bitdefender

TOTAL SECURITY 2009

Guia de usuário

bitdefender

BitDefender Total Security 2009

Guia de usuário

Publicado 2009.01.05

Nota Legal

bitdefender

Índice

Acordo de Licença de Software para Usuários Finais

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

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

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

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

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

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

CONCESSÃO DE LICENÇA. Pela presente, a BITDEFENDER concede-lhe a si, e apenas a si a seguinte licença não-exclusiva, limitada, não-transmissível e passível de 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 da aquisição do BitDefender e expira no final do período para o qual a licença foi adquirida.

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

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

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

modificar, traduzir, ou fazer qualquer tentativa para descobrir a fonte do código do BitDefender.

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

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

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

ALGUNS ESTADOS NÃO PERMITEM A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE POR DANOS INCIDENTAIS OU ACIDENTAIS

CONSEQUENTES DO USO OU TESTE DAS SOLUÇÕES BITDEFENDER, PORTANTO A LIMITAÇÃO ACIMA OU EXCLUSÃO PODERÁ NÃO SE APLICAR A VOCÊ.

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

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

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

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.

Preços, custos e taxas para uso do BitDefender poderão ser alterados sem aviso.

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

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

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

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

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

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

Prefácio

Este manual é dirigido a todos os usuários que escolheram **BitDefender Total Security 2009** como a solução de segurança para o seu computador pessoal. A informação apresentada neste manual é útil e acessível para todas as pessoas que trabalham com o sistema operacional Windows, independentemente do seu nível de conhecimento de informática.

Este manual dá-lhe uma descrição completa do **BitDefender Total Security 2009**, da Empresa e da equipa que o desenvolveu, também irá guiá-lo através do processo de instalação, e explicar-lhe como o pode configurar. Irá ficar a saber como usar o **BitDefender Total Security 2009**, como o actualizar, testar e personalizar. Em resumo, irá ficar a saber como tirar partido do melhor que o BitDefender tem para lhe oferecer.

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.
support@bitdefender.com	Mensagens de e-mail são inseridas no texto para informação sobre contato.
“Prefácio” (p. xvii)	Esta é uma referência interna, a algum lugar dentro do documento.
`filename`	Arquivos e pastas são impressos em caracteres do tipo `monospaced`.

Aparência	Descrição
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 passo a passo para a instalação do BitDefender numa estação de trabalho. Este é um manual bastante completo de instruções sobre como instalar e usar **BitDefender Total Security 2009**. Começando pelos requisitos necessários para uma instalação bem-sucedida, é guiado de seguida através de todo o processo de instalação. No final, é-lhe apresentado o procedimento de remoção para o caso de necessitar desinstalar o BitDefender.

Administração básica. Descrição da administração e manutenção inicial do BitDefender

Administração Avançada. Uma apresentação detalhada das capacidades de segurança providas pelo BitDefender. É ensinado sobre como configurar e usar todos os módulos BitDefender de forma a proteger efectivamente o seu computador contra todo o tipo de ameaças (malware, spam, hackers, conteúdo inapropriado e por aí fora).

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

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

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

3. Convite a Comentários

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

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

Importante

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

Instalação

1. Requisitos de Sistema

Só pode instalar o BitDefender Total Security 2009 nos computadores que tenham os seguintes sistemas operativos:

- 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)
- 210 MB de espaço disponível em disco (recomendável 250 MB)

Para Windows Vista

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- 210 MB de espaço disponível em disco (recomendável 250 MB)

Para Windows Home Server

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- 210 MB de espaço disponível em disco (recomendável 250 MB)

1.2. Requisitos de Software

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

A protecção antiphising está disponível apenas para:

- Internet Explorer 6.0 (ou superior)
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

Encriptação para Instant Messaging (IM) está disponível para:

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

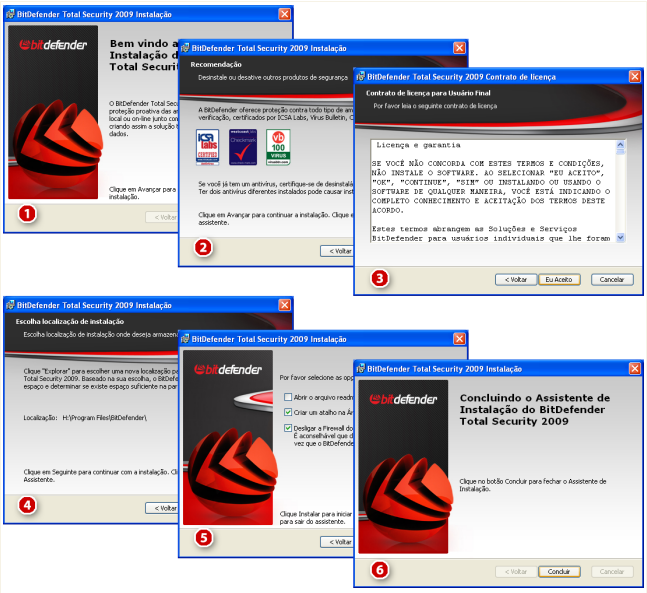
A protecção Antispam é fornecida para todos os clientes de e-mail POP3/SMTP. No entanto a barra de ferramentas do Antispam BitDefender apenas se integra em:

- Microsoft Outlook 2000 / 2002 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 1.5 e 2.0

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 Total Security 2009:

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

   BitDefender Total Security 2009 avisa-o em caso de ter outro produto 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 Total Security 2009 será instalado em `C:\Programas\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.
   - **Colocar um atalho no ambiente de trabalho** - para colocar um atalho do BitDefender Total Security 2009, no seu ambiente de trabalho, 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.
   - **Desligar a Firewall do Windows** - para desligar a Firewall do Windows.

