados também serão verificados. Com essa opção ativada, o computador ficará lento. Você pode definir o tamanho máximo de arquivos a serem analisados (em kilobytes, digite 0 se quiser que todos os arquivos sejam analisados) e a profundidade máxima dos arquivos para analisar.
Primeira Ação.		Selecionar do menu drop-down a primeira ação a ser executada sobre um arquivo infectado ou suspeito.

Opção		Descrição
	Negar acesso e continuar	Caso um arquivo infectado seja detectado, o acesso a ele será negado.
	Desinfetar o arquivo	Remove o código malware dos arquivos infectados.
	Apagar arquivo	Apaga o arquivo infectado imediatamente, sem avisar.
	Mover o arquivo para a quarentena	Move os arquivos infectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Segunda Acão		Selecione através do menu a segunda ação a ser tomada em arquivos infectados, caso a primeira ação falhe.
	Negar acesso e continuar	Caso um arquivo infectado seja detectado, o acesso a ele será negado.
	Apagar arquivo	Apaga o arquivo infectado imediatamente, sem avisar.
	Mover o arquivo para a quarentena	Move os arquivos infectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Não analisar arquivos maiores que [x] Kb		Digite o tamanho máximo dos arquivos a serem verificados. Se o tamanho for 0Kb, todos os arquivos serão verificados.
Analisar compartilhamentos de rede	**Verificar todos os arquivos**	Todos os arquivos acessados na rede serão analisados, não importando o tipo.
	Analisar apenas os aplicativos	Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`;

Opção		Descrição
		.lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Verificar as extensões definidas pelo usuário	Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";".

- **Analisar tráfego de e-mail** - analisa o tráfego de e-mail.

  As seguintes opções estão disponíveis:

Opção	Descrição
Analisar e-mail de entrada	Analisa todas as mensagens de e-mail de entrada.
Analisar e-mail de saída	Analisa todas as mensagens de e-mail de saída.

- **Analisar tráfego de internet (HTTP)** - Analisa o tráfego HTTP.
- **Exibir alerta quando um vírus é encontrdo** - uma janela de alerta será exibida quando um vírus for encontrado em um arquivo ou e-mail.

  Para um arquivo infectado a janela de alerta conterá o nome do vírus, a localização, a ação a ser tomada e a referência onde achar mais informação. Para um e-mail infectado a janela de alerta também conterá informação sobre o remetente e o destinatário.

  Caso um arquivo suspeito é detectado você pode executar um assistente que o ajudará a mandar este arquivo para o Laboratório BitDefender para uma melhor análise. Você pode digitar o seu endereço de e-mail para receber informação sobre este relatório.

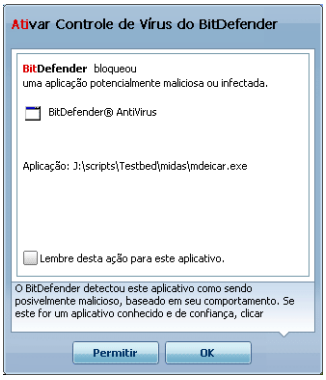
- **Analisar arquivos recebidos/enviados por MI.** Para analisar todos os arquivos enviados ou recebidos via Yahoo Messenger ou Windows Live Messenger, selecione a caixa correspondente.

Clique em **OK** para guardar as alterações e fechar a janela.

18.1.3. Configurando as definições do Controle Ativo de Vírus

O Controle Ativo de Vírus do BitDefender (CAV) fornece uma camada de proteção contra as novas ameaças para as quais ainda não foram desenvolvidas vacinas. Monitoriza constantemente o comportamento dos aplicativos sendo executados no seu computador e alerta-o se um aplicativo apresentar um comportamento suspeito.

O CAV pode ser configurado para alertar-lo e solicitar uma ação sempre que um aplicativo tentar executar uma ação maliciosa.



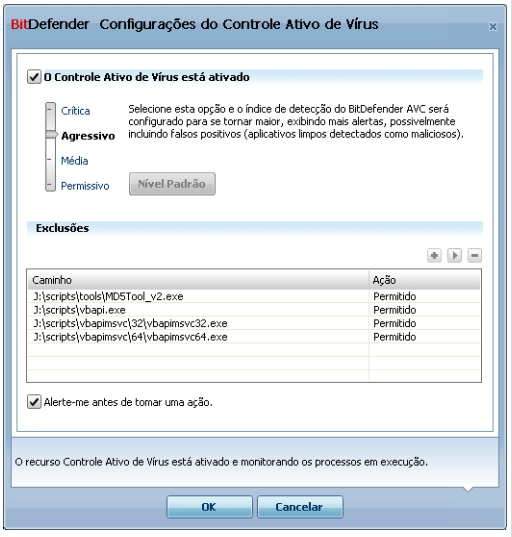
Alerta do CAV BitDefender

Se conhece e confia no aplicativo detectado, clique em **Permitir**.

Se deseja fechar imediatamente o aplicativo, clique em **OK**.

Selecione o campo**Lembrar esta ação para este aplicativo** antes de fazer sua escolha e o BitDefender irá executar a mesma ação para a ação detectada no futuro. A regra então criada será listado na tabela em **Exclusões**.

Para configurar O Controle Ativo de Vírus, clique em **Definições do BD CAV**.



Definições do BitDefender CAV

Selecione a opção correspondente para ativar o Controle Ativo de Vírus.

Importante

Mantenha o Controle Ativo de Vírus ativado para ficar protegido contra vírus desconhecidos.

Se você quiser ser alertado e questionado sobre uma ação pelo Controle Ativo de Vírus sempre que um aplicativo tentar executar uma ação possivelmente maliciosa, selecione o campo **Pergunte-me antes de executar uma ação**.

Configurar Nível de Proteção

O nível de proteção do Controle Ativo de Vírus muda automaticamente quando você define um novo nível de proteção em tempo-real. Se não está satisfeito com a configuração padrão, você pode configurar o nível de proteção manualmente.

Nota

Lembre-se que se você alterar o nível de proteção atual da proteção em tempo-real, o nível de proteção do CAV irá mudar também. Se você configurou a proteção em tempo real para **Tolerável**, o Controle Ativo de Vírus é automaticamente desativado e você não pode configurá-lo.

Arraste a barra deslizante ao longo da escala para definir o nível de proteção que considera apropriado para as suas necessidades de segurança.

Nível de Proteção	Descrição
Crítico	Uma monitoração rigorosa de todos os aplicativos para possíveis ações maliciosas.
Por Padrão	As taxas de detecção são elevados e falsos positivos são possíveis.
Médio	A Monitoração de Aplicativos é moderada, alguns falsos positivos ainda são possíveis.
Permissivo	Taxas de detecção são baixas e não existem falsos positivos.

Gerenciando a lista de Aplicativos Confiáveis/não confiáveis

Você pode adicionar aplicativos que você conhece e confia à lista de aplicativos confiáveis. Estes aplicativos não serão mais verificados pelo Controle Ativo de Vírus do BitDefender e irão automaticamente ter acesso permitido. D mesmo modo, os aplicativos que você sempre deseja negar o acesso podem ser adicionados à lista de aplicativos não confiáveis e o Controle Ativo de Vírus do BitDefender irá automaticamente bloqueá-los.

Os aplicativos para o qual você criou regras estão listados na tabela **Exclusões**. O caminho para o aplicativo e a ação que você definiu para ele (permitir ou bloquear) é exibido para cada regra.

Para gerenciar a lista, use os botões colocados acima da tabela:

- **Adicionar** - adicionar um novo aplicativo à lista.
- **Remover** - remover um aplicativo da lista.
- **Editar** - edita uma regra de aplicativo.

18.1.4. Desativando a Proteção em Tempo-real

Se deseja desativar a Proteção em Tempo-real, uma janela de aviso irá aparecer. Deverá confirmar a sua escolha ao selecionar no menu durante quanto tempo deseja que a sua proteção em tempo-real fique desativada. Pode desativar a sua proteção em tempo-real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção

Esta é uma incidência de segurança critica. Recomendamos que desative a proteção em tempo-real o menor tempo possível. Quando a mesma está desativada você deixa de estar protegido contra ameaças de malware.

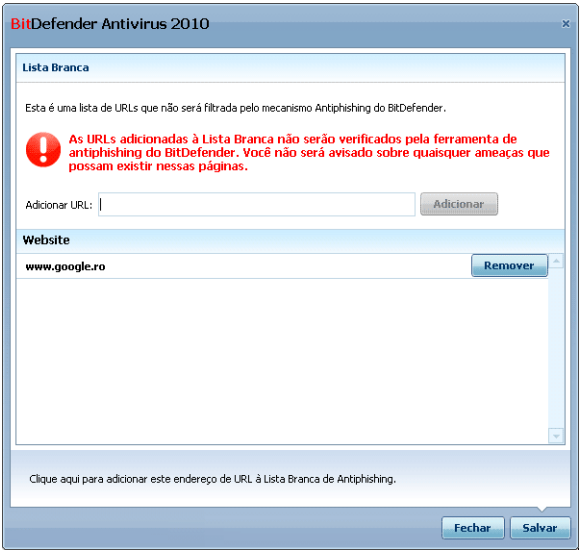
18.1.5. Configurar Proteção Antiphishing

O BitDefender oferece uma proteção Antiphishing em tempo-real para:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live Messenger(MSN)

Você pode escolher desativar a proteção Antiphishing completamente ou somente para determinadas aplicações.

Pode clicar em **Lista Branca** para configurar e gerir a lista dos sites web que não devem ser analisados pelos motores de antiphishing do BitDefender.



Lista Branca do AntiPhishing

Pode ver toda a lista dos sites web que não estão a ser analisados pelos motores de antiphishing do BitDefender.

Para adicionar um site à Lista Branca, insira o seu endereço no campo **Novo endereço** e depois clique em **Adicionar**. A lista branca deve de conter apenas os websites em que confia plenamente. Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Nota

Você pode facilmente gerenciar a proteção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada ao Internet Explorer. Para mais informações, por favor, vá para *"Integração com Exploradores web"* (p. 202).

Para remover um site web da lista branca, selecione-a e clique o botão correspondente **Remover**.

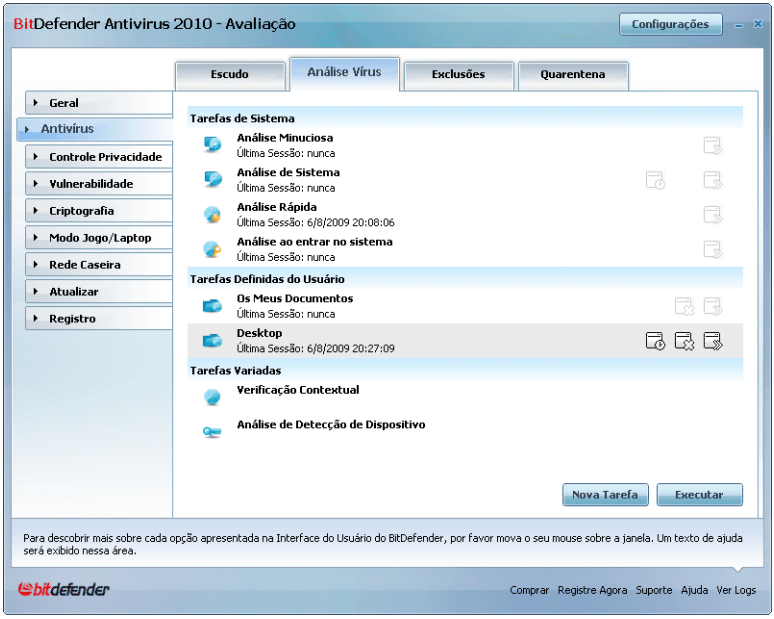
Clique **Salvar** para salvar as alterações e fechar a janela.

18.2. Análise por demanda

O objetivo principal para o BitDefender é manter seu computador livre de vírus. Isso é feito primordialmente mantendo novos vírus fora de seu computador e verificando seus e-mails e novos arquivos copiados para seu sistema.

Há o risco que um vírus já esteja alojado em seu sistema, antes mesmo de você instalar o BitDefender. É por isso que é uma ótima idéia verificar seu computador contra vírus residentes após instalar o BitDefender. E é definitivamente uma boa idéia verificar seu computador freqüentemente contra vírus.

Para configurar e iniciar a análise por demanda, vá para **Antivirus>Análise de Vírus** no Modo Avançado.



Tarefas de Análise

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados. Você pode analisar o computador sempre que desejar,ao executar as tarefas padrão deanálise, ou as suas próprias tarefas de análise (tarefas definidas pelo usuário). Pode também agendá-las para que se executem regularmente, ou quando o sistema estiver sem ser usado, de forma a não interferir com o seu trabalho

18.2.1. Tarefas de Análise

O BitDefender vem com diversas tarefas, criadas por padrão, que cobrem as incidências de segurança mais comuns. Pode também criar as suas próprias tarefas personalizadas.

Cada tarefa tem uma janela de **Propriedades** que o permite configurar a tarefa e ver os resultados da análise. Para mais informação, consulte *"Configurar Tarefas de Análise" (p. 117)*.

Existem três categorias de tarefas de análise:

- **Tarefas do Sistema** - contém a lista das tarefas padrão do sistema. As seguintes tarefas estão disponíveis:

Tarefa Padrão	Descrição
Análise Minuciosa	Analisa todo o sistema. Na configuração padrão, analisa em busca de todo tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração padrão, ele analisa todos os tipos de malware além de rootkits.
Análise Rápida do Sistema	Analisa os diretórios do `Windows` e dos `Arquivos de Programas`. Na configuração padrão, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.
Análise Autologon	Analisar os itens que são executados quando o usuário entra no Windows. Por default, a análise de autologon está desabilitada. Se você deseja usar esta tarefa, clique com o botão direito do mouse nela, selecione **Agendar** e programe a tarefa para rodar **quando o sistema iniciar**. Você poderá especificar em quanto tempo, após o início, a tarefa deverá começar a rodar (em minutos).

Nota

Um vez que as tarefas **Análise Minuciosa** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inativo.

- **Tarefas do Usuário** - contém as tarefas definidas pelo usuário.

  Uma tarefa chamada `Os Meus Documentos` é fornecida. Use esta tarefa para analisar pastas de usuários atuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

- **Tarefas Misc** - contém uma lista de tarefas de análise variadas. Estas tarefas de análise dizem respeito a tipos de análise alternativas que não podem ser executadas a partir desta janela. Apenas pode modificar as suas configurações ou ver os relatórios de análise.

Três botões estão disponíveis à direita de cada tarefa:

- **Agendar Tarefas** - indica que a tarefa seleccionada é agendada para mais tarde. Clique neste botão para abrir a janela **Propriedades**, barra Agendador, onde poderá ver a tarefa agendada e modificá-la.
- **Apagar** - remove a tarefa seleccionada.

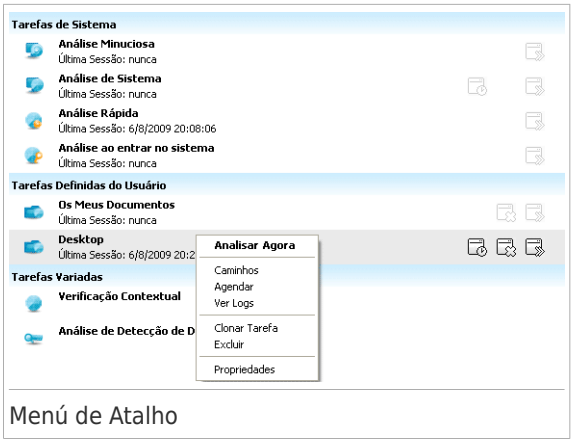
  Nota
  Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **Analisar Agora** - executa a tarefa seleccionada dando início a uma análise imediata.

À esquerda de cada tarefa pode ver o botão**Propriedades**, que o permite configurar a tarefa ou ver os relatórios da análise.

18.2.2. Usando o Menú de Atalho

Um menú de atalho está disponível para cada tarefa. Clique com o botão direito do mouse sobre a tarefa para a abrir.



Menú de Atalho

Os seguintes comandos estão disponíveis no menu de atalho:

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.
- **Caminhos** - abre a janela**Propriedades**, AbaCaminhos, onde você pode mudar o caminho de analise para a tarefa selecionada.

  Nota
  No caso de tarefas do sistema, esta opção é substituída por **Mostrar Caminho das Tarefas**, onde apenas poderá ver o alvo da análise.

- **Agenda** - abre a janela **Propriedades**, AbsAgenda, onde você poderá agendar a tarefa selecionada.
- **Visualizar Logs** - abre a janela **Propriedades**, AbaLogs, onde você pode ver os relatórios gerados após as tarefas selecionadas serem executadas.
- **Clonar tarefa** - Duplica a tarefa selecionada. Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
- **Apagar** - apaga a tarefa selecionada.

  Nota
  Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **Propriedades** - abre a janela **Propriedades**, abaResumo, onde você pode mudar as configurações da tarefa selecionada.

Nota

Devido à sua natureza em particular da categoria **Tarefas Diversas**, somente as opções **Visualizar Logs** e **Propriedades** estarão disponíveis neste caso.

18.2.3. Criando Tarefas de Análise

Para criar uma tarefa de análise, use um dos seguintes métodos:

- Clonar uma tarefa existente, renomeie e faça as alterações necessárias na janeçaPropriedades .
- Clique em **Nova Tarefa** para criar uma nova tarefa e configurá-la.

18.2.4. Configurar Tarefas de Análise

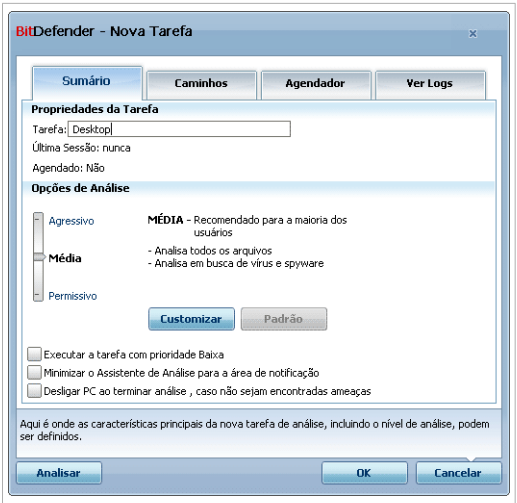
Cada tarefa de análise tem as sua própria janela de**Propriedades**, onde pode configurar as opções de análise, definir o alvo da análise, agendar a tarefa ou ver os relatórios. Para abrir esta janela clique no botão **Propriedades**, localizado no lado direito da tarefa (ou dê em clique com o botão direito do mouse sobre a tarefa e depois clique em **Propriedades**).

Nota

Para mais informação sobre ver os logs e a barra de **Logs** tab, por favor consulte "*Ver os Relatórios da Análise*" (p. 137).

Configurar Definições da Análise

Para configurar as opções de análise de uma específica tarefa de análise, clique com o lado direito do mouse e selecione **Propriedades**. A seguinte análise irá aparecer:



Sumário

Aqui pode ver a informação acerca da tarefa (nome, a última vez que se executou e o seu estado de agendamento) e definir as configurações da análise.

Escolher Nível de Análise

Pode facilmente configurar a análise ao escolher o nível de análise. Arraste o marcador ao longo da escala para definir o nível de análise apropriada.

Existem 3 níveis de análise:

Nível de Proteção	Descrição
Permissivo	Oferece uma eficiência razoável de detecção. O consumo de recursos é baixo. Apenas programas são analisados em busca de vírus. Além da análise clássica baseada em assinaturas, a análise heurística também é utilizada.
Por Padrão	Oferece uma boa eficiência de detecção. O nível de consumo de recursos é moderado. Todos os arquivos são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em vacinas, a análise heurística também é utilizada.

Nível de Proteção	Descrição
Elevado	Oferece uma elevada eficiência de detecção. O nível de consumo de recursos é elevado. Todos os arquivos e arquivos são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.

Uma série de opções gerais estarão disponíveis para o processo de análise:

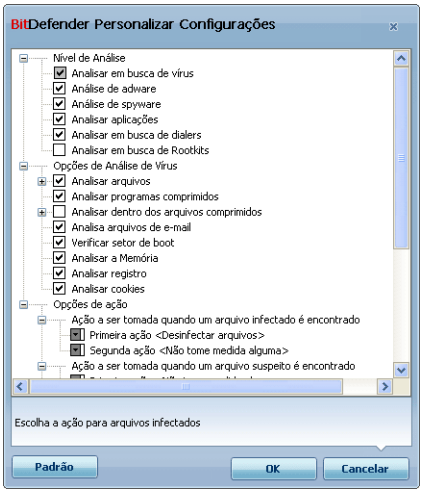
- **Executar a análise com Baixa prioridade.** Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação.
- **Minimizar o Assistente de Análise para a barra de tarefas.** Minimiza a janela de verificação para a Área de notificação. Clique duplamente no ícone BitDefender para abrir.
- **Desligar o PC quando a análise for concluída e se não forem encontradas ameaças**

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Personalizar o Nível de Análise

Os usuários avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de arquivos, diretorios ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Clique em **Personalizar** - para definir as suas próprias opções de análise. Uma nova janela irá aparecer.



Configurações da Varredura

As opções de análise são organizadas como um menu expansível muito semelhante aos menus usados para explorar o Windows. Clique na caixa com "+" para abrir uma opção ou na caixa com "-" para fechar uma opção.

As opções de análise são agrupadas em 3 categorias:

- **Nível de Análise.** Especifica o tipo de malware que deseja que o BitDefender analise, selecionando as opções apropriadas da categoria **Nível de Análise**.

Opção	Descrição
Analisar em busca de vírus	Analisa em busca de vírus. O BitDefender também detecta corpos incompletos de vírus, removendo assim qualquer possível ameaça de segurança que possa vir a afetar o seu sistema.
Analisar em busca de adware	Analisa em busca de ameaças de adware. Estes arquivos serão tratados como arquivos infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa.
Analisar em busca de spyware	Analisa em busca de ameaças de spyware. Estes arquivos serão tratados como arquivos infectados.

Opção	Descrição
Analisar aplicações	Analisar aplicações legítimas que podem ser usadas como ferramenta de espionagem, para ocultar aplicações maliciosas ou outras intenções maliciosas.
Analisa em busca de dialers	Analisa aplicativos conectando-se a números de alto custo. Estes arquivos serão tratados como arquivos infectados. O software que inclua componentes de conexão deste tipo poderá deixar de funcionar se esta opção estiver ativa.
Analisar em busca de Rootkits	Analisa em busca de objectos ocultos (arquivos e processos), conhecidos por rootkits.

- **Opções de análise de vírus.** Especifique os tipos de objetos a serem analisados (arquivos, e-mail, etc.) e outras opções. Isto é feito através da seleção de certas opções da categoria **Opções de análise de vírus**.

Opção		Descrição
Verificar arquivos	**Verificar todos os arquivos**	Todos os arquivos acessados serão verificados, não importando o tipo.
	Verificar apenas os arquivos de programas	Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` e `nws`.
	Verificar as extensões definidas pelo usuário	Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";".
Analisar arquivos comprimidos		Arquivos de backup acessados também serão verificados.
Verificar dentro dos arquivos comprimidos		Analisa dentro de arquivos comprimidos, como `.zip`, `.rar`, `.ace`, `.iso` e outros. Selecione o campo**Analisar arquivos chm e instaladores**se você deseja analisar estes tipos de arquivos.

Opção	Descrição
	Analisar arquivos comprimidos aumenta o tempo da análise e requer mais recursos do sistema. Você pode definir o tamanho máximo dos arquivos a serem analisados em kilobytes (KB), digitando o tamanho neste campo **Limitar o tamanho dos arquivos analisados para**.
Analisar arquivos de e-mail	Para verificar dentro de arquivos de e-mails.
Verificar setores de boot	Para verificar o setor de boot do sistema.
Verificar Memória	Analisa a memória em busca de vírus e outro malware.
Verificar registo	Analisa entradas de registo.
Verificar cookies	Analisa os arquivos cookie.

- **Opções de ação.** Especifique as ações à serem tomadas em cada categoria de arquivos detectados usando as opções nesta categoria.

  Nota

  Para definir uma nova ação, clique em **Primeira Ação** e selecione a opção desejada do menu. Especifique a **Segunda ação** que será executada no caso da primeira falhar.

  ▶ Selecione a ação a ser tomada sobre o arquivo infectado. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Ação	Nenhuma ação será tomada em arquivos infectados. Esses arquivos aparecerão no arquivo de relatório.
Desinfetar arquivos	Remover o código de malware dos arquivos infectados detectados.
Apagar arquivos	Apaga o arquivo infectado imediatamente, sem avisar.
Mover arquivos para a quarentena	Move os arquivos infectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

- Selecionar a ação a tomar sobre um arquivo suspeito. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Ação	Nenhuma ação será executada sobre os arquivos suspeitos. Estes arquivos aparecerão no arquivo de relatório.
Apagar arquivos	Apaga imediatamente e sem qualquer aviso, os arquivos suspeitos.
Mover arquivos para a quarentena	Move os arquivos suspeitos para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

Nota

Há arquivos suspeitos detectados pela análise heurística. Recomendamos que os envie para o Laboratório do BitDefender.

- Selecionar a ação a ser tomada sobre os objetos ocultos (rootkits). As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Ação	Nenhuma ação será levada a cabo sobre os arquivos ocultos. Estes arquivos aparecerão no arquivo de relatório.
Renomear arquivos	Altera o nome de arquivos escondidos ao adicionar `.bd.ren` ao nome. Como resultado, você será capaz de pesquisar e encontrar esses arquivos em seu computador, caso existam.
Mover arquivos para a quarentena	Move os arquivos ocultos para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

Nota

Por favor verifique se esses arquivos escondidos não são arquivos que você escondeu intencionalmente do Windows. Eles são arquivos escondidos por programas especiais, conhecidos como rootkits. Os Rootkits não são maliciosos por natureza. Porém são comumente utilizados para criar vírus e spywares não detectados por programas normais de Antivírus.

▶ **Opções de ação para arquivos protegidos por senha e criptografados.** Arquivos criptografados usando o Windows podem ser importantes para você. Esta é a razão pela qual você pode configurar diversas ações a serem tomadas sobre os arquivos infectados ou suspeitos de que são criptografados usando o Windows. Outra categoria de arquivos que exigem ações especiais são arquivos protegidos por senha. Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha. Utilize estas opções para configurar as ações a serem tomadas sobre arquivos protegidos por senha e arquivos criptografados pelo Windows.

