bitdefender

FREE EDITION 2009

Guia de usuário

bitdefender

Copyright© 2009 BitDefender

BitDefender Free Antivírus 2009
Guia de usuário

Publicado 2009.12.03

Copyright© 2009 BitDefender

Nota Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida em qualquer forma e meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou qualquer armazenamento e recuperação de informações, sem permissão escrita de um representante autorizado da BitDefender. Poderá ser possível a inclusão de breve citações em revisões apenas com a menção da fonte citada. O conteúdo não pode ser modificado em qualquer modo.

Aviso e Renúncia. Este produto e sua documentação são protegidos por direitos autorais. A informação neste documento é providenciada na " essência ", sem garantias. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não têm responsabilidade sobre qualquer pessoa ou entidade em respeito à perda ou dano causado direta ou indiretamente pela informação contida neste documento.

Este livro contém links para Websites de terceiras partes que não estão baixo controle da BitDefender, e a BitDefender não é responsável pelo conteúdo de qualquer site acessado por link. Se acessar a um site de terceiras partes mencionado neste manual, faz isso à sua própria conta e risco. A BitDefender fornece esses links apenas para facilitar, e a inclusão do link não implica que a BitDefender endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiras partes.

Marcas Registradas. Nomes de marcas registradas podem aparecer neste livro. Todas as marcas registradas ou não registradas neste documento são de propriedade única de seus respectivos donos.

Índice

Acordo de Licença de Software para Usuários Finais

SE VOCÊ NÃO CONCORDA COM ESTES TERMOS E CONDIÇÕES, NÃO INSTALEO SOFTWARE. AO SELECIONAR "EU ACEITO", "OK", "CONTINUE", "SIM" OUINSTALANDO OU USANDO O SOFTWARE DE QUALQUER MANEIRA, VOCÊ ESTÁINDICANDO O COMPLETO CONHECIMENTO E ACEITAÇÃO DOS TERMOS DESTEACORDO.

Estes termos abrangem as Soluções e Serviços BitDefender para usuários individuais que lhe foram licenciadas, 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 electrônica (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, você estará concordando 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 royaltie 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 de instalação do BitDefender e expira no final do período para o qual a licença foi instalada: 1 Ano.

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 formaas 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 deum 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 suporta todo o risco pela qualidade e desempenho do BitDefender. A BITDEFENDER não será responsável, em 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.

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.

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.

Esta licença de uso do BitDefender está sujeita a mudanças sem prévio aviso a você.

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.

BITDEFENDER SRL Preciziei Boulevard, no. 24, West Gate Building H2, ground floor, 6th district, Bucharest, Romania

Prefácio

Este guia foi elaborado para todos os usuários do BitDefender Free Antivírus 2009. A informação aqui apresentada é própria não somente para usuários preparados em computadores, mas também para qualquer pessoa apta a usar Windows.

Este manual lhe mostrará como instalar, configurar e usar o BitDefender Free Antivírus 2009. Você aprenderá como aproveitar melhor o BitDefender.

Desejamos a você uma agradável e útil leitura.

1. Convenções usadas neste livro

1.1. Convenções tipográficas

Vários estilos de texto são usados para implementar a leitura. O aspecto e significado dos mesmos estão representados 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.
sales@bitdefender.com	Mensagens de e-mail são inseridas no texto para informação sobre contato.
“Prefácio” (p. xi)	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. A Estrutura do Livro

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

Instalação. Instruções do passo a passo para instalar o BitDefender numa estação de trabalho. Este é um amplo tutorial sobre a instalação do **BitDefender Free Antivírus 2009**. Começando pelos pré-requisitos para uma instalação com sucesso, você será guiado através de todo o processo de instalação. Finalmente, o processo de remoção está descrito, caso você precise desinstalar o BitDefender.

Administração básica. Descrição da administração e manutenção inicial do BitDefender

Administração Avançada. Uma detalhada apresentação da Visão Avançada da interface. Você está apto a configurar operações de análises e atualizações.

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

Ajuda. Onde procurar e onde perguntar por ajuda caso algo aconteça fora do esperado.

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

1. Requisitos de Sistema

Você poderá instalar BitDefender Free Antivírus 2009 somente em computadores rodando com os seguintes sistemas operacionais:

- Windows XP com Service Pack 2 (32/64 bit) ou superior
- Windows Vista (32/64 bit) ou Windows Vista com Service Pack 1
- Windows Home Server

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 do Sistema

Para Windows XP

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- 300 MB de espaço disponível no disco rígido (recomendado 350 GB)

Para Windows Vista

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- 300 MB de espaço disponível no disco rígido (recomendado 350 GB)

Para Windows Home Server

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- 300 MB de espaço disponível no disco rígido (recomendado 350 GB)

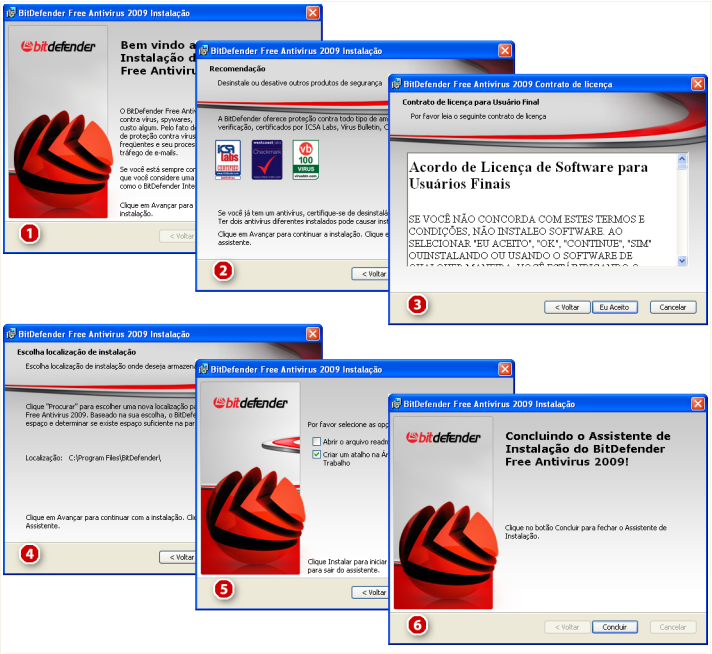
1.2. Requisitos de Software

- Internet Explorer 6.0 (ou superior)
- .NET Framework 1.1 (disponível no kit de instalação)

2. Instalar BitDefender

Localize o arquivo de instalação e clique duplamente sobre ele. Um assistente será carregado e irá guiá-lo através do processo de instalação:

Antes de executar o assistente de instalação, o BitDefender irá verificar se existem novas versões do pacote de instalação. Se uma nova versão estiver disponível, será avisado para o descarregar. Clique **Sim** para descarregar a nova versão ou **Não** para continuar a instalar a versão do arquivo de instalação.



Passos de instalação

Siga estes passos para instalar o BitDefender Free Antivírus 2009:

1. Clique em **Próximo** para continuar ou clique **Cancelar** se você quiser sair da instalação.
2. Clique em **Próximo**.

BitDefender Free Antivírus 2009 alertará você caso houver 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.

3. 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.

4. Como padrão, o BitDefender Free Antivirus 2009 será instalado em `C:\Program Files\BitDefender\BitDefender 2009`. 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 Free Antivirus 2009 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.

   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.

   Espere até que a instalação termine.

6. 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.

Se aceitou as definições padrão do caminho da instalação, poderá ver uma pasta com o nome `BitDefender` nos `Programas` que contém a subpasta `BitDefender 2009`.

3. Upgrade para Versão Paga

A versão paga de BitDefender automaticamente atualizará suas assinaturas contra malwares a cada hora. Além da proteção em tempo real, elas também oferecem vários outros benefícios com o objetivo de proteger seu computador e sua dentidade na internet.

A fim de efetuar o upgrade o BitDefender Free Antivirus 2009 para uma versão paga, siga estes passos:

1. Compre o produto BitDefender que preeencha suas necessidades. Você pode clicar no **Upgrade** link, localizado na parte inferior do painel de controle do BitDefender, ir até a página web onde você poderá comprar um produto BitDefender.
2. Instalar a versão paga do BitDefender: clique duas vezes no arquivo de instalação e siga o assistente de instalação. Você não precisa remover o BitDefender Free Antivirus 2009 antes.

4. Remover ou Reparar o BitDefender

Se você pretende reparar ou desinstalar o **BitDefender Total Antivirus 2009**, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar** → **Programas** → **BitDefender 2009** → **Reparar ou Desinstalar**.

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 isto lhe for solicitado, e depois, clique em **Instalar** para reinstalar o BitDefender Free Antivírus 2009.

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

- **Remover** - para remover todos os componentes instalados. Recomendamos que escolha **Desinstalar** para uma reinstalação limpa.

  Se escolher desinstalar BitDefender, surgirá uma nova janela.

  Clique em **Desinstalar** para dar início à desinstalação do BitDefender Free Antivírus 2009 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`.

Ocorreu um erro ao desinstalar o BitDefender

Se ocorrer um erro ao desinstalar o BitDefender, o processo de desinstalção será cancelado e surgirá uma nova janela. Clique **Desinstalar** para se certificar que o BitDefender foi removido completamente. A Ferramenta de Desinstalação removerá

todos os arquivos e chaves de registo que não tenham sido removidos durante o processo de desinstalação automática.

Administração básica.

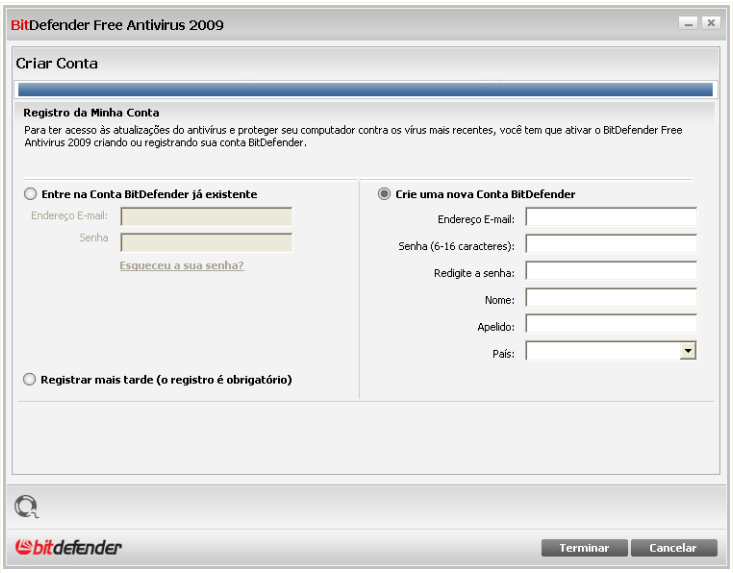
5. Introdução

BitDefender Free Antivírus 2009 oferece proteção básica contra vírus, spywares, rootkits e outros custos sem custo algum. Uma vez que seu objetivo é cobrir somente as mínimas necessidades de proteção contra vírus, ele é atualizado com frequência menor e não analise o tráfego da internet e e-mails.

BitDefender Free Antivírus 2009 é pré-registrado com uma chave que lhe permite usar o produto por um ano a partir da data de sua instalação. Assim que esta licença expirar, BitDefender parará de funcionar.

5.1. Ativar BitDefender

Na primeira ocasião que você ligar seu computador após a instalação, lhe será solicitado criar uma conta. A conta é necessária para poder ativar o produto. Você precisa criar sua conta dentro de 15 após a instalação do BitDefender. Caso contrário, BitDefender não mais efetuará atualizações de antivirus.



Criar 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. 12)
- "Já tenho uma conta BitDefender" (p. 12)

Nota

Se escolher registrar sua conta mais tarde, o BitDefender vai lhe notificar que você precisa ativar seu produto e isso irá lhe ajudar a solucionar este problema. Para mais informações, por favor consulte a seção "*Reparando Incidências*" (p. 28).

Não tenho uma conta BitDefender

Para criar uma conta BitDefender, selecione **Criar uma nova conta BitDefender** e fornecer a devida informação. 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.
- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - selecciona o país onde reside.

Nota

Use o endereço de e-mail e a senha que nos forneceu para fazer log in na sua conta em http://myaccount.bitdefender.com.

Para criar com sucesso uma conta deverá em primeiro lugar ativar o seu endereço de e-mail. Verifique o seu endereço de e-mail e siga as instruções descrita no e-mail enviado para você pelo serviço de registo da BitDefender.

Clique em **Finalizar**.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Neste caso, forneça a senha da sua conta.

Se já possui uma conta ativa, selecione **Entrar numa conta BitDefender existente** e forneça o endereço de e-mail e a senha da sua conta.