Importante

Recomendamos que desligue a Firewall do Windows uma vez que BitDefender Total Security 2009 já inclui uma firewall avançada. Executar 2 firewalls no mesmo computador poderá causar problemas.

- **Desligar o Windows Defender** - para desligar o Windows Defender; esta opção apenas surge no Windows Vista.

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

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.

Importante

Após completar a instalação e reiniciar o computador, aparecerá um assistente de registo e um assistente de configuração . Complete estes assistentes de forma a registar e configurar o BitDefender Total Security 2009 e criar uma conta BitDefender.

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`.

2.1. Assistente de Registro

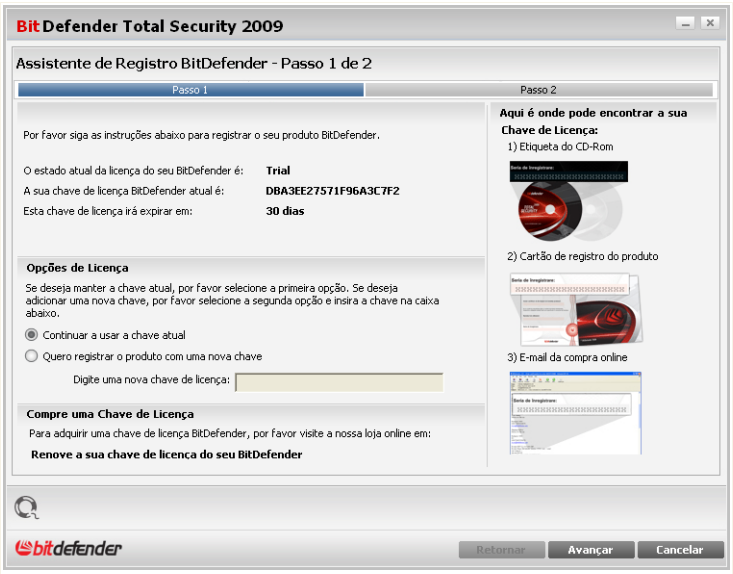
A primeira vez que iniciar o seu computador após a instalação um assistente de registo irá aparecer. O assistente ajuda-o a registar o seu BitDefender e a configurar uma conta BitDefender.

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

Nota

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

2.1.1. Passo 1/2 - Registar o BitDefender Total Security 2009



Registro

Pode ver o estado do registo do BitDefender, a actual chave de licença e quantos dias faltam para a licença expirar.

Para continuar a avaliar o produto, selecione **Continuar a avaliar o produto**.

Para registar o BitDefender Total Security 2009:

1. Seleccione **Desejo registar o produto com uma nova chave**.
2. Insira a chave de licença no campo de edição.

Nota

Pode encontrar a sua chave de licença:

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

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

Clique em **Seguinte** para continuar.

2.1.2. Passo 2/2 - Criar uma conta BitDefender

Criar uma Conta

Se não deseja criar uma conta BitDefender neste momento, seleccione **Saltar o registo** e clique em **Terminar**. De outra forma, actue de acordo com a sua presente situação:

- “Não tenho uma conta BitDefender” (p. 9)
- “Já tenho uma conta BitDefender” (p. 9)

Importante

Você precisa se registrar criando uma conta dentro de 15 dias após ter instalado BitDefender (se você o fizer, o prazo limite se extenderá para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus.

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 pelo menos seis caracteres em 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.

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**

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.

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**

Clique em **Finalizar**.

2.2. Assistente de Configuração

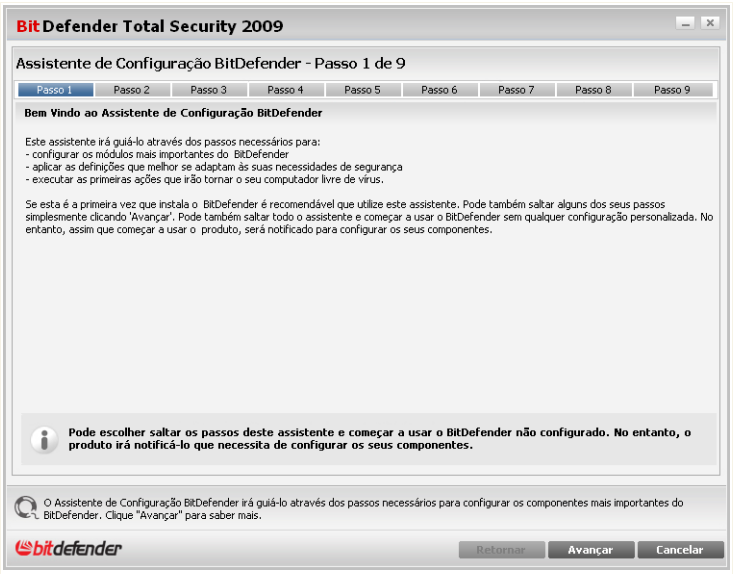
Um vez completado o asssitente de registo, aparecerá o assistente de configuração. O assistente ajuda-o a configurar os módulos específicos do produto e a preparar o BitDefender para executar tarefas de segurança muito importantes.

Completar a acção do assistente não é obrigatória; no entanto, recomendamos que a termine de forma a poupar tempo e a assegurar que o seu sistema fica seguro ainda antes do BitDefender Total Security 2009 estar instalado.

Nota

Se você não quer seguir este assistente, clique em **Cancelar**. BitDefender irá notificá-lo sobre os componentes que necessita de configurar quando abrir o interface do usuário.

2.2.1. Passo 1/9 - Janela Boas-vindas



Janela de Boas-Vindas

Clique em **Seguinte** para continuar.