– **Executar quando um arquivo encriptado for encontrado .** Escolha a ação a ser tomada com os arquivos infectados que foram criptografados pelo Windows. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Nenhuma Ação	Apenas registrar arquivos infectados que foram criptografados pelo Windows. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.
Desinfetar arquivos	Remover o código de malware dos arquivos infectados detectados. A desinfecção pode falhar nalguns casos, tais como quando o arquivo infectado se encontra dentro de um arquivo de correio específico.
Apagar arquivos	Apaga o arquivo infectado imediatamente, sem avisar.
Mover arquivos para a quarentena	Mover os arquivos infectados da sua localização original para a Quarentena O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

– **Ação a executar quando um arquivo encriptado suspeito for encontrado .** Escolha a ação a ser tomada com os arquivos suspeitos que foram criptografados pelo Windows. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Nenhuma Ação	Apenas registrar os arquivos suspeitos que foram criptografados pelo Windows. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.

Ação	Descrição
Apagar arquivos	Apaga imediatamente e sem qualquer aviso, os arquivos suspeitos.
Mover arquivos para a quarentena	Move os arquivos suspeitos para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

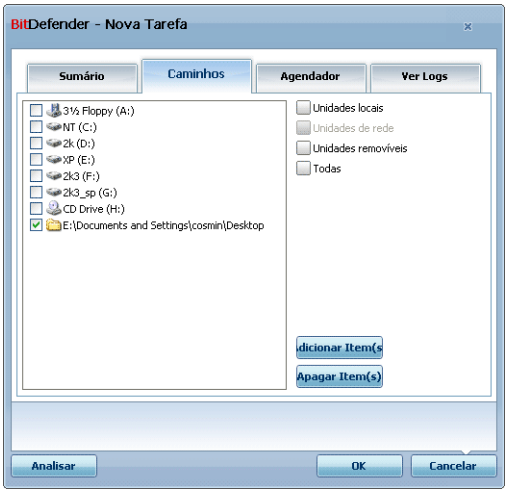
- **Ação a executar quando um arquivo protegido por senha for encontrado .** Selecione a ação a ser tomada sobre os arquivos detectados protegidos por senha. As seguintes opções estão disponíveis:

Ação	Descrição
Apenas Log	Apenas manter registo dos arquivos comprimidos protegidos por senha no relatório da análise. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.
Solicitar senha	Quando é detectado um arquivo protegido por senha, pedir ao usuário para inserir a senha de forma a analisar o arquivo.

Se você clicar em **Padrão** você carregará as configurações padrão. Clique em **OK** para guardar as alterações e fechar a janela.

Definir Alvo da Análise

Para definir o alvo de uma tarefa de análise de usuário em específico, clique com o botão direito na tarefa e selecione **Caminhos**. Alternativamente, se você já estiver na janela de propriedades de uma tarefa, selecione a aba **Caminhos**. A seguinte análise irá aparecer:



Alvo da Análise

Pode ver a lista das drives locais amovíveis e de rede, como também, se houver, os arquivos e as pastas adicionada previamente. Todos os items seleccionados serão analisados quando a tarefa for executada.

Essa seção contém os seguintes botões:

- **Adicionar Diretórios** - abre uma janela onde você pode selecionar o(s) arquivo(s) / diretórios(s) que deseja verificar.

  Nota
  Use arrastar & soltar para incluir arquivos/pastas na lista.

- **Deletar Item(s)** - remove arquivo o(s) arquivo(s) / a(s) pasta(s) previamente selecionados da lista de objetos a serem analisados.

  Nota
  Apenas os arquivos/pastas que foram inclusos posteriormente podem ser removidos, mas não os que foram “vistos” automaticamente pelo BitDefender.

Além dos botões explicados acima existem algumas opções que possibilitam seleção rápida de local de verificação.

- **Unidades locais** - para verificar as unidades locais.
- **Unidades de rede** - para verificar todas as unidades da rede.

- **Unidades removíveis** - para verificar as unidades removíveis (CD-ROM, disquete, etc).
- **Todas** - para verificar todas as unidades, não importando se são locais, na rede ou removíveis.

Nota

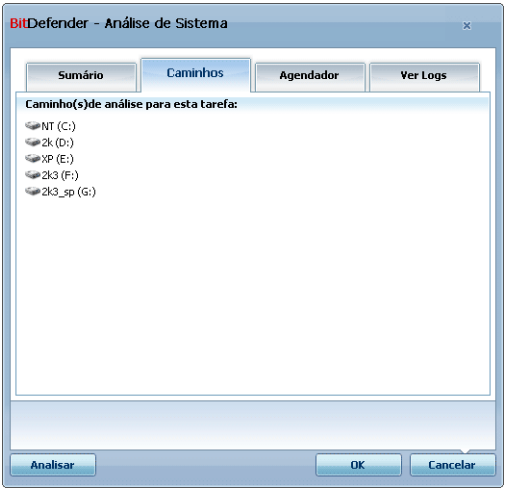
Se você quer verificar todo o seu computador contra vírus selecione a caixa correspondente a **Todas**.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Ver o Alvo da Análise das Tarefas de Sistema

Não pode modificar os alvos de análise das tarefas de análise a partir da categoria **tarefas do Sistema**. Apenas pode ver o alvo da análise deles.

Para ver o alvo da análise de uma determinada tarefa de análise do sistema, faça clique com o botão direito do mouse sobre a tarefa selecione **Mostrar Caminho da Tarefa**. Para **Análise de Sistema**, por exemplo, a janela a seguir aparecerá.



Alvo da Análise da Análise Completa do Sistema

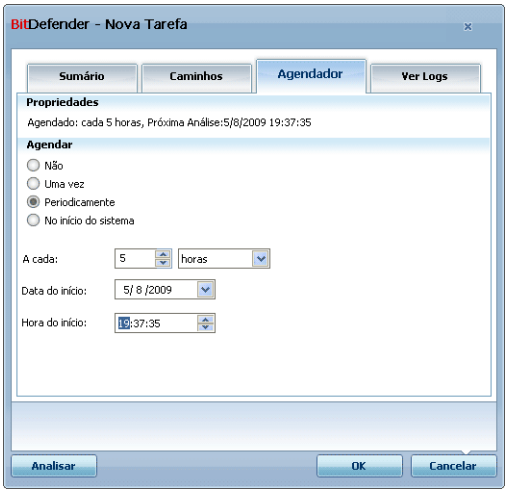
Análise do Sistema e **Análise Minuciosa** analisarão todas os diretórios locais, enquanto **Análise Rápida do Sistema** analisará apenas as pastas `Windows` e `Arquivos de Programas`.

Clique em **OK** para fechar a janela. Para executar uma tarefa, apenas clique em **Analisar**.

Agendar Tarefas de Análise

Com tarefas complexas, o processo de análise leva algum tempo, e funciona melhor se fechar todos os outros programas. É por isso que é melhor agendar tais tarefas para quando não estiver a utilizar o seu computador e este tenha entrado no modo de descanso.

Para ver o agendamento de uma tarefa específica ou para modificá-la, clique com o botão direito na tarefa e selecione **Agendamento**. Se você já estiver na janela de Propriedades da tarefa, selecione a aba **Agendamento**. A seguinte análise irá aparecer:



Agendador

Se houver, pode ver a tarefa agendada.

Quando agendar uma tarefa, deve de escolher uma das seguintes opções:

- **Não agendada** - executa a tarefa apenas quando o usuário a solicita.
- **Uma vez** - Executa a análise uma só vez, num determinado momento. Definir a data de início e a hora nos campos**Iniciar Data/Hora**
- **Periodicamente** - executa a análise periódicamente, em determinados intervalos (minutos, horas, dias, semanas, meses) começando com uma data e hora especificada.

  Se você quer que a análise seja repetida após certos intervalos, selecione **Periodicamente** e digite na caixa **A cada** o número de

minutos/horas/dias/semanas/meses indicando a frequncia desse processo. Você também deve definir a data de início e a hora nos campos **Data/Hora de Início**.

- **No iniciar do sistema** - Executa a análise, após um determinado número de minutos especificados, após o usuário entrar no Windows.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

18.2.5. Analisando Arquivos e Diretórios

Antes de inciar um processo de análise, você deve certificar-se que o BitDefender está atualizado com as vacinas de malware mais recentes. Analisar o seu computador utilizando vacinas desatualizadas pode impedir que o BitDefender detecte novos malwares criados desde a última atualização. Para verificar quando a última atualização foi feita, vá em **Atualização** no Modo Avançado.

Nota

Para que o BitDefender execute uma verificação completa, você precisará fechar todos os programas abertos. Especialmente seu cliente de e-mail (i.e. Outlook, Outlook Express ou Eudora) deve ser.

Dicas de Análise

Aqui estão mais algumas dicas de análise que podem ser úteis para você:

- Dependendo do tamanho do seu disco rígido, executar uma Análise detalhada (tal como Análise Minuciosa ou Análise do Sistema) pode demorar um pouco (até uma hora ou mais). Portanto, você deve executar essas análises quando não precisar usar seu computador por um longo tempo (por exemplo, durante a noite).

  Você pode agendar a análise para iniciar quando for conveniente. Certifique-se de deixar o seu computador executando. Com o Windows Vista, certifique-se que o seu computador não está no modo de espera quando a tarefa é agendada para ser executada.

- Se você baixa freqüentemente arquivos da Internet para um diretório específico, crie uma nova tarefa de análise e configure esse diretório como alvo de análise. Agendar a tarefa para executar todos os dias ou mais vezes.

- Existe um tipo de malware que altera configurações do Windows, se configurando para ser executado na inicialização do sistema. Para proteger seu computador contra malware, você pode agendar a tarefa**Análise Auto-logon** para rodar quando o sistema for iniciado. Observe que a análise de vírus durante a inicialização do computador pode afetar o desempenho do sistema por um curto período de tempo.

Métodos de Análise

O BitDefender permite quatro tipos de verificação solicitada:

- Análise imediata - executa uma tarefa de análise das tarefas do sistema/usuário.
- Análise Contextual - clique com o botão direito em um arquivo ou diretório e selecione **Analisar com o BitDefender**.
- Verificação Arraste & Solte - arraste e solte um arquivo ou pasta sobre a Barra de Atividade;
- Análise manual - Use a Análise Manual do BitDefender para selecionar diretamente os arquivos ou pastas a serem analisados.

Verificação imediata

Para analisar o seu computador ou parte dele, você pode executar as tarefas de análise padrão, ou pode criar as suas próprias tarefas de análise. Isto denomina-se verificação imediata.

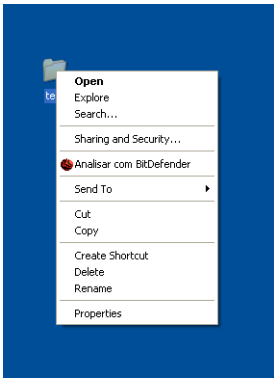
Para executar uma tarefa de análise, use um dos seguintes métodos:

- faça duplo-clique com o rato sobre a tarefa desejada da lista.
- clique no botão **Analisar agora** da correspondente tarefa.
- selecione a tarefa e depois clique em **Executar Tarefa**.

O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

Verificação contextual

Para analisar um arquivo ou pasta, sem configurar uma nova tarefa de análise, pode usar o menu contextual. A isto chamamos de análise contextual.



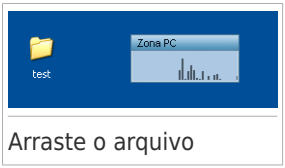
Verificação Contextual

Clique com o botão direito do mouse sobre o arquivo ou pasta que você deseja analisar e selecione **Análisar com BitDefender**. O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

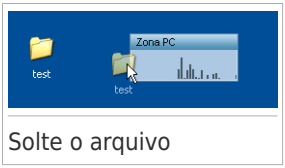
Pode modificar as opções de análise e ver os relatórios ao acessar à janelas das **Propriedades** da tarefa **Análise de Menu Contextual**.

Verificação Arraste & Solte

Arraste o arquivo ou pasta que você quer verificado e solte-o sobre a **Barra de Atividade**, como nas imagens abaixo.



Arraste o arquivo



Solte o arquivo

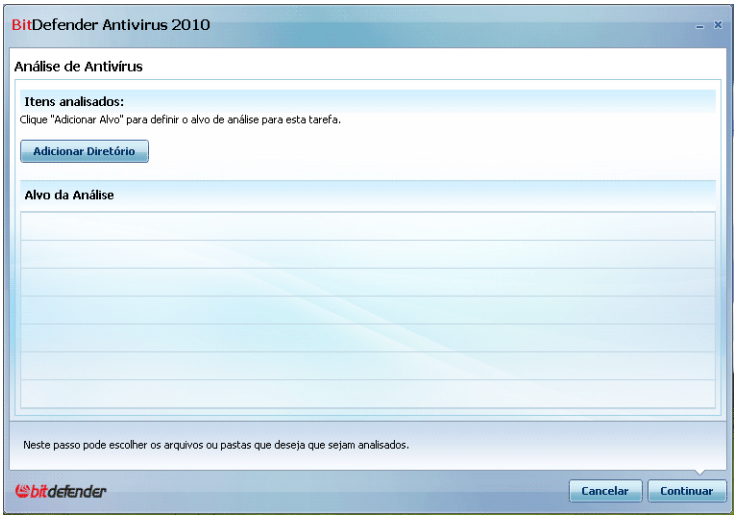
O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

Verificação Manual

A análise manual consiste em selecionar diretamente o objecto a ser analisado usando a opção de Análise Manual BitDefender a partir do grupo de programas BitDefender no Menu Iniciar.

Nota
A análise manual é muito útil, pois pode ser executada enquanto o Windows se encontra em Modo de Segurança.

Para selecionar o objeto que será analisado pelo BitDefender, no menu Iniciar do Windows, siga o caminho**Iniciar → Programas → BitDefender 2010 → Análise Manual BitDefender**. A seguinte análise irá aparecer:



Verificação Manual

Clique **Adicionar Pasta**, selecione o destino que você deseja analisar e clique **OK**. Se você quiser analisar multiplas pastas, repita esta ação para cada localidade adicional.

O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela. Clique no botão **Remover Todos Caminhos** para remover todas as localizações que foram adicionadas à lista.

Quando você terminar de selecionar os locais, clique **Continuar**. O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

Assistente do analisador Antivírus

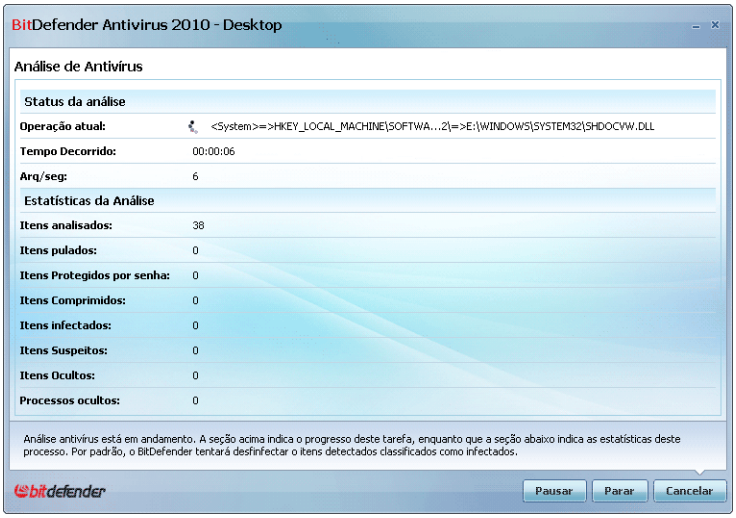
Quando você iniciar uma análise avulsa, o assistente de análise Antivírus será exibido. Siga o processo guiado de três passos para completar o processo de análise.

Nota

Se o assistente de análise não aparecer, a análise pode estar configurada para executar silenciosamente no computador, enquanto você o utiliza. Você pode visualizar o ícone Progresso da análise na área de notificação. Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da análise.

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Espere que o BitDefender termine a análise.

Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Arquivos comprimidos protegidos por senha. Se o BitDefender detecta um arquivo protegido por senha durante a análise e a ação padrão está configurada para **Perguntar a senha**, você será questionado a fornecer a senha. Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha. As seguintes opções estão disponíveis:

- **Senha.** Se você deseja que o BitDefender analise o arquivo, selecione essa opção e digite a senha. Se você não sabe a senha, escolha uma das outras opções.
- **Não solicite uma senha e não analise este objeto.** Selecione essa opção para pular a análise desse arquivo.

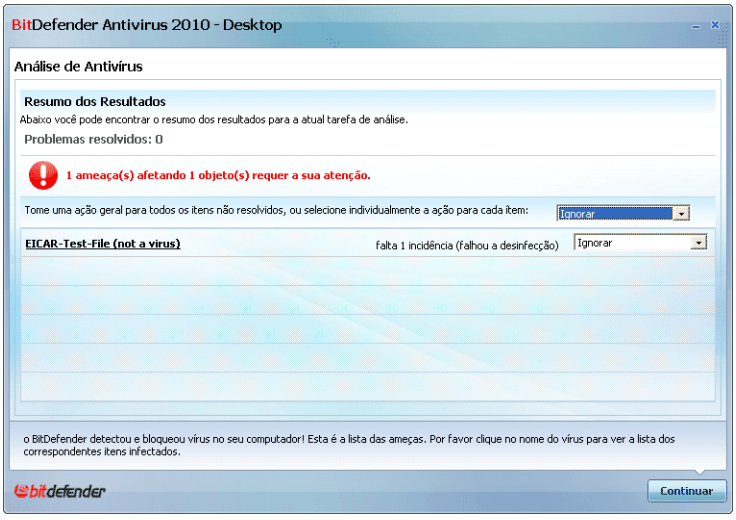
- **Pular todos os itens protegidos por senha.** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha. O BitDefender não será capaz de os analisar, porém um registro será mantido no relatório da análise.

Clique em **OK** para continuar.

Parando ou suspendendo a análise. Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá diretamente para o último passo do assistente. Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

Passo 2/3 - Selecionar as ações

Quando a análise é completada, surge uma nova janela, onde pode ver os resultados da análise.



Ações

Pode ver o número de incidências que afectam o seu sistema.

Os objectos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objectos infectados.

Você pode escolher uma ação geral a ser executada para todos os problemas ou escolher ações separadas para cada grupo de problemas.

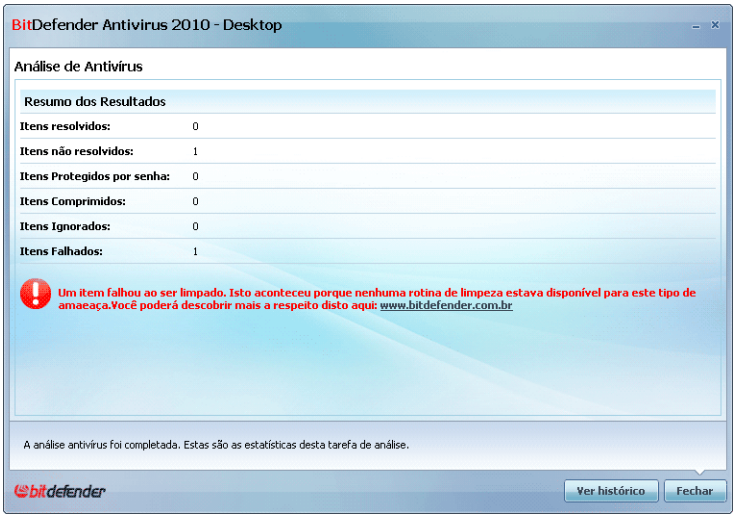
Uma ou várias das seguintes opções podem aparecer no menu:

Ação	Descrição
Não Tomar Ação	Nenhuma ação será tomada em arquivos detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.
Desinfetar	Remove o código malware dos arquivos infectados.
Apagar	Apaga os arquivos detectados.
Mover para a quarentena	Move os arquivos detectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Renomear arquivos	Altera o nome de arquivos escondidos ao adicionar `.bd.ren` ao nome. Como resultado, você será capaz de pesquisar e encontrar esses arquivos em seu computador, caso existam. Por favor verifique se esses arquivos escondidos não são arquivos que você escondeu intencionalmente do Windows. Eles são arquivos escondidos por programas especiais, conhecidos como rootkits. Os Rootkits não são maliciosos por natureza. Porém são comumente utilizados para criar vírus e spywares não detectados por programas normais de Antivírus.

Clique em **Continuar** para aplicar as acções especificadas.

Passo 3/3 - Ver Resultados

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela.



Sumário

Pode ver o sumário dos resultados. Se você quiser informações detalhadas do processo de análise, clique **Visualizar Relatório** para visualisar o relatório de análise.

Importante
Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado.

Clique em **Fechar** para fechar a janela.

BitDefender Não Pode Resolver Algumas Incidências

Na maioria dos casos o BitDefender desinfecta com sucesso o arquivo infectado ou isola a infecção. No entanto, existem incidências que não puderam ser resolvidas.

Nesse caso, recomendamos que contacte o Suporte Técnico BitDefender em www.bitdefender.com.br. Os nossos membros do suporte ajudá-lo-ão a resolver as incidências que esteja a experimentar.

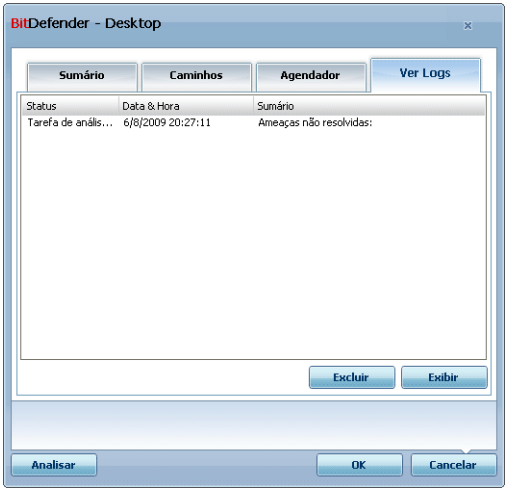
BitDefender Detectou Arquivos Suspeitos

Arquivos suspeitos são arquivos detectados pela análise heurística e que poderão estar infectados com malware cuja a vacinas de detecção ainda não foi disponibilizada.

Se foram detectados arquivos suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender. Clique **OK** para enviar estes arquivos para análise no Laboratório do BitDefender.

18.2.6. Ver os Relatórios da Análise

Para ver os resultados da análise após a tarefa ter sido executada, faça clique com o botão direito do mouse sobre a mesma e selecione **Ver os Relatórios da Análise**. A seguinte análise irá aparecer:



Relatórios da Análise

Aqui pode ver os relatórios gerados cada vez que uma tarefa foi executada. Cada arquivo no relatório contém informação sobre o estado do processo de análise registado, a data e hora quando a análise foi feita e um resumo dos resultados da análise.

Dois botões estão disponíveis:

- **Apagar** - apaga o relatório selecionado.
- **Mostrar** - abre o relatório selecionado. O relatório da análise será aberto no seu explorador da internet.

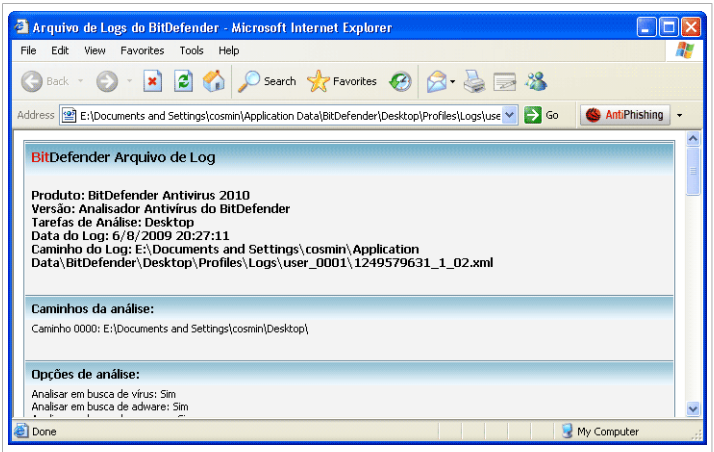
Nota

Também, para ver ou apagar um arquivo, clique com o lado direito do mouse sobre o arquivo e selecione a opção correspondente do menu de atalho.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Exemplo de Relatório da Análise

A seguinte figura representa um exemplo de um relatório de análise:



Exemplo de Relatório da Análise

O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

18.3. Objectos a Excluir da Análise

Há casos em que tem de excluir certos arquivos de serem analisados. Por exemplo, poderá querer excluir um arquivo de teste EICAR da análise no acesso ou os arquivos `.avi` da análise a pedido.

BitDefender permite-lhe excluir objectos da análise no-acesso e da análise a-pedido, ou de ambas. Esta definição tem o propósito de diminuir o tempo de análise e evitar interferência com o seu trabalho.

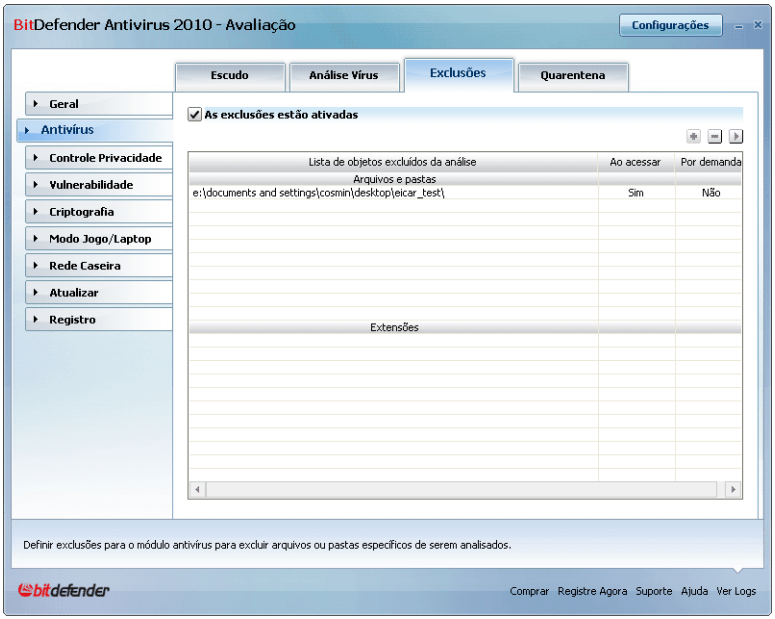
Dois tipos de objectos podem ser excluidos da análise:

- **Caminhos** - o arquivo ou pasta (incluindo os objectos que contém) indicados por um determinado caminho serão excluídos da análise.
- **Extensões** - todos os arquivos com um determinada extensão serão excluídos da análise.