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

Clique em **Finalizar**.

5.2. Abra o BitDefender

Para acessar a interface principal do BitDefender Antivírus 2009, utilize o menu Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2009** → **BitDefender Antivírus 2009** ou mais rapidamente, clicando duas vezes no **ícone do BitDefender** na área de notificação.

5.3. Modo de Visão do Interface do usuário

O BitDefender Free Antivírus 2009 vai de encontro às necessidades tanto de iniciantes, como de pessoas mais técnicas. Assim, a interface gráfica do usuário foi desenhada para facilitar o uso de ambos.

Pode escolher entre o Modo de Visão Básico ou Avançado do BitDefender consoante a sua experiência como usuário do produto.

Nota
Pode facilmente escolher um desses modos de visão ao clicar respectivamente no botão **Mudar Modo Básico** ou **Mudar Modo Avançado** .

5.3.1. Modo Básico

O Modo Básico é uma interface simples que ajuda a monitorar e corrigir problemas de segurança, e tomar medidas preventivas para proteger o seu computador.

Modo Básico

- Como pode facilmente notar, na parte superior da janela existem dois botões e uma barra de estado.

Item	Descrição
Definições	Abre uma janela onde você pode facilmente ativar ou desativar importantes módulos de segurança.
>Mudar Modo Avançado	Abre a janela de Visualização Avançada. Aqui é onde você pode configurar em detalhes cada módulo do BitDefender. O BitDefender irá lembrar dessa opção na próxima vez que você abrir a interface com o usuário.
Histórico	Contém informação sobre as vulnerabilidades de segurança do seu computador e ajuda-o a repará-las.

- No meio da janela há duas abas. As abas são apresentadas em detalhes na "*Modo Básico*" (p. 30) seção.

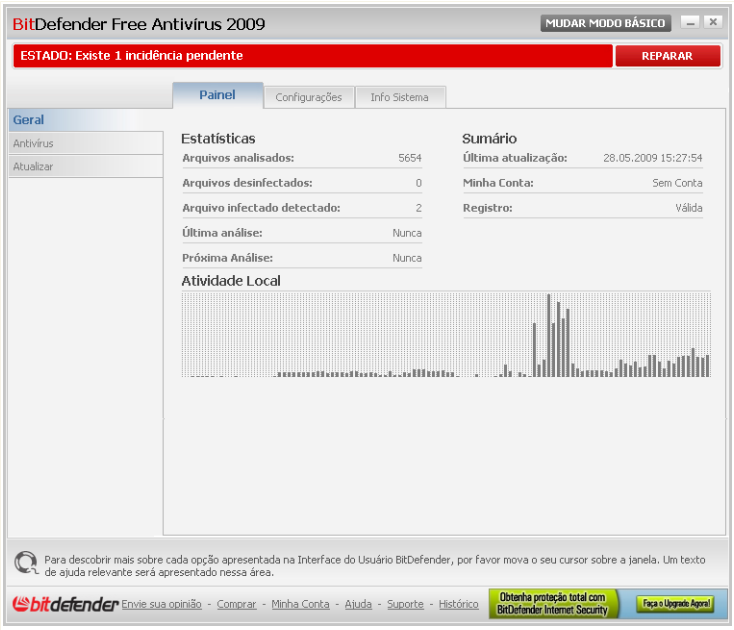
Barra	Descrição
Painel	Mostra estatísticas significativas do produto e links para as mais importantes tarefas on-demand.
Antivírus	Mostra o estado do módulo Antivirus que ajuda-o a manter o seu BitDefender actualizado e o seu computador livre de vírus.

- E mais ainda, a janela de Modo Básico do BitDefender contém diversos atalhos úteis.

Link	Descrição
Envie seu comentário	Abre uma página da web aonde voê poderá nos enviar seus comentários.
Atualização de versão	Abre uma página de internet onde você poderá comprar um produto BitDefender. A versão paga de BitDefender automaticamente atualizará suas assinaturas contra malwares a cada hora. Além da proteção em tempo real, elas também oferecem vários outros benefícios com o objetivo de proteger seu computador e sua dentidade na internet.
Minha Conta	Abre uma página de internet onde você pode logar em sua conta da BitDefender. Para informações sobre a conta BitDefender, por favor consulte a seção "*Como ativar o BitDefender*" (p. 105).
Ajuda	Abre o arquivo Ajuda, o qual lhe mostrará como usar o BitDefender.
Suporte	Abre uma página da internet que lhe oferece informação técnica útil para suporte.
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

5.3.2. Modo Avançado

A Visualização Avançada dá acesso a cada componente específico do BitDefender. É onde você consegue configurar o BitDefender em detalhes.



Modo Avançado

- Como pode facilmente notar, na parte superior da janela existe um botão e uma barra de estado.

Item	Descrição
Mudar para Modo Básico	Abre a janela de visualização Básica O BitDefender irá lembrar dessa opção na próxima vez que você abrir a interface com o usuário.
Histórico	Contém informação sobre as vulnerabilidades de segurança do seu computador e ajuda-o a repará-las.

- Do lado esquerdo da janela existe um menu que contém todos os módulos de segurança.

Nota
Os módulos da interface de Visualização Avançada são mostradas em detalhes na seção "Administração Avançada" (p. 42) desse guia do usuário.

Módulo	Descrição
Geral	Permite-lhe aceder 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 excepções e configurar o módulo de quarentena.
Actualização	Permite-lhe obter info das últimas actualizações, actualizar o produto e configurar o processo de actualização em detalhe.

- E mais ainda, a janela do Modo Avançado BitDefender contém diversos atalhos úteis.

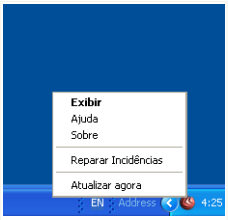
Link	Descrição
Envie seu comentário	Abre uma página da web aonde voê poderá nos enviar seus comentários.
Atualização de versão	Abre uma página de internet onde você poderá comprar um produto BitDefender. A versão paga de BitDefender automaticamente atualizará suas assinaturas contra malwares a cada hora. Além da proteção em tempo real, elas também oferecem vários outros benefícios com o objetivo de proteger seu computador e sua dentidade na internet.
Minha Conta	Abre uma página de internet onde você pode logar em sua conta da BitDefender. Para informações sobre a conta BitDefender, por favor consulte a seção "*Como ativar o BitDefender*" (p. 105).
Ajuda	Abre o arquivo Ajuda, o qual lhe mostrará como usar o BitDefender.
Suporte	Abre uma página da internet que lhe oferece informação técnica útil para suporte.

Link	Descrição
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

5.4. Ícone BitDefender na Área de Notificação

Para gerir todo o produto mais rapidamente, pode também usar o icone 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.



Icone BitDefender

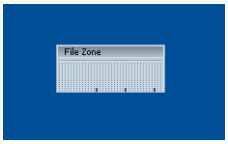
- **Mostrar** - abre a interface principal do BitDefender.
- **Ajuda** - abre o arquivo de ajuda, que explica em detalhes como configurar e utilizar o BitDefender Free Antivírus 2009.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **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 mais informações, por favor consulte a seção "*Reparando Incidências*" (p. 28).
- **Atualizar agora** - realiza uma atualização imediata. Surge uma nova janela, onde pode ver o estado da actualização.

Se existirem incidências criticas a afectar a segurança do seu sistema, um ponto de exclamação é mostrado sobre o icone do BitDefender. Pode passar o mouse sobre o ícone e ver o número de incidências que afectam a segurança do seu sistema.

5.5. Barra de Actividade da Análise

A **Barra de atividade de verificação** é uma visualização gráfica da atividade de verificação em seu sistema. Essa pequena janela só está disponível quando a interface está em Visualização Avançada. Se você alternar para a Visualização Básica, a barra de atividade da análise desaparecerá.

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

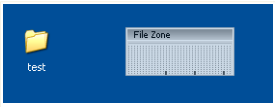


Barra de Actividade da Análise

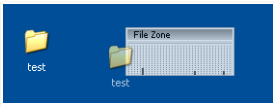
Nota
A Barra de Actividade da Análise irá avisá-lo quando a protecção em tempo-real está desactivada ao mostrar-lhe uma cruz vermelha sobre a **Zona PC**).

5.5.1. 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 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. As opções de análise são padrão e você não pode as alterar.

5.5.2. 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. Se a interface está em Modo Básico de visualização, clique no botão **Mudar Modo Avançado**, localizado no canto superior direito da janela.

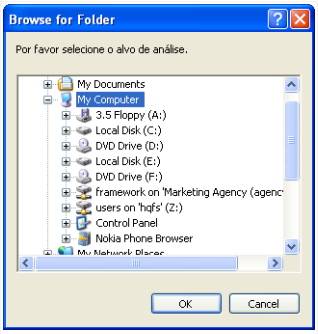
   Importante
   A barra de atividade da Análise só está disponível quando a interface está em Visualização Avançada.

3. Clique em **Geral** no menu do lado esquerdo.
4. Clique na barra **Definições** .
5. Marque a opção **Ativar a barra de Atividade da Análise (na tela de atividade do produto)**.

5.6. 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 aceder à Análise Manual BitDefender, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar → Programas → BitDefender 2009 → Análise Manual BitDefender**. A seguinte análise irá aparecer:



Análise Manual BitDefender

Tudo o que tem de fazer é explorar as pastas, seleccionar a que deseja analisar e clicar **OK**. 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. 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.

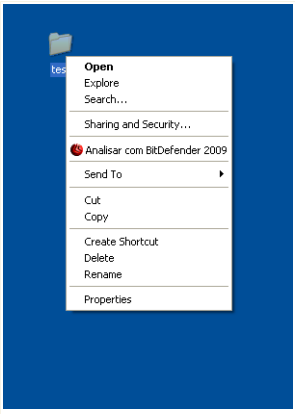
Para iniciar o Windows no Modo de Segurança, reinicie seu computador e aperte a tecla `F8` até aparecer o menu Opções Avançadas do Windows. Você pode escolher várias opções de inicialização no Modo de Segurança. Você pode desejar escolher a opção **Modo de Segurança com Rede** para poder acessar a internet.

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.

5.7. 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.

- Analisar com o BitDefender 2009

5.7.1. Analisar com BitDefender 2009

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 2009** 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.

2. Se a interface está em Modo Básico de visualização, clique no botão **Mudar Modo Avançado**, localizado no canto superior direito da janela.
3. Clique em **Antivírus** no menu do lado esquerdo.
4. Clique na aba **Análise Vírus Scan**.
5. Clique com o botão direito sobre a tarefa **Análise Contextual** e selecione **Abrir**. Uma janela aparecerá.
6. 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.
7. Clique em **OK** para salvar as alterações.
8. Clique em **OK** para confirmar e aplicar as novas opções de análise.

Nota
Você não deve alterar as opções de análise desse método de análise a não ser que você tenha plena certeza do que está fazendo.

5.8. Assistente do analisador Antivírus

Sempre que você iniciar uma análise avulsa (por exemplo, clicar com o botão direito do mouse em cima de um diretório e selecionar a opção **Analisar com o BitDefender 2009**), o assistente de análise de vírus do BitDefender 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.

5.8.1. 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.

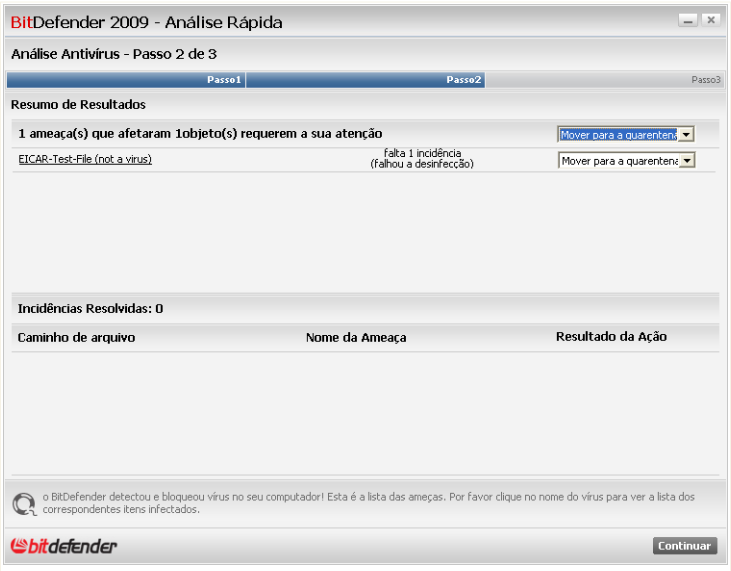
- **Não desejo digitar uma senha para esse objeto.** Selecione essa opção para pular a análise desse arquivo.
- **Não desejo digitar a senha para qualquer objeto (pular todos os objetos protegidos por senha).** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha. 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 directamente 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.