2.2.2. Passo 2/9 - Escolher Modo de Visão

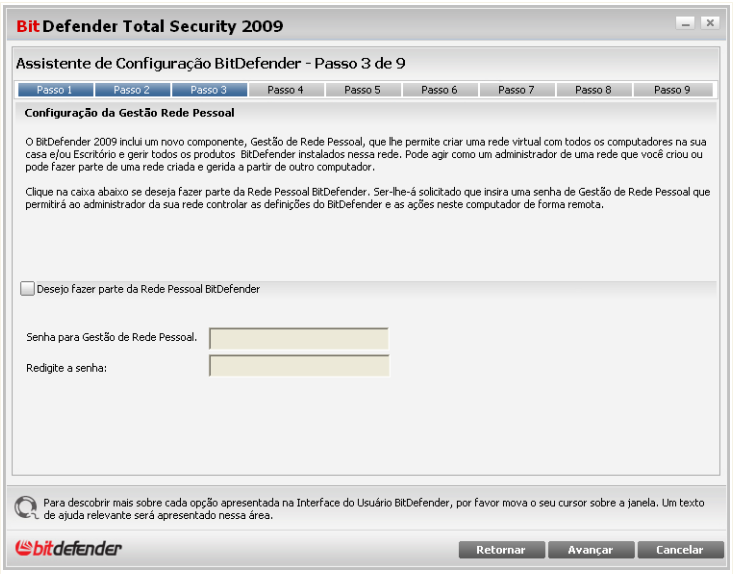
Modos de Visão

Escolha entre dois modos de visão do interface do utilizador dependendo da sua experiência como usuário do BitDefender:

- **Modo Básico.** Interface simples adequado para principiantes e a usuários que querem levar a cabo tarefas básicas e resolver problemas facilmente. Apenas tem de seguir os avisos e alertas do BitDefender e reparar as incidências que aparecerem.
- **Modo Avançado.** Interface avançado adequado a usuários mais técnicos que querem configurar totalmente o produto a seu gosto. Pode configurar cada componente do produto e levar a cabo tarefas avançadas.

Clique em **Seguinte** para continuar.

2.2.3. Passo 3/9 - Configurar a Rede BitDefender



Configuração da Rede BitDefender

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

Se deseja que este computador faça parte da rede Pessoal BitDefender, siga estes passos:

1. Seleccione**Quero fazer parte da rede Pessoal BitDefender**.
2. Insira a mesma senha administrativa em cada um dos campos de edição.

Importante

A senha permite ao administrador gerir os produtos BitDefender noutro computador.

Clique em **Seguinte** para continuar.

2.2.4. Passo 4/9 - Configurar o Controle de Identidade

Configuração do Controle de Identidade

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

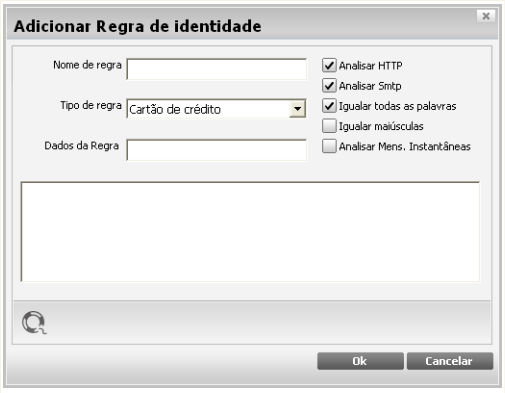
Se deseja usar Controle de Identidade, siga estes passos:

1. Selecionar **Eu desejo configurar agora** .
2. Criar regras para proteger a sua informação sensível. Para mais informação, por favor consulte o “Criar Regras de Controle de Identidade” (p. 15).
3. Se necessário, defina excepções específicas para as regras que criou. Para mais informação, por favor consulte o “Definir Excepções do Controle de Identidade” (p. 16).

Clique em **Seguinte** para continuar.

Criar Regras de Controle de Identidade

Para criar uma regra de Controle de Identidade, clique **Adicionar**). A janela de configuração irá aparecer.



Regra de Controle de Identidade

Deve definir os seguintes parâmetros:

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

> ***Nota***
> Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

De forma a facilmente identificar a informação que a regra bloqueou, forneça uma descripção detalhada da descripção da regra na caixa de edição.

Para especificar o tipo de tráfego a ser analisado, configure estas opções:

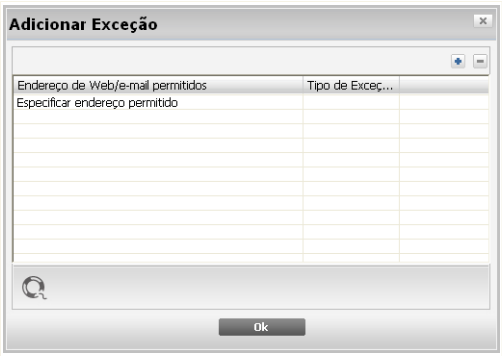
- **Analisar HTTP** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar SMTP** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
- **Analisar Mensagens Instantâneas** - analisa todo o tráfego Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

Clique **OK** para adicionar a regra.

Definir Excepções do Controle de Identidade

Há casos em que necessita de definir excepções para especificar as regras de identidade. Consideremos o caso em que criou uma regra que evita que o número do seu cartão de crédito seja enviado por HTTP (web). Sempre que o seu cartão de crédito seja submetido num site web a partir da sua conta de utilizador, a respectiva página web é bloqueada. Se deseja por exemplo, pagar uma compra online numa loja virtual (que você sabe ser segura), terá de especificar uma excepção para a respectiva regra.

Para abrir a janela onde pode gerir as excepções, clique em **Excepções**.