Nota

Os objetos excluídos da análise por demanda não serão analisados, independentemente deles serem acessados por você, ou por um aplicativo.

Para ver e gerenciar os objetos excluídos, vá para **Antivírus>Exceções** no Modo Avançado.



Exceções

Pode ver os objectos arquivos, pastas, extensões) que são excluídos da análise. Pode ver por objecto se o mesmo está excluído da análise no-acesso, análise a-pedido, ou ambas.

Nota

As exceções definidas aqui NÃO serão aplicada à análise contextual. Análise Contextual é um tipo de análise por demana: Você da um clique com o botão direito do mouse no arquivo ou diretório que pretende analisar e seleciona **Analisar com o BitDefender**.

Para apagar um item da lista, escolha-o e clique no botão **Remover**.

Para editar uma entrada da lista, selecione-a e clique no botão **Editar**. Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o

tipo de análise da qual quer que eles sejam excluídos. Faça as alterção necessárias e clique **OK**.

Nota

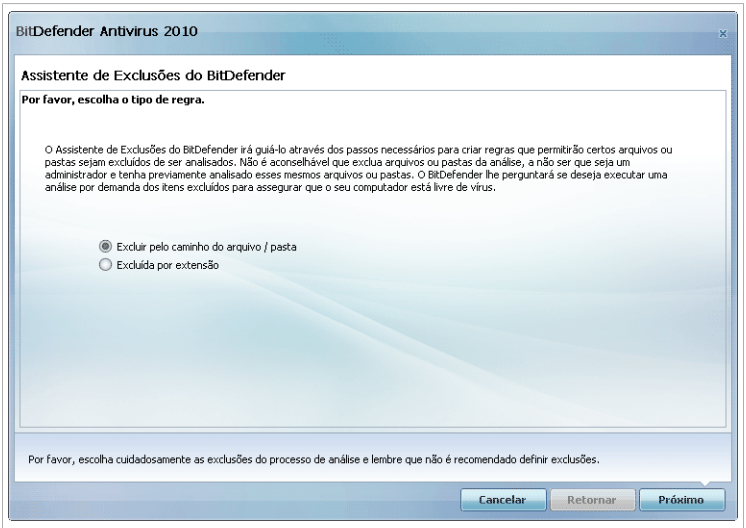
Pode também clicar no objecto usando o botão direito do mouse e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

Clique em **Remover** para reverter as alterações feitas à lista de regras, desde que as mesmas não tenham sido guardadas anteriormente ao clicar **Aplicar**.

18.3.1. Excluir Caminhos da Análise

Para excluir caminhos da análise, clique no botão **Adicionar**. Será guiado através do processo de exclusão de caminhos da análise através de um assistente de configuração que lhe irá aparecer.

Passo 1/4 - Seleccionar o Tipo de Objecto

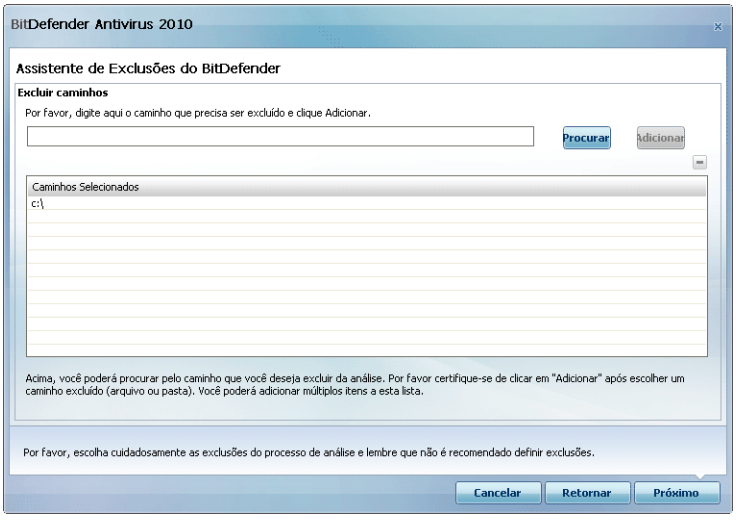


Tipo de Objecto

Selecione a opção de excluir um caminho da análise.

Clique em **Próximo**.

Passo 2/4 - Especificar Os Caminhos a Excluir



Caminhos a Excluir

Para especificar os caminhos a excluir da análise use os seguintes métodos:

- Clique em **Explorar**, selecione o arquivo ou pasta que deseja excluir da análise e depois clique **Adicionar**.
- Insira o caminho que deseja que seja excluído da análise no campo editado e clique em **Adicionar**.

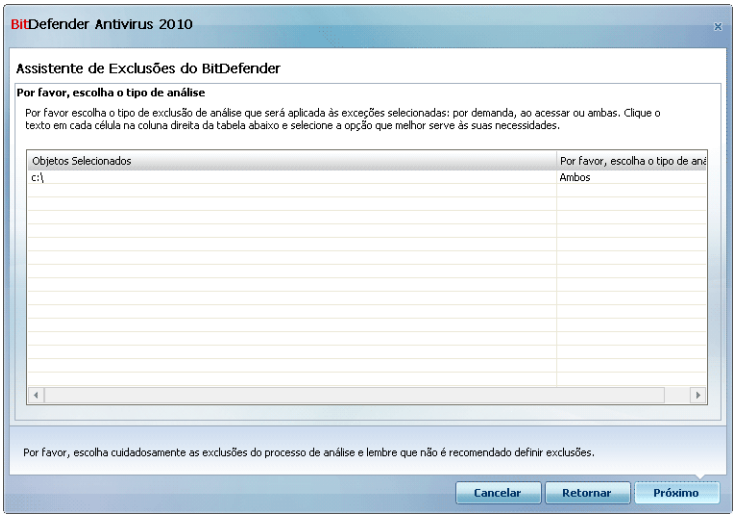
Nota
Se o caminho inserido não existe, uma mensagem de erro surgirá. Clique em **OK** e verifique se o caminho é válido ou não.

Os caminhos surgirão na lista à medida que os adicione. Pode adicionar tantos caminhos quanto os que deseje.

Para apagar um item da lista, escolha-o e clique no botão **Remover**.

Clique em **Próximo**.

Passo 3/4 - Seleccionar o Tipo de Análise



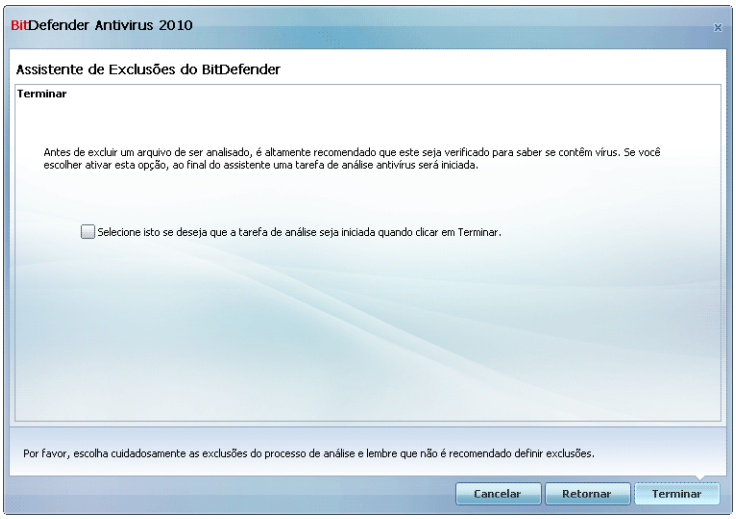
Tipo de Análise

Pode ver a lista que contém os caminhos a serem excluídos da análise e o tipo de análise do qual eles são excluídos.

Como padrão, os caminhos selecionados são excluídos da análise no-acesso e por demanda. Para alterar isto, clique na coluna à direita e selecione a opção desejada da lista.

Clique em **Próximo**.

Passo 4/4 - Analisar arquivos Excluidos



Analisar arquivos Excluidos

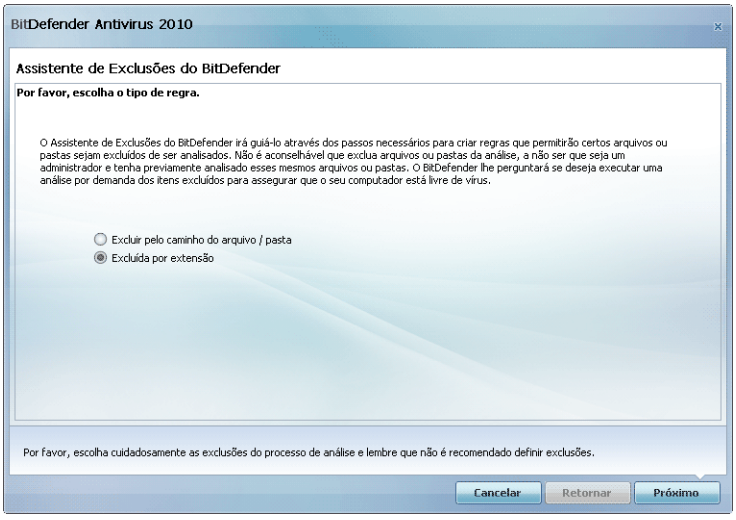
É altamente recomendável analisar os arquivos nos caminhos especificados para ter a certeza de que não estão infectados. Selecione a caixa de seleção para analisar estes arquivos antes de os excluir da análise.

Clique em **Finalizar**.

18.3.2. Excluir Extensões da Análise

Para excluir extensões da análise, clique no botão **Adicionar** . Será guiado através do processo de excluir extensões da análise através de um assistente de configuração que irá lhe irá aparecer.

Passo 1/4 - Seleccionar o Tipo de Objecto

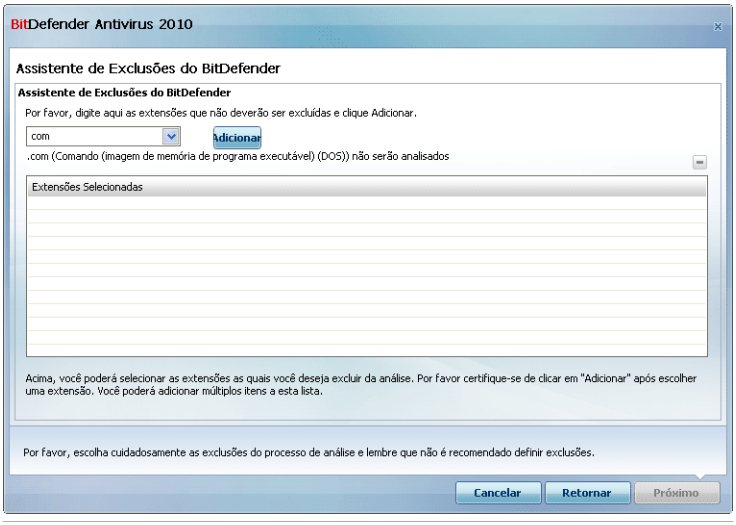


Tipo de Objecto

Selecione a opção de excluir extensões da análise.

Clique em **Próximo**.

Passo 2/4 – Especificar Extensões a Excluir



Extensões a Excluir

Para especificar as extensões a serem excluídas da análise use os seguintes métodos:

- Selecione a partir do menu a extensão que deseja excluir da análise e clique em **Adicionar**.

> **Nota**
> O menu contém uma lista de extensões registadas no seu sistema. Quando selecciona uma extensão, pode ver a sua descripção, caso a mesma esteja disponível.

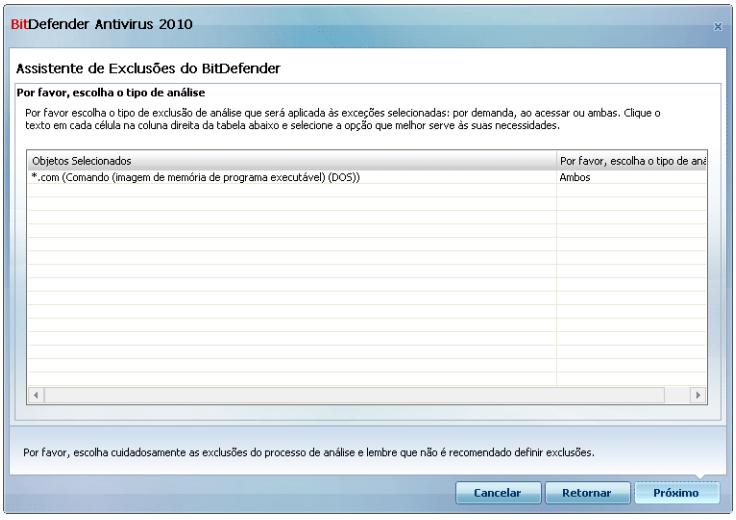
- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

As extensões aparecerão na lista à medida que as adiciona. Pode adicionar tantas extensões quantas as que desejar.

Para apagar um item da lista, escolha-o e clique no botão **Remover**.

Clique em **Próximo**.

Passo 3/4 - Seleccionar o Tipo de Análise



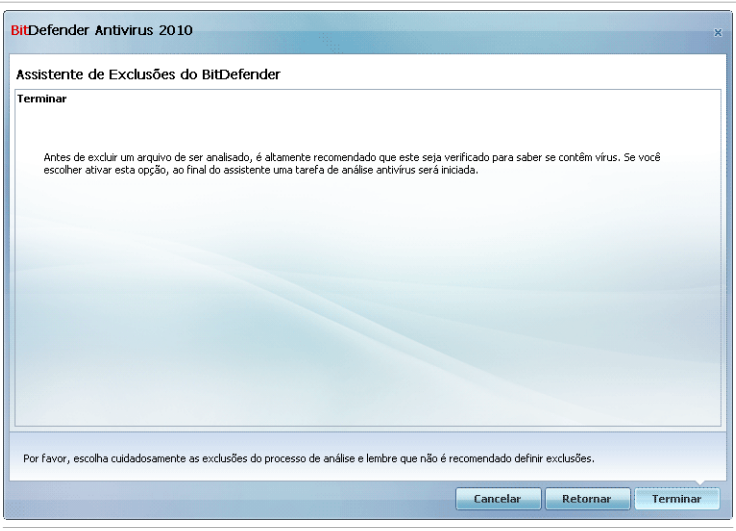
Tipo de Análise

Pode ver uma lista contendo as extensões a serem excluídas da análise o o tipo de análise da qual são excluídas.

Como padrão, as extensões seleccionadas são excluídas da análise a acessar ou por demanda. Para alterar isto, clique na coluna da direita e selecione a opção que deseja, a partir da lista.

Clique em **Próximo**.

Passo 4/4 - Seleccionar o Tipo de Análise



Tipo de Análise

É altamente recomendável analisar os arquivos com as extensões especificadas para ter a certeza de que não estão infectados

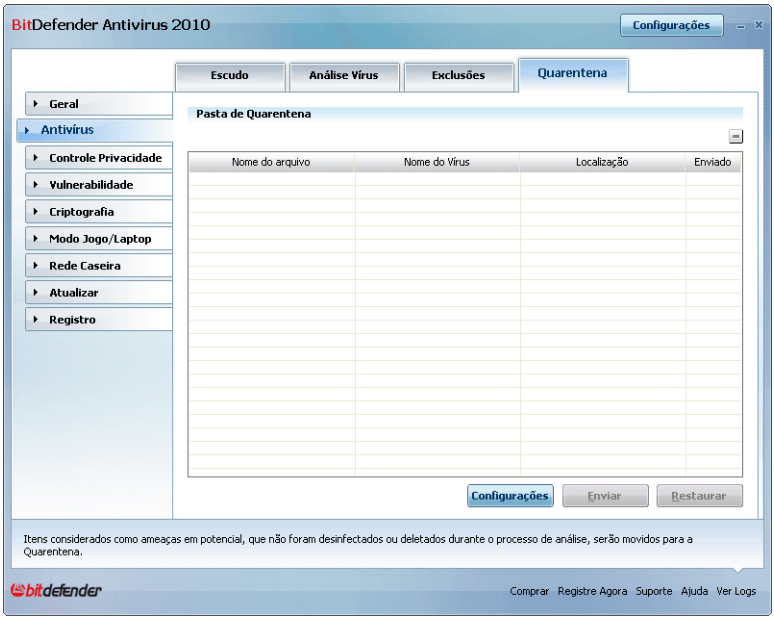
Clique em **Finalizar**.

18.4. Área de Quarentena

O BitDefender permite isolar os arquivos infectados ou suspeitos em uma área segura, chamada quarentena. Isolando esses arquivos, o risco de ser infectado desaparece e, ao mesmo tempo, você tem a possibilidade de enviar esses arquivos para futura análise da BitDefender Labs.

Além disso, o BitDefender analisa os arquivos em quarentena após cada atualização da vacina de malware. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

Para visualizar e gerenciar os arquivos da quarentena e para configurar as definições, vá para **Antivírus>Quarentena** no Modo Avançado.



Quarentena

A seção de Quarentena mostra todos os arquivos atualmente isolados na pasta da Quarentena. Para cada arquivo em quarentena pode ver o seu nome, o nome do vírus detectado, o caminho da sua localização original e a data de submissão.

Nota
Quando o vírus está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executado ou lido.

18.4.1. Gerir arquivos em Quarentena

Pode enviar qualquer arquivo selecionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**. Como padrão, o BitDefender envia automaticamente os arquivos em quarentena a cada 60 minutos.

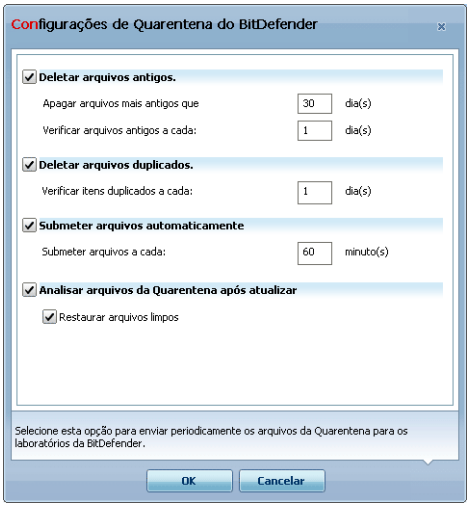
Para deletar um arquivo selecionado da quarentena, clique no botão **Deletar** . Se você quiser restaurar um arquivo selecionado para sua localização orignal, clique **Restaurar**.

Menu contextual. Está disponível um menu contextual, que lhe permite gerenciar facilmente os arquivos em quarentena. As mesmas opções mencionadas previamente

estão disponíveis. Pode também selecionar **Atualizar** para atualizar a seção de Quarentena.

18.4.2. Configurar opções da Quarentena

Para configurar as definições da quarentena, clique em **Configuração**. Uma nova janela irá aparecer.



Opções da quarentena

Ao usar a configuração da quarentena, pode definir o BitDefender para executar automaticamente as seguintes acções:

Apagar arquivos antigos. Para apagar automaticamente arquivos antigos da quarentena, selecione a opção correspondente. Deve especificar o número de dias após os quais os arquivos em quarentena deverão ser apagados e a frequência com a qual o BitDefender deve de verificar esta situação.

Nota
Por default, o BitDefender verificará os arquivos antigos todos os dias e deletará todos aqueles com mais de 30 dias.

Deletar arquivos duplicados. Para apagar automaticamente arquivos duplicados na quarentena, selecione a opção correspondente. Deve especificar o número de dias entre duas verificações consecutivas de duplicados.

Nota

Como padrão, o BitDefender irá verificar arquivos duplicados na quarentena diariamente.

Enviar os arquivos automaticamente. Para enviar automaticamente arquivos em quarentena, selecione a opção correspondente. Deve de especificar a frequência com que deseja enviar os arquivos.

Nota

Como padrão, o BitDefender envia automaticamente os arquivos em quarentena a cada 60 minutos.

Analisar os arquivos em quarentena após a atualização. Para analisar automaticamente arquivos em quarentena após a atualização, selecione a opção correspondente. Pode escolher mover automaticamente os arquivos limpos para a sua localização original seleccionado a opção **Restaurar arquivos Limpos**.

Clique em **OK** para guardar as alterações e fechar a janela.

19. Controle Privacidade

O BitDefender monitora dúzias de locais potenciais no seu sistema onde o spyware pode agir, e também verifica quais quer mudanças feitas no seu sistema ou software. É eficiente para o bloqueio de Cavalos de Tróia e outras ferramentas instaladas por hackers, que tentam comprometer sua privacidade e enviar seus dados pessoais, como número de cartões de crédito, do seu computador para o hacker.

19.1. Estado do Controle de Privacidade

Para configurar o Controle de Privacidade e ver a informação desta atividade, vá para **Controle de Privacidade>Status** no Modo Avançado.

Estado do Controle de Privacidade

Pode ver se o Controle de Privacidade está ativo ou inativo. Se deseja mudar o estado do Controle de Privacidade, limpe ou marque a correspondente caixa de seleção.

Importante

Para evitar roubo de informação e proteger a sua privacidade mantenha o **Controle de Privacidade** activado.

O Controle de Privacidade protege o seu computador usando estes controles de proteção importantes:

- Controle de Identidade - protege os seus dados confidenciais ao filtrar o tráfego de saída web (HTTP) e de e-mail (SMTP) e o tráfego de mensagens instantâneas de acordo com as regras que criou na seção de Identidade.
- O Controle do Registo - irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.
- O Controle de Cookies - irá pedir a sua permissão sempre que um novo site web tentar definir uma cookie.
- O Controle de script - irá pedir a sua permissão sempre que um site web tente ativar um script ou outro conteúdo ativo.

Ao fundo da seção poderá ver as **Estatísticas do Controle de Privacidade**.

19.1.1. Configurar Nível de Proteção

Pode escolher o nível de proteção que melhor se adapta às suas necessidades de segurança. Arraste o barra deslizante ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de proteção:

Nível de Proteção	Descrição
Permissivo	Todos os controles de proteção estão desabilitados.
Por Padrão	Apenas **Controle de Identidade** esta habilitado.
Agressivo	**Controle de Identidade**, **Controle do Registro**, **Controle de Cookie** e **Controle de Script** estão ativados.

Você pode personalizar o nível de proteção clicando em **Personalizar Nível**. Na janela que lhe irá aparecer, escolha o controles de proteção que deseja ativar e clique em **OK**.

Clique em **Nível Padrão** para posicionar a barra deslizante no nível padrão.

19.2. Controle de Identidade

Manter informação confidencial segura é um assunto importante que nos preocupa a todos. O roubo de dados tem crescido com o desenvolvimento das comunicações por Internet e atualmente se faz uso de novos métodos para enganar as pessoas e retirar-lhes informação privada.

Qualquer que seja o seu e-mail o seu número de cartão de crédito, quando eles caem em mãos erradas, essa informação poderá causar-lhe danos: poderá

encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao acessar à sua conta e verificar que está vazia.

O Controle de Identidade protege-o contra o roubo de informação sensível quando se encontra on-line. Baseado nas regras que criar, o Controle de Identidade analisa o tráfego web, de e-mail e de mensagens instantâneas que sai do seu computador em busca de chaves de caracteres específicos (por exemplo, o seu número de cartão de crédito). Se houver uma correspondência, a respectiva página web, e-mail ou mensagem instantânea é bloqueada.

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária. Suporte multi-usuário é fornecido de forma a que os usuários de diferentes contas do Windows possam configurar e usar as suas próprias regras de identidade. Se a sua conta do Windows é uma conta de administrador, as regras que você criou podem ser configuradas também para ser aplicadas quando outros usuários do computador estiverem conectados às suas contas de usuários.

Porque usar o Controle de Identidade?

- O Controle de Identidade é bastante eficaz a bloquear spyware keylogger. Este tipo de aplicações maliciosas grava as teclas que pressionou no teclado e envia-as para a Internet para uma pessoa maliciosa (hacker). O hacker pode descobrir informação sensível a partir de dados roubados, tais como números de contas bancárias e palavras-passe, e usá-las em benefício pessoal.

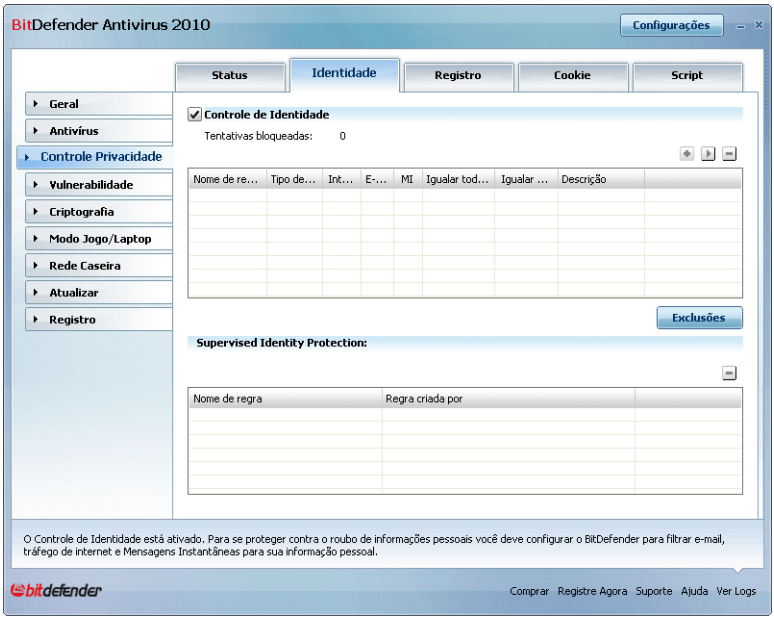
  Supondo que tal aplicativo funciona de forma a evitar a detecção antivírus, o mesmo não pode enviar os dados roubados por e-mail, web ou mensagens instântaneas se você tiver criado as regras de proteção de identidade adequadas.

- O Controle de Identidade protege-o contra as tentativas de phishing (tentativas de roubar informação pessoal). As tentativas de phishing mais comuns fazem uso de um e-mail enganador para o levar a inserir informação pessoal numa página web falsa.

  Por exemplo, você poderá receber um e-mail dizendo que é do seu banco a pedir-lhe que atualize os dados da sua conta bancária com urgência. O e-mail traz um link para uma página web onde deve de inserir a sua informação pessoal. Apesar de parecerem legítimos, o e-mail e o link para a página web são falsos. Se clicar no link do e-mail e inserir a sua informação pessoal na página web falsa, estará a revelar esta informação às pessoas maliciosas que organizaram a tentativa de phishing.