5.8.2. Passo 2/3 - Seleccionar as acções

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.

Pode escolher uma acção geral a ser levada a cabo para todas as incidências ou pode escolher acções separadas para cada grupo de incidências.

Uma ou várias das seguintes opções podem aparecer no menu:

Ação	*Descrição*
Não Tomar Acção	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.

5.8.3. 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 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.

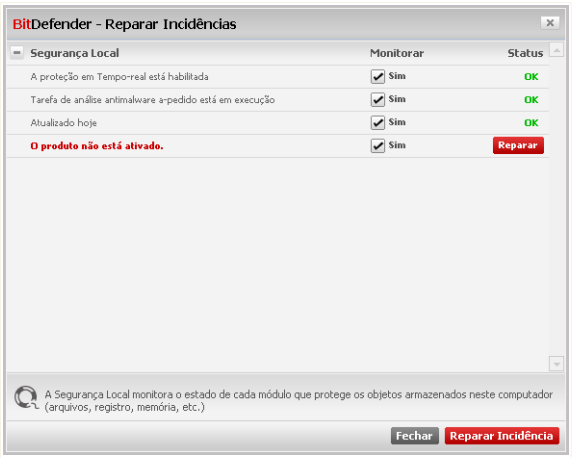
Se foram detectados arquivos suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender. Clique **OK** para enviar estes arquivos para análise no Laboratório do BitDefender.

6. Reparando Incidências

Sabemos que é importante ser avisado sempre que há um problema que pode afetar a segurança do seu computador. Ao monitorar cada módulo de segurança, o BitDefender irá lhe avisar não somente quando você configura definições que podem afetar a segurança do seu computador, mas também quando você esquece de fazer tarefas importantes.

Na área superior da janela do BitDefender há uma barra de estatus mostrando o número de problemas pendentes. Clique **Consertar todos os problemas** ou **Consertar este problema** para consertar problemas pendentes. Uma janela de estatus de segurança aparecerá.

Nota
Se nenhuma ameaça afeta a segurança de seu sistema, a barra de status fica verde.



Barra de Estado

As incidências respeitantes à segurança local são descritas em frases bastante explicítas. Ao mesmo tempo com cada frase, se existe algo que poderá afectar a segurança do seu computador, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Há problemas que podem aparecer:

Incidência	*Descrição*
Protecção de arquivos em Tempo-real está activada	Assegura que todos os arquivos serão analisados, à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.
Você nunca analisou o seu computador em busca de malware	É altamente recomendável que leve a cabo uma análise a-pedido tão depressa quanto possível para verificar que os arquivos armazenados no seu computador estão livres de malware.
Você não tem efetuado uma análise de seu computador à procura de malwares faz x dia(s)	É altamente recomendável que leve a cabo uma análise a-pedido tão depressa quanto possível para verificar que os arquivos armazenados no seu computador estão livres de malware.
A Atualização Automática está desativada	Por favor mantenha a actualização automática activada para assegurar que as vacinas de malware do seu produto BitDefender são actualizadas numa base regular.
A atualização não foi executada a x dias	Por favor atualize o BitDefender imediatamente. Se o BitDefender não estiver atualizado, não poderá detectar os malwares mais recentes quando efetuar uma análise de seu computador.
Actualizar Agora	A atualização do produto e das vacinas de malware estão sendo executadas.
O produto não está ativado	Para ativar o produto, você deve criar uma conta no BitDefender.

Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.

Se você quiser excluir um incidente da monitoração, basta desmarcar a caixa de seleção da coluna **Monitorar**.

7. Modo Básico

O Modo Básico é uma interface simples que ajuda a monitorar e corrigir problemas de segurança, e tomar medidas preventivas para proteger o seu computador. A Visualização Básica está organizada em duas abas:

Barra	Descrição
Painel	Mostra estatísticas significativas do produto e links para as mais importantes tarefas on-demand.
Antivírus	Mostra o estado do módulo Antivirus que ajuda-o a manter o seu BitDefender actualizado e o seu computador livre de vírus.

No lado direito de cada aba, você pode ver uma Tasks área. Aqui você poderá encontrar links para as tarefas on-demand pré-definidas. Use estas tarefas para analisar seu computador e para atualizar o BitDefender.

7.1. Aba do Painel

Ao clicar na barra Painel ser-lhe-á mostrado estatísticas importante do produto e o seu estado de registo juntamente com links para as mais importantes tarefas a-pedido.

Painel

O painel é composto de várias secções:

- **Status** - Alerta se incidentes afetam o seu computador e ajuda você a resolvê-los. Clique **Consertar todos os problemas** ou **Consertar este problema** para consertar problemas pendentes. Para mais informações, por favor consulte a seção "*Reparando Incidências*" (p. 28).
- **Overview** - Exibe informação geral do produto.

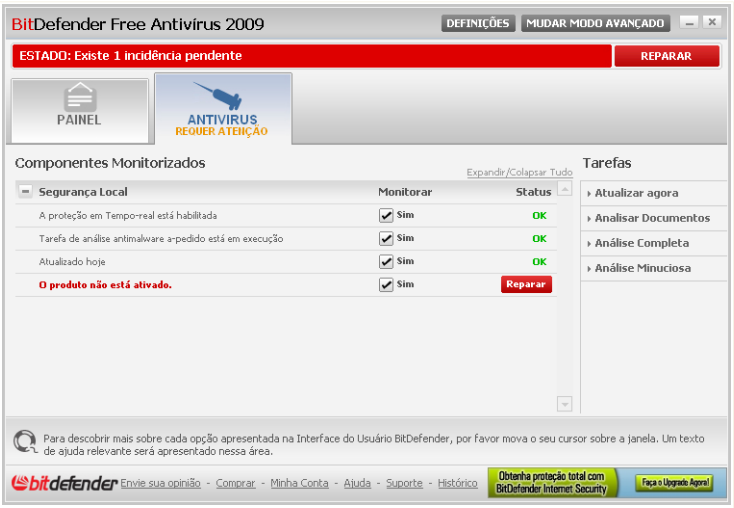
Item	*Descrição*
Registro	Seu produto é válido por 1 ano a partir da data de instalação.
Minha Conta	Indica o endereço de e-mail de sua conta BitDefender. Você deve criar uma conta BitDefender para poder ativar o seu produto. Para informações sobre a conta BitDefender, por favor consulte a seção "*Como ativar o BitDefender*" (p. 105).
Última actualização	Indica quando o o seu produto BitDefender foi atualizado pela última vez. Por favor, execute atualizações regularmente para que o BitDefender possa detectar até mesmo o mais recentes vírus.

Item	Descrição
Última análise	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.

- **Tasks** - Fornece links para as tarefas de segurança mais importantes:
  - **Atualizar agora** - realiza uma atualização imediata.
  - **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.
  - **Análise Minuciosa do Sistema** - inicia uma análise minuciosa no seu computador (incluindo arquivos comprimidos).

7.2. Aba Antivírus

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



Antivírus

A aba Antivírus é organizada em duas seções:

- **Componentes Monitorados** - Permite-lhe ver a lista completa dos componentes monitorados. Você pode escolher quais componentes deseja monitorar. Recomenda-se permitir a opção de monitoramento para todos eles.
- **Tasks** - Aqui você encontra links para as tarefas de segurança mais importantes:
  - **Atualizar agora** - realiza uma atualização imediata.
  - **Analisar os Meus Documentos** - inicia uma análise rápida no diretório Documentos e Configurações.
  - **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.
  - **Análise Minuciosa do Sistema** - inicia uma análise minuciosa no seu computador (incluindo arquivos comprimidos).

7.2.1. Componentes Monitorizados

Sabemos que é importante ser avisado sempre que há um problema que pode afetar a segurança do seu computador. Ao monitorar cada módulo de segurança, o BitDefender irá lhe avisar não somente quando você configura definições que podem afetar a segurança do seu computador, mas também quando você esquece de fazer tarefas importantes.

As incidências respeitantes à segurança local são descritas em frases bastante explicítas. Ao mesmo tempo com cada frase, se existe algo que poderá afectar a segurança do seu computador, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
Protecção de arquivos em Tempo-real está activada	Assegura que todos os arquivos serão analisados, à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.
Você nunca analisou o seu computador em busca de malware	É altamente recomendável que leve a cabo uma análise a-pedido tão depressa quanto possível para verificar que os arquivos armazenados no seu computador estão livres de malware.
Você não tem efetuado uma análise de seu computador à procura de malwares faz x dia(s)	É altamente recomendável que leve a cabo uma análise a-pedido tão depressa quanto possível para verificar que os arquivos armazenados no seu computador estão livres de malware.
A Atualização Automática está desativada	Por favor mantenha a actualização automática activada para assegurar que as vacinas de

Incidência	Descrição
	malware do seu produto BitDefender são actualizadas numa base regular.
A atualização não foi executada a x dias	Por favor atualize o BitDefender imediatamente. Se o BitDefender não estiver atualizado, não poderá detectar os malwares mais recentes quando efetuar uma análise de seu computador.
Actualizar Agora	A atualização do produto e das vacinas de malware estão sendo executadas.
O produto não está ativado	Para ativar o produto, você deve criar uma conta no BitDefender.

Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.

Se você quiser excluir um incidente da monitoração, basta desmarcar a caixa de seleção da coluna **Monitorar**.

7.3. Tarefas

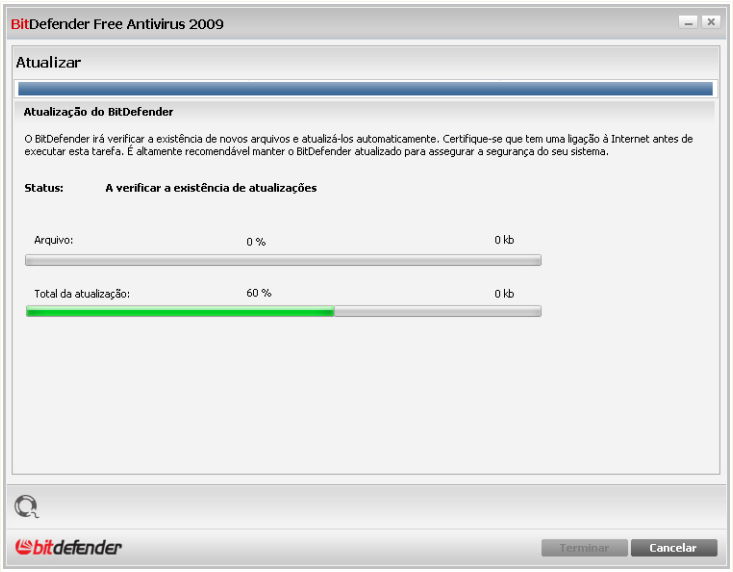
No lado direito de cada aba, você pode ver uma **área de tarefas.** As seguintes tarefas estão disponíveis:

- **Atualizar agora** - realiza uma atualização imediata.
- **Analisar os Meus Documentos** - inicia uma análise rápida no diretório Documentos e Configurações. Esta tarefa aparece somente na aba **Antivírus**.
- **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.
- **Análise Minuciosa do Sistema** - inicia uma análise minuciosa no seu computador (incluindo arquivos comprimidos).

7.3.1. Actualizar 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.

Por padrão,BitDefender verificará se há atualizações ao ligar seu computador e **a cada 24 horas** depois disso. No entanto, se deseja actualizar o BitDefender, clique em **Actualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Actualizar o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

O processo de actualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de actualização não afectará 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.

7.3.2. A analisar com BitDefender

Para analisar o seu computador em busca de malware, execute uma tarefa de análise em particular, clicando no respectivo botão. A seguinte tabela aprsenta todas as tarefas disponíveis, com uma descrição de cada uma delas:

Tarefa	Descrição
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 Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Nota
Um vez que as atrefas **Análise Minuciosa do Sistema** 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 inactivo.

Quando você executar uma análise, o Assistente de Análise Antivírus será exibido. 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. 23).

8. Rapidamente Habilita/Desabilita Configurações

Para ativar ou desativar rapidamente as configurações do BitDefender, abra o BitDefender, mude para o modo Básico e clique no botão **Configurações** localizado no canto superior direito da janela.

Definições Básicas

As configurações estão agrupadas em duas categorias.

- Segurança Local
- Configuração Geral

Clique na caixa com "+" para abrir uma categoria ou clique na caixa "-" para fechar uma categoria.

8.1. Segurança Local

Pode activar/desactivar os módulos de segurança com um clique.