Excepções do Controle de Identidade

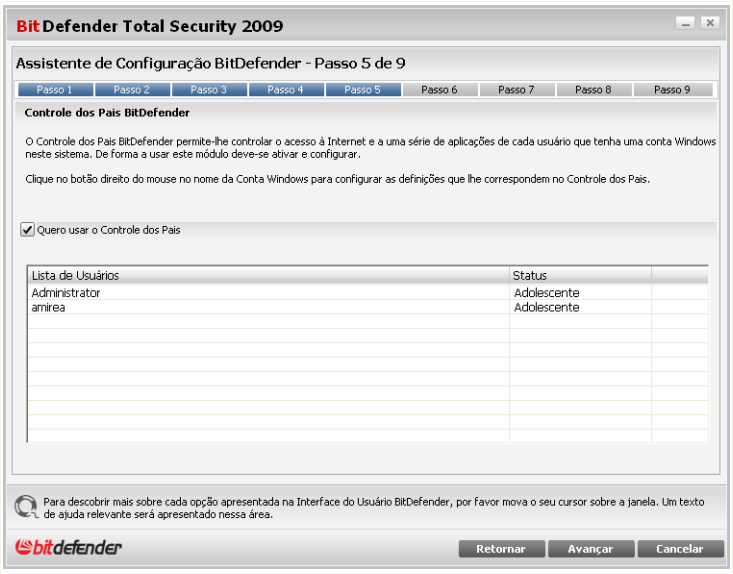
Para adicionar uma excepção, siga os seguintes passos:

1. Clique no botão **Adicionar** para adicionar a nova entrada à tabela.
2. Duplo-clique em **Especificar endereço permitido** e inserir o endereço web ou endereço de e-mail que deseja adicionar como excepção.
3. Duplo-clique em**Escolher Tipo** e escolha do menu a opção correspondente ao tipo de endereço que inseriu anteriormente.
   - Se especificou um endereço web, seleccione **HTTP**.
   - Se especificou um endereço de e-mail, seleccione**SMTP**.

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

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

2.2.5. Passo 5/9 - Configurar o Controle dos Pais



Configuração do Controle dos Pais

O Controle dos Pais BitDefender permite-lhe controlar o acesso à Internet e a determinadas aplicações para cada conta de usuário no sistema.

Se deseja usar o Controle dos Pais, siga estes passos:

1. Selecione **Quero usar o Controle dos Pais**
2. Clique botão direito do mouse no nome de cada conta do Windows e selecione o perfil do Controle dos Pais a ser aplicado.

Perfil	*Descrição*
Criança	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para usuários menores de 14. São bloqueadas as páginas web com um potencial conteúdo prejudicial para as crianças (porno, sexualidade, drogas, hacking, etc.).
Adolescente	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para usuários entre os 14 e os 18 anos de idade. São bloqueadas as páginas web com um conteúdo sexual, pornográfico ou adulto.
Adulto	Oferece um acesso sem restrições a todas as páginas web independentemente do seu conteúdo.

Nota

Para configurar totalmente ou desativar o Controle dos Pais para uma determinada conta do Windows, mude para o Modo Avançado e vá para Controle dos Pais. Pode configurar o Controle dos Pais para bloquear:

- Páginas web inapropriadas.
- ligação à Internet, durante determinados períodos de tempo (tal como o período de estudo).
- páginas web, mensagens de e-mail e mensagens instântaneas que contenham determinadas palavras-chave.
- aplicações tais como: jogos, programas de partilha de arquivos e outros.
- mensagens instântaneas enviadas por contacto IM para além dos que estão permitidos.

Clique em **Seguinte** para continuar.

2.2.6. Passo 6/9 - Configurar Relatório de Vírus

Opções do Relatório de Vírus

O BitDefender pode enviar anonimamente relatórios dos vírus que foram encontrados no seu computador para o Laboratório da BitDefender de forma a ajudar-nos a rastrear os surtos de vírus.

Você pode configurar uma das seguintes opções:

- **Enviar relatórios de vírus** - envia a BitDefender relatórios com os vírus identificados em seu computador. .
- **Activar Detecção de Surtos BitDefender** - envia relatórios de potenciais surtos de vírus para o Laboratório da BitDefender.

Nota
O relatório não contém dados confidenciais, tais como seu nome, endereço de IP ou outros, e não será usado para propósitos comerciais.

Clique em **Seguinte** para continuar.

2.2.7. Passo 7/9 - Seleccionar as Tarefas a Serem Executadas

Seleção das Tarefas

Preparar o BitDefender Total Security 2009 para levar a cabo tarefas importantes para a segurança do seu sistema. As seguintes opções estão disponíveis:

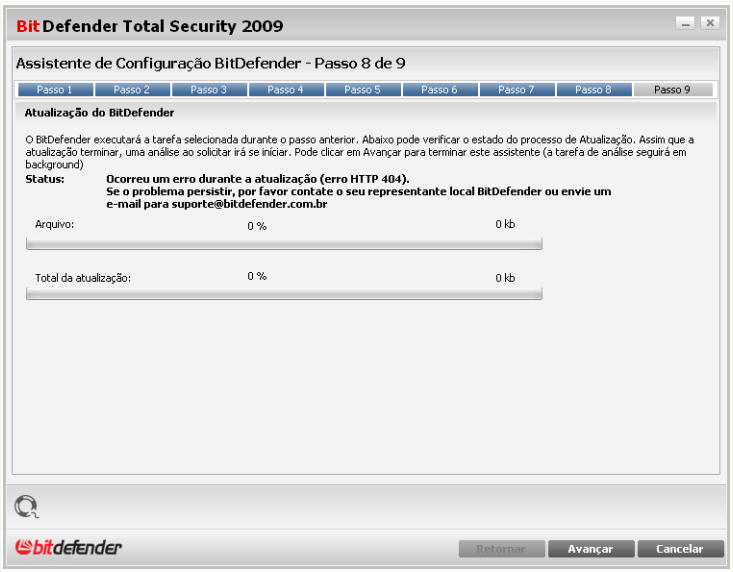
- **Atualizar as engines BitDefender (poderá ser necessário reiniciar)** - durante o próximo passo, será efetuada a atualização das engines BitDefender de forma a proteger o seu computador contra as ameaças mais recentes.
- **Executar uma análise rápida do sistema (poderá ser necessário reiniciar)** - durante o próximo passo, uma análise rápida do sistema será executada de forma a que o BitDefender se certifique que os seus arquivos nas pastas `Windows` e `Programas` não estão infectados.
- **Executar uma análise completa diária às 2 AM** - Executa uma análise completa diária às 2 AM.