  Se as regras de proteção de identidade estiverem feitas, não poderá enviar informação pessoal (tal como o número do seu cartão de crédito) para uma página web a não ser que tenha definido essa página web como uma excepção.

Para configurar o Controle de Identidade, vá para**Controle de Identidade>Identidade** no Modo Avançado.



Controle de Identidade

Se deseja usar Controle de Identidade, siga estes passos:

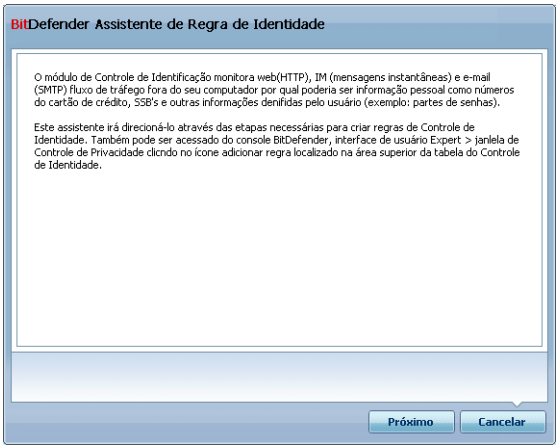
1. Selecione o campo **Habilitar Controle de Identidade**.
2. Criar regras para proteger a sua informação sensível. Para mais informação, por favor consulte o "*Criar Regras de Identidade*" (p. 154).
3. Se necessário, defina exceções específicas para as regras que criou. Para mais informação, por favor consulte o "*Definir Exceções*" (p. 158).
4. Se você é um administrador no computador, você pode excluír você mesmo das regras de identidade, criadas por outros administradores.

   Para mais informações, por favor consulte "*Regras Definidas por outros Administradores*" (p. 159).

19.2.1. Criar Regras de Identidade

Para criar uma regra de proteção de identidade clique no botão **Adicionar** e siga o assistente de configuração.

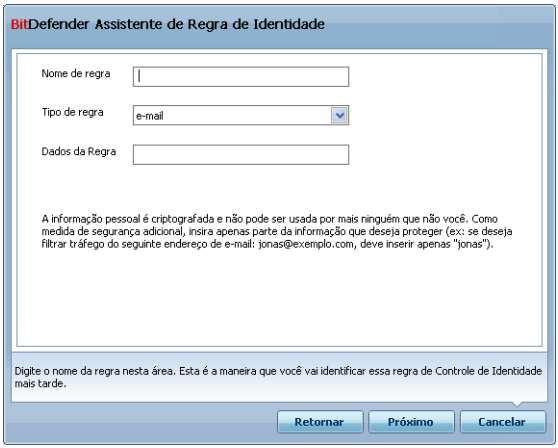
Passo 1/4 - Janela de Boas-vindas



Janela de Boas-Vindas

Clique em **Próximo**.

Passo 2/4 - Definir Tipo de Regra e Dados



Definir Tipo de Regra e Dados

Deve definir os seguintes parâmetros:

- **Nome Regra** - insira o nome da regra no campo editável.
- **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
- **Dados Regra** - insira os dados que quer proteger com a regra no campo editável. Por exemplo, se deseja proteger o seu número de cartão de crédito, insira o mesmo ou parte dele aqui.

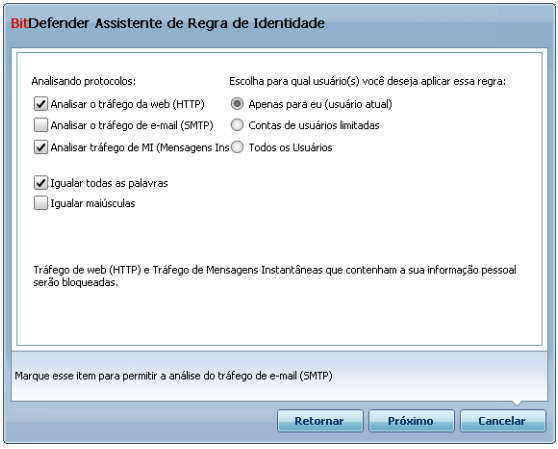
Nota

Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

Clique em **Próximo**.

Passos 3/4 - Selecionar Tipos de Tráfego e Usuários



Selecionar Tipo de Tráfego e Usuários

Selecione o tráfego que você deseja que o BitDefender analise. As seguintes opções estão disponíveis:

- **Analisar Internet (tráfego de HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar e-mail (tráfego de SMTP)** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.

- **Analisar tráfego de Mensagens Instantâneas** - analisa todo o tráfego de Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

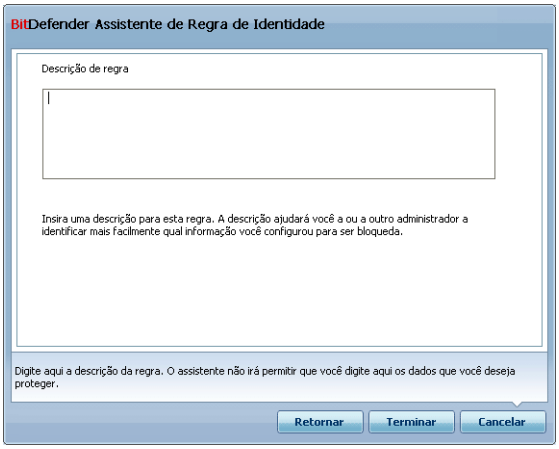
Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

Especificar os usuários os quais as regras se aplicam.

- **Somente para mim (usuário atual)** - a regra se aplicará somente à sua conta de usuário.
- **Contas limitadas de usuários** - A regra se aplicará a você e a todas as contas limitadas do Windows.
- **Todos os usuários** - a regra se aplicará a todas as contas do Windows.

Clique em **Próximo**.

Passo 4/4 - Descrever Regra



Descrever Regra

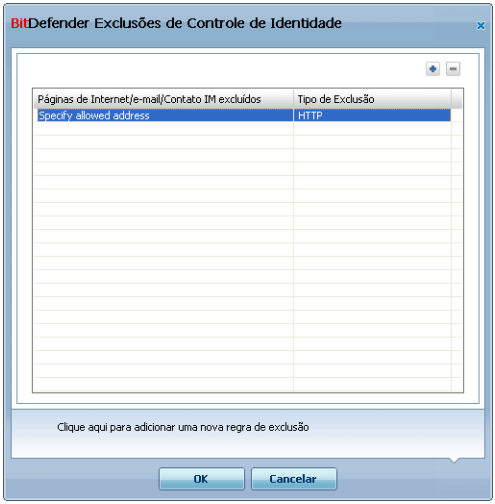
Insira uma breve descrição da regra no campo de edição. Uma vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

Clique em **Finalizar**. A regra aparecerá na tabela.

19.2.2. Definir Exceções

Há casos em que você necessita definir exceções para especificar as regras de identidade. Consideremos o caso em que criou uma regra que evita que o número do seu cartão de crédito seja enviado por HTTP (web). Sempre que o seu cartão de crédito seja submetido num site web a partir da sua conta de utilizador, a respectiva página web é bloqueada. Se deseja por exemplo, pagar uma compra online numa loja virtual (que você sabe ser segura), terá de especificar uma excepção para a respectiva regra.

Para abrir a janela onde você pode gerenciar exceções, clique**Exceções**.



Exclusões

Para adicionar uma excepção, siga os seguintes passos:

1. Clique no botão **Adicionar** para adicionar a nova entrada à tabela.
2. Dê um duplo-clique em **Especificar item excluído** e inserir o endereço web, endereço de e-mail ou o contato IM que deseja adicionar como exceção.
3. De um duplo clique**Tipo de tráfego** e escolha no menu a opção correspondente ao tipo de endereço previamente inserido.
   - Se especificou um endereço web, selecione **HTTP**.
   - Se você especificou um endereço de e-mail, selecione **E-mail (SMTP)**.
   - Se você especificou um contato IM, selecione **IM**.

Para remover uma exceção da lista, selecione-a e clique no botão **Remover** .

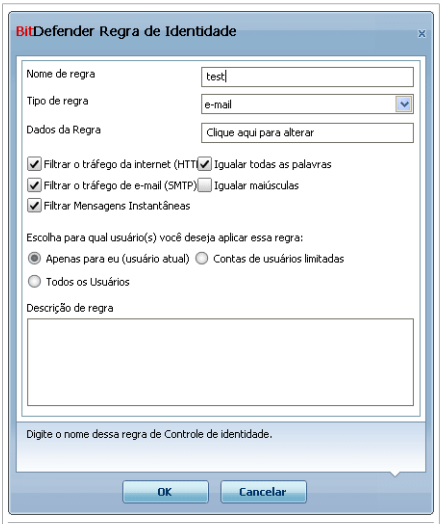
Clique em **OK** para salvar as alterações.

19.2.3. Gerir Regras

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas selecione-a e clique no botão **Apagar**.

Para editar uma regra selecione-a e clique no botão **Editar** ou de um duplo clique sobre esta regra. Uma nova janela aparecerá.



Editar Regra

Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

19.2.4. Regras Definidas por outros Administradores

Quando você não é o único usuário com direitos de administrador em seu computador, os outros administradores podem criar regras de identidade eles mesmos. Se você deseja que regras criadas por outros usuários não se apliquem quando você se logar, BitDefender permite que você mesmo exclua qualquer regra que você não tenha criado.

Você pode ver uma lista de regras criadas pelos administradores na tabela em **Controle de Regras**. Para cada regra, o nome e usuário que as criou estão listados na tabela.

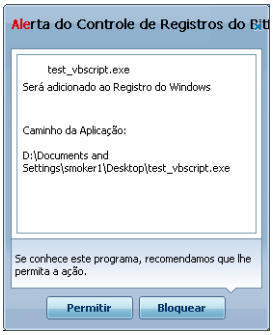
Para se remover de uma regra, selecione a regra na tabela e clique no botão **Remover**.

19.3. Controle de Registro

Uma parte muito importante do sistema operacional Windows é chamada de **Registro**. É aqui que o Windows mantém suas configurações, programas instalados, informações de usuário e informações do gênero.

O **Registro** é também usado para definir quais programas deverão ser iniciados automaticamente quando o Windows inicia. Vírus costumam usar isso para serem executados automaticamente quando o usuário reinicia seu computador.

O **Controle de Registro** fica de olho no Registro do Windows – Isso é útil também para detectar Trojans. Você será alertado sempre que um programa tentar modificar uma entrada de registro para ser executado na inicialização do Windows.



Alerta do Registro

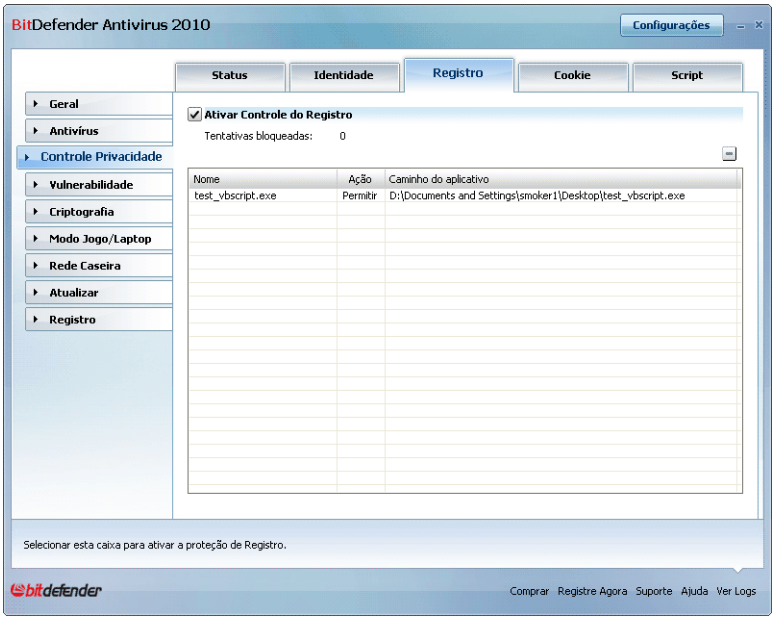
Poderá ver o programa que está a tentar alterar o registo do Windows.

Se não reconhece o programa e lhe parecer suspeito, clique em **Bloquear** para evitar que ele modifique o registo do Windows. De outra forma, clique em **Permitir** para permitir a modificação.

Baseado na sua resposta, a regra é criada e listada na tabela de regras. A mesma ação será aplicada sempre que este programa tentar modificar uma entrada no registo.

Nota
O BitDefender normalmente irá alertá-lo quando você instalar novos programas que precisam rodar após a próxima inicialização de seu computador. Na maioria dos casos, esses programas são legítimos e podem ser confiados.

Para configurar o Controle do Registo, vá para **Controle de Privacidade>Registro** no Modo Avançado.



Controle de Registro

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas selecione-a e clique no botão **Apagar**.

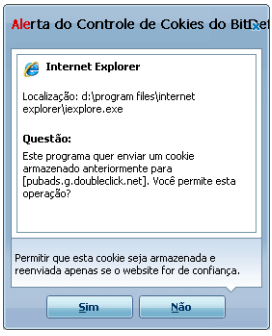
19.4. Controle de Cookie

Cookies são uma ocorrência muito comum na Internet. Eles são pequenos arquivos gravados em seu computador. Websites criam esses cookies para manter controle de informações específicas sobre você.

Cookies normalmente são usados para tornar sua vida mais fácil. Por exemplo, eles podem ajudar o site a lembrar de seu nome e preferências, para que você não tenha que inseri-los a cada visita.

Mas os cookies podem também ser usados para comprometer sua privacidade, vigiando seus padrões de navegação.

É aí que o **Controle de Cookie** ajuda. Quando ativado, o **Controle de Cookie** pedirá sua permissão sempre que um novo site tentar colocar um cookie:



Alerta de cookie

Você pode ver o nome do aplicativo que está tentando enviar o cookie.

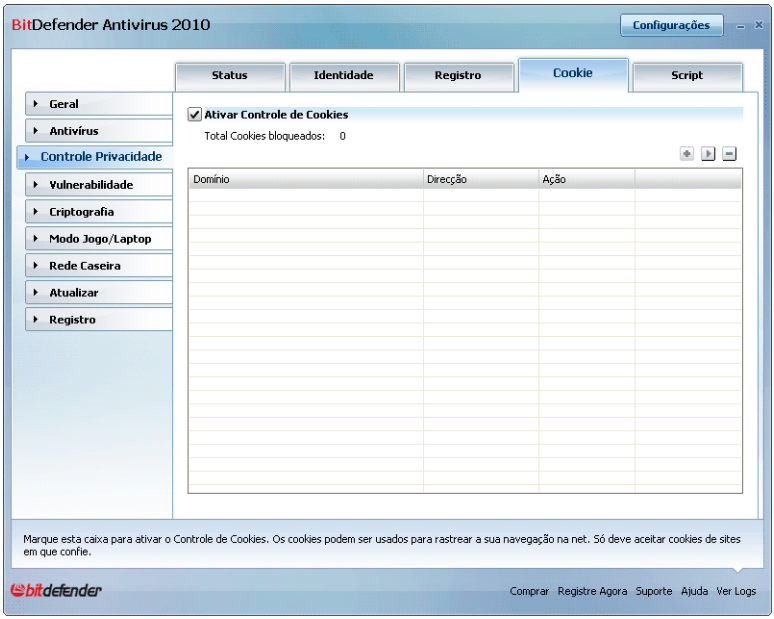
Clique em **Sim** ou **Não** e uma regra será criada, aplicada e listada na tabela regras.

Isso ajudará você a escolher quais sites tem ou não sua confiança.

Nota

Por causa do grande número de cookies usados hoje na Internet, o **Controle de Cookie** pode ser bem chato no início. No início, ele fará várias perguntas sobre sites tentando colocar cookies em seu computador. Conforme você adicionar seus sites comuns à lista de regras, surfar na Internet será tão fácil quanto antes.

Para configurar o Controle de Cookies, vá para **Controle de Privacidade>Cookie** no Modo Avançado.



Controle de Cookie

Pode ver as regras criadas até agora listadas na tabela.

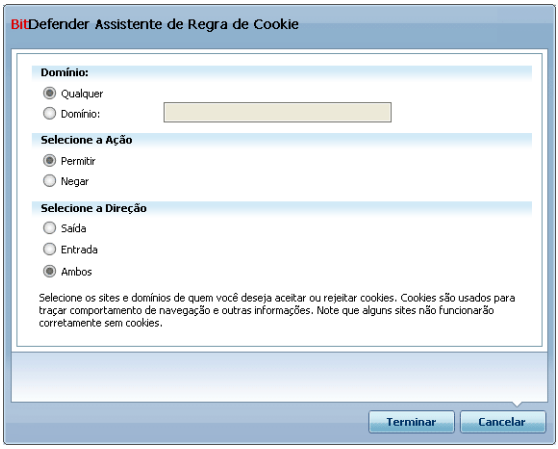
Importante
A prioridade das regras é de baixo para cima, ou seja, a última regra tem a maior prioridade. Arraste & solte regras para mudar a prioridade.

Para apagar uma regra, apenas selecione-a e clique no botão **Apagar**. Para modificar os parâmetros da regra, selecione-a e clique no botão **Editar** ou dê um duplo clique sobre ela. Faça as mudanças desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

19.4.1. Janela de configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



Selecione endereço, ação e direção

Você pode configurar parâmetros:

- **Domínio** - digite o domínio em que você quer aplicar a regra.
- **Ação** - selecione a ação da regra.

Ação	Descrição
Permitir	Os cookies daquele domínio serão executados.
Negar	Os cookies daquele domínio não serão executados.

- **Direção** - selecione a direção do tráfego.

Tipo	Descrição
Saída	A regra será aplicada apenas para os cookies que forem devolvidos para o site conectado.
Entrada	A regra será aplicada apenas para os cookies que forem recebidos do site conectado.
Ambos	As regras valem para as duas direções.

Nota
Você pode aceitar cookies mas nunca devolvê-los definindo a ação como **Negar** e a direção como **Saída**.

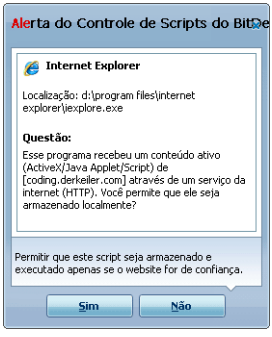
Clique em **Finalizar**.

19.5. Controle de Scripts

Scripts e outros códigos tais como Controles ActiveX e Java applets, que são usados para criar páginas da web interativas, podem ter efeitos danosos. Elementos ActiveX , por exemplo, podem ganhar acesso total a seus dados e eles podem ler dados de seu computador, apagar informações, capturar senhas e interceptar mensagens enquanto você esta on-line. Você pode apenas aceitar conteúdo ativo de sites de sua total confiança.

O BitDefender deixa você escolher entre executar estes elementos ou bloquear a execução.

Com o **Controle de Scripts** você será responsável por quais websites você confia ou não. O BitDefender pedra sua permissão sempre que um site tentar ativar um script ou outro conteúdo ativo:

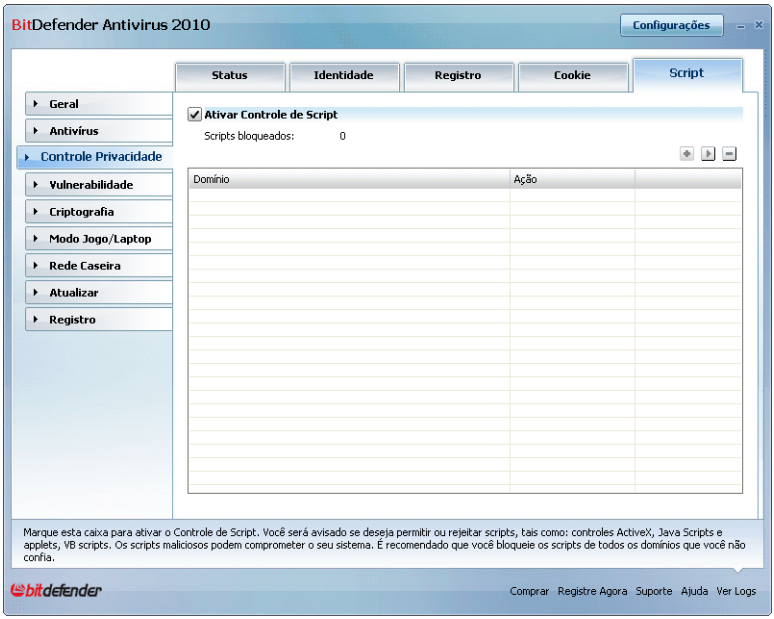


Alerta de script

Você pode ver o nome do recurso.

Clique em **Sim** ou **Não** e uma regra será criada, aplicada e listada na tabela regras.

Para configurar o Controle de Script, vá para **Controle de Privacidade>Script** no Modo Avançado.



Controle de Scripts

Pode ver as regras criadas até agora listadas na tabela.

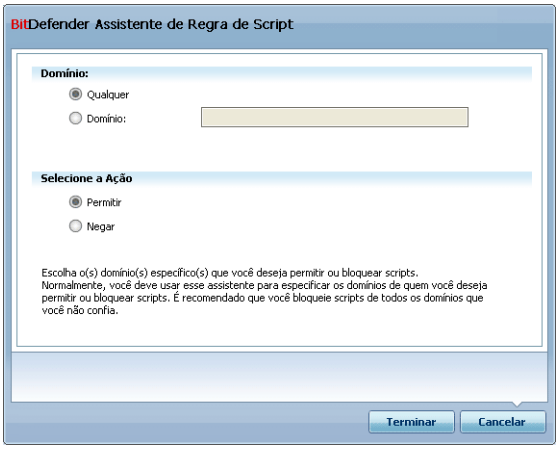
Importante
A prioridade das regras é de baixo para cima, ou seja, a última regra tem a maior prioridade. Arraste & solte regras para mudar a prioridade.

Para apagar uma regra, apenas selecione-a e clique no botão **Apagar**. Para modificar os parâmetros da regra, selecione-a e clique no botão **Editar** ou dê um duplo clique sobre ela. Faça as mudanças desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

19.5.1. Janela de configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



Selecione endereço e ação

Você pode configurar parâmetros:

- **Domínio** - digite o domínio em que você quer aplicar a regra.
- **Ação** - selecione a ação da regra.

Ação	Descrição
Permitir	Os scripts daquele domínio serão executados.
Negar	Os scripts daquele domínio não serão executados.

Clique em **Finalizar**.

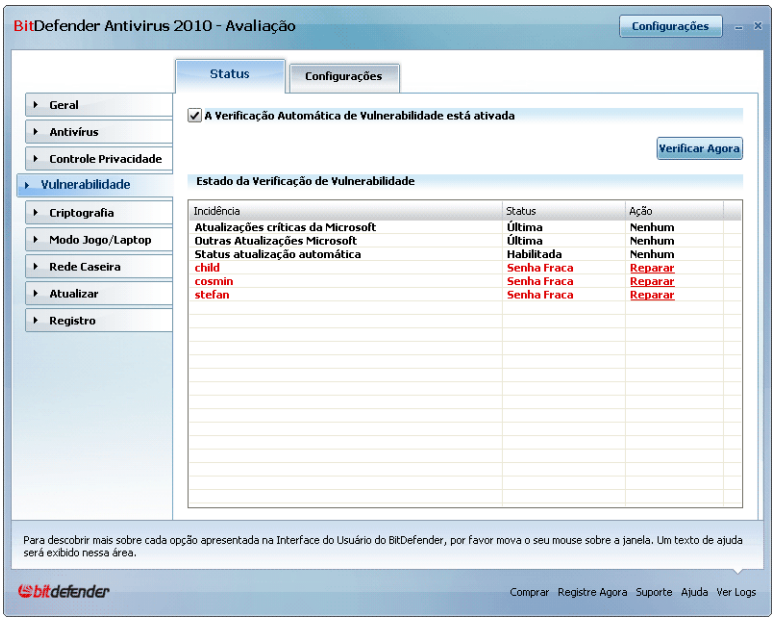
20. Vulnerabilidade

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operacional e as aplicações que usa regularmente. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, senhas fortes (senhasque não são fáceis de adivinhar) devem de ser criadas para cada conta de usuário do Windows.

O BitDefender analisa regularmente o seu sistema em busca de vulnerabilidades e notifica-o das incidências existentes.

20.1. Status

Para configurar a análise automática de vulnerabilidades, ou executar uma, vá para **Vulnerabilidade>Status** no Modo Avançado.



Status de Vulnerabilidade

A tabela mostra os problemas cobertos na última análise de vulnerabilidade e o seu estatus. Você pode ver a ação que deve ser tomada para consertar cada situação de vulnerabiliade, caso esta exista. Se a ação é **Nenhuma**, então o ponto detectado não representa um ponto de vulnerabilidade.

Importante

Para ser automaticamente notificado acerca das vulnerabilidades do seu sistema e aplicações, mantenha a **Análise Automática de Vulnerabilidades** activada.

20.1.1. Consertando pontos vulneráveis

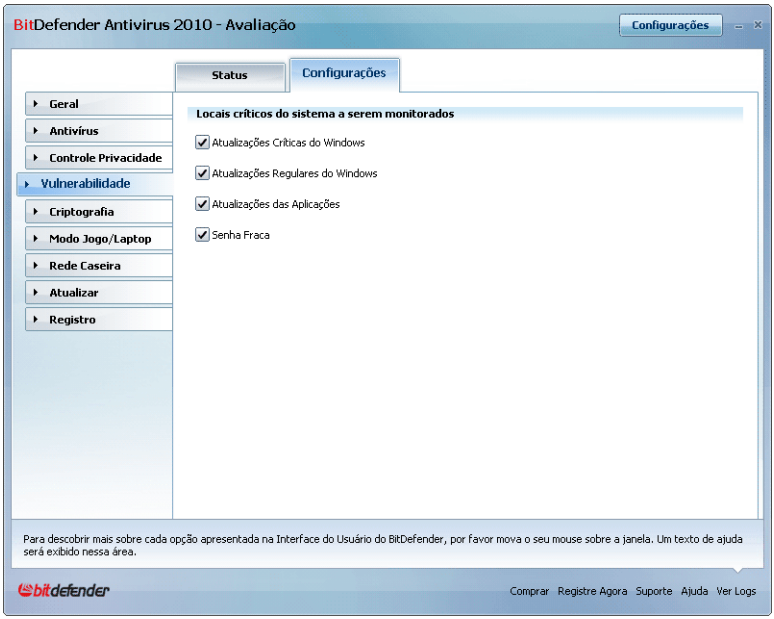
Dependendo da incidência, para consertar uma vulnerabilidade específica, proceda da seguinte forma:

- Se houver alguma atualização do Windows disponível, clique **Instalar** em **Ação** coluna para instalá-las.
- Se um aplicativo estiver desatualizado, use o link **Página Inicial** fornecido para efetuar o download e instalar a versão mais atualizada do aplicativo.
- Se um usuário do Windows tiver uma senha fraca, clique **Corrigir** para forçar o usuário a trocar a senha no próximo logon ou mude a senha você mesmo Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

Você pode clicar **Verificar Agora** e seguir as instruções para consertar os pontos vulneráveis passo a passo. Para maiores informações, por favor vá para *"Assistente de Verificação de Vulnerabilidades"* (p. 63).