Módulo de Segurança	Descrição
Protecção Antivirus & Antispyware de Arquivos em Tempo-Real	A protecção de arquivos em tempo-real assegura que todos os arquivos acedidos por si ou por uma aplicação são analisados.
Actualização Automática	A atualização automática assegura que os produtos e as vacinas recentes sejam baixadas da Internet e instalados automaticamente, periodicamente.

8.2. Configurações Gerais

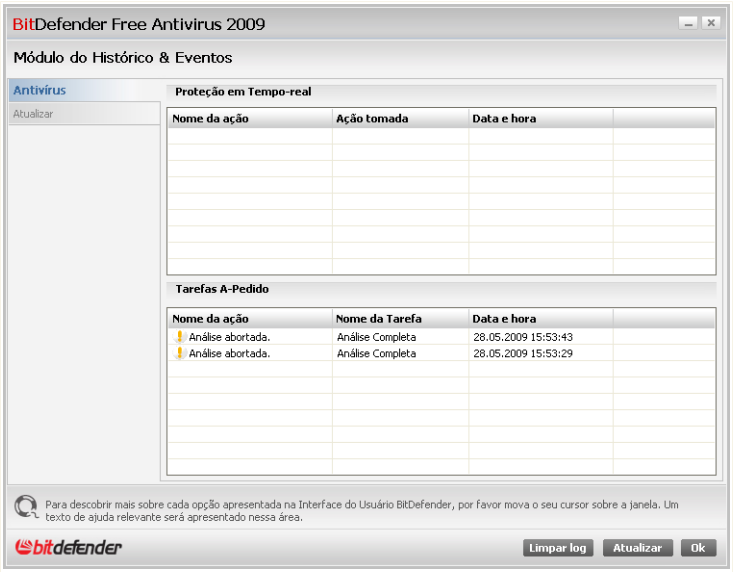
Você pode ativar ou desativar as configurações gerais com apenas um clique.

Item	Descrição
Notícias BitDefender	Ao activar esta opção, irá receber notícias importantes sobre a empresa BitDefender, sobre as actualizações do produto ou sobre novas ameaças de segurança.
Notificações de Alerta do Produto	Ao activar esta opção, irá receber alertas de informação.
Barra de Actividade 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 Actividade da Análise*" (p. 18).
Carregar o BitDefender ao iniciar o Windows	Ao habilitar essa opção, o BitDefender é carregado ao iniciar o Windows. Nós recomendamos que você mantenha esta opção selecionada.
Enviar Relatórios de Vírus	Ao activar 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 activar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém

Item	Descrição
	qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

9. Histórico

O link **Histórico** no fundo da janela do Centro de Segurança BitDefender abre uma outra janela com o histórico & de eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança. Por exemplo, pode facilmente verificar se a actualização foi executada com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc.



Eventos

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

- **Antivírus**
- **Actualização**

Uma lista de eventos está disponível para cada categoria. Cada evento vem com a seguinte informação: uma breve descripção, a acção 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 Log** se deseja remover antigos logs ou **Actualizar** para se certificar que os logs mais recentes são mostrados.

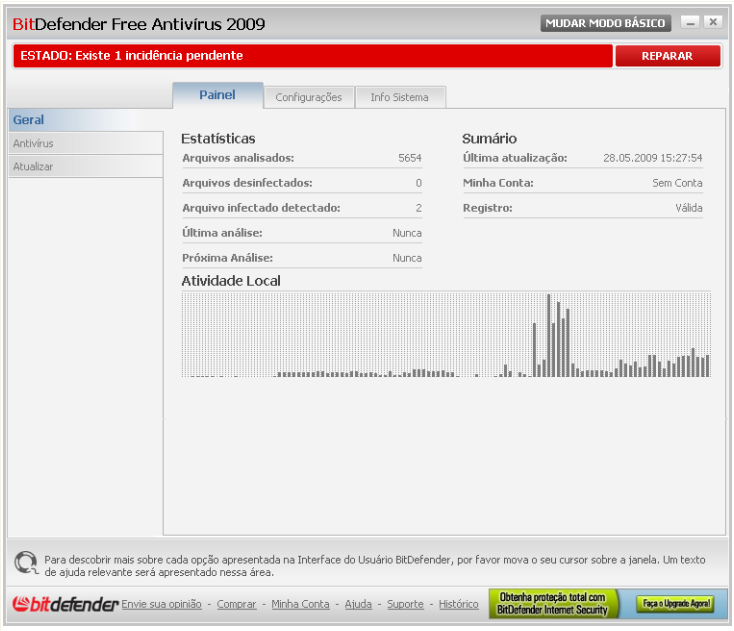
Administração Avançada

10. Geral

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

10.1. Painel

Para ver as estatísticas da actividade do produto e o seu estado de registo, vá a **Geral>Painel** no Modo Avançado.



Painel

O painel de controle está dividido em três seções:

- **Estaísticas** - Mostra informação importante com respeitoà actividade do BitDefender.

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 vírus detectados no seu sistema até ao momento da sua última análise.
Última análise	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 **Antivírus**, na aba Análise de Vírus, e execute a Análise Completa ou a Análise Minuciosa do Sistema.
Próxima análise	Indica a próxima vez em que o computador será analisado. Para descobrir como você pode configurar o BitDefender para analisar automaticamente seu computador, por favor vá para "*Como Agendar uma Análise no Computador*" (p. 112).

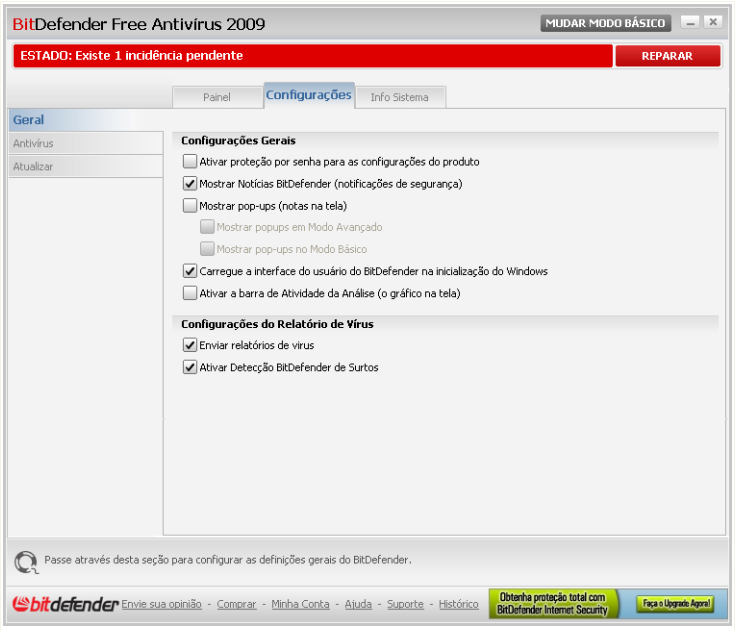
- **Overview** - Exibe informação geral do produto.

Item	Descrição
Última actualização	Indica quando o o seu produto BitDefender foi atualizado pela última vez. Por favor, execute atualizações regularmente para que o BitDefender possa detectar até mesmo o mais recentes vírus.
Minha Conta	Indica o endereço de e-mail de sua conta BitDefender. Você deve criar uma conta BitDefender para poder ativar o seu produto. Para informações sobre a conta BitDefender, por favor consulte a seção "*Como ativar o BitDefender*" (p. 105).
Registro	Seu produto é válido por 1 ano a partir da data de instalação.

- **Zona PC** - Indica a evolução do número de objectos analisados pelo BitDefender Antimalware. A altura da barra indica a intensidade do tráfego durante esse intervalo de tempo.

10.2. Configurações

Para efetuar as configurações gerais do BitDefender, vá para **Configuração>Geral** no modo Avançado.



Configurações Gerais

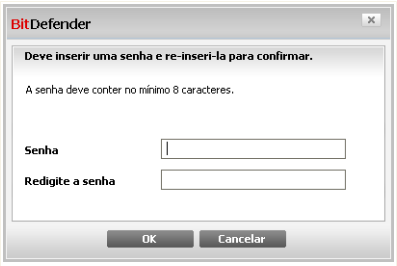
Aqui você pode ajustar o comportamento integral do BitDefender. Por padrão, o BitDefender é carregado na inicialização do Windows e então roda minimizado na área de notificação.

10.2.1. 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:

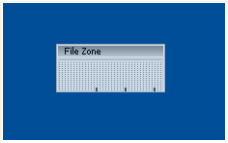


Confirmar senha

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.

- **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 para mostrar pop-ups somente quando usar o Modo Básico ou o Modo Avançado.
- **Carregar a interface do usuário do BitDefender junto com o Windows** - o BitDefender iniciará automaticamente quando o sistema iniciar. Nós recomendamos que você mantenha esta opção selecionada.
- **Permitir que a barra de Análise de Atividades(na tela gráfica de atividade do produto)** - mostra a Barra de Análise de Atividade sempre que você se logar ao Windows. Limpe esta caixa se deseja que a barra de Actividade da Análise não seja mostrada daí em diante.



Barra de Actividade 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 Visualização Avançada.

10.2.2. 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.

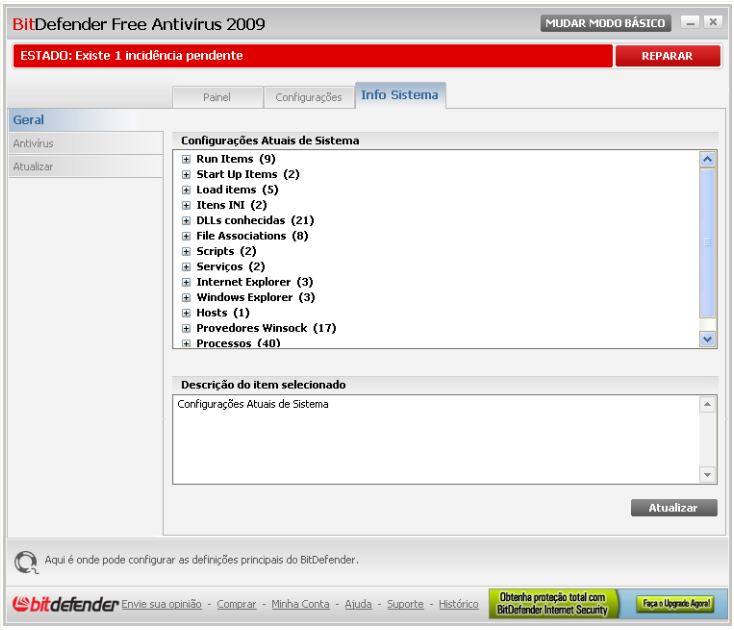
- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  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.

10.3. 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 actividade da seu sistema e as aplicações instaladas nele como também identificar possíveis infecções.

Para obter a informação do sistema, vá para**Geral>Info 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 actual associação de arquivos para o modo por defeito. 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**.

11. 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:

- Protecção em Tempo-real - previne que novas ameaças de malware entrem no seu sistema. Por exemplo, ao abrir um documento em Word, BitDefender o analisará para procurar por ameaças conhecidas.

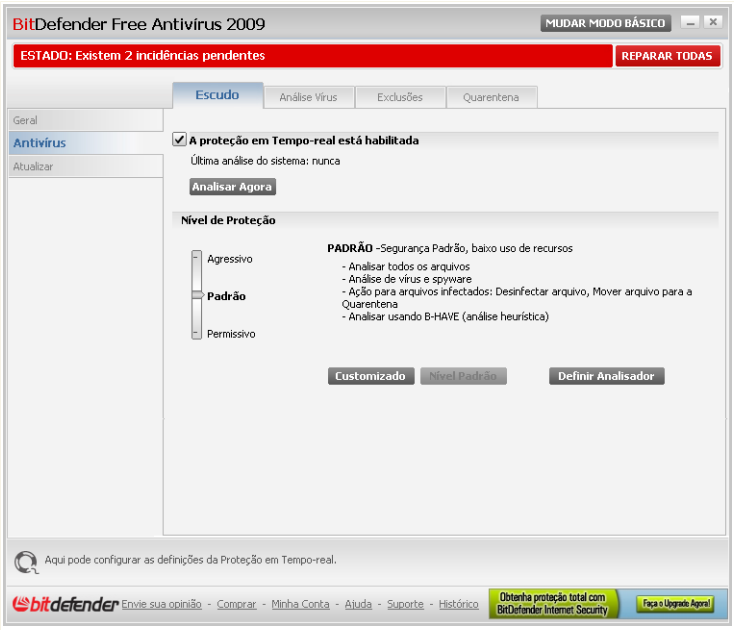
  Nota
  A proteção em Tempo-real, também referida como análise no acesso - os arquivos são analisados à medida que os usuários lhes acessem.