Importante
Recomendamos que tenha estas opções ativas antes de avançar para o próximo passo de forma a assegurar a segurança do seu sistema.

Se selecionar apenas a última opção ou nenhuma opção, irá saltar o próximo passo.

Clique em **Seguinte** para continuar.

2.2.8. Passo 8/9 - Esperar que as Tarefas Terminem

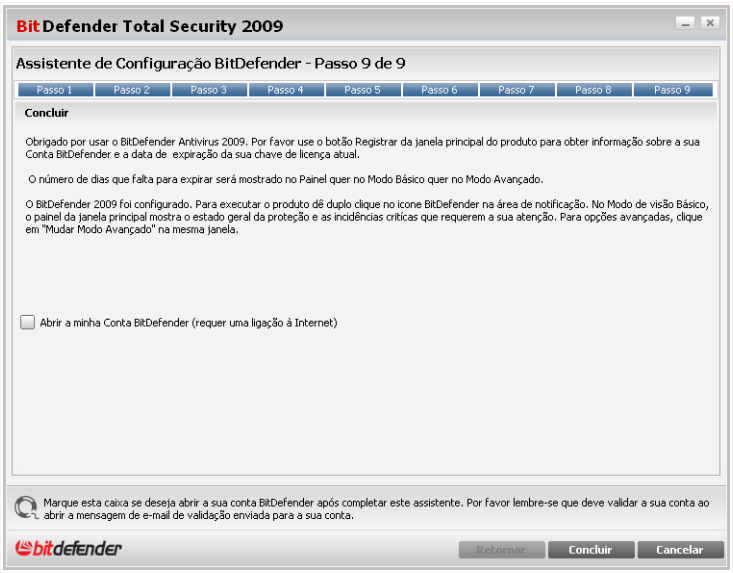


Estado das Tarefas

Esperar que as tarefas terminem. Pode ver o estado das tarefas selecionadas no passo anterior.

Clique em **Seguinte** para continuar.

2.2.9. Passo 9/9 - Terminar



Terminar

Seleccione**Abrir a minha conta BitDefender** - para entrar na sua conta BitDefender. Necessita para tal de estar ligado à Internet.

Clique em **Finalizar**.

3. Atualização de versão

Para atualizar uma versão mais antiga do BitDefender para o BitDefender Total Security 2009, siga os passos aseguir:

1. **Opcional!** Se aquela versão BitDefender inclui Antispam, você pode salvar a Lista de Amigos e Spammers a fim de usá-la após o processo de upgrade ter finalizado. Para maiores informações, por favor consulte o arquivo "help (ajuda)" ou o manual do usuário do produto.
2. Remova a versão antiga da BitDefender de seu computador. Para maiores informações, por favor consulte o arquivo "help (ajuda)" ou o manual do usuário do produto.
3. Reinicie o computador.
4. Instale BitDefender Antivirus 2009 como descrito na "*Instalar BitDefender*" (p. 4) seção deste guia do usuário.

4. Remover ou Reparar o BitDefender

Se pretende reparar ou desinstalar o **BitDefender Total Security 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 tal lhe for solicitado, e depois, clique em **Instalar** para reinstalar BitDefender Total Security 2009.

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

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

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

  Se escolher desinstalar BitDefender, surgirá uma nova janela.

  Importante
  Ao remover o BitDefender, deixará de estar protegido contra os vírus, spyware e os hackers. Se deseja que a Firewall do Windows e o Windows Defender sejam activados após desinstalar o BitDefender, seleccione as correspondentes caixas de selecção durante o próximo passo.

  Clique em **Desinstalar** para dar início à desinstalação do BitDefender Total Security 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

Uma vez instalado o BitDefender o seu computador fica protegido.

5.1. Iniciar o BitDefender Total Security 2009

O primeiro passo para obter o melhor do seu BitDefender é dar início à aplicação.

Para aceder ao interface principal do BitDefender Total Security 2009, use o menu do Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2009** → **BitDefender Total Security 2009**ou mais rapidamente, duplo clique no **ícone BitDefender** que está na área de notificação.

5.2. Modo de Visão do Interface do usuário

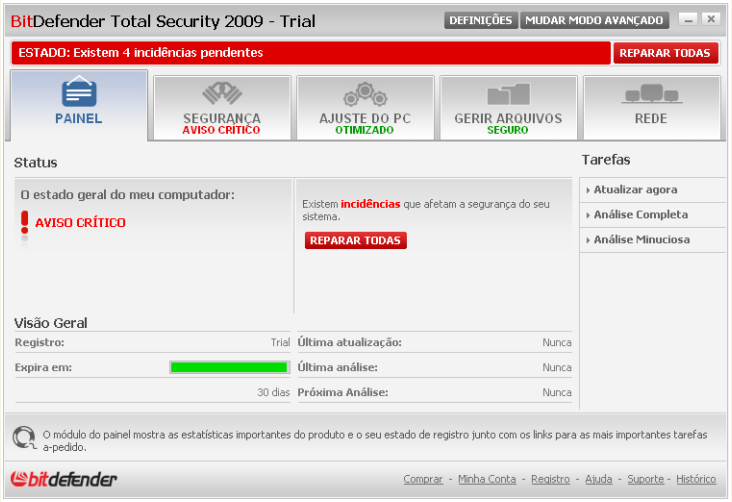
O BitDefender Total Security 2009 quer dos principiantes quer das pessoas mais técnicas. Assim, o interface gráfico do usuário foi desenhado para servir quer uns quer outros.