20.2. Configurações

Para configurar as definições da análise automática de vulnerabildades, vá para **Vulnerability>Settings** in Expert Mode.



Definições da Análise Automática de Vulnerabilidades

Selecione as caixas que correspondem às vulnerabilidades do sistema que deseja que sejam regularmente verificadas.

- **Atualizações Críticas do Windows**
- **Atualizações Regulares do Windows**
- **Atualização do Aplicativo**
- **Palavras-passe Fracas** .

Nota

Se limpar a a caixa correspondente a uma determinada vulnerabilidade, o BitDefender não o irá mais notificar acerca das incidências relacionadas.

21. Criptografia de Mensagens Instantâneas (IM)

De forma padrão, BitDefender cifra todas as suas sessões de chat desde que:

- O seu parceiro de chat tenha instalada uma versão do BitDefender que suporte a cifragem MI e a mesma esteja habilitada para o programa de mensagens usado durante o chat.
- E o seu parceiro de chat esteja a usar quer o Yahoo Messenger ou o Windows Live (MSN) Messenger.

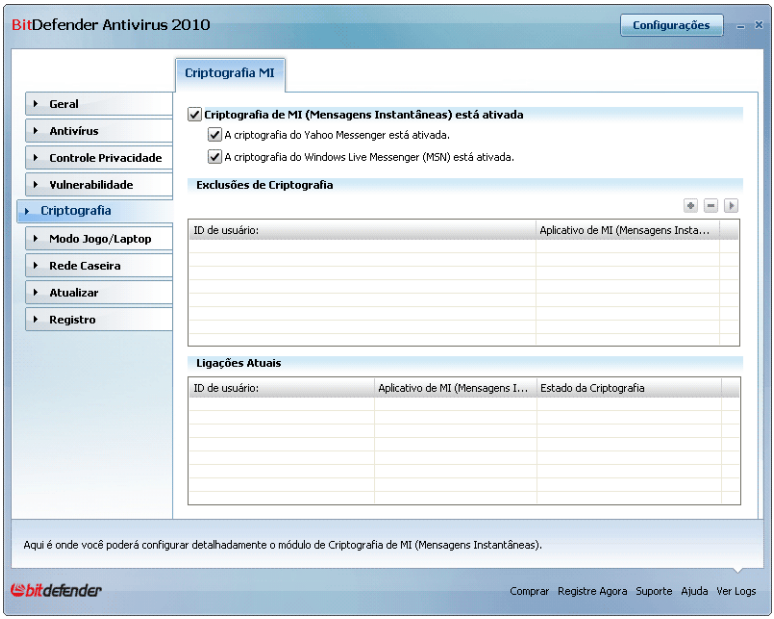
Importante

O BitDefender não criptografará uma conversa caso o outro contato estiver usando um aplicativo de mensagens instantâneas tal como o Meebo, ou outro aplicativo tal como Yahoo! Messenger ou o Windows Live()MSN).

Para configurar a criptografia de Mensagens Instantâneas, vá para **Criptografia>Criptografia MI** no Modo Avançado.

Nota

Pode configurar facilmente a cifragem das mensagens instantâneas usando a barra de ferramentas a partir da janela de chat. Para mais informações, por favor, vá para "*Integração aos programas de Mensagens Instantâneas*" (p. 205).



Criptografia de Mensagens Instantâneas

Como padrão, a Criptografia de Mensagens Instantâneas está ativada para o Yahoo! Messenger e o Windows Live (MSN) Messenger. Você pode escolher desativar a Criptografia de Mensagens Instantâneas para apenas um aplicativo de chat ou para todos.

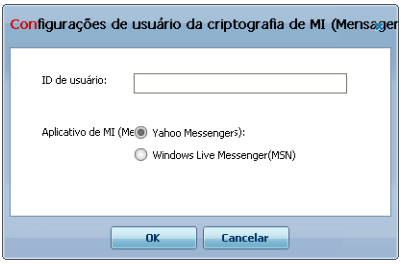
São mostradas duas tabelas:

- **Exclusões da Criptografia** - lista os IDs dos usuários e o programa de IM associado para os quais a criptografia está desativada. Para remover um contato da lista , selecione-o e clique no botão **Remover**.
- **Conexões Atuais** - lista as atuais conexões de mensagens (IDs dos usuários e o programa de IM associado) e se devem ou não ser criptografadas. Uma conexão poderá não ser criptografada pelas seguintes razões:
  - Você desativou explicitamente a criptografia para o respectivo contato.
  - O seu contato não tem instalado uma versão do BitDefender que suporte a criptografia de Mensagens Instantâneas.

21.1. Desativar a Criptografia para usuários Específicos

Para desativar a criptografia para um determinado usuário, siga estes passos:

1. Clique no botão **Adicionar** para abrir a janela de configuração.



Adicionar contatos

2. Insira no campo de edição o ID do usuário do seu contato.
3. Selecione o aplicativo de mensagens instantâneas associada ao contato.
4. Clique em **OK**.

22. Modo de Jogo / Portátil

O módulo do modo de Jogo / Portátil permite-lhe configurar os modos especiais de operação do BitDefender.

- O Modo Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema enquanto estiver jogando.
- O Modo Portátil evita que as tarefas agendadas sejam executadas quando o seu portátil esteja em modo de bateria de forma a economizar a mesma.

22.1. Modo de Jogo

O Modo de Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema. Quando liga o Modo de Jogo, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender estão desativados.
- O nível da proteção em tempo-real do BitDefender é definido como **Permissivo**.
- As atualizações não são executadas por padrão.

Nota
Para mudar esta configuração, vá para Atualizar>Configurações e limpe a **Não atualizar se o Modo Game (Jogo)estiver ativado** selecione a opção.

- As tarefas de análise agendadas são desativadas por padrão.

Por padrão, o BitDefender entra automaticamente em Modo Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender, ou quando uma aplicativo vai para tela cheia. Pode entrar manualmente em Modo Jogo usando uma tecla de atalho como padrão `Ctrl+Alt+Shift+G`. É fortemente recomendado que saia do Modo Jogo quando acaba de jogar (Pode usar a mesma tecla de atalho padrão `Ctrl+Alt+Shift+G`).

Nota
Enquanto no Modo de Jogo, pode ver a letra G sobre o  icone do BitDefender.

Para configurar o Modo Jogo, vá para **Modo Jogo / Laptop>Modo Jogo** no Modo Avançado

Modo de Jogo

No topo da seção, você pode ver o estado do Modo de Jogo. Você pode clicar em **Ligar o Modo Jogo** ou **Desligar o Modo Jogo** para alterar o estado atual.

22.1.1. Configurar Modo de Jogo Automático

O Modo de Jogo Automático permite que o BitDefender entre automaticamente em Modo de Jogo quando um jogo é detectado. Você pode configurar uma das seguintes opções:

- **Usar a lista padrão de jogos do BitDefender** - para entrar automaticamente em Modo Jogo quando você inicia um jogo da lista dos jogos conhecidos do BitDefender. Para ver esta lista, cique em **Gerenciar Jogos** e depois em **Lista de Jogos**.
- **Entrar em Modo Jogo quando um programa estiver em tela cheia** - para entrar automaticamente em Modo Jogo quando um aplicativo estiver em tela cheia.
- **Adicionar o aplicativo à lista de jogos?** - para ser solicitado a adicionar o novo aplicativo à lista de jogos quando deixar o modo de tela cheia. Ao adicionar um novo aplicativo à lista de jogos, da próxima vez que jogar o BitDefender entrará automaticamente em Modo Jogo.

Nota
Se não deseja que o BitDefender entre automaticamente em Modo de Jogo, limpe a caixa de selecção **Modo de Jogo Automático**.

22.1.2. Gerir a Lista de Jogos

O BitDefender entra automaticamente em Modo Jogo quando inicia um aplicativo que se encontra na lista de jogos. Para ver e gerir a lista de jogos, clique em **Gerir Jogos**. Uma nova janela irá aparecer.

Lista de Jogos

Novas aplicações são adicionadas automaticamente à lista quando:

- Inicia um jogo da lista de jogos conhecidos do BitDefender. Para ver esta lista, clique em **Lista de Jogos**.
- Após sair do modo de tela cheia, você adiciona o aplicativo à lista de jogos a partir da janela de notificação.

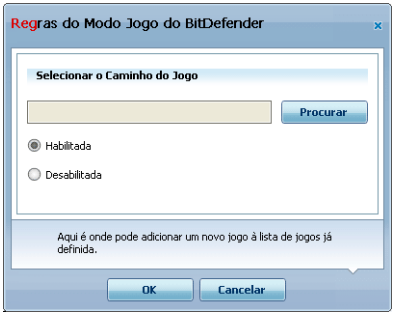
Se deseja desativar o Modo Jogo Automático para um determinado aplicativo da lista, limpe a correspondente caixa de seleção. Você deve desativar o Modo de Jogo Automático para as aplicações que regularmente entram em modo de tela cheia, tais como os navegadores da Internet e os leitores de filmes.

Para gerir a lista de jogos, pode usar os botões colocados no topo da tabela:

- **Adicionar** - adicionar um novo aplicativo à lista de jogos.
- **Remover** - remover um aplicativo da lista de jogos.
- **Editar** - editar um registro existente na lista de jogos.

Adicionar ou Editar Jogos

Quando adiciona ou edita uma entrada da lista de jogos, a seguinte janela aparecerá:



Adicionar Jogo

Clique em **Explorar** para selecionar o aplicativo e o caminho da mesma no campo de edição.

Se você não quiser entrar automaticamente em Modo Jogo quando o aplicativo selecionado é executado, selecione **Desativar**.

Clique em **OK** para adicionar a entrada à lista de jogos.

22.1.3. Configurar as Definições do Modo de Jogo

Para configurar o comportamento das tarefas agendadas, use estas opções:

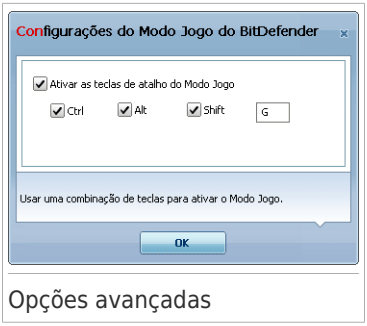
- **Ativar este módulo para modificar as tarefas agendadas do Antivírus** - para impedir a execução de tarefas de análise agendadas enquanto estiver no Modo Jogo. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executa a tarefa imediatamente após sair do Modo de Jogo.

22.1.4. Mudar a Hotkey do Modo de Jogo

Pode entrar manualmente em Modo Jogo usando uma tecla de atalho como padrão `Ctrl+Alt+Shift+G`. Se deseja mudar a hotkey, siga estes passos:

1. Clique em **Configuração Avançada**. Uma nova janela irá aparecer.



Opções avançadas

2. Por baixo da opção **Usar HotKey** , defina a hotkey desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

   Por exemplo, de deseja usar a hotkey `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir `D`.

   Nota
   Remover a marca de seleção próximo de **Ativar Tecla de Atalho** irá desativar a tecla de atalho.

3. Clique em **OK** para salvar as alterações.

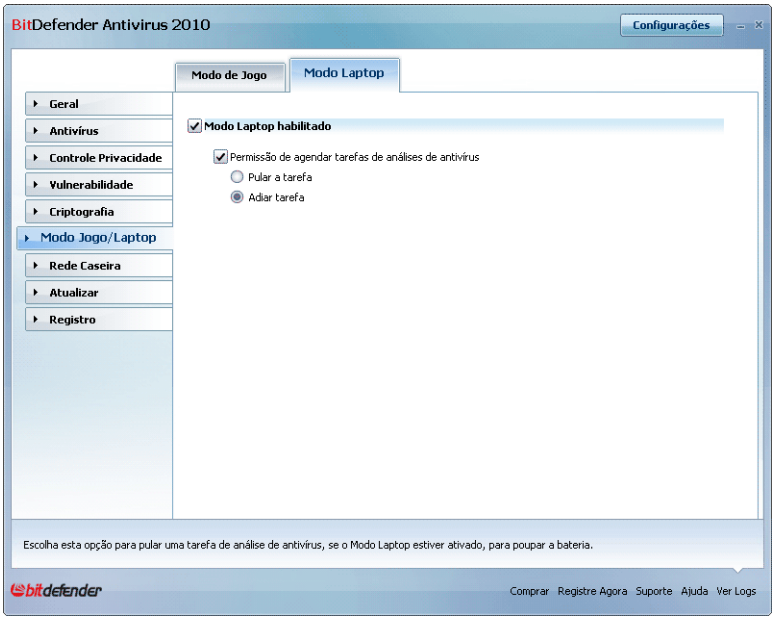
22.2. Modo Laptop

O Modo Portátil foi especialmente desenhado para os usuários de laptops. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o laptop estiver a funcionar a bateria.

Enquanto estiver no Modo laptop, por padrão, as tarefas agendadas não serão executadas.

O BitDefender detecta quando o seu portátil está a funcionar a bateria e automaticamente entra em Modo de Portátil. De igual forma, O BitDefender sai automaticamente do Modo de Portátil quando detecta que o seu portátil já não está a funcionar a bateria.

Para configurar o Modo Laptop, vá para **Modo Jogo/Laptop>Modo Laptop** no Modo Avançado



Modo Laptop

Pode ver se o Modo de Portátil está ou não ligado. Se o Modo de Portátil está ligado, o BitDefender aplicará as definições configuradas para o portátil a funcionar a bateria.

22.2.1. Configurar Definições do Modo de Portátil

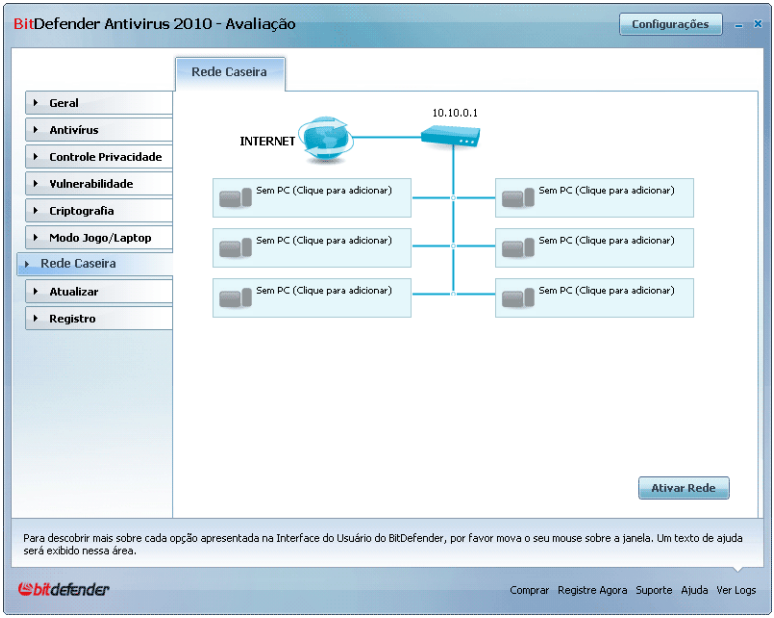
Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Ativar este módulo para modificar as tarefas agendadas do Antivírus** - para impedir a execução de tarefas de análise agendadas enquanto estiver no Modo Laptop. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada assim que sair do Modo de Portátil.

23. Rede Caseira

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador.



Mapa de Rede

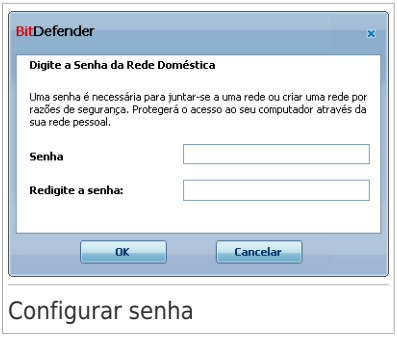
Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

1. Adira à rede pessoal do BitDefender no seu computador. Aderir à rede consiste em configurar uma senha administrativa para o gestor da rede pessoal.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a senha).
3. Volte para o seu computador e adicione os computadores que deseja gerir.

23.1. Aderir à Rede BitDefender

Para aderir à rede pessoal BitDefender, siga os seguintes passos:

1. Clique em **Ativar Rede**. Será notificado para configurar a senha de gestão de rede pessoal.



Configurar senha

2. Insira a mesma senha em cada um dos campos editáveis.
3. Clique em **OK**.

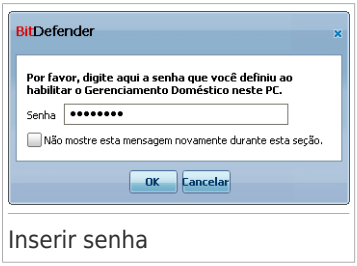
Pode ver o nome do computador a aparecer no mapa de rede.

23.2. Adicionar Computadores à Rede BitDefender

Antes que possa adicionar um computador à rede doméstica BitDefender, deve de configurar a sua senha de gestão de rede pessoal no respectivo computador.

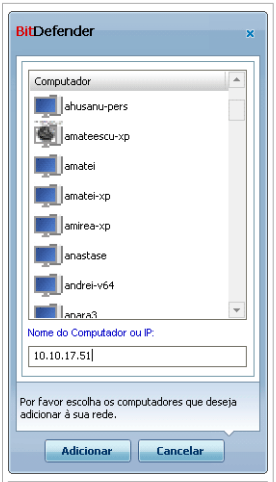
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

1. Clique em **Adicionar Computador**. Será notificado para inserir a sua senha de gestão de rede pessoal local.



Inserir senha

2. Insira a senha de gestão rede pessoal e clique em **OK**. Uma nova janela irá aparecer.



Adicionar Computador

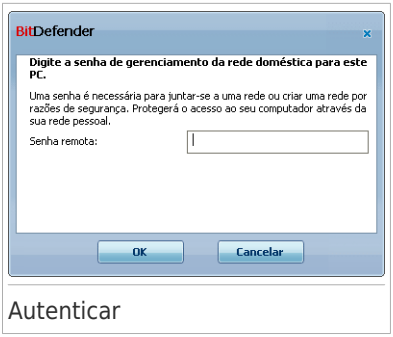
Pode ver a lista dos computadores na rede. O significado do ícone é o seguinte:

Indica um computador on-line sem produtos BitDefender instalados.

Indica um computador on-line com o BitDefender instalado.

Indica um computador offline com o BitDefender instalado.

3. Faça uma das coisas seguintes:
   - Selecione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
4. Clicando **Adicionar**. Será notificado para inserir a sua senha de gestão de rede pessoal do respectivo computador.



Autenticar

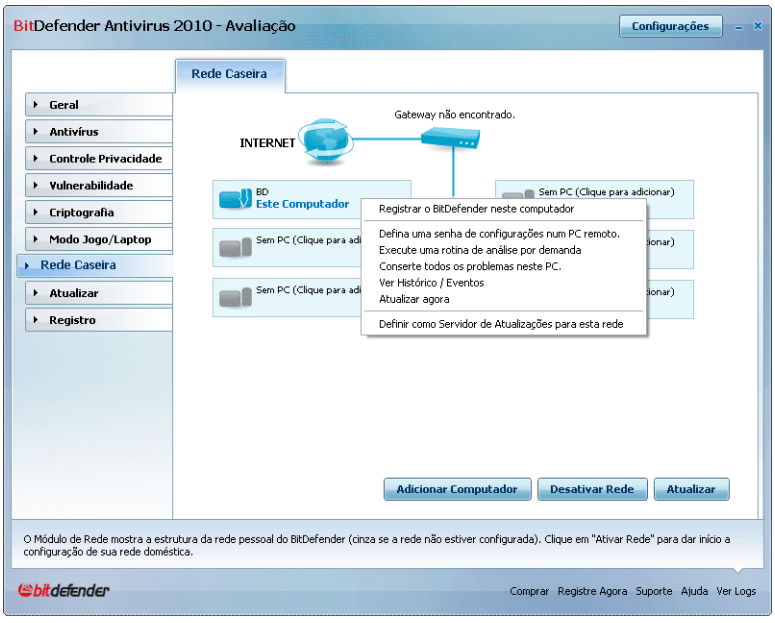
5. Insira a senha de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**. Se forneceu a senha correta, a nome do computador selecionado aparecerá no mapa de rede.

Nota

Pode adicionar até cinco computadores neste mapa de rede.

23.3. Gerir a Rede BitDefender

Uma vez que tenha criado com sucesso a sua rede pessoal BitDefender pode gerir todos os produtos BitDefender a partir de um único computador.



Mapa de Rede

Se mover o curso do seu mouse sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afetar a segurança do sistema, o estado de registo do BitDefender).

Se você clicar em um nome de computador no mapa da rede, você poderá ver todas tarefas administrativas que você pode executar no computador remoto.

- **Remover o PC da rede doméstica**

Permite que você remova o PC da rede doméstica.

- **Registar o BitDefender neste computador**

  Permite que você registre o BitDefender neste computador digitando uma licença.

- **Definir uma senha para as definições em um PC remoto**

  Permite você criar uma senha para restringir o acesso às configurações do BitDefender neste PC.

- **Executar uma tarefa de análise por demanda**

  Permite você executar uma análise por demanda num computador remoto. Você pode executar qualquer das seguintes tarefas de análise: Analisar Meus Documentos, Análise de Sistema ou Análise Minuciosa do Sistema.

- **Reparar todas as incidências neste computador**

  Permite que você corriga ocorrências que estão afetando a segurança deste computador seguindo o assistente Corrigir Todas Ocorrências.

- **Ver Histórico/Eventos**

  Permite que você acesse o módulo **História&Eventos** do produto BitDefender instalado neste computador.

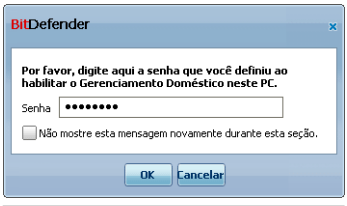
- **Atualizar Agora**

  Inicia o processo de atualização do produto BitDefender instalado neste computador.

- **Definir este computador como Servidor de Atualizações desta Rede**

  Permite que você defina este computador como um servidor de atualização para todos produtos BitDefender instalados nesta rede. Usando esta opção irá reduzir o tráfego de internet, porque apenas um computador na rede irá se conectar e fazer o download das atualizações.

Antes de executar uma tarefa num computador específico, voê será notificado para inserir a senha de gerenciamento de rede doméstica local.



Inserir senha

Insira a senha de gestão rede pessoal e clique em **OK**.

Nota

Se você planeja executar várias tarefas, selecione **Não me mostrem mais esta mensagem durante esta sessão**. Ao selecionar esta opção, não será notificado novamente pela senha durante esta sessão.

24. Atualizar

Novo malware é achado e identificado todos os dias. É por isso que é muito importante manter o BitDefender atualizado com as últimas assinaturas de malware.

Se você se conectar a Internet através de banda-larga ou DSL, o BitDefender se encarrega da atualização. Ele verifica novas assinaturas de vírus quando você liga o seu computador e toda **hora** depois.

Se uma atualização for detectada, poderá ser notificado para confirmar a atualização ou a mesma é levada a cabo automaticamente, dependendo das definições automáticas da atualização.

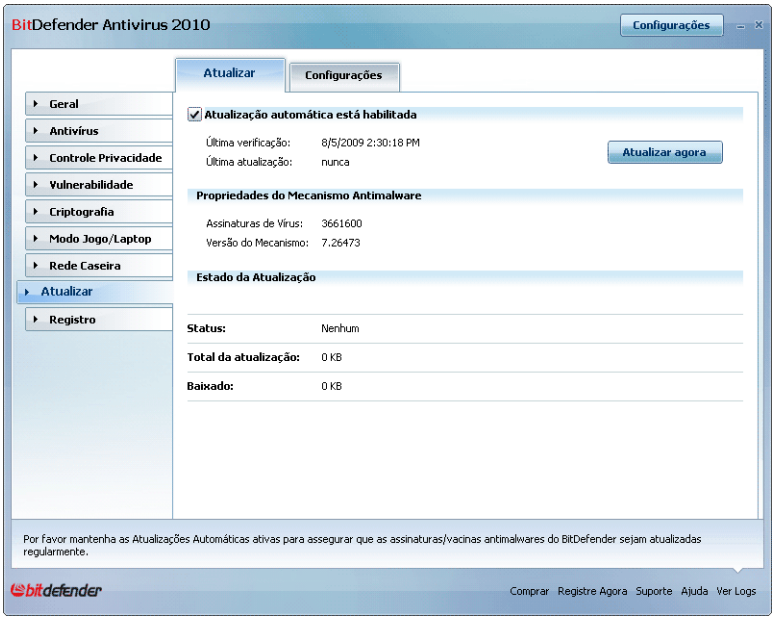
O processo de atualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Atualizações vêm das seguintes formas:

- **Atualização dos mecanismos antivírus** - conforme novas ameaças aparecem, os arquivos contendo as vacinas de vírus devem ser atualizados para assegurar proteção permanente atualizada contra eles. Esta atualização também é conhecido como **Atualização de Definições de Vírus**.
- **Atualizações para os mecanismos antispyware** - novas vacinas de spyware serão adicionadas a base de dados. Esta atualização também é conhecido como **Atualização Antispyware**.
- **Atualização do produto** - quando uma nova versão do produto é lançada, novos recursos e técnicas de verificação são introduzidos para aprimorar a performance do produto. Esta atualização também é conhecido como **Atualização de versão do produto**.

24.1. Atualização Automática

Para ver informações relacionadas com atualizações e executar atualizações automáticas, vá para **Atualização>Atualização** no Modo Avançado.



Atualização Automática

Aqui pode-se ver quando foi feita a última atualização e a última verificação de atualizações, além de informações da última atualização executada (se bem-sucedida ou se ocorreram erros). Também a informação acerca da versão do mecanismo e o número de vacinas são mostrados.