- 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.

11.1. Protecção em Tempo-real

O BitDefender Free Antivírus 2009 oferece contínua proteção em tempo real contra uma vasta gama de malwares analisando tdos os arquivos acessados. Entretanto, não analisa mensagens de e-mail, tráfego de internet e comunicações através de softwares de mensagens instatâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Para configurar a proteção em tempo real, vá para **Escudo>Antivírus** no modo Avançado.



Protecção em Tempo-real

Pode ver se a protecção em tempo-real está activada ou desactivada. Se deseja mudar o actual estado da protecção em Tempo-real, limpe ou seleccione a respectiva caixa de selecção.

Importante
Para prevenir que o seu computador seja infectado por vírus mantenha activa a **Protecção em Tempo-real**.

Para dar início a uma análise rápida, clique **Analisar Agora**.

11.1.1. Configurar Nível de Protecção

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

Existem 3 níveis de protecção:

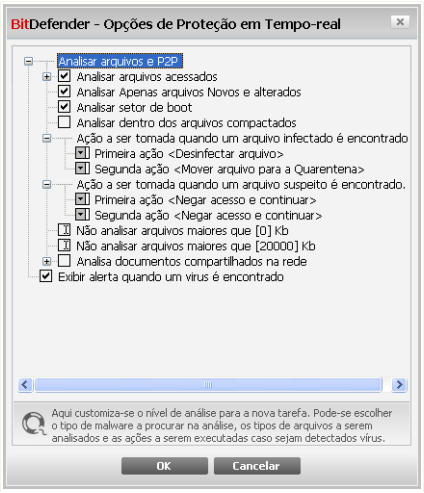
Nível de Protecção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Os programas serão analisados somente à procura de vírus. Além da análise tradicional baseada em assinaturas, uma análise heurística será efetuada. As ações tomadas para arquivos infectados são: limpeza de arquivos e barrar acesso.
Por Defeito	Oferece segurança standard. O nível de consumo de recursos é baixo. Todos os tipos de arquivos são analisados à procura de vírus e spywares, com restrições específicas. Além da análise pelo método tradicional de assinaturas, uma análise heurística será efetuada. As ações tomadas para arquivos infectados são as seguintes: limpeza de arquivo e barrar acesso.
Agressivo	Oferece uma segurança elevada. O nível de consumo de recursos é moderado. Todos os arquivos são escaneados para a procura de vírus e spywares. Compartilhamentos de redes também são analisadas. Além do tradiconal método de análise de assinaturas, uma análise heurística é também efetuada. As ações tomadas para os arquivos infectados são: limpeza de arquivos e barrar acesso.

Para aplicar as configurações por defeito da protecção em tempo-real clique em **Nível por Defeito**.

11.1.2. Personalizando Nível de Protecção

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 customizar a proteção em tempo real clicando **Nível de customização**. A seguinte análise irá aparecer:



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 P2P** são opções de análise aplicadas ao arquivos que você tenta acessar (abrir, renomear, etc).

Opção		*Descrição*
Analisar arquivos acedidos	**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`;

Opção		Descrição
		.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 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. Seleccione **Excluir da análise dialers e aplicações** se deseja excluir este tipo 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.
Analisar o sector de arranque		Para verificar o setor de boot do sistema.
Verificar dentro dos arquivos compactados		Arquivos de backup acessados também serão verificados. Com essa opção ativada, o computador ficará lento.
Verificar programas compactados		Todos os programas compactados serão verificados.
Primeira Acção.		Seleccionar do menu drop-down a primeira acção a levar a cabo 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 do que [x] Kb		Digite o tamanho máximo dos arquivos a serem verificados. Se o tamanho for 0Kb, todos os arquivos serão verificados.
Não analisar arquivos maiores do que [20000] Kb		Insira o tamanho máximo dos arquivos comprimidos a serem analisados em kilobytes (KB). Se deseja analisar todos os arquivos, independentemente do seu tamanho, insira 0.
Não analisar partilhas de redes		Se esta opção estiver ativada, BitDefender não irá analisar as partilhas de rede, permitindo um acesso de rede mais rápido. Recomendamos que ative esta opção apenas se a rede de que faz parte estiver protegida por uma solução antivírus.

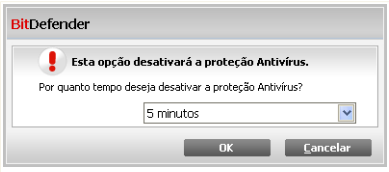
- **Mostra um aviso quano um vírus é encontrado** - abre uma janela de alerta quando um vírus é encontrado num arquivo acessado. A janela de alerta mostra o nome do vírus, o caminho no disco do arquivo infectado.

  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.

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

11.1.3. Desactivando a Protecção em Tempo-real

Se deseja desactivar a Protecção em Tempo-real, uma janela de aviso irá aparecer.



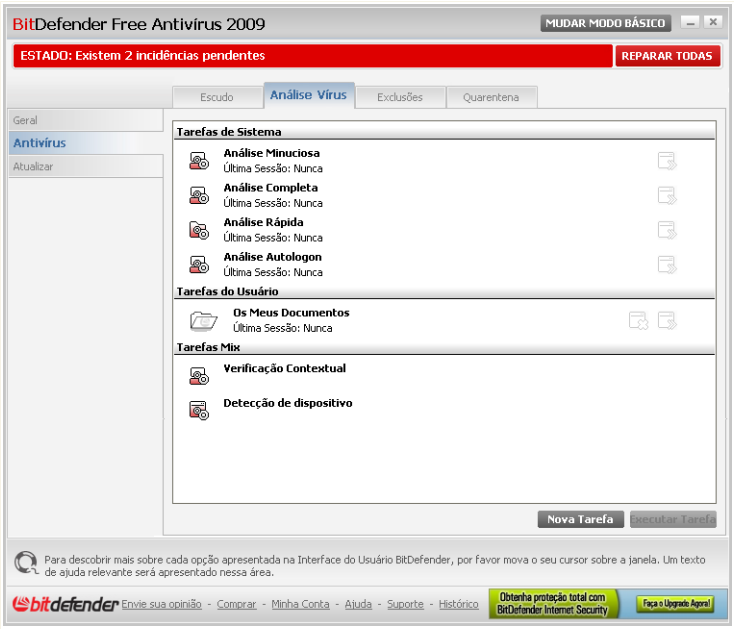
Desactivar Protecção em Tempo-real

Deverá confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a sua protecção em tempo-real fique desactivada. Pode desactivar a sua protecção 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 desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças do malware.

11.2. Análise A-pedido

Para configurar e iniciar uma análise on-demand, vá para**Antivírus>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. Pode analisar o computador sempre que desejar ao executar as tarefas de análise por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo usuário). Pode também agendá-las para que se executem numa base regular ou quando o sistema está sem ser usado de forma a não interferir com o seu trabalho

11.2.1. Tarefas de Análise

O BitDefender vem com diversas tarefas, criadas por defeito, 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. 60).

Existem três categorias de tarefas de análise:

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

Tarefa Padrão	*Descrição*
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Rápida do Sistema	Analisa as pastas `Windows`, `Programas` e `All Users`. 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 atrefas **Análise Minuciosa do Sistema** 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 inactivo.

- **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.

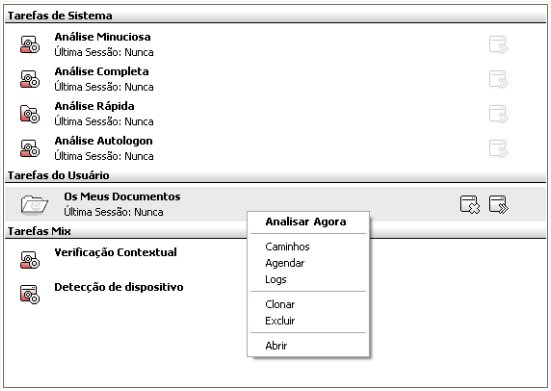
> ***Nota***
> Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **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.

11.2.2. 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 substituida por **Mostrar Caminho Tarefas**, onde apenas poderá ver o alvo da sua análise.

- **Agenda** - abre a janela **Propriedades**, AbsAgenda, onde você poderá agendar a tarefa selecionada.
- **Logs** - abre a janela **Propriedades**, AbaLogs, onde você pode ver os relatórios gerados após as tarefas selecionadas serem executadas.
- **Duplicar** - 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.

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

Nota
Devido à sua natureza em particular da categoria **Tarefas Misc**, somente as opções **Logs** e **Abrir** estarão disponíveis.

11.2.3. Criando Tarefas de Análise

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

- Duplique uma tarefa de análise, renomeia-a e faça as alterações necessárias na janela Propriedades;
- Clique em **Nova Tarefa** para criar uma nova tarefa e configurá-la.

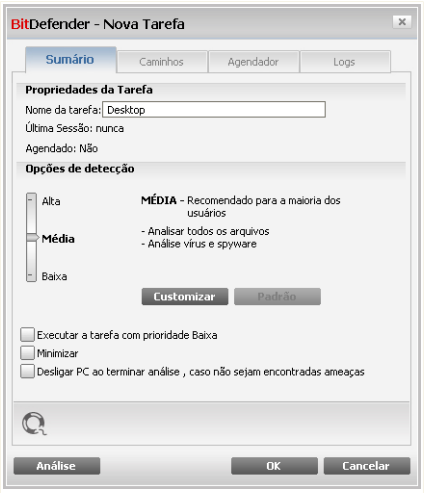
11.2.4. Configurar Tarefas de Análise

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 **Abrir** , localizado no lado direito da tarefa (ou faça clique-botão direito sobre a tarefa e depois faça clique em **Abrir**).

Nota
Para mais informação sobre ver os logs e a barra de **Logs** tab, por favor consulte "*Ver os Relatórios da Análise*" (p. 81).

Configurar Definições da Análise

Para configurar as opções de análise de uma específica tarefa de análise, faça clique-botão direito e seleccione **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 Protecção	*Descrição*
Baixo	Oferece uma eficiência razoável de detecção. O consumo de recursos é baixo. Programas são apenas analisados em busca de vírus. Para além da tradicional análise baseada em vacinas, a análise heurística também é utilizada.
Médio	Oferece uma boa eficiência de detecção. O nível de consumo de recursos é moderado.

Nível de Protecção	Descrição
	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.
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:

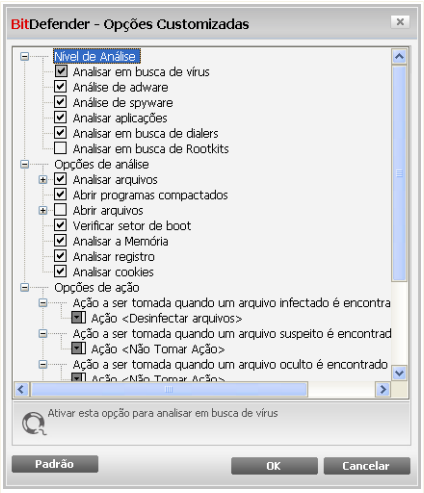
- **Executar a análise com Baixa prioridade.** Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação.
- **Minimizar na barra de ferramentas.** Minimiza a janela de verificação para a Área de notificação. Clique 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 em busca de ao seleccionar determinadas opções 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 afectar 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.

Opção	Descrição
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.
Analisa em busca de dialers	Procura aplicações de ligação para números de valor acrescentado. Estes arquivos serão tratados como arquivos infectados. O software que inclua componentes de ligação deste tipo poderá deixar de funcionar se esta opção estiver activa.
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 ";".

Opção	Descrição
Abrir programas compactados	Arquivos de backup acessados também serão verificados.
Abrir arquivos	Analisa dentro de arquivos comprimidos, como `.zip`, `.rar`, `.ace`, `.iso` e outros. Se você quiser pesquisar todos os tipos de arquivos (incluindo instaladores e arquivos .chm), você também tem que selecionar **Executar análise minuciosa**. Analisar arquivos comprimidos aumenta o tempo da análise e requer mais recursos do sistema. Pode clicar em **Limite de tamanho dos arquivos** e inserir o tamanho máximo em kilobytes (KB) dos arquivos a serem analisados.
Abrir arquivos de e-mails	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 a acção a tomar sobre cada categoria de arquivos detectados usando as opções da categoria **Opções de acção**.

Nota

Para definir uma nova acção, faça clique na actual acção e seleccione a opção desejada no menu. Se escolher ignorar os arquivos detectados ou se a acção escolhida falhar, terá de escolher uma acção no assistente de análise.