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** .

5.2.1. Modo Básico

Modo Básico é um interface simples que lhe dará acesso a todos os módulos num nível básico. Terá de manter o rasto dos avisos e alertas criticos e reparar incidências indesejáveis.



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 pode facilmente activar ou desactivar módulos de segurança importantes (Firewall, Modod Stealth, Actualização Automática, Modo de Jogo, etc.).
>Mudar Modo Avançado	Abre a janela de Modo Avançado. Aqui pode ver a lista completa dos módulos e será capaz de configurar em detalhe cada um dos componentes. O BitDefender manterá esta opção da próxima vez que abrir o interface do usuário.
Status	Contém informação sobre as vulnerabilidades de segurança do seu computador e ajuda-o a repará-las.

- No meio da janela estão disponíveis cinco barras.

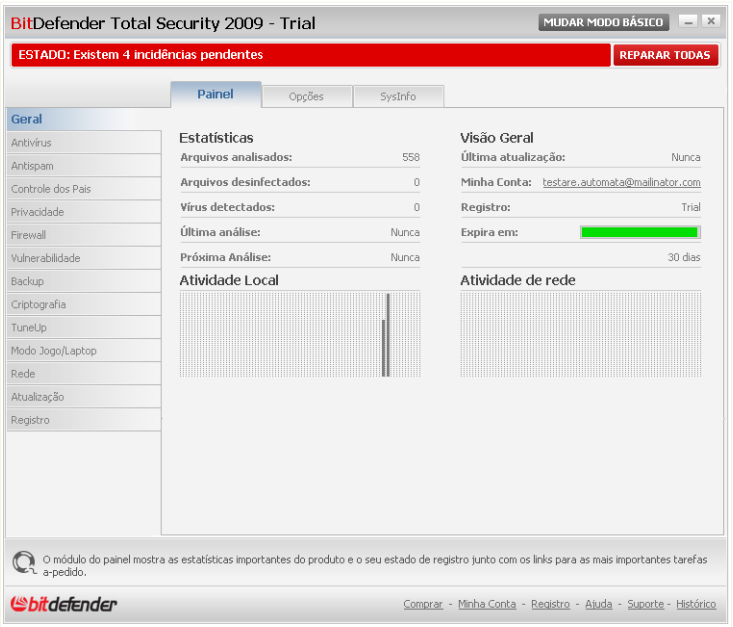
Barra	Descrição
Painel	Mostra informação substancial das estatísticas do produto e do seu estado de registo juntamente com links para as mais importantes tarefas a-pedido.
Segurança	Mostra o estado dos módulos de segurança (antivírus, antiphishing, firewall, antispam, encriptação IM, privacidade, análise de vulnerabilidade e actualização) juntamente com os links para as tarefas de antivírus, actualização e análise de vulnerabilidade.
TuneUp	Mostra o estado das opções do BitDefender desenhadas para melhorar o desempenho do seu sistema juntamente com os links das tarefas de tuneup.
Gerir arquivos	Mostra o estado do cofre de arquivos e dos módulos de backup juntamente com os links para os cofres de arquivos e das tarefas de backup.
Rede	Mosta a estrutura da rede pessoal BitDefender.

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

Link	Descrição
Minha Conta	Permite-lhe criar ou fazer login à sua conta BitDefender. A conta BitDefender dá-lhe acesso a suporte técnico gratuíto.
Registar	Permite-lhe inserir uma nova chave de licença ou ver a actual e o estado do seu registo.
Ajuda	Dá-lhe acesso ao arquivo de ajuda que o ensina a como usar o BitDefender.
Suporte	Permite o contacto com a equipa de suporte BitDefender.
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

5.2.2. Modo Avançado

Modo Avançado dá-lhe acesso a cada componente específico do produto BitDefender. Será capaz de configurar definições avançadas como também mantê-las controladas.



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 do Modo Básico. É aqui onde pode ver o interface básico BitDefender incluindo os módulos principais (Segurança, Tuneup, Gestão Arquivo, Rede) e um painel. O BitDefender memoriza esta opção para a próxima vez que abrir o interface do usuário.

Item	Descrição
Status	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.

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.
Antispam	Permite-lhe manter a pasta A Receber livre de SPAM e também configurar as definições do antispam em detalhe.
Firewall	A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.
Controle de Privacidade	Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.
Controle dos Pais	Permite-lhe proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.
Tarefas de Backup	Permite-lhe fazer backup dos seus dados no seu computador, numa drive amovível ou num local de rede para assegurar que os pode restaurar quando necessário.
Encriptação	Permite-lhe encriptar as comunicações do Yahoo e Windows Live (MSN) Messenger e também encriptar localmente os seus arquivos críticos, as suas pastas ou partições.
Vulnerabilidade	Permite-lhe manter o software crucial para o seu PC sempre actualizado.

Módulo	Descrição
Tuneup	Permite-lhe melhorar o desempenho do seu computador ao desfragmentar o seu disco, limpar o registo e os arquivos duplicados, etc.
Modo de Jogo/Portátil	Permite-lhe adiar as tarefas agendadas BitDefender enquanto o seu portátil está a funcionar a bateria e também elimina alertas e pop-ups enquanto está a jogar.
Rede	Permite-lhe configurar e gerir vários computadores do seu lar.
Actualização	Permite-lhe obter info das últimas actualizações, actualizar o produto e configurar o processo de actualização em detalhe.
Registro	Permite-lhe registar o BitDefender Total Security 2009, mudar a chave de licença ou criar uma conta BitDefender.