Se abrir esta seção durante uma atualização, você poderá ver o status do download.

Importante
Para estar protegido contra as mais recentes ameaças mantenha a **Aualização Automática** ativada.

Você pode obter as vacinas de malware do seu BitDefender ao clicar em **Mostrar Lista de Vírus**. Um arquivo HTML que contém todas as assinaturas disponíveis será criado e aberto no navegador de internet. Você pode procurar uma assinatura específica de malware entre a base de dados ou clicar em **Lista de Vírus do BitDefender** para acessar a base de dados de assinaturas BitDefender on-line.

24.1.1. Solicitando uma Atualização

A atualização automática também pode ser feita a qualquer hora clicando em **Atualizar Agora**. Também conhecido por **Atualização a pedido do usuário**.

O módulo de **Atualização** irá conectar ao servidor de atualização do BitDefender e verificará se uma atualização está disponível. Caso seja verdadeiro, dependendo das opções configuradas na seção Opções de Atualização Manual você será indagado a confirmar a atualização ou a mesma será feita automaticamente.

Importante
Talvez seja necessário reiniciar o computador depois da atualização. Caso seja necessário, recomendamos que o faça o mais rápido possível.

Nota
Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o BitDefender a pedido do usuário.

24.1.2. Desabilitar Atualização Automática

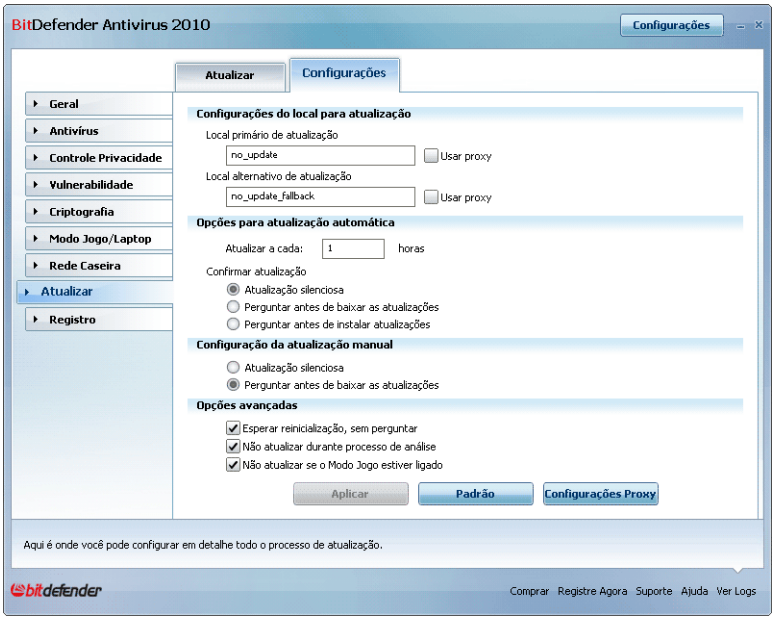
Se você desabilitar a atualização automática, uma janela de alerta aparecerá. Você tem que confirmar a sua escolha ao selecionar no menu durante quanto tempo deseja que a atualização automática fique desativada. Você pode desativar a atualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desative a actualização automática pelo menor tempo possível. Se o BitDefender não for atualizado regularmente, não será capaz de proteger você contra as ameaças mais recentes.

24.2. Atualizar as Configurações

Atualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy. Por padrão, o BitDefender verificará as atualizações de hora em hora, via Internet, e instalará as que estejam disponíveis sem alertar você.

Para configurar as definições de atualização e gerenciar proxies, vá para **Atualização>Configurações** no Modo Avançado.



Atualizar as Configurações

As configurações da atualização estão agrupadas em 4 categorias (**Configuração da Localização da Atualização**, **Configuração de atualização automática**, **Configuração de Atualização Manual** e **Configuração Avançada**). Cada categoria será descrita separadamente.

24.2.1. Definir local para atualização

Para definir a localização da atualização, use as opções da categoria **Configuração da Localização da Atualização** .

Nota

Configure estas definições apenas se estiver conectado a uma rede local que armazena localmente as vacinas de malware do BitDefender ou se liga à Internet através de um servidor proxy.

Para atualizações melhores e mais rápidas, você pode configurar dois locais de atualização: uma **Local de atualização primária** e uma **Local de atualização alternativa**. Como padrão, estas localizações são iguais:`http://upgrade.bitdefender.com`.

Para modificar um dos locais de atualização, insira o URL do servidor-espelho local no campo **URL** que corresponde ao novo local para o qual deseja mudar.

Nota

Recomendamos que defina como local primário de atualização o local servidor-espelho e deixar o local alternativo de atualização como está, como um plano de backup em caso do servidor-espelho local ficar indisponível.

No caso em que a empresa usa um servidor proxy para se conectar à Internet, selecione **Usar proxy** depois clique em **Definições de proxy** para configurar as definições do proxy. Para mais informação, por favor consulte "*Gerir Proxies*" (p. 191)

24.2.2. Configurar Atualização Automática

Para configurar o processo de atualização automática do BitDefender, use as opções na categoria **Configuração Atualização Automática** .

Você pode definir o número de horas entre duas análises consecutivas de atualizações no campo **Atualizar a cada**. Por padrão, o intervalo de tempo da atualização é de 1 hora.

Para definir como é que o processo de atualização automática tem que ser feito, selecione uma das seguintes opções:

- **Atualização Silenciosa** - O BitDefender faz download automaticamente e implementa a atualização.
- **Perguntar antes de fazer download das atualizações** - todas as vezes que uma atualização estiver disponível, você será indagado antes do download ser feito.
- **Perguntar antes de instalar atualizações** - todas as vezes que uma atualização for feita em download, você será indagado antes de ela ser instalada.

24.2.3. Configurar Atualização Manual

Para definir como a atualização manual (atualização a pedido do usuário) deve ser executada, selecione uma das seguintes opções na categoria **Configuração Atualização Manual**:

- **Actualização silenciosa** - a atualização manual será feita em segundo plano automaticamente.
- **Perguntar antes de fazer download das atualizações** - todas as vezes que uma atualização estiver disponível, você será indagado antes do download ser feito.

24.2.4. Configurar Opções Avançadas

Para evitar que o processo de atualização do BitDefender interfira com o seu trabalho, configure as opções na categoria **Configuração Avançada**:

- **Esperar reinicialização, sem perguntar** - Se uma atualização requerer uma inicialização, o produto continuará funcionando com os arquivos antigos até o sistema reiniciar. O usuário não será indagado para reiniciar o sistema, sendo assim o processo de atualização do BitDefender não irá interferir no trabalho do usuário.
- **Não atualizar se a análise estiver ocorrendo** - O BitDefender não vai atualizar se estiver ocorrendo uma análise. Desta forma, o processo de atualização do BitDefender não vai interferir com as tarefas de análise.

  Nota
  Se o BitDefender for atualizado enquanto a análise estiver ocorrendo, o processo de análise será cancelado.

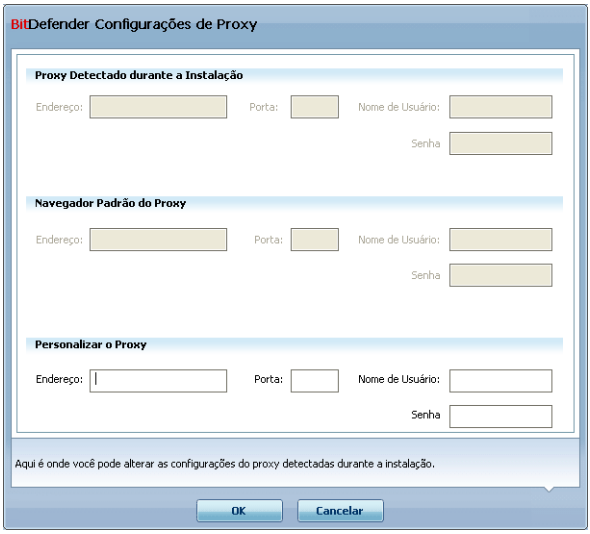
- **Não atualizar se o modo de jogo estiver ligado** - O BitDefender não atualizará se o Modo de Jogo estiver ligado. Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.

24.2.5. Gerir Proxies

Se a sua empresa usa um servidor proxy para se conectar à Internet, você deverá especificar as definições do proxy de forma a que o BitDefender se atualize sozinho. Do contrário, o BitDefender usará as definições do proxy do administrador que instalou o produto, ou o navegador padrão do atual usuário, se existir um.

Nota
As definições do proxy só podem ser configuradas por usuários com direitos administrativos no computador ou por power users (usuários que sabem a senha da configuração do produto).

Para gerenciar as definições de proxy, clique em **Definições de Proxy**. Uma nova janela irá aparecer.



Gestor Proxy

Existem três categorias de definições de proxy:

- **Proxy detectado durante a instalação** - as definições de proxy detectadas na conta de administrador durante a instalação e que podem ser configuradas apenas se você estiver logado com essa conta. Se o servidor proxy requer um nome de usuário e uma senha, você deverá especificá-los nos campos correspondentes.
- **Proxy Padrão do Navegador** - configurações de proxy do usuário atual, extraído do navegador padrão. Se o servidor proxy requer um nome de usuário e uma senha, você deve especificá-las nos campos correspondentes.

  Nota
  Os browsers de internet suportados são o Internet Explorer, Mozilla Firefox e Opera. Se por padrão, você utiliza outro explorador, o BitDefender não será capaz de obter as definições do proxy do atual usuário.

- **Proxy Personalizado** - definições de proxy que você pode configurar se estiver logado como administrador.

  As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o BitDefender usa para se ligar ao servidor proxy.
  - **Usuário do proxy** - digite um usuário reconhecido pelo Proxy.

- **Senha do proxy** - digite a senha válida para o usuário especificado anteriormente.

Quando tentar ligar-se à Internet, cada conjunto de definições do proxy é experimentado na sua vez, até que o BitDefender se consiga ligar.

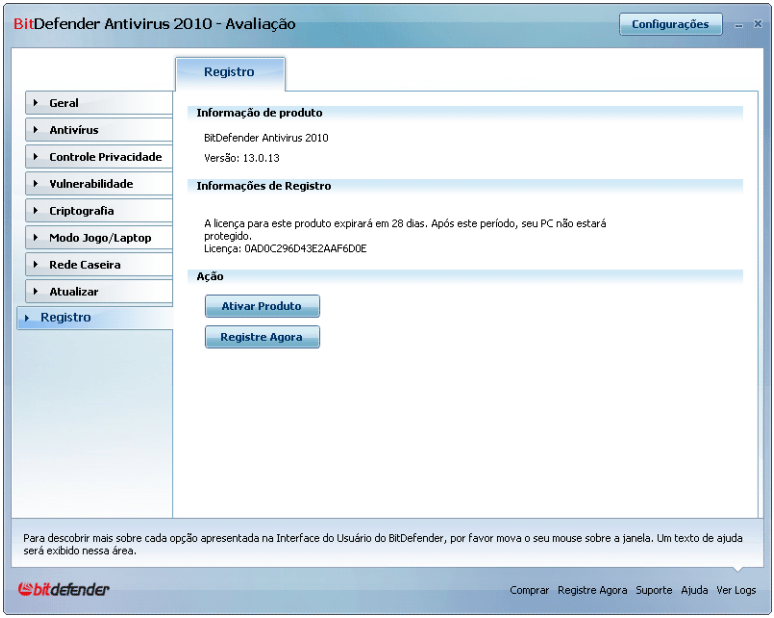
Primeiro, o conjunto que contém as suas definições do proxy será utilizado para se conectar à Internet. Se esse não funcionar, as definições de proxy detectadas durante a instalação serão experimentadas logo a seguir. Finalmente se nenhuma dessa funcionar, as definições de proxy do usuário atual serão retiradas do seu navegador padrão e usadas para obter a conexão à Internet.

Clique em **OK** para guardar as alterações e fechar a janela.

Clique em **Aplicar** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

25. Registro

Para encontrar uma completa informação sobre o seu produto BitDefender e o status do registo, vá para**Registo** no Modo Avançado.



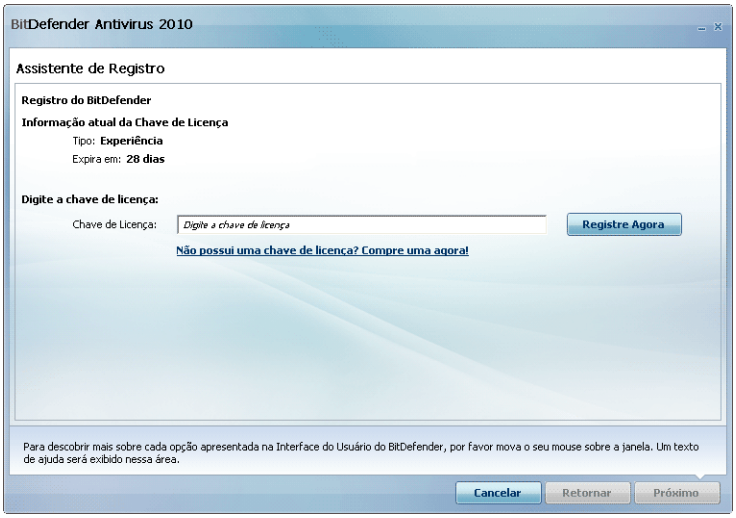
Registro

Esta seção mostra:

- **Informação do Produto** : O produto BitDefender e a sua versão.
- **Informação de Registo** : o endereço de e-mail usado para entrar na sua conta BitDefender (se configurada), a atual chave de licença e o número de dias que faltam para a licença expirar.

25.1. Registrando o BitDefender Antivírus 2010

Clique **Registrar Agora** para abrir a janela de registro do produto.



Registro

Você pode ver o estado do registo do BitDefender, a chave de licença atual e quantos dias faltam para a licença expirar.

Para registrar o BitDefender Antivírus 2010:

1. Insira a chave de licença no campo de edição.

Nota

Pode encontrar a sua chave de licença:

- Na bolsa do CD.
- ou no cartão de registo do produto.
- no e-mail da sua compra on-line.

Se não possuir uma chave de licença BitDefender, clique no link que lhe facultamos para ir até à loja on-line do BitDefender e adquirir uma.

2. Clique **Registrar Agora**.
3. Clique em **Finalizar**.

25.2. Criar uma conta BitDefender

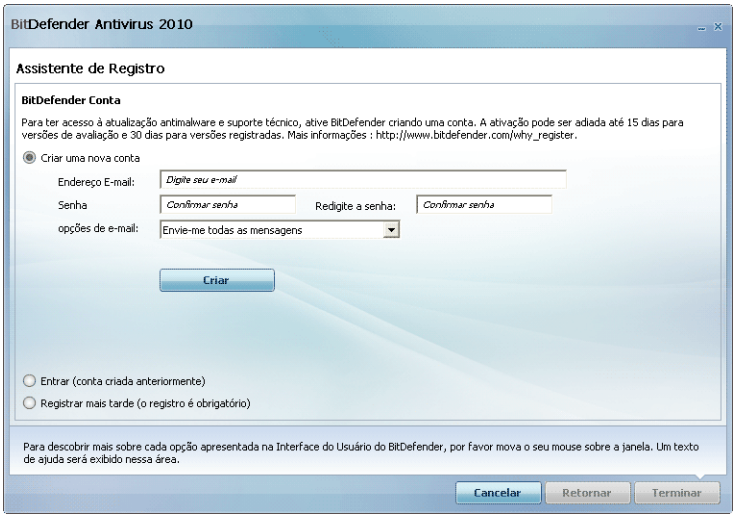
Como parte do processo de registro, você PRECISA criar sua conta BitDefender. A sua cnta BitDefender lhe oferece acesso às atualizações de virus BitDefender, suporte técnico grátis, além de ofertas e promoções especiais. Se perder a sua

chave de licença BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Importante

Você deve criar uma conta dentro de 15 dias após instalar o BitDefender (Se você registrar com uma chave de licença, o prazo limitie é extendido para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus.

Se você não tiver criado uma conta do BitDefender ainda, clique em **Ativar produto** para abrir a janela de registro.



Criar uma Conta

Se não deseja criar uma conta BitDefender neste momento, selecione **Registrar mais tarde** e clique em **Terminar**. De outra forma, actue de acordo com a sua presente situação:

- “Não tenho uma conta BitDefender” (p. 196)
- “Já tenho uma conta BitDefender” (p. 197)

Não tenho uma conta BitDefender

Para criar uma conta BitDefender com sucesso, siga estes passos:

1. Selecione **Criar uma nova conta**.

2. Digite as informações necessárias nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   - **E-mail** - insira o seu endereço de e-mail.
   - **Senha** - insira uma Senha para a sua conta BitDefender. A senha deve ter entre 6 e 16 caracteres de tamanho.
   - **Re-insira a senha** - insira novamente a senha previamente definida.

   
   Nota
   Uma vez que a conta é ativada, você pode usar o endereço de e-mail fornecido e senha para fazer o log in na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Selecione uma das opções disponíveis do menu:
   - **Enviar todas as mensagens**
   - **Enviem-me apenas mensagens referentes ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique **Criar**.
5. Clique **Finalizar** para completar o assistente.
6. **Ative sua conta.** Antes de ser capaz de usar a sua conta, você deve ativá-la. Verifique seu e-mail e siga as instruções no e-mail enviado a você pelo serviço de registro da BitDefender.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Neste caso, forneça a senha de sua conta e clique em **Entrar**. Clique **Finalizar** para completar o assistente.

Se você já tiver uma conta ativa, mas o BitDefender não a detectou, siga estes passos para registrar o produto para aquela conta:

1. Selecione **Entrar (na conta criada previamente)**.
2. Digite o endereço de email e senha da sua conta nos campos correspondentes.

   
   Nota
   Se não se lembra da sua senha, clique em **Esqueceu a sua senha?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Selecione uma das opções disponíveis do menu:
   - **Enviar todas as mensagens**

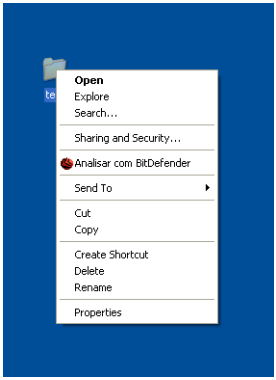
- **Enviem-me apenas mensagens referentes ao produto**
- **Não me enviem quaisquer mensagens**

4. Clique em **Entrar**.
5. Clique **Finalizar** para completar o assistente.

Integração com o Windows e Programas de terceiros

26. Integração ao Menu Contextual do Windows

O menu contextual do Windows aparecer sempre que você clica com o botão direito em cima de um arquivo, diretório ou objetos em sua Área de Trabalho.



Menu Contextual do Windows

O BitDefender se integra ao menu contextual do Windows para lhe auxiliar a analisar facilmente arquivos à procura de vírus. Você pode rapidamente localizar a opção BitDefender no menu contextual ao procurar pelo ícone do BitDefender.

26.1. Analisar com o BitDefender

Você pode facilmente analisar arquivos, diretórios e até mesmo discos inteiros utilizando o menu contextual do Windows. Clique com o botão direito do mouse sobre o objeto que você deseja analisar e selecione a opção **Analisar com o BitDefender** do menu. O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

Opções de detecção. As opções de análise são pré-configuradas para obter os melhores resultados em detecção. Se arquivos infectados forem detectados, o BitDefender irá tentar os desinfectar (remover o código malware). Se a desinfecção falhar, o wizard do analisador Antivírus irá permitir que você especifique outras ações a serem tomadas nos arquivos infectados.

Se você deseja alterar as opções de análise, siga os seguintes passos:

1. Abra o BitDefender e troque a interface de usuário para Modo Avançado.
2. Clique em **Antivírus** no menu do lado esquerdo.
3. Clique na aba **Análise Vírus Scan**.

4. Clique com o botão direito sobre a tarefa **Análise Contextual** e selecione **Abrir**. Uma janela aparecerá.
5. Clique em **Personalizar** e configure as opções de análise conforme necessário. Para descobrir o que uma opção faz, mantenha o cursor do mouse sobre ela e leia a descrição mostrada na parte inferior da janela.
6. Clique em **OK** para salvar as alterações.
7. Clique em **OK** para confirmar e aplicar as novas opções de análise.

Importante

Você não deve alterar as opções de análise desse método de análise a não ser que você tenha plena certeza do que está fazendo.

27. Integração com Exploradores web

BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet. Analisa os sites web que acede e alerta-o no caso de haver alguma ameaça de phishing. Uma Lista Branca de sites web que não serão analisados pelo BitDefender pode ser configurada.

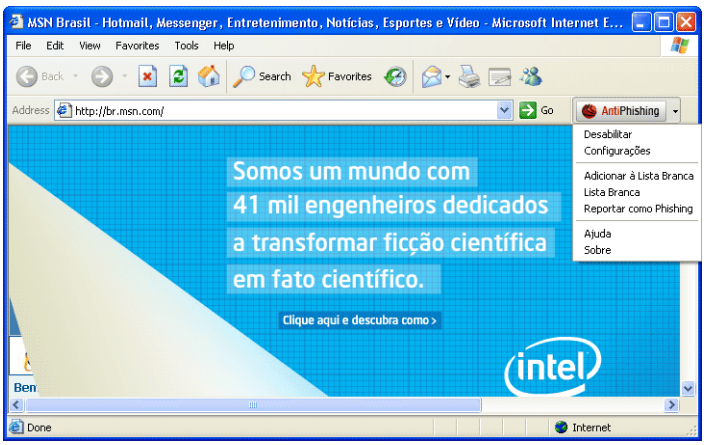
BitDefender integra-se diretamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes exploradores da Internet:

- Internet Explorer
- Mozilla Firefox

Você pode facilmente gerenciar a proteção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada num dos navegadores da internet acima.

A barra de ferramentas antiphishing, representada pelo ícone do BitDefender, está localizado no lado superior do navegador da internet. Clique nele de forma a abrir o menu da barra de ferramentas.

Nota
Se não consegue ver a barra de ferramentas, abra o menu **Ver** siga para **Barras de ferramentas** e selecione **Barra de Ferramentas BitDefender**.



Barra de Ferramentas do Antiphishing

Os seguintes comandos estão disponíveis no menu da barra de ferramentas:

- **Ativar / Desativar** - ativa / desativa a proteção Antiphishing do BitDefender na janela atual no navegador de internet.
- **Configuração** - abre uma janela onde pode especificar as definições da barra de ferramentas do antiphishing. As seguintes opções estão disponíveis:
  - **Proteção em Tempo Real Internet Antiphishing** - detecta e alerta você em tempo real se um site da internet está phished (configurado para roubar informações pessoais). Essa opção controla a proteção antiphishing do BitDefender apenas no navegador de internet atual.
  - **Avisar antes adicionar à lista branca** - será consultado antes de ser adicionado um site web à Lista Branca.
- **Adicionar à Lista Branca** - adiciona o atual site à Lista Branca.

Nota

Adicionar um site à Lista Branca significa que o BitDefender não irá mais analisar esse site em busca de tentativas de phishing. Recomendamos que adicione à Lista Branca apenas os sites em que confia totalmente.

- **Lista Branca** - abre a Lista Branca.

Lista Branca do AntiPhishing

Pode ver toda a lista dos sites web que não estão a ser analisados pelos motores de antiphishing do BitDefender. Se deseja remover um site da Lista Branca de

forma a que seja notificado acerca de qualquer possibilidade de ameaça de phishing existente nesse site, clique no botão **Remover** ao pé do mesmo.

Pode adicionar sites à Lista Branca nos quais confia absolutamente, de forma a que eles não sejam mais analisados pelos motores antiphishing. Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

- **Reportar como Phishing** - informar ao laboratório do BitDefender que você considera o respectivo site como sendo utilizado para phishing. Ao reportar sites que estejam phished, você ajuda a proteger outras pessoas contra roubo de identidade.
- **Ajuda** - abre a documentação eletrônica.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

28. Integração aos programas de Mensagens Instantâneas

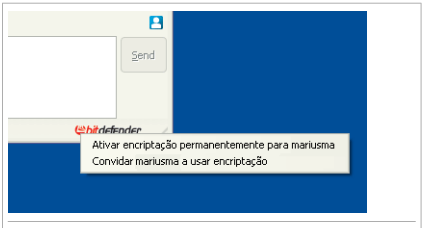
O BitDefender oferece uma função de proteção que permite cifrar os seus documentos confidenciais e as suas conversas através do Yahoo Messenger e MSN Messenger.

De forma padrão, BitDefender cifra todas as suas sessões de chat desde que:

- O seu parceiro de chat tenha instalada uma versão do BitDefender que suporte a cifragem MI e a mesma esteja habilitada para o programa de mensagens usado durante o chat.
- E o seu parceiro de chat esteja a usar quer o Yahoo Messenger ou o Windows Live (MSN) Messenger.

Importante
O BitDefender não irá criptografar uma conversa caso o outro participante utilize um aplicativo de chat baseado em web, como o Meebo, ou outro aplicativo de chat web que suporte o Yahoo Messenger ou MSN.

Pode configurar facilmente a cifragem das mensagens instantâneas usando a barra de ferramentas a partir da janela de chat. A barra de ferramentas deve estar localizada no canto inferior direito da janela de bate-papo. Procure o ícone do BitDefender para encontrá-lo.



Barra de Ferramentas do BitDefender

Nota
A barra de ferramentas indica que uma conversa está criptografada ao exibir uma pequena chave próximo ao logo do BitDefender.

Ao clicar na barra de ferramentas do BitDefender são fornecidas as seguintes opções:

- **Desabilita a criptografia permanentemente para esse `contato`.**
- **Convida o `contato` a utilizar criptografia.** Para criptografar suas conversas, o contato deve instalar e utilizar o BitDefender e utilizar um programa de Mensagens Instantâneas compatíveis.

Como proceder

29. Como Analisar Arquivos e Diretórios

A análise é fácil e flexível com o BitDefender. Há 4 maneiras de configurar o BitDefender para analisar arquivos e diretórios à procura de vírus e outros malware:

- Utilizando o Menu Contextual do Windows
- Utilizando Tarefas de Análise
- Utilizando a Análise Manual do BitDefender
- Utilizando a barra de atividade do analisador

Uma vez que você iniciar uma análise, o assistente de análise Antivírus irá aparecer e guiá-lo através do processo. Para informações detalhadas sobre esse assistente, por favor consulte a seção "*Assistente do analisador Antivírus*" (p. 51).