- Seleccione a acção a ser tomada sobre o arquivo infectado. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Acção	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.

- Seleccionar a acção a tomar sobre um arquivo suspeito. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo 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.

- Seleccionar a acção a ser tomada sobre os objectos ocultos (rootkits). As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Acção	Nenhuma acção 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 Acção	Apenas registrar arquivos infectados que foram criptografados pelo Windows. Após a analisar

Ação	Descrição
	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 Acção	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.
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.

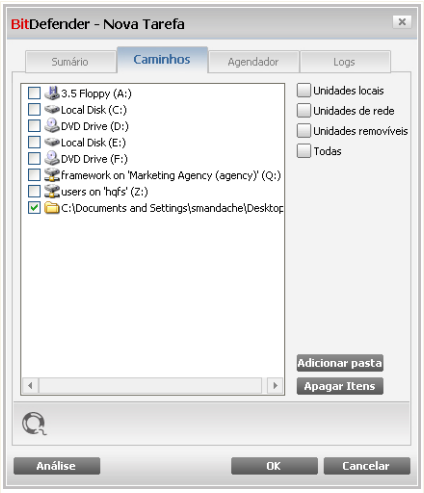
○ **Ação a executar quando um arquivo protegido por senha for encontrado .** Seleccione a ação a ser tomada sobre os arquivos detectados protegidos por senha. As seguintes opções estão disponíveis:

Ação	Descrição
Log não analisou	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 ver o alvo da análise de uma determinada tarefa de análise do sistema de um usuário específico, faça clique com o botão direito do mouse sobre a tarefa selecione **Mostrar Caminho da Tarefa**. 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 Itens** - abre uma janela onde você pode selecionar o(s) arquivo(s) / pasta (s) que deseja verificar.

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

- **Apagar item (ns)** - remove os arquivos/pastas que foram selecionados anteriormente na lista de objetos a serem verificados.

  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.

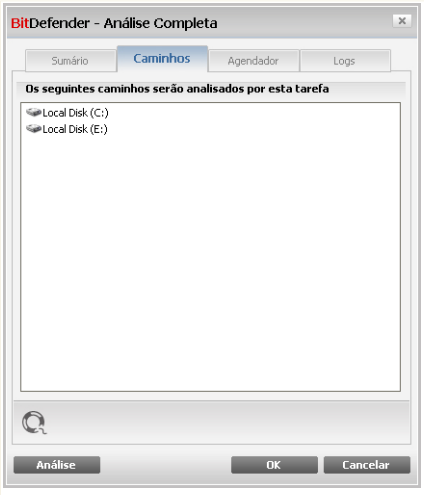
Nota
Se você quer verificar todo o seu computador contra vírus selecione a caixa correspondente a **Todas**.

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**. Por exemplo, para **Análise Completa do Sistema**, a seguinte janela irá aparecer:



Alvo da Análise da Análise Completa do Sistema

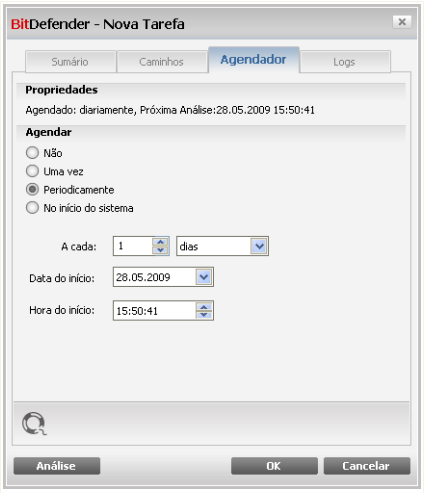
Análise Completa do Sistema e **Análise Minuciosa do Sistema** analisarão todas as drives locais, enquanto **Análise Rápida do Sistema** apenas analisará as pastas `Windows` e `Programas`.

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 determinada tarefa ou modificá-la, faça clique com o botão direito do mouse sobre a tarefa seleccione **Agendar Tarefa**. 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 verificação periodicamente, em determinados intervalos de tempo (horas, dias, semanas, meses, anos) começando com uma data e hora específica.

  Se você quer que a verificação se repita após certos intervalos, selecione a caixa de seleção correspondente a **Periodicamente** e digite na caixa **A cada** o número de minutos / horas / dias / semanas / anos em que você quer repetir esse processo. Deve de definir a data de início e a hora nos campos**Iniciar Data/Hora**.
- **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**.

11.2.5. 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 (como Análise Minuciosa ou Análise Completa) 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 o computador contra este tipo de malware, você pode agendar uma tarefa **Análise ao iniciar** para ser executada ao iniciar o sistema. 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 oferece três tipos de análise on-demand:

- 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 2009**.
- Verificação Arraste & Solte - arraste e solte um arquivo ou pasta sobre a Barra de Atividade;
- Análise manual - Use a Análise Manual do BitDefender para seleccionar directamente os arquivos ou pastas a serem analisados.

Verificação imediata

Para analisar o seu computador ou parte dele pode usar as tarefas de análise por defeito ou pode criar as suas próprias tarefas de análise. Isto denomina-se verificação imediata.

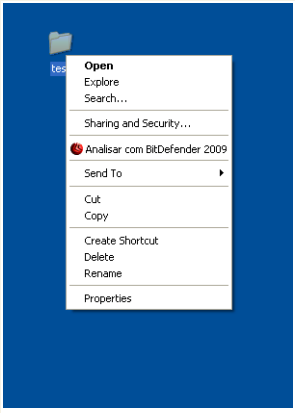
Para executar uma tarefa de análise, use um dos seguintes métodos:

- faça duplo-clique com o rato sobre a tarefa desejada da lista.
- clique no botão **Analisar agora** da correspondente tarefa.
- seleccione 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.



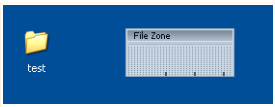
Verificação Contextual

Clique com o botão direito do mouse sobre o objeto que você deseja analisar e selecione a opção **Analisar com o BitDefender 2009**. O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

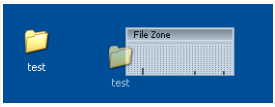
Pode modificar as opções de análise e ver os relatórios ao aceder à janelas das **Propriedades** da tarefa **Análise de Menu Contextual**.

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

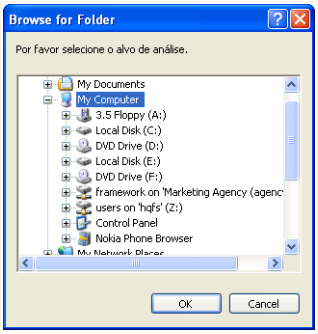
O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.

Verificação Manual

A análise manual consiste em selecionar directamente 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 seleccionar o objecto a ser analisado por BitDefender, no menu Iniciar do Windows, siga o seguinte caminho **Iniciar** → **Programas** → **BitDefender 2009** → **Análise Manual BitDefender**. A seguinte análise irá aparecer:



Verificação Manual

Escolha o objecto que deseja analisar e clique **OK**. 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:

- **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.

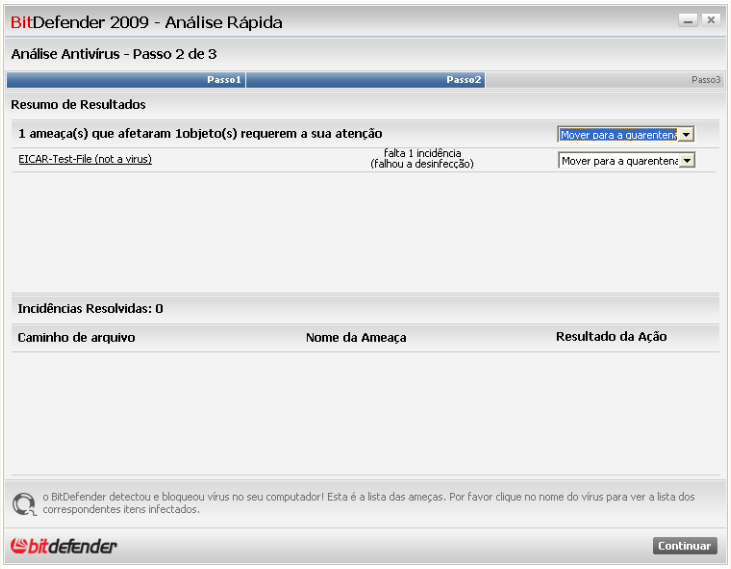
- **Não desejo digitar uma senha para esse objeto.** Selecione essa opção para pular a análise desse arquivo.
- **Não desejo digitar a senha para qualquer objeto (pular todos os objetos protegidos por senha).** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha. 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 directamente 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 - Seleccionar as acções

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.

Pode escolher uma acção geral a ser levada a cabo para todas as incidências ou pode escolher acções separadas para cada grupo de incidências.

Uma ou várias das seguintes opções podem aparecer no menu:

Ação	*Descrição*
Não Tomar Acção	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 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.

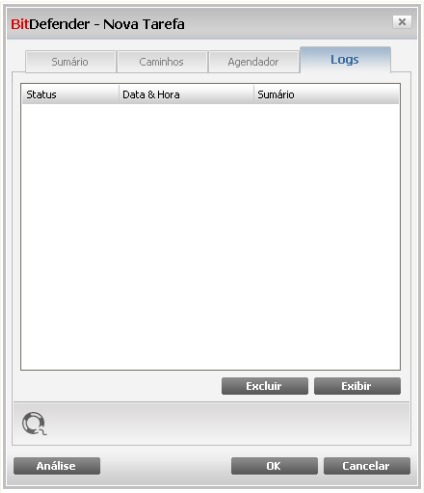
BitDefender Detectou Arquivos Suspeitos

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.

11.2.6. 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.

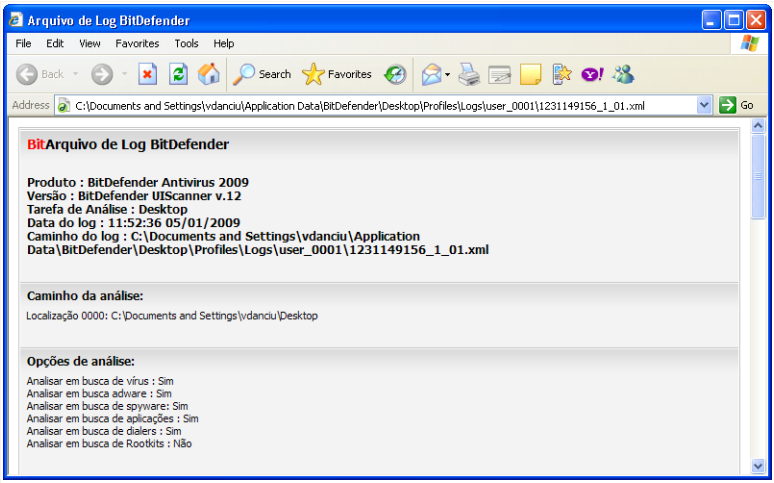
Nota

Também, para ver ou apagar um arquivo, faça duplo-clique com o rato sobre o arquivo e seleccione 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.

11.3. 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.

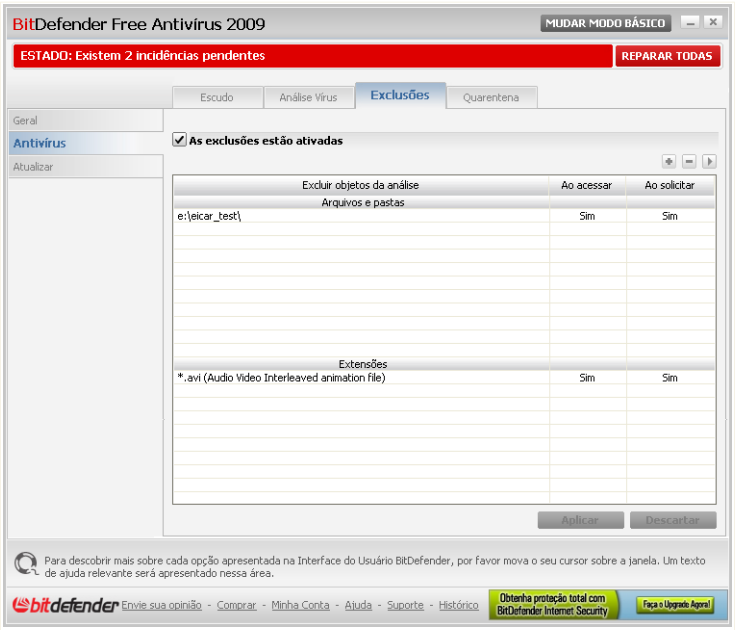
Dois tipos de objectos podem ser excluidos da análise:

- **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 objectos excluídos da análise a-pedido não serão analisados, independentemente de eles serem acedidos por si ou por uma aplicação.