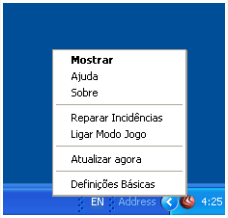
- E mais ainda, a janela do Modo Avançado BitDefender contém diversos atalhos úteis.

Link	Descrição
Minha Conta	Permite-lhe criar ou fazer login à sua conta BitDefender. A conta BitDefender dá-lhe acesso a suporte técnico gratuíto.
Registar	Permite-lhe inserir uma nova chave de licença ou ver a actual e o estado do seu registo.
Ajuda	Dá-lhe acesso ao arquivo de ajuda que o ensina a como usar o BitDefender.
Suporte	Permite o contacto com a equipa de suporte BitDefender.
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

5.3. 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 duplo-clique neste ícone, o BitDefender irá abrir. Também 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 o o BitDefender.
- **Ajuda** - abre o arquivo de ajuda que explica em detalhe o BitDefender Total Security 2009.
- **Acerca** - abre a página web do BitDefender.
- **Reparar todos incidências** - ajuda-o a removeras vulnerabilidades de segurança.
- **Ligar / desligar Modo de Jogo** - Liga/desliga Modo de Jogo .
- **Atualizar agora** - realiza uma atualização imediata. Surge uma nova janela, onde pode ver o estado da actualização.
- **Configuração Básica** - permite-lhe facilmente activar ou desactivar ímportantes módulos de segurança. Surge uma nova janela, onde os pode activar ou desactivar com um simples clique.

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

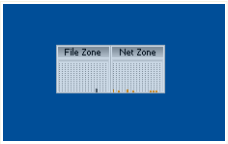
Se existirem incidências criticas a afectar a segurança do seu sistema, um ponto de exclamação é mostrado sobre o icone do BitDefender. Pode passar o mouse sobre o ícone e ver o número de incidências que afectam a segurança do seu sistema.

5.4. Barra de Actividade da Análise

A **Barra de atividade de verificação** é uma visualização gráfica da atividade de verificação em seu sistema.

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

As barras laranjas apresentadas na **zona Net** mostram o número de Kbytes transferidos (enviados e recebidos da Internet) a cada segundo, numa escala de 0 a 100.



Barra de Actividade

Nota
A barra de actividade da Análise avisa-o quando a protecção em Tempo-real ou a Firewall está desactivada ao mostrar uma cruz vermelha sobre a área correspondente (**zona PC** ou **zona Net**).

Pode usar a **Barra de Actividade da Análise** para analisar objectos. Apenas arraste os objectos que deseja analisar para cima dela. Para mais informação, por favor consulte o "*Verificação Arraste & Solte*" (p. 196).

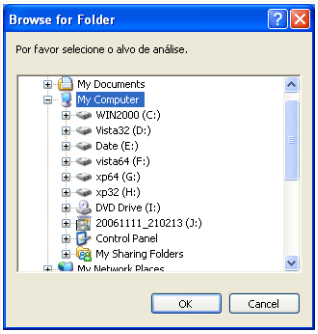
Quando você não quiser mais a visualização gráfica, basta clicar nela com o botão direito e escolher **Ocultar**. Para ocultar completamente esta janela, siga os seguintes passos:

1. Clique em**Mudar Modo Avançado** (se estiver em **Modo Básico**).
2. Clique no módulo **Geral** do lado esquerdo do menu.
3. Clique na barra **Definições** .
4. Desmarcar a caixa **Activar a barra de Actividade da Análise (gráfico no ecrã)** .

5.5. Análise Manual BitDefender

Se deseja analisar rapidamente uma determinada pasta, pode usar a Análise Manual 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 Analisador BitDefender irá surgir e guiá-lo através do processo de análise.

5.6. Modo de Jogo

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

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

Enquanto no Modo de Jogo, pode ver a letra`G` sobre o icone do BitDefender.

5.6.1. Usar o Modo de Jogo

Se deseja ligar o Modo de Jogo, pode usar um dos seguintes métodos:

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

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

5.6.2. Mudar a Hotkey do Modo de Jogo

Se deseja mudar a hotkey, siga estes passos:

1. Clique em**Mudar Modo Avançado** (se estiver em **Modo Básico**).
2. Clique em **Modo Jogo / Modo laptop** do lado esquerdo do menu.
3. Clique na barra **Modo de Jogo**
4. Clique no botão **Configuração Avançada** .
5. Por baixo da opção **Usar HotKey** , defina a hotkey desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).

- No campo de edição, insira a letra correspondente à tecla que deseja usar.

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

Nota
Remover a marca da caixa ao lado de **Usar HotKey** irá desactivar a hotkey.

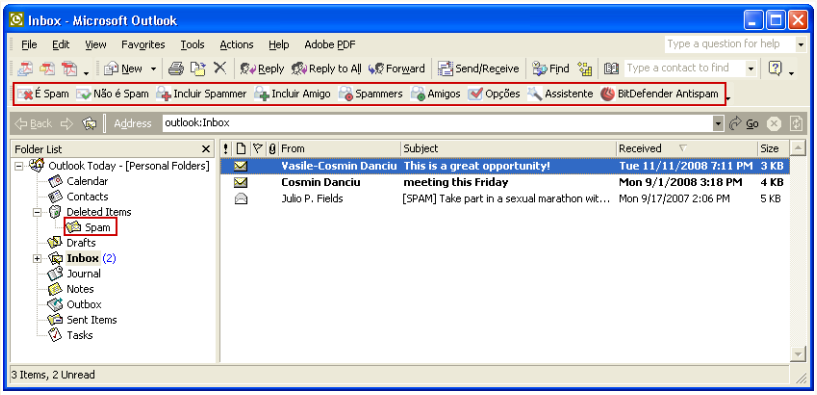
5.7. Integração com Clientes de Mail

BitDefender integra-se directamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes clientes de mail:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

5.7.1. Barra de ferramentas Antispam

Na parte superior do cliente de mail você pode ver a barra de ferramentas Antispam.