29.1. Utilizando o menu contextual do Windows

Esta é a maneira mais fácil e recomendada de analisar um arquivo ou diretório em seu computador. Clique com o botão direito do mouse sobre o objeto que você deseja analisar e selecione a opção **Analisar com o BitDefender** do menu. Siga o assistente de análise Antivírus para concluir a análise.

Situações típicas da maneira que você pode utilizar esse método de análise:

- Você suspeita que um arquivo específico ou diretório esteja infectado.
- Sempre que você faz download de arquivos da Internet e suspeita que podem ser perigosos.
- Analisar um compartilhamento de rede antes de copiar os arquivos para o computador.

29.2. Utilizando Tarefas de Análise

Se você quiser analisar o seu computador ou pastas específicas regularmente, você deve considerar a utilização de tarefas de análises. As tarefas de análise instruem o BitDefender sobre os locais a serem analisados, e quais opções de análise devem ser aplicadas. Além disso, você pode agendar eles para rodar regularmente ou em um horário específico.

Para analisar seu computador usando a tarefa de análise, você deve abrir a interface do BitDefender e executar a tarefa pretendida de análise. Dependendo do modo de visualização da interface do usuário, diferentes passos têm que ser executados para executar a tarefa de análise.

Executando a Tarefa de Análise em Modo Básico

No Modo Básico, você só pode executar uma varredura padrão de todo o computador clicando em **Analisar Agora**. Siga o assistente de análise Antivírus para concluir a análise.

Executando as Tarefas de Análise em Modo Intermediário

No Modo Intermediário, você pode executar uma série de tarefas de análises pré-configuradas. Você também pode configurar e executar tarefas personalizadas de análise para verificar locais específicos no seu computador utilizando opções personalizadas de análise. Siga esses passos pra executar uma tarefa de análise no Modo Intermediário:

1. Clique na aba **Antivírus**.
2. No lado esquerdo da área de Tarefas Rápidas, clique em **Análise do Sistema** para iniciar uma análise de todo o computador. Para executar uma análise diferente, clique na seta no botão e selecione a tarefa de análise desejada. Para configurar e executar tarefas personalizadas, clique em **Análise Customizada**. Essas são as tarefas de análise disponíveis:

Tarefa de Análise	Descrição
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração padrão, ele analisa todos os tipos de malware além de rootkits.
Análise Minuciosa	Analisa todo o sistema. Na configuração padrão, analisa em busca de todo tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Analisar o diretório Meus Documentos	Use esta tarefa para analisar pastas de usuários atuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.
Análise Pessoal	Esta opção lhe ajuda a configurar e a executar uma tarefa de análise personalizada para especificar o que analisar e as opções gerais de análise. Você pode salvar tarefas personalizadas de análise, assim você pode acessá-las mais tarde, no Modo Intermediário ou no Modo Avançado.

3. Siga o assistente de análise Antivírus para concluir a análise. Se você escolher executar uma tarefa de análise, você precisa completar o Assistente de Análise Personalizada.

Executando Tarefas de Análise no Modo Avançado

No Modo Avançado, você pode executar todas as tarefas pré-configuradas de análise, e também alterar as opções de análise. Além disso, você pode criar tarefas de análise personalizadas caso deseje analisar locais específicos em seu computador. Siga esses passos pra executar uma tarefa de análise no Modo Avançado:

1. Clique em **Antivírus** no menu do lado esquerdo.
2. Clique na aba **Análise Vírus Scan**. Aqui você pode encontrar um número de tarefas de análise padrão e criar suas próprias tarefas de análise. Estas são as tarefas padrão de análise que você pode utilizar:

Tarefa Padrão	Descrição
Análise Minuciosa	Analisa todo o sistema. Na configuração padrão, analisa em busca de todo tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração padrão, ele analisa todos os tipos de malware além de rootkits.
Análise Rápida do Sistema	Analisa os diretórios do `Windows` e dos `Arquivos de Programas`. Na configuração padrão, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.
Meus Documentos	Use esta tarefa para analisar pastas de usuários atuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

3. De um clique-duplo na tarefa de análise que você deseja executar.
4. Siga o assistente de análise Antivírus para concluir a análise.

29.3. Utilizando a Análise Manual do BitDefender

A análise Manual do BitDefender permite que você especifique o diretório ou a partição do disco rígido sem a necessidade de criar uma tarefa de análise. Essa característica foi designada para ser utilizada quando o Windows está sendo executado no Modo de Segurança. Se seu sistema está infectado com um vírus resistente, você pode tentar removê-lo iniciando o Windows em Modo de Segurança e analisar cada partição do disco utilizando a Análise Manual do BitDefender.

Para analisar seu computador usando a Análise Manual do BitDefender, siga esses passos:

1. No Menu Iniciar, 

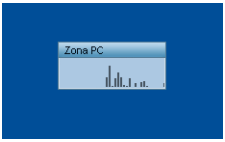
siga o caminho **Iniciar → Programas → BitDefender 2010 → Análise Manual BitDefender**. Uma nova janela irá aparecer.
2. Clique **Adicionar Pasta** para selecionar o alvo da análise. Uma nova janela irá aparecer.
3. Selecione o alvo da análise:
   - Para analisar sua Área de trabalho, selecione **Área de trabalho**.
   - Para analisar uma partição inteira do disco rígido, selecione-a a partir do Meu Computador.
   - Para analisar um diretório específico, procure e selecione o respectivo diretório.
4. Clique em **OK**.
5. Clique **Continuar** para iniciar a análise.
6. Siga o assistente de análise Antivírus para concluir a análise.

O que é Modo de Segurança?
O Modo de Segurança é um modo especial de iniciar o Windows, utilizado principalmente para resolver problemas afetando a operação normal do sistema. Esses problemas variam de conflitos em drivers até vírus que não permitem que o Windows inicie normalmente. No Modo de Segurança, o Windows carrega apenas o mínimo de componentes e drivers básicos do sistema operacional. Apenas poucos aplicativos trabalham no Modo de Segurança. É por essa razão que a maioria dos vírus estão inativos e podem ser facilmente removidos, quando utilizamos o Windows em Modo de Segurança.
Para iniciar o Windows no Modo de Segurança, reinicie seu computador e aperte a tecla F8 até aparecer o menu Opções Avançadas do Windows. Você pode escolher várias opções de inicialização no Modo de Segurança. Você pode desejar escolher a opção **Modo de Segurança com Rede** para poder acessar a internet.

Nota

Para mais informações sobre o Modo de Segurança, visite a página de Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**). Você também pode encontrar informações úteis ao pesquisar na internet.

29.4. Utilizando a Barra de Atividade da Análise



Barra de Atividade da Análise

A **Barra de atividade de verificação** é uma visualização gráfica da atividade de verificação em seu sistema. Esta pequena janela esta disponível por padrão apenas noModo Avançado.

Você pode utilizar a barra de atividade da Análise para rapidamente analisar arquivos e diretórios. Arraste e solte o arquivo ou diretório que você deseja que seja analisado, na Barra de Atividade da Análise. Siga o assistente de análise Antivírus para concluir a análise.

Nota

Para mais informações, por favor consulte a seção “*Barra de Atividade da Análise*” (p. 29).

30. Como Agendar uma Análise no Computador

Analisar o seu computador periodicamente é uma das melhores práticas para manter o computador livre de malware. O BitDefender permite que você agende tarefas de análise para que você possa analisar o seu computador automaticamente.

Para agendar o BitDefender para analisar o seu computador, siga esses passos:

1. Abra o BitDefender e troque a interface de usuário para Modo Avançado.
2. Clique em **Antivírus** no menu do lado esquerdo.
3. Clique na aba **Análise Vírus Scan**. Aqui você pode encontrar um número de tarefas de análise padrão e criar suas próprias tarefas de análise.
   - Tarefas de Sistema estão disponíveis e podem ser executados em cada conta de usuário do Windows.
   - As tarefas de usuário estão disponíveis e só podem ser executadas pelo usuário que as criou.

   Estas são as tarefas de análise padrão que você pode agendar:

Tarefa Padrão	Descrição
Análise Minuciosa	Analisa todo o sistema. Na configuração padrão, analisa em busca de todo tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração padrão, ele analisa todos os tipos de malware além de rootkits.
Análise Rápida do Sistema	Analisa os diretórios do `Windows` e dos `Arquivos de Programas`. Na configuração padrão, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.
Análise Autologon	Analisar os itens que são executados quando o usuário entra no Windows. Para utilizar esta função, você terá que agendá-la para ser executada na inicialização do sistema. Por default, a análise de autologon está desabilitada.
Meus Documentos	Use esta tarefa para analisar pastas de usuários atuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de

Tarefa Padrão	Descrição
	trabalho segura e aplicações limpas a serem executadas no arranque.

Se nenhuma dessas tarefas de análise suprirem as suas necessidades, você pode criar uma nova tarefa de análise, que pode ser agendada para ser executada conforme necessário.

4. Clique com o botão direito do mouse na tarefa de análise e selecione **Agendar**. Uma nova janela irá aparecer.
5. Agende a tarefa para ser executada conforme necessário:
   - Para executar a análise apenas uma vez, selecione **Uma vez** e especifique o dia e hora de início.
   - Para executar a tarefa de análise após a inicialização do sistema, selecione **Ao iniciar o sistema**. Você poderá especificar em quanto tempo, após o início, a tarefa deverá começar a rodar (em minutos).
   - Para executar a análise regularmente, selecione **Periodicamente** e especifique a frequência e a data e hora de início.

   Nota

   Por exemplo, para analisar o seu computador todos os Sábados às 2:00 horas, você deve configurar o agendamento da seguinte maneira:

   a. Selecione **Periodicamente**.

   b. No campo **A cada**, digite 1 e selecione **Semanas** do menu. Desta forma, a tarefa é executada uma vez por semana.

   c. Definir como início o próximo Sábado.

   d. Configurar como hora de início `2:00:00`.

6. Clique em **OK** para salvar o agendamento. A tarefa de análise será executada automaticamente, de acordo com o horário que você definiu. Se o computador é desligado quando o chega o horário agendado, a tarefa será executada na próxima vez que você iniciar seu computador.

Resolução de Problemas e Obtendo Ajuda

31. Resolução de Problemas

Este capítulo apresenta alguns problemas que podem ocorrer ao utilizar o BitDefender e fornece-lhe as soluções possíveis para estes problemas. A maioria destes problemas podem ser resolvidos através da configuração adequada das definições do produto.

Se você não encontrar o seu problema aqui, ou se as soluções apresentadas não o resolvem, você pode entrar em contato com o suporte técnico do BitDefender, conforme indicado no capítulo "*Suporte*" (p. 220).

31.1. Problemas na Instalação

Este artigo lhe ajudará a resolver os problemnas de instalação mais comuns com o BitDefeder. Estes problemas, podem ser agrupados nas seguintes categorias:

- Erros ao validar a instalação: o assistente de instalação não pode ser executado devido a condições específicas no seu sistema.
- As Instalações Falharam: você iniciou uma instalação a partir do assistente de instalação, mas ela não foi efetuada com sucesso.

31.1.1. Erros na Validação da Instalação

Quando você iniciar o assistente de instalação, um número de condições será verificado para validar se a instalação pode ser iniciada. A seguinte tabela apresenta os erros mais comuns de validação de instalação e soluções para superá-los.

Erro	Descrição&Solução
Você não tem privilégios suficientes para instalar o programa.	Para poder executar o assistente de instalação e instalar o BitDefender, você precisa privilégios de administrador. Faça uma das seguintes: ● Entre numa conta de administrador do Windows e execute o assistente de instalação novamente. ● Clique com o botão-direito no arquivo de instalação e selecione **Executar como**. Digite o nome de usuário e senha de uma conta de administrador do Windows no sistema.
O instalador detectou uma versão anterior do BitDefender que não foi instalada adequadamente.	O BitDefender foi instalado anteriormente no seu sistema, mas a instalação não foi removida completamente. Estas condições bloqueiam uma nova instalação do BitDefender.

Erro	Descrição&Solução
	Para superar este erro e instalar o BitDefender, siga estes passos: 1. Vá parawww.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador. 2. Execute a ferramenta de desinstalação usando privilégios de administrador. 3. Reinicie seu computador. 4. Inicie o assistente de instalação novamente para instalar o BitDefender.
O produto da BitDefender não é compatível com seu sistema operacional.	Você está tentando instalar um produto da BitDefender num sistema operacional incompatível. Por favor verifique o *"Requisitos de Sistema"* (p. 2) para descobrir os sistemas operacionais onde você pode instalar o BitDefender. Se seu sistema operacional é o Windows XP Service Pack 1, ou sem nenhum Service Pack, você pode instalar o Service Pack 2, ou superior e então executar o assistente de instalação novamente.
O arquivo de instalação foi desenhado para um tipo diferente de processador.	Se você teve um erro como este, você está tentando riodar uma versão incorreta do arquivo de instalação. Há duas instalações do arquivo de instalação do BitDefender: uma para processadores de 32 bit e outra para processadores de 64 bit. Para ter certeza que você tem a versão correta para seu sistema, baixe o arquivo de instalação diretamente do www.bitdefender.com.

31.1.2. A Instalação Falhou

Há várias possibilidade de falhas de instalação:

- Durante a instalação, uma tela de erros aparece. Você poderá ser solicitado a cancelar a instalação, ou um botão poderá ser oferecido para executar uma ferramenta de desinstalação que limpará o sistema.

Nota

Imediatemante após você iniciar a instalação, você poderá ser notificado que não há espaço livre suficiente no disco para instalar o BitDefender. Neste caso, libere a quantidade necessária de espaço no disco na partição onde você quer instalar o BitDefender e então resuma ou reinicie a instalação.

- A instalação trava para e, possivelmente, o sistema para, Apenas uma reinicialização do sistema restaura sua operação.
- A instalação foi concluída, mas você não pode utilizar algumas ou todas as funções do BitDefender.

Para solucionar uma falha na instalação e instalar o BitDefender, siga estes passos:

1. **Limpe o sistema após a instalação que falhou.** Se a instalação falhar, algumas chaves e arquivos de registro do BitDefender poderão permanecer em seu sistema. Estes arquivos remanescente poderão evitar uma nova instalação do BitDefender. Elas também podem afetar o desempenho do sistema e sua estabilidade. É por isto que você precisa removê-los antes de tentar instalar o produto novamente.

   Se a tela de erro fornece um botão para executar uma ferramenta de desinstalação, clique nesse botão para limpar o sistema. Caso contrário, proceda do seguinte modo:

   a. Vá parawww.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.

   b. Execute a ferramenta de desinstalação usando privilégios de administrador.

   c. Reinicie seu computador.

2. **Verifique possíveis causas do motivo que a instalação falhou.** Antes de preceder para reinstalar o produto, verifique e remova possíveis condições que podem ter causado a falha na instalação:

   a. Verifique se você tem alguma outra solução de segurança instalada, pois ela poderão afetar o funcionamento do BitDefender. Se este for o caso, recomendamos que você remova todas as outras soluções de segurança e então reinstale o BitDefender.

   b. Você também deve verificar se o seu sistema está infectado. Faça uma das seguintes:

      - Use o CD de Recuperação do BitDefender para analisar seu computador e remover qualquer ameaça existente. Para mais informações, por favor vá para “CD de Resgate BitDefender” (p. 223).
      - Abra uma janela no Internet Explorer e vá para www.bitdefender.com e execute uma análise online (clique no **botão** análise online).

3. Tente novamente para instalar o BitDefender. Recomendamos que você baixe e execute a última versão do arquivo de instalação a partir de www.bitdefender.com.
4. Se a instalação falhar novamente, contate a BitDefender para suporte, como descrito em “*Suporte*” (p. 220).

31.2. Os Serviços da BitDefender não estão respondendo

Este artigo ajuda você a solucionar o erro *Os Serviços do BitDefender não estão respondendo*. Você pode encontrar esse erro da seguinte forma:

- O ícone do BitDefender no área de notificação está cinza e uma janela popup informa que os serviços da BitDefender não estão respondendo.
- A janela do BitDefender mostra que os serviços do BitDefender não estão respondendo.

O erro pode ser causado por uma das seguintes condições:

- Uma importante atualização está sendo instalada.
- Erro temporário de comunicação entre os serviços do BitDefender.
- Alguns dos serviços do BitDefender estão parados.
- outras soluções de segurança sendo executadas em seu computador ao mesmo tempo com o BitDefender.
- vírus no seu sistema afetam o funcionamento normal do BitDefender.

Para solucionar este erro, tente estas soluções:

1. Espere um pouco e veja se alguma coisa muda. O erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até que o BitDefender seja carregado. Abra o BitDefender para ver se o erro persiste. Reiniciar o computador normalmente resolve o problema.
3. Verifique se você tem alguma outra solução de segurança instalada, pois ela poderão afetar o funcionamento do BitDefender. Se este for o caso, recomendamos que você remova todas as outras soluções de segurança e então reinstale o BitDefender.
4. Se o erro persistir, poderá ser um problema mais sério (por exemplo, você pode estar infectado com um vírus que pode interferir com o BitDefender). Favor entrar em contato com BitDefender para suporte, como descrito na seção "*Suporte*" (p. 220).

31.3. A Remoção do BitDefender Falhou

Este artigo ajuda a solucionar erros que poderão ocorrer ao remover o BitDefender. Há duas situações possíveis:

- Durante a remoção, uma tela de erros aparece. Uma tela fornece um botão para executar uma ferramenta de desinstalação que limpará o sistema.
- A remoção trava e, possivelmente, seu sistema congela. Clique **Cancelar** para abortar a remoção. Se não funcionar, reinicie o sistema.

Se a remoção falhar, algumas chaves do registro e arquivos do BitDefender poderão permanecer em seu sistema. Estes arquivos remanescentes poderão evitar uma nova instalação do BitDefender. Elas também podem afetar o desempenho do sistema e sua estabilidade. Para remover completamente o BitDefender de seu sistema, você precisa executar a ferramenta de desinstalação.

Se a remoção falhar com um erro na tela, clique no botão para executar a ferramenta de desinstalação para limpar o sistema. Caso contrário, proceda do seguinte modo:

1. Vá parawww.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.
2. Execute a ferramenta de desinstalação usando privilégios de administrador. A Ferramenta de Desinstalação removerá todos os arquivos e chaves de registo que não tenham sido removidos durante o processo de desinstalação automática.
3. Reinicie seu computador.

Se esta informação não foi útil, você pode contatar a BitDefender para suporte, como descrito na seção "*Suporte*" (p. 220).

32. Suporte

Como um fornecedor valioso, o BitDefender se esforça para fornecer aos clientes um nível inigualável de suporte rápido e preciso. A Base de Conhecimento do BitDefender fornece artigos que contém as soluções para a maioria dos seus problemas e questões relacionadas ao BitDefender. Se você não encontrar a solução na Base de Conhecimento, você pode entrar em contato com o Atendimento ao Cliente do BitDefender. Os representantes do suporte irão responder suas perguntas em tempo hábil e prestar toda a assistência que necessitar.

32.1. BitDefender Knowledge Base

O BitDefender Knowledge Base é um repositório on-line de informação sobre os produtos BitDefender. Ele armazena em formato facilitado relatórios sobre resultados de problemas técnicos e questionamentos sendo analisados pela equipe de suporte e desenvolvimento BitDefender, com artigos de informações gerais sobre prevenção de vírus, gerenciamento das soluções e explicações detalhadas.

O BitDefender Knowledge Base é aberto ao público e gratuito. Este rico meio de informação é outra forma de providenciar aos clientes BitDefender conhecimento técnico e visão necessária. Todas as requisições sobre problemas encontrados por clientes BitDefender eventualmente acabam chagando ao BitDefender Knowledge Base, como relatórios de bugfix e arquivos de ajuda.

O BitDefender Knowledge Base está disponível em http://kb.bitdefender.com.

32.2. Pedir Ajuda

A fim de pedir ajuda, você deve usar o sistema web BitDefender Self-Service. Basta seguir estes passos:

1. Vá em http://www.bitdefender.com/help. Aqui você pode encontrar a Base de Conhecimento do BitDefender. A Base de Conhecimento do BitDefender armazena inúmeros artigos que contém soluções para as questões relacionadas ao BitDefender.
2. Pesquise a Base de Conhecimento do BitDefender Knowledge para artigos que podem fornecer uma solução para o problema.
3. Por favor, leia o artigo relevante e tente executar a solução proposta.
4. Se esta solução não resolver o seu problema, use o link no artigo para entrar em contato com o Atendimento ao Cliente do BitDefender.
5. Entrar na sua conta BitDefender
6. Entre em contato com os representantes do suporte do BitDefender, por e-mail, chat ou telefone.

32.3. Informação sobre contato

Comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

32.3.1. Endereços Web

Departamento de Vendas: vendas@bitdefender.com.br
Suporte Técnico: www.bitdefender.com/help
Documentação: documentation@bitdefender.com
Programa de Parcerias: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Relações Públicas: pr@bitdefender.com
Oportunidades de Emprego: jobs@bitdefender.com
Envio de Vírus: virus_submission@bitdefender.com
Envio de Spam: spam_submission@bitdefender.com
Relato de Abuso: abuse@bitdefender.com
Página Web de Produtos: http://www.bitdefender.com/links/br/homepage.html
Arquivos de Produtos FTP: ftp://ftp.bitdefender.com/pub
Distribuidores Locais: http://www.bitdefender.com/site/Partnership/list/
BitDefender Knowledge Base: http://kb.bitdefender.com

32.3.2. Escritórios do BitDefender

Os escritórios BitDefender estão prontos a responder quaisquer dúvidas na respectiva área de operação, comercialmente e assuntos gerais. Seus endereços respectivos estão listados abaixo.

E.U.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefone (escritório&vendas): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/help
Página da Web http://www.bitdefender.com

Alemanha

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2

59439 Holzwickede
Deutschland
Escritório: +49 2301 91 84 222
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://kb.bitdefender.de
Página da Web http://www.bitdefender.de

UK e Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-mail: info@bitdefender.co.uk
Telefone +44 (0) 8451-305096
Vendas: sales@bitdefender.co.uk
Suporte Técnico: http://www.bitdefender.com/help
Página da Web http://www.bitdefender.co.uk

Espanha

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefone +34 902190765
Vendas: comercial@bitdefender.es
Suporte Técnico: www.bitdefender.es/ayuda
Website: http://www.bitdefender.es

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefone de Vendas: +40 21 2063470
E-mail de vendas: sales@bitdefender.ro
Suporte Técnico: http://kb.bitdefender.ro
Website: http://www.bitdefender.ro

CD de Resgate BitDefender

33. Sumário

O BitDefender Antivírus 2010 vem com um CD de inicialização (CD de Resgate BitDefender), o qual pode ser utilizado para analisar e desinfectar todo o sistema antes do sistema operacional iniciar.

Você deve usar o CD de Resgate BitDefender a qualquer momento que o seu sistema operacional não estiver funcionando corretamente por infecção de vírus. Isto normalmente acontece quando você não usa um produto antivírus.

A atualização das vacinas de vírus é feita automaticamente, sem a intervenção do usuário quando você executa o CD de Resgate BitDefender.

O CD de Emergência BitDefender é uma distribuição do Knoppix recompilada por BitDefender, que integra a mais recente solução BitDefender de segurança para Linux dentro do CD ao Vivo GNU/Linux Knoppix, que lhe oferece uma proteção instantânea de antivírus que é capaz de analisar e desinfectar discos rígidos existentes (incluindo partições Windows NTFS). Ao mesmo tempo, o CD de Restauração do BitDefender pode ser usado para recuperar a sua preciosa informação quando você não consegue iniciar o Windows.

Nota

O CD de Emergência BitDefender pode ser descarregado a partir deste local na net: http://download.bitdefender.com/rescue_cd/

33.1. Requisitos de Sistema

Antes de iniciar o CD de Restauração do BitDefender, você deve, em primeiro, lugar verificar se o seu sistema possui os seguintes requisitos.

Processador

Compatível com x86, mínimo de 166 MHz. Um processador de geração i686, de 800MHz, seria uma melhor escolha mínima.

Memória

512 MB de memória RAM (1 GB recomendado)

CD-ROM

O CD de Restauração do BitDefender, é executado a partir do CD-ROM, portanto um CD-ROM e uma BIOS capaz de iniciar a partir do mesmo são necessários.

Conexão a Internet

Embora o CD de Restauração do BitDefender, possa ser executado sem conexão com a Internet, os processos de atualização requerem um link HTTP ativo, mesmo que seja através de um servidor proxy. Portanto, para ter uma proteção atualizada, a conexão com a Internet é PRIMORDIAL.

Resolução gráfica

Placa gráfica Standard SVGA compatível.

33.2. Software incluído

O CD de Resgate BitDefender inclui os seguintes pacotes de programas.

Xedit
Este é um arquivo de um editor de texto.

Vim
Este é um poderoso arquivo de um editor de texto, contendo uma sintaxe highlighting, uma GUI e muito mais. Para mais informação consulte a página web da Vim.

Xcalc
Este é uma calculadora.

RoxFiler
RoxFiler é um rápido e poderoso gestor de arquivos gráficos.

Para mais informação, consultar a página internet da RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) um gestor de arquivos em modo de texto.

Para mais informação, consultar apágina internet da MC.

Pstree
Pstree mostra processos que estão a decorrer.

Top
Top mostra as tarefas do Linux.

Xkill
Xkill mata um cliente com os seus recursos X.

Partition Image
Partition Image ajuda-o a guardar partições em arquivos de sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 para um arquivos de imagem. Este programa pode ser útil para propósitos de backup.

Para mais informação, consulte a página web da Partimage.

GtkRecover
GtkRecover é uma versão da GTK da recuperação do prgrama de consola. Ajuda-o a recuperar um arquivo.

Para mais informação, consulte a página web da GtkRecover.

ChkRootKit
ChkRootKit é uma ferramenta que o ajuda a analisar o seu computador em busca de rootkits.

Para mais informação, consulte a página web do ChkRootKit.

Nessus Network Scanner

Nessus um analisador remoto de segurança para Linux, Solaris, FreeBSD, e Mac OS X.

Para mais informação, consulte a página web do Nessus.

Iptraf

Iptraf é um Software de Monitorização de Rede por IP.

Para mais informação, consulte a página web do Iptraf.

Iftop

Iftop mostra num interface o grau de utilização de banda.

Para mais informação, consulte a página web do Iftop.

MTR

MTR é uma ferramenta de diagnóstico de rede.