Para ver os objectos excluídos da análise, vá para **Antivírus>Excepções** 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 avulsa: Você da um clique com o botão direito do mouse no arquivo ou diretório que pretende verificar e seleciona **Analisar com o BitDefender 2009**.

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

Para editar uma entrada da lista, seleccione-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**.

11.3.1. 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.

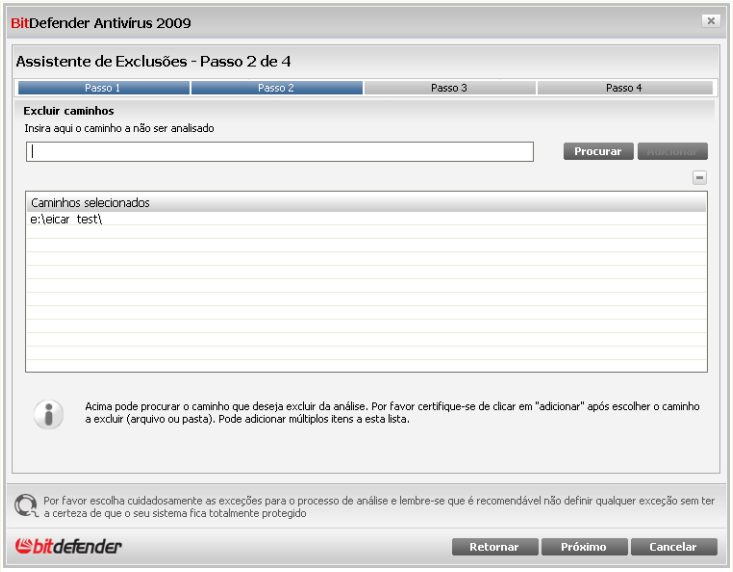
Passo 1/4 - Seleccionar o Tipo de Objecto

Tipo de Objecto

Seleccione 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**.

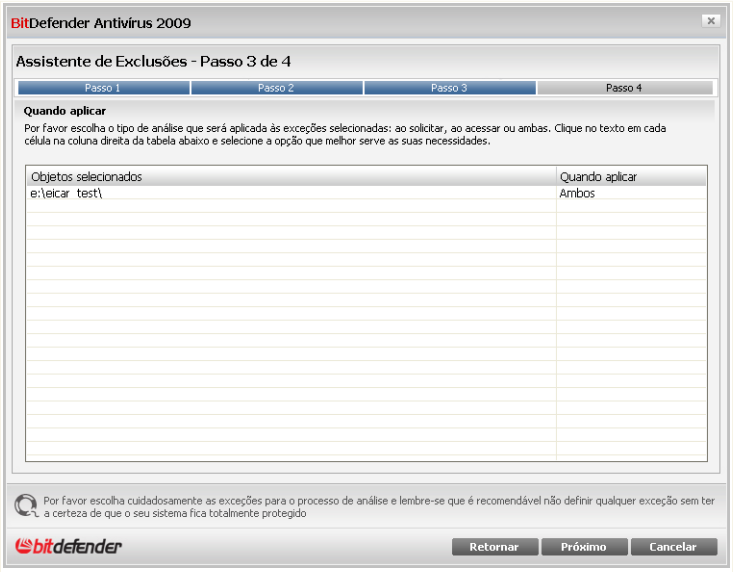
> ***Nota***
> Se o caminho inserido não existe, uma mensagem de erro surgirá. Clique em **OK** e verifique se o caminho é válido ou não.

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.

Por defeito, os caminhos seleccionados são excluídos da análise no-acesso e a-pedido. Para alterar isto, clique na coluna à direita e seleccione 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**.

Clique em **Aplicar** para salvar as modificações.

11.3.2. 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.

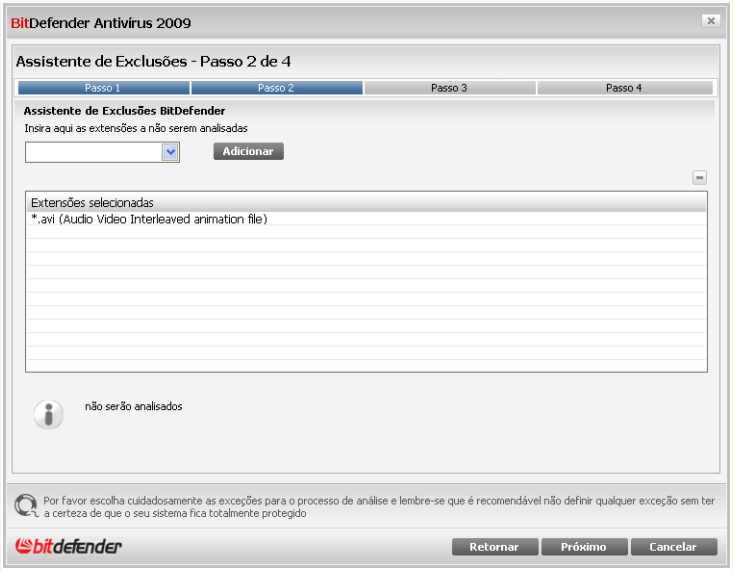
Passo 1/4 - Seleccionar o Tipo de Objecto

Tipo de Objecto

Seleccione a opção de excluir uma extensão 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:

- Seleccione 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.

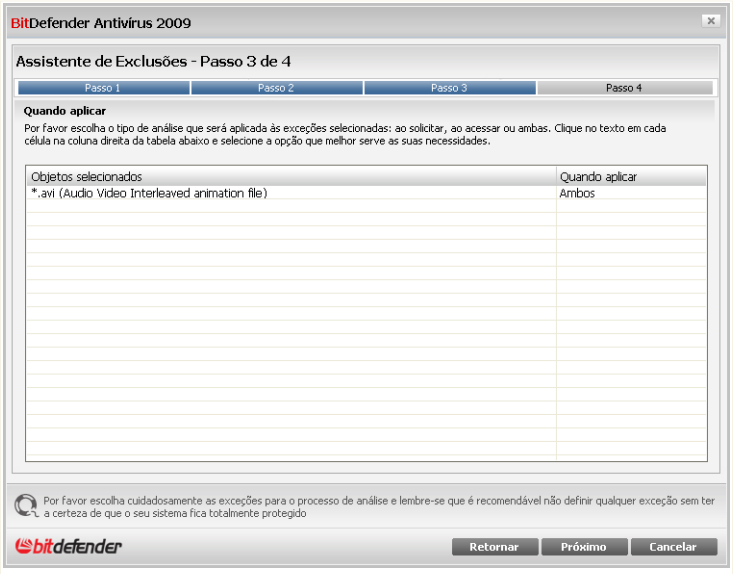
- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

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.

Por defeito, as extensões seleccionadas são excluidas da análise no-acesso e a-pedido. Para alterar isto, clique na coluna da direita e seleccione 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**.

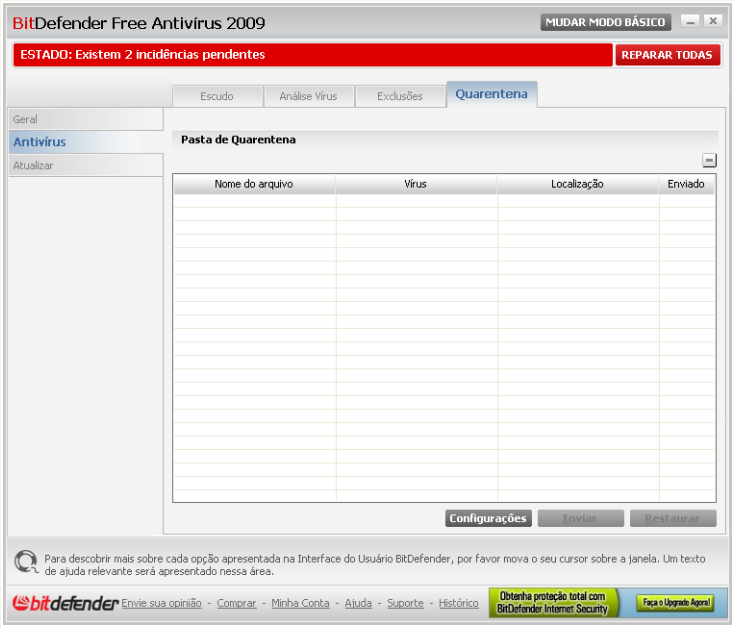
Clique em **Aplicar** para salvar as modificações.

11.4. 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 ver e gerir os arquivos em quarentena e configurar as definições da quarentena, 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.

11.4.1. Gerir arquivos em Quarentena

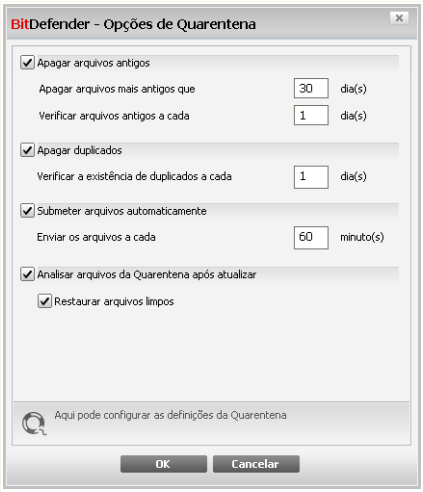
Pode enviar qualquer arquivo selecionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**. Por defeito o BitDefender envia automaticamente os arquivos em quarentena a cada 60 minutos.

Para apagar um arquivo selecionado da lista de quarentena clique no botão **Remover** . Se deseja restaurar o arquivo selecionado para a sua localização original clique em **Restaurar**.

Menu contextual. Está disponível um menu contextual, que lhe permite gerir facilmente os arquivos em quarentena. As mesmas opções mencionadas previamente estão disponíveis. Pode também selecionar **Actualizar** para atualizar a seção de Quarentena.

11.4.2. 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.

Apagar 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
Por defeito, o BitDefender irá verificar arquivos duplicados na quarentena a cada dia.

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
Por defeito 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.

12. 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 está conectado à internet através de banda larga ou ADSL, BitDefender cuidará disto por sí só. Ele checará por atualizações ao ligar seu computador e depois disso a cada **24 horas**.

Se uma actualização é detectada, poderá ser notificado para confirmar a actualização ou a mesma é levada a cabo automaticamente, dependendo das definições automáticas da actualização.

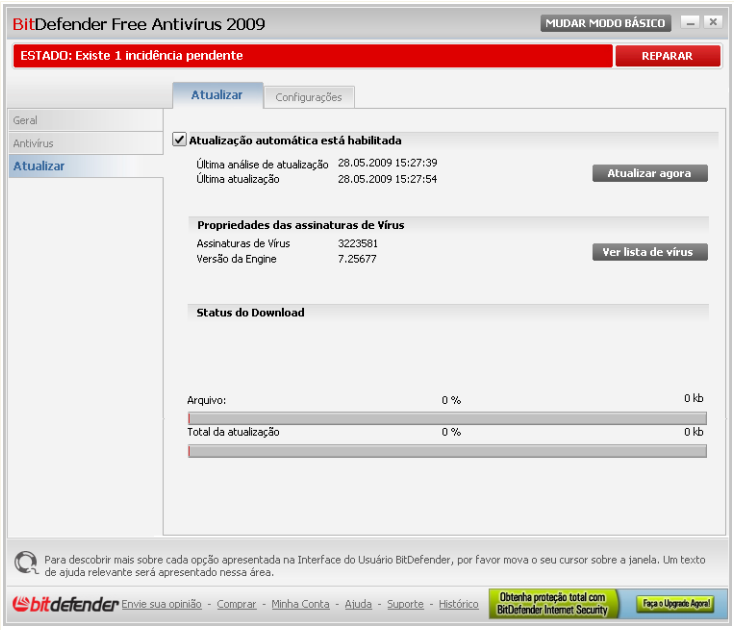
O processo de atualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

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**.

12.1. Atualização Automática

Para ver informação relacionada com actualizações e executar actualizações automáticas, clique em **Actualização>Actualização** 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 secção durante uma actualização, poderá o estado do download.

Importante
Para estar protegido contra as mais recentes ameaças mantenha a **Actualização Automática** activada.

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 browser da internet. Pode procurar uma assinatura específica de malware por entre a base de dados ou clicar **Lista de Vírus BitDefender** para aceder à base de dados de assinaturas BitDefender on-line.

12.1.1. Solicitar uma Actualização

A atualização automática também pode ser feita a qualquer hora clicando em **Atualizar Agora**. Também conhecido por **Atualização a pedido do usuário**.