Para mais informação, consulte a página web da MTR.

PPPStatus

PPPStatus mostra as estatísticas acerca do tráfego TCP/IP de entrada e saída.

Para mais informação, consulte a página web da PPPStatus.

Wavemon

Wavemon é um aplicativo de monitoramento para dispositivos de redes wireless.

Para mais informação, consulte a página web da Wavemon.

USBView

USBView mostra informação acerca de dispositivos ligados ao USB bus.

Para mais informação, consulte a página web da USBView.

Pppconfig

Pppconfig ajuda-o a definir automaticamente uma conexão por dial up ppp.

DSL/PPPoe

DSL/PPPoe configura uma conexão PPPoE (ADSL).

I810rotate

I810rotate toggles o video output em i810 hardware usando o i810switch(1).

Para mais informação, consulte a página internet da I810rotate.

Mutt

Mutt é um poderoso cliente de e-mail MIME baseado em texto.

Para mais informação, consulte a página internet da Mutt.

Mozilla Firefox

Mozilla Firefox é um browser de internet bastante conhecido.

Para mais informação, consulte a página internet da Mozilla Firefox.

Elinks

Elinks um browser de internet em modo de texto.

Para mais informação, consulte a página internet da Elinks.

34. Como Usar o CD de Emergência BitDefender

Este capítulo comtém informação sobre como começar e parar o CD de Emergência BitDefender, analisar o seu computador em busca de malware como também guardar dados do seu comprometido PC Windows para um dispositivo amovível. No entanto ao usar as aplicações que vem com o CD, pode fazer muita tarefas cuja descripção vai muito para além deste manual de usuário.

34.1. Iniciar CD de Resgate BitDefender

Para iniciar o CD, configure a BIOS do seu computador para iniciar diretamente do CD, coloque o CD no drive e reinicie o computador. Tenha certeza que o seu computador pode iniciar do CD.

Espere até a próxima tela aparecer e siga as instruções na tela para iniciar o CD de Resgate BitDefender.

Boot Splash Screen

Ao iniciar o computador, a atualização das vacinas dos vírus é feita automaticamente. Essa tarefa pode demorar um pouco.

Quando o processo finalizar você verá o próximo desktop. Você pode agora usar o CD de Resgate BitDefender.

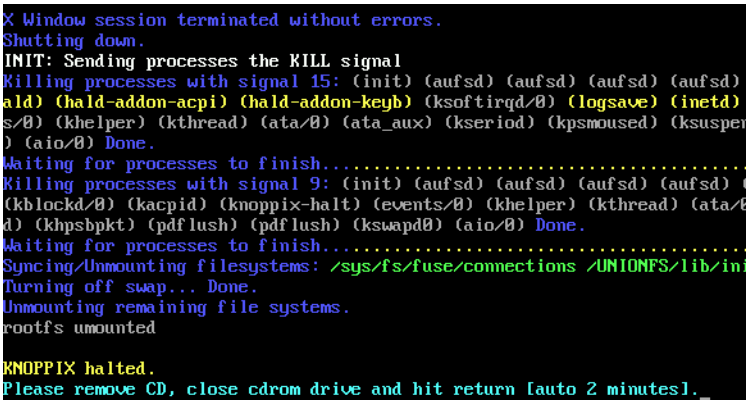
O Desktop

34.2. Parar o CD de Resgate BitDefender

Pode desligar em segurança o seu computador ao seleccionar **Sair** a partir do menu do CD de Emergência BitDefender (clique botão-direito para o abrir) ou ao emitir o comando **halt** num terminal.

Escolha "EXIT"

Quando o CD de Restauracào do BitDefender fechar com sucesso todos os programas, mostrará uma tela como a seguinte imagem. Você pode remover o CD de forma a iniciar a partir do seu disco rígido. Agora é OK desligar o seu computador ou reiniciá-lo.



Espere por esta mensagem enquanto estiver a desligar

34.3. Como executo uma verificação antivírus?

Um assistente aparecerá quando o processo de arranque terminar e permite-lhe analisar totalmente o seu computador. Tudo o que tem de fazer é clicar no botão **Iniciar** .

Nota
Se a resolução da sua tela não for suficiente, será solicitado que você inicie a análise em modo de texto.

Siga o processo guiado de três passos para completar o processo de análise.

1. Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

   Nota
   O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

2. Pode ver o número de incidências que afectam o seu sistema.

   As incidências são mostradas em grupos. Clique na caixa com "+" para abrir um grupo ou na caixa com "-" para fechar um grupo.

   Pode escolher uma ação geral a ser tomada para cada grupo de incidências ou pode selecionar separar as ações para cada incidência.
3. Pode ver o sumário dos resultados.

Se você deseja analisar apenas um diretório, você pode usar uma das seguintes alternativas:

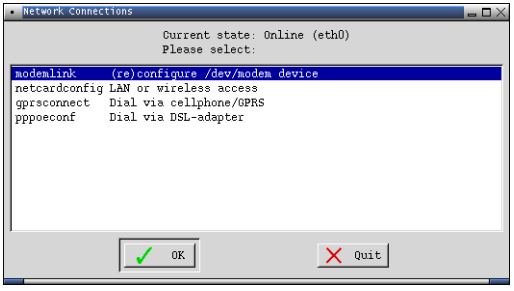
- Utilize o **Analisador BitDefender para Unices**.
  1. Dê um duplo clique no ícone INICIAR ANÁLISE na área de trabalho. Isto irá iniciar o **Analisador BitDefender para Unices**.
  2. Clique em **Analisador**, uma nova janela irá aparecer.
  3. Selecione o diretório que você deseja analisar e clique em **Abrir** para iniciar a análise usando o mesmo assistente que apareceu quando você reiniciou o computador pela primeira vez.
- Navegue pelas pastas, clique com o botão direito em um arquivo ou pasta e selecione **Enviar para**. Então escolha **Analisador do BitDefender**.
- Ou você pode digitar o próximo comando no terminal. O **BitDefender Antivirus Scanner** irá começar pelo arquivo ou pasta selecionada como local padrão de verificação.

```
# bdscan /path/to/scan/
```

34.4. Como posso configurar a conexão à Internet?

Se você estiver em uma rede DHCP e você tiver uma placa de rede ethernet, uma conexão de Internet já deveria estar detectada e configurada. Para uma configuração manual, siga os próximos passos.

1. Duplo Clique sobre o atalho das Ligações de Rede no Ambiente de Trabalho. A seguinte janela irá aparecer:



Ligações de Rede

2. Selecione o tipo de conexão que você está usando e clique em OK.

Conexão	Descrição
modemlink	Selecione este tipo de conexão quando você estiver usando um modem e uma linha telefônica para acessar a Internet.
netcardconfig	Selecione este tipo de conexão quando você estiver usando uma rede de área local (LAN) para acessar a Internet. É também utilizada para conexões sem fio.
gprsconnect	Selecione este tipo de conexão quando você está usando a internet em uma rede de telefone móvel usando o protocolo GPRS (General Packet Radio Service). Você também pode usar um modem GPRS em vez de um telefone móvel.
pppoeconf	Selecione este tipo de conexão quando estiver uando um modem DSL (Digital Subscriber Line) para acessar a Internet.

3. Siga as instruções na tela. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.

Importante

Tenha em mente que apenas ativou o modem ao selecionar as opções acima mencionadas. Para configurar a conexão da rede siga estes passos.

1. Clique botão direito do mouse sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
2. Selecione **Terminal (como raiz)**.
3. Insira os seguintes comandos:

```
# pppconfig
```

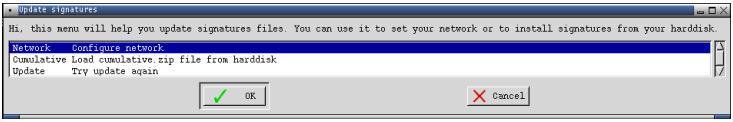
4. Siga as instruções na tela. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.

34.5. Como eu posso atualizar o BitDefender?

No momento de inicialização, a atualização de assinaturas de vírus é feita automaticamente. No entanto, se você pulou esta etapa, ou simplesmente deseja atualizar após inicializar o computador, existem duas maneiras de atualizar o BitDefender.

- Utilize o **Analisador BitDefender para Unices**.
  1. Dê um duplo clique no ícone INICIAR ANÁLISE na área de trabalho. Isto irá iniciar o **Analisador BitDefender para Unices**.
  2. Clique em **Atualizar**.

- Utilize o atalho **Atualizar assinaturas** na área de trabalho.
  1. De um clique duplo no atalho da Atualização das Vacinas na Área de Trabalho. A seguinte janela irá aparecer.



Atualização das Vacinas

  2. Faça uma das coisas seguintes:
     - Selecione **Cumulativa** para instalar as vacinas já salvas no seu disco rigido, navegando em seu computador e localizando o arquivo `cumulative.zip`.
     - Selecione **Atualização** para conectar-se imediatamente à internet e baixar as últimas vacinas de vírus.
  3. Clique em **OK**.

34.5.1. Como posso atualizar o BitDefender através de um proxy?

Se existe um servidor proxy entre o seu computador e a internet, algumas configurações têm de ser feitas para poder atualizar a assinatura de vírus.

Para atualizar o BitDefender sobre um proxy, utilize uma das seguintes opções:

- Utilize o **Analisador BitDefender para Unices**.
  1. Dê um duplo clique no ícone INICIAR ANÁLISE na área de trabalho. Isto irá iniciar o **Analisador BitDefender para Unices**.
  2. Clique em **Configurações**, uma nova janela irá aparecer.
  3. Sobre **Configurações de Atualização**, selecione a caixa de seleção **habilitar o Proxy HTTP**. Especifique o host do proxy, a ser especificado como: `host[:port]`), usuário do Proxy, a ser especificado como: `[domain\]usuário`) e senha. Selecione a caixa de seleção **ignorar o servidor proxy quando não estiver disponível** para uma conexão direta a ser utilizada quando o servidor proxy não estiver disponível.
  4. Clique em **Salvar**.
  5. Clique em **Atualizar**.

- Utilizar Terminal (como administrador).
  1. Clique botão direito do mouse sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
  2. Selecione **Terminal (como raiz)**.
  3. Digite o comando: **cd /ramdisk/BitDefender-scanner/etc**.
  4. Digite o comando: **mcedit bdscan.conf** para editar este arquivo usando o GNU Midnight Commander (mc).

5. Uncomment a seguinte linha: `#HttpProxy =` (apenas apague o sinal #) e especifique o domínio, nome, senha e a porta do servidor proxy. Por exemplo, a linha respectiva deverá parecer-se com o seguinte:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```

6. Prima **F2** para guardar o arquivo atual, confirme o guardar, e depois prima **F10** para o fechar.
7. Digite o comando: **bdscan update**.

34.6. Como posso salvar os meus dados?

Vamos assumir que você não consegue iniciar o seu Windows PC devido a incidências desconhecidas. Ao mesmo tempo, você necessita desesperadamente acessar alguma informação importante do seu computador. Eis aqui uma situação em que o CD de Recuperação do BitDefender se revela extremamente útil.

Para guardar os seus dados do computador para um dispositivo amovível, tal como um stick de memória USB, siga os seguintes passos:

1. Coloque o CD de Emergência BitDefender na drive de CDs, e o stick de memória na entrada USB e depois reinicie o computador.

   Nota

   Se conectar o stick de memória mais tarde, tem de montar o dispositivo amovível seguindo os seguintes passos:

   a. Faça duplo-clique com o rato sobre o atalho do Terminal Emulator no Ambiente de Trabalho.
   b. Insira o seguinte comando:

      ```
      # mount  /media/sdb1
      ```

      Lembre-se que dependendo da configuração do seu computador poderá ser `sda1` em vez de `sdb1`.

2. Espere que o CD de Restauração do BitDefender termine a inicializãção. A seguinte janela irá aparecer.

Tela da Área de Trabalho

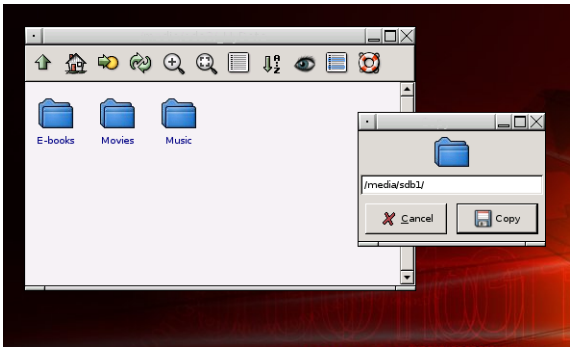
3. Faça duplo clique sobre a partição onde os dados que deseja salvar se encontram (ex. `[sda3]`).

   Nota
   Quando está a trabalhar com o CD de Emergência BitDefender, estará a lidar com nomes de partições baseado em Linux. Assim, `[sda1]` provavelmente corresponderá à partição Windows `(C:)`, `[sda3]` a `(F:)`, e `[sdb1]` ao stick de memória.

   Importante
   Se o computador não for desligado correctamente, é possível que certas partições não sejam montadas automaticamente. Para montar uma partição siga estes passos.
   a. Faça duplo-clique com o rato sobre o atalho do Terminal Emulator no Ambiente de Trabalho.
   b. Insira o seguinte comando:

   ```
   # mount  /media/partition_name
   ```

4. Explore as suas pastas e abra a directoria que deseja. Por exemplo, `Meus Dados` que contém as sub-directorias `Filmes`, `Música` e `E-books` .
5. Clique botão direito do mouse sobre o diretorio desejado e selecione **Copiar**. A seguinte janela irá aparecer:



Guardar Dados

6. Insira `/media/sdb1/` na correspondente caixa de texto e clique em **Copiar**.

   Lembre-se que dependendo da configuração do seu computador poderá ser `sda1` em vez de `sdb1`.

34.7. Como faço para usar o modo console?

Se a sua resolução de tela não é alta o suficiente para executar a interface gráfica do usuário, você pode executar o BitDefender Rescue CD no modo de console. O modo de texto simples permite que você execute uma varredura completa no seu computador.

Para executar o CD no modo de console, configure a BIOS do seu computador para inicializar o CD, coloque o CD no drive e reinicie o computador. Espere até a tela de inicialização aparecer e selecione **Iniciar o knoppix em modo console**.

Após iniciar, siga as instruções na tela para executar uma varredura completa do seu computador.

O BitDefender detecta as partições do disco rígido e atualiza automaticamente o banco de dados de assinaturas de malware antes da análise começar. Se algum arquivo infectado for encontrado, o BitDefender irá desinfectá-lo. Após o processo de análise ser concluído, o log de análise é exibido.

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Glossário

ActiveX

ActiveX é um modelo para escrever programas para que outros programas e seus sistemas operacionais possam buscá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para fazer páginas da Web interativas que se parecem e se comportam como programas de computador, melhor que páginas estáticas. Com o ActiveX, usuários podem perguntar ou responder questões, apertar botões e interagir de outras formas com a página. Controles ActiveX são também escritos usando Visual Basic.

O ActiveX é notável para uma completa falta de controles de segurança; especialistas em segurança de computador desencorajam seu uso pela Internet.

Adware

O Adware é sempre combinado com um programa host sem custo enquanto o usuário concordar em aceitar o adware. Não existem implicações neste tipo de instalação, pois o usuário concordou com o propósito do aplicativo.

No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar a performance do seu sistema. Além disto, a informação que alguns destes programas coleta pode causar problemas de privacidade para usuários que não estão totalmente cientes do funcionamento do programa.

Arquivo

Um disco, fita ou diretório que contém arquivos que podem ter sido gravados como backup.

Um arquivo que contém um ou mais arquivos em formato comprimido.

Backdoor

Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores os mantenedores. A motivação para tais furos não pe sempre sinistra, alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso em campo para serviço dos técnicos ou programa de manutenção dos programadores do fabricante.

Setor de boot

O setor de boot é um setor no começo de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para inicializar os discos, o setor de boot também um programa que carrega o sistema operacional.

Vírus de boot

Um vírus que infecta o setor de boot do disco rígido ou de um disquete. Uma tentativa de inicialização com um disquete infectado com vírus de boot fará

com que o vírus se torne ativo na memória. Toda vez que você reiniciar seu sistema daquele ponto em diante, você terá um vírus ativo na memória.

Navegador

Termo simplificado para navegador da web, um programa utilizado para localizar e exibir páginas da Internet. Os dois mais populares são Netscape Navigator e Microsoft Internet Explorer. Ambos são navegadores gráficos o que significa que podem exibir tanto gráficos como texto. Em adição, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, através de plugins para alguns formatos.

Linha de comando

Na interface de linha de comando, os usuários digitam os comando em um espaço fornecido diretamente na tela usando comandos da linguagem.

Cookie

Dentro da indústria da Internet, os cookies são descritos como pequenos arquivos de texto que contém informações sobre computadores individuais que podem ser analisados e usados pelos anunciantes para rastrear gostos e interesses on-line. Nesse reino, a tecnologia de cookies está sendo desenvolvida ainda e a intenção é direcionar os anúncios diretamente aos seus interesses. É uma espada de dois gumes para muitos porque por um lado é eficiente e pertinente porque só vê anúncios que interessam a você. E por outro lado, envolve “rastrear” e “seguir” a onde você vai e onde está clicando. Compreensível assim, existe um debate sobre a privacidade e muitas pessoas que se sentem ofendidas pelo fato de serem observados com um número SKU (você sabe, o código de barras na parte traseira dos pacotes que são lidos na saída do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é exato.

Unidade de disco

É uma máquina que lê e escreve dados em um disco.

Uma unidade de disco rígido lê e escreve em um disco rígido.

Uma unidade de disquete acessa disquetes.

Os discos rígidos podem ser internos (armazenado dentro do computador) ou externos (armazenado em uma caixa separada que está conectada ao computador).

Download

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um periférico. O termo é muitas vezes usado para descrever o processo de copiar um arquivo de um serviço on-line para seu próprio computador. Download também pode se referir a copiar um arquivo de um servidor de rede para um computador na rede.

E-mail
Correio eletrônico. Um serviço que envia mensagens para computadores em redes locais ou mundiais.

Eventos
Uma ação ou ocorrência detectada por um programa. Eventos podem ser ações de usuários, tais como clicar com botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como sem memória.

Falso positivo
Ocorre quando a verificação identifica um arquivo infectado quando de fato não está.

Extensão do arquivo
É a parte do arquivo, após o ponto final, indica o tipo de dados que estão armazenados no arquivo.

Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles são usualmente de uma a três letras e / ou números (alguns sistemas operacionais antigos não suportam mais que três). Exemplos: "c" para códigos em C, "ps" para PostScript, "txt" para texto.

Heurística
Um método baseado em regras para identificar novos vírus. Esse método de verificação não se baseia em definições de vírus específicas. A vantagem da verificação heurística é que ela não é enganada por uma nova variante do vírus. Entretanto. Entretanto ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo".

IP
Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, e fragmentação e montagem dos pacotes IP.

Java applet
Um programa em Java que é projetado para ser executado somente em uma página web. Para usar um aplicativo em uma página web, você deve especificar o nome do aplicativo e o tamanho (comprimento e largura em pixels) que o aplicativo pode utilizar. Quando a página da web é acessada, o navegador descarrega-a de um servidor e executa na máquina do usuário (o cliente). Os aplicativos diferem dos programas em que eles são comandados por um protocolo estrito de segurança.

Por exemplo, mesmo um aplicativo funcione em um cliente, eles não podem ler ou escrever dados na máquina do cliente. Adicionalmente, os aplicativos são mais restringidos de modo que só podem ler e escrever dados nos domínios aos quais servem.

Vírus de macro

Um tipo de vírus de computador que é codificado como uma macro dentro de um documento. Muitas aplicações, como Microsoft Word e Excel, suportam poderosa linguagem de macro.

Essas aplicações permitem a você colocar uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto.

Cliente de e-mail

É um aplicativo que lhe permite enviar e receber e-mails.

Memória

São áreas internas de armazenamento do computador. O termo memória identifica o armazenamento de dados que vem em forma de chips. Todo computador vem com uma certa quantidade de memória física, geralmente referida com memória RAM.

Não heurística

Esse método de verificação confia em definições de vírus específicas. A vantagem da verificação não heurística é que ela não pode ser enganada por algo pode parecer um vírus, e não gera falsos alarmes.

Programas comprimidos

Um arquivo em formato comprimido. Muitos sistemas operacionais e aplicativo contêm comandos que permitem a você comprimir um arquivo de modo que ocupe menos memória. Por exemplo: suponha que você tenha um texto que contém dez caracteres de espaço consecutivos. Normalmente, isso requereria dez bytes de armazenamento.

Entretanto, um programa que compacta arquivos substituiria os caracteres de espaço por caractere especial série-espaço seguido do número de espaços que estão sendo substituídos. Esta é apenas uma técnica de compactação, existem muitas outras.

Caminho

As direções exatas de um arquivo em um computador. Estas direções são descritos geralmente por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre dois pontos quaisquer, com os canais de comunicação entre dois computadores.

Phishing

O ato de enviar e-mail a um usuário declarando falsamente ser uma empresa legítima em uma tentativa de enganar o usuário a entregar informações que serão usadas para roubo de identidade. O e-mail direciona o usuário a uma página web onde é perguntado a fornecer informação pessoal, tais como senhas, cartão de crédito, cadastros e contas em bancos, que a empresa legítima em

questão já possui. A página web, no entanto, é falsa e existe apenas para roubar informação do usuário.

Vírus polimórfico

Um vírus que muda sua forma cada vez que um arquivo é infectado. Como não têm nenhum padrão binário consistente, tais vírus são duros de identificar.

Porta

Uma interface no computador na qual você pode conectar um dispositivo. Computadores pessoais possuem vários tipos de portas. Internamente, existem vários tipos de portas conectando unidades de disco, monitores e teclados. Externamente, os computadores pessoais possuem portas conectando modems, impressoras, mouse e outros dispositivos periféricos.

Em redes TCP/IP e UDP, um ponto final a uma conexão lógica. A número da porta identifica que tipo de porta é. Por exemplo, porta 80 é usada para tráfego HTTP.

Arquivo de relatório

Um arquivo que lista as ações que ocorreram. Por exemplo BitDefender mantém um arquivo de relatório com uma lista dos caminhos verificados, as pastas, o número de arquivos e arquivos comprimidos verificados, quantos arquivos infectados e suspeitos foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, arquivos, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam arquivos críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar arquivos e relatórios e evitarem ser detectados.

Script

Outro termo para um arquivo de macro ou arquivo de comandos, um script é uma lista de comandos que podem ser executados sem a interação do usuário.

Spam

Lixo eletrônico em forma de mensagens. Normalmente conhecido como e-mail não solicitado.

Spyware

Qualquer software que coleta informação do usuário através da conexão de Internet sem o seu consentimento, normalmente para propósitos de propaganda. Aplicativos spyware são tipicamente distribuídos de forma oculta juntamente com programas freeware ou shareware que podem ser baixados da Internet; no entanto, deve ser notado que a maioria dos programas shareware e freeware não apresentam spyware. Uma vez instalado, o spyware monitora a atividade do usuário na Internet e transmite essa informação de forma oculta para outra pessoa. O spyware pode coletar também endereços de e-mail e até mesmo número de cartões de crédito e senhas.

A similaridade do spyware com o cavalo de tróia é que o usuário instala algo que não deseja instalando algum outro produto. Um modo comum de se tornar uma vítima de spyware é baixar alguns programas de compartilhamento de arquivos (peer-to-peer) que estão disponíveis hoje em dia.

Colocando de lado as questões de ética e privacidade, o spyware prejudica o usuário consumindo memória do computador e conexão com a Internet quando manda a informação de volta a sua base usando a conexão de Internet do usuário. Porque o spyware usa a memória e os recursos do sistema, os aplicativos sendo executados podem levar o sistema ao colapso ou instabilidade geral.

Itens para inicializar

Qualquer arquivo colocado nessa pasta será executado quando o computador iniciar. Por exemplo uma tela de boas-vindas, um arquivo de som, um aviso de calendário ou um aplicativo pode ser um item para inicializar.

Área de Notificação

Introduzido com o Windows 95, a área de notificação é localizada na barra de tarefas do Windows (geralmente na parte inferior próxima ao relógio) e contém miniaturas de ícones para fácil acesso de funções do sistema como fax, modem, volume, e outros. Dois cliques ou um clique como o botão direito do mouse para ver ou acessar detalhes dos controles.

TCP/IP

Transmission Control Protocol/Internet Protocol - Protocolo de controle de transmissão / protocolo da Internet. Um conjunto de protocolos largamente utilizados na Internet que fornece comunicação através de redes de computadores interconectadas com diversas arquiteturas de hardware e vários sistemas. O TCP/IP inclui padrões de como os computadores comunicam e convenções para conexões da rede e roteamento de tráfego.

Trojan

Um programa destrutivo que oculta um aplicativo benigno. Ao contrário do vírus, um cavalo de tróia não se replica mas pode ser muito destrutivo. Um dos tipos mais incidentes de cavalos de tróia é um programa que diz se livrar dos vírus do seu computador, mas ao invés disso ele introduz vírus em seu computador.

O termo vem da estória de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante seus inimigos, os Troianos como uma oferta de paz. Mas depois dos troianos arrastarem o cavalo para dentro dos muros da cidade, os soldados Gregos saíram furtivamente da barriga do cavalo e abriram os portões da cidade, permitindo que seus compatriotas derrubassem e capturassem Tróia.

Atualizar

Uma nova versão do programa ou driver do produto projetado para substituir uma versão antiga do mesmo produto. Além disso, as rotinas de instalação verificam se uma versão mais antiga está instalada no seu computador, caso contrário, você não pode instalar.

O BitDefender possui um módulo de atualização que permita a você verificar manualmente por atualizações ou deixa que ele automaticamente atualize o produto.

Virus

Um programa ou uma parte do código que é carregado no seu computador sem o seu conhecimento e se executa contra a sua vontade. A maioria dos vírus pode também se duplicar. Todos os computadores são feitos pelo homem. Um simples vírus pode fazer uma cópia dele mesmo repetidamente é fácil de se produzir. Mesmo um simples vírus é perigoso porque pode rapidamente usar toda memória disponível a fazer os sistema parar. O tipo de vírus mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança.

Definições de vírus

É um padrão binário de vírus, utilizado pelo programa antivírus para detectar e eliminar os vírus.

Worm

Um programa que se propaga pela rede, se reproduzindo enquanto isso. Ele não pode se anexar a outros programas.