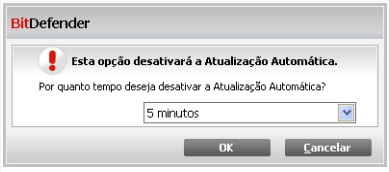
O módulo de **Atualização** irá conectar ao servidor de atualização do BitDefender e verificará se uma atualização está disponível. Caso seja verdadeiro, dependendo das opções configuradas na seção Opções de Atualização Manual você será indagado a confirmar a atualização ou a mesma será feita automaticamente.

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.

12.1.2. Desabilitar Atualização Automática

Se você desabilitar a atualização automática, uma janela de alerta aparecerá.



Desabilitar Atualização Automática

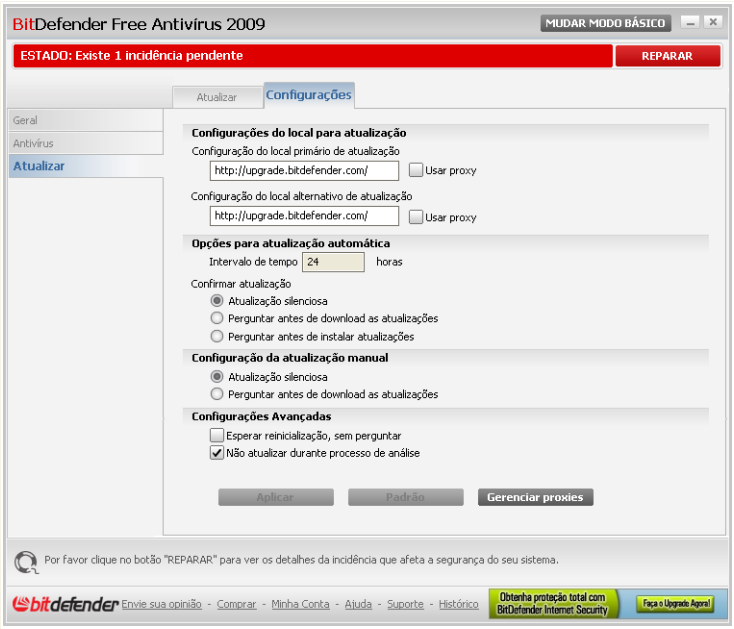
Tem de confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a actualização automática fique desactivada. Pode desactivar a actualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Importante
Se o BitDefender não estiver atualizado, não poderá detectar os malwares mais recentes quando efetuar uma análise de seu computador.

12.2. Atualizar as Configurações

Atualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy.

Para configurar as definições de actualização e gerir proxies, clique em **Actualização>Configuração** no Modo Avançado.



Atualizar as Configurações

As configurações da actualização estão agrupadas em 4 categorias (**Configuração da Localização da Actualização**, **Configuração de actualização automática**, **Configuração de Actualização Manual** e **Configuração Avançada**). Cada categoria será descrita separadamente.

12.2.1. Definir local para atualização

Para definir a localização da actualização, use as opções da categoria **Configuração da Localização da Actualização** .

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 primário** e uma **Local de atualização alternativo**. Por defeito estas localizações são iguais:`http://upgrade.bitdefender.com`.

Para modificar um dos locais de actualização, insira o URL do local mirror no campo **URL** que corresponde ao novo local para o qual deseja mudar.

Nota
Recomendamos que defina como local primário de actualização o local mirror e deixar o local alternativo de actualização como está, como um plano de backup em caso do local mirror ficar indisponível.

No caso em que a empresa usa um servidor proxy para se ligar à Internet, seleccione **Usar proxy** de depois clique em **Gerir proxies** para configurar as definições do proxy. Para mais informação, por favor consulte "*Gerir Proxies*" (p. 101)

12.2.2. Configurar Atualização Automática

Para configurar o processo de actualização automática do BitDefender, use as opções na categoria **Configuração Actualização Automática** .

BitDefender checará por atualizações a cada 24 horas através da internet e instalará as atualizações disponíveis sem avisá-lo. Você não poderá mudar o intervalo de checagem das atualizações.

Para definir como é que o processo de actualização automática tem de ser feito, seleccione 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.

12.2.3. 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 actualização 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.

12.2.4. Configurar Opções Avançadas

Para evitar que o processo de actualização 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 actualizar se a análise estiver a decorrer** - O BitDefender não vai actualizar se estiver a decorrer uma análise. Desta forma, o processo de actualização do BitDefender não vai interferir com as tarefas de análise.

Nota
Se o BitDefender for actualizado enquanto a análise estiver a decorrer, o processo de análise será cancelado.

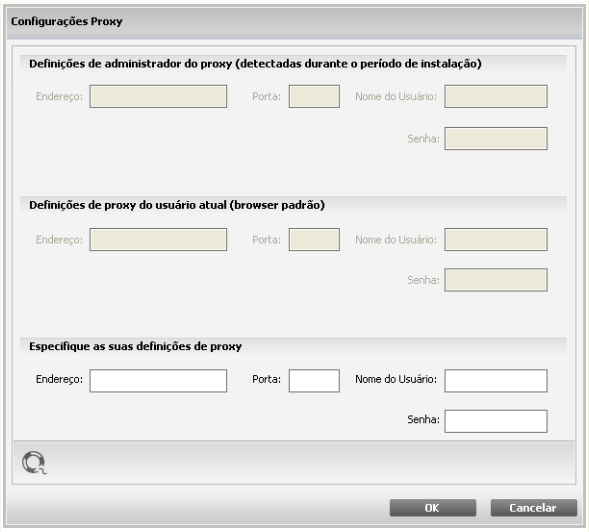
12.2.5. Gerir Proxies

Se a sua empresa usa um servdior proxy para se ligar à Internet, deverá especificar as definições do proxy de forma a que o BitDefender se atualize sozinho. De outra forma, usará as definições do administrador que instalou o produto ou o usuário atual por defeito do browser, caso haja algum.

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 gerir as definições do proxy, clique em **Gerir proxies**. A janela **Gestor Proxy** irá aparecer.



Gestor Proxy

Existem três categorias de definições de proxy:

- **Definições de proxy de administrador (detectados durante o período de instalação)** - as definições de proxy detectadas da conta de administrador durante a instalação e que podem ser configuradas apenas se estive logged com essa conta. Se o servidor proxy requer um nome de usuário e uma senha, deverá inseri-los nos campos correspondentes.
- **Definições de proxy do usuário atual (do browser por defeito)** - as definições de proxy do usuário atual, extraidas do explorador por defeito. Se o servidor proxy requer um nome de usuário e uma senha, deverá inseri-los nos campos correspondentes.

Nota
Os browsers de internet suportados são o Internet Explorer, Mozilla Firefox e Opera. Se utiliza outro explorador por defeito, o BitDefender não será capaz de obter as definições do proxy do atual usuário.

- **O seu próprio conjunto de definições de proxy** - definições de proxy que pode configurar se estiver logged in 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 ligar a 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 serã retiradas do seu browser por defeito e usadas para obter a ligação 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.

Como proceder

13. Como ativar o BitDefender

Para ativar o produto, você deve criar uma conta no BitDefender. BitDefender lhe avisará para criar uma conta na primeira vez que você reiniciar seu computador após ter sido instalado. Se você não criar uma conta neste momento, você precisa ativar o BitDefender mais tarde, da seguinte forma:

1. Abra o BitDefender. Você pode usar o  menu Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2009** → **BitDefender Free Antivírus 2009**, ou clique duas vezes no ícone na barra de ferramentas do sistema.
2. Clique **Conserte todos os problemas/Conserte este problema**. Uma nova janela irá aparecer.
3. Clique no botão **Consertar** correspondente ao problema **O produto não está ativado**.
4. Clique **Sim**. Uma nova janela irá aparecer.
5. Selecione **Criar uma nova conta BitDefender** e preencha as informações requisitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   - **Endereço de E-mai** - digite o seu endereço de e-mail. Uma mensagem de e-mail de confirmação da conta será enviado para este endereço de e-mail, logo que a sua conta for criada.
   - **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 definida anteriormente.
   - **Primeiro nome** - digite o seu primeiro nome.
   - **Último nome** - digite o seu último nome.
   - **País** - selecciona o país onde reside.
6. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Escolha uma das seguintes opções:
   - **Enviem-me todas as mensagens da BitDefender**
   - **Enviem-me apenas as mensagens mais importantes**
   - **Não me enviem quaisquer mensagens**

7. Clique em **Finalizar** para enviar as informações fornecidas e criar sua conta BitDefender.
8. Clique em **OK** para confirmar que você irá ativar sua conta.
9. **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.

Após a ativação, você pode clicar no link **Minha Conta** para logar em sua conta. O link está localizado no canto inferior direito da tela do BitDefender.

Importante

Você precisa criar sua conta dentro de 15 após a instalação do BitDefender. Se você não criar uma conta BitDefender em tempo hábil, o BitDefender deixará de receber as atualizações regulares de vacina contra malwares. Se as assinaturas contra malwares estiverem desatualizadas, BitDefender poderá não estar apto a detectar qualquer malware.

14. 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. 23).

14.1. 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 2009** 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.

14.2. 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 (Modo Básico ou Modo Avançado), diferentes etapas devem ser seguidas para executar a tarefa de análise.

Executando a Tarefa de Análise em Modo Básico

No Modo Básico, você pode executar apenas um número pré configurado de tarefas de análise. Siga esses passos pra executar uma tarefa de análise no Modo Básico:

1. Clique na aba **Antivírus**.
2. No lado direito, em **Tarefas**, clique na tarefa de análise que você deseja executar. Essas são as tarefas de análise disponíveis:

Tarefa de Análise	*Descrição*
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o 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.

3. Siga o assistente de análise Antivírus para concluir a análise.

Executando as 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

customizadas 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 do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
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.

14.3. 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:

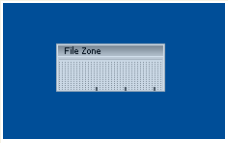
1. No Menu Iniciar, siga o caminho **Iniciar** → **Programas** → **BitDefender 2009** → **Análise Manual BitDefender**. Uma nova janela irá aparecer.
2. Selecione o alvo da análise:
   - Para analisar sua Área de trabalho, selecione **Área de trabalho**.
   - Para analisar uma partição inteira do disco rígido, selecione-a a partir do Meu Computador.
   - Para analisar um diretório específico, procure e selecione o respectivo diretório.
3. Clique em **OK** para iniciar a análise.
4. 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.

14.4. Utilizando a Barra de Atividade da Análise



Barra de Actividade da Análise

A **Barra de atividade de verificação** é uma visualização gráfica da atividade de verificação em seu sistema. Essa pequena janela só está disponível quando a interface está em Visualização Avançada.

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 Actividade da Análise*" (p. 18).

15. 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. Você pode usar o  menu Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2009** → **BitDefender Free Antivírus 2009**, ou clique duas vezes no ícone na barra de ferramentas do sistema.
2. Se a interface está em Modo Básico de visualização, clique no botão **Mudar Modo Avançado**, localizado no canto superior direito da janela.
3. Clique em **Antivírus** no menu do lado esquerdo.
4. 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 do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Rápida do Sistema	Analisa os diretórios do `Windows` e dos `Arquivos de Programas`. Na configuração padrão, analisa

Tarefa Padrão	Descrição
	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 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.

5. Clique com o botão direito do mouse na tarefa de análise e selecione **Agendar**. Uma nova janela irá aparecer.
6. 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`.

7. 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.

Contato

16. 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.

16.1. Endereços Web

Departamento de Vendas: sales@bitdefender.com
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
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

16.2. 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.

16.2.1. E.U.A

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefone (escritório&vendas): 1-954-776-6262
Vendas: sales@bitdefender.com
Página da Web http://www.bitdefender.com

16.2.2. Alemanha

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Escritório: +49 2301 91 84 222
Vendas: vertrieb@bitdefender.de
Página da Web http://www.bitdefender.de

16.2.3. 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
Página da Web http://www.bitdefender.co.uk

16.2.4. Espanha

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefone +34 902190765
Vendas: comercial@bitdefender.es
Website: http://www.bitdefender.es

16.2.5. 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
Website: http://www.bitdefender.ro

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 compactado.

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 uma aplicação que permite a você 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 compactados

Um arquivo em formato compactado. Muitos sistemas operacionais e programas contêm comando que permitem a você compactar 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 compactados 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 uma aplicação pode ser um item para inicializar.

Barra de tarefas

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 uma aplicação benigna. Ao contrário do vírus, um cavalo de tróia não se replica mas pode ser muito destrutivo. Uma dos tipos mais incidentes de cavalos de tróia é um programa que diz se livras 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.