Barra de ferramentas Antispam

Importante
A diferença entre o BitDefender Antispam for Microsoft Outlook e Outlook Express / Windows Mail é que mensagens SPAM são movidas para a pasta **Spam** no Microsoft Outlook e no Outlook Express elas são movidas para a pasta **Itens Excluídos** Em ambos os casos as mensagens são marcadas como SPAM na linha do assunto.

A pasta **Spam** criada pelo BitDefender for Microsoft Outlook é listada no mesmo nível dos itens da **Lista de Pastas**(Calendário, Contatos, etc).

Cada botão será explicado abaixo:

- **É Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado é spam. O e-mail será marcado como SPAM e será movido para a pasta de **Spam**.

  Mensagens futuras com as mesmas características serão marcadas como SPAM.

  Nota
  Você pode escolher um e-mail ou quantas mensagens quiser.

- **Não é Spam** - envia uma mensagem para o módulo Bayesiano indicando que o e-mail selecionado não é Spam. O e-mail será movido da pasta **Spam** para a **Caixa de entrada**.

  Mensagens futuras com as mesmas características não serão marcadas como SPAM.

  Nota
  Você pode escolher um e-mail ou quantas mensagens quiser.

  Importante
  O botão **Não é Spam** fica ativo quando você escolhe uma mensagem marcada como Spam pelo BitDefender (normalmente essas mensagens estão localizadas na pasta **Spam**).

- **Adicionar spammer** - adiciona o remetente do e-mail seleccionado para a **Lista de Spammers**.

Adicionar Spammer

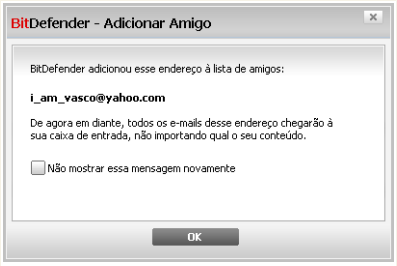
Escolher **Não mostrar essa mensagem novamente** se você não quer que lhe seja pedido confirmação quando você inclui um endereço de spammer na lista.

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

Mensagens futuras daquele endereço serão marcadas como SPAM.

Nota
Você pode selecionar um remetente ou quantos você quiser.

- **Adicionar amigo** - adiciona o remetente do e-mail seleccionado à **Lista de Amigos**.



Adicionar Amigo

Escolher **Não mostrar essa mensagem novamente** se você não quer que lhe seja pedido confirmação quando você inclui um endereço de amigos na lista.

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

Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.

Nota
Você pode selecionar um remetente ou quantos você quiser.

- **Spammers**- abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo.

Nota
Qualquer mensagem vinda de um e-mail na **Lista de Spammers** será marcado como Spam, sem pais processamentos.

Lista de Spammers

Aqui você pode incluir ou remover entradas da **Lista de Spammers**.

Se você quer incluir um endereço de e-mail marque o campo **E-mail** digite-o e clique no botão ⊠. O endereço aparecerá na **Lista de Spammers**.

Importante
Syntax: nome@domínio.com.

Se você quer incluir um domínio marque o campo **Domínio** digite-o e clique no botão ⊠ O domínio aparecerá na **Lista de Spammers**.

Importante
Syntax:

- @domínio.com, *domínio.com e domínio.com - todos os e-mails vindos de domínio.com serão marcados como Spam;
- *domínio* - todos os e-mails vindos de domínio (não importa quais os sufixos do domínio) serão marcados como Spam;
- *com - todos os e-mails contendo o sufixo de domínio com serão marcados como Spam.

Para importar endereços de e-mail de **Livro de Endereços do Windows**/**Pastas do Outlook Express** para o **Microsoft Outlook**/**Outlook Express** / **Windows Mail** seleccione a opção apropriada do menu expansível**Importar endereços de e-mail de**.

Para o **Microsoft Outlook Express / Windows Mail** uma nova janela aparecerá onde você poderá selecionar a pasta que contém os endereços de e-mail que você deseja adicionar a **Lista de spammers**. Escolha os endereços e clique em **Selecionar**.

Em ambos os casos os e-mails aparecerão na lista de importação. Escolha os endereços desejados e clique em para incluí-los na **Lista de Spammers**. Se você clicar em todos os e-mails serão inclusos na lista.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Salvar**/ **Carregar** para salvar / carregar a **Lista de Spammers** num local desejado. O arquivo terá a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique em **Aplicar** e **OK** para salvar e fechar a **Lista de Spammers**.

- **Amigos** - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo.

> ***Nota***
> Qualquer mensagem vinda de um endereço contido na **Lista de amigos**, será automaticamente entregue em sua Caixa de entrada sem mais processamentos.

Lista de amigos

Aqui você pode incluir ou remover entradas da **Lista de amigos**.

Se pretender adicionar um endereço de e-mail seleccione a opção **E-mail**, insira-o e clique no botão ⊠. O endereço irá aparecer na **Lista de amigos**.

Importante
Syntax: nome@domínio.com.

Se você quer incluir um domínio marque o campo **Domínio** digite-o e clique no botão ⊠. O domínio aparecerá na **Lista de amigos**.

Importante
Syntax:

- @domínio.com, *domínio.com e domínio.com - todos os e-mails vindos de domínio.com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;
- *domínio* - todos os e-mails vindos de domínio (não importa quais os sufixos do domínio) chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;
- *com - todos os e-mails contendo o sufixo de domínio com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;

Para importar endereços de e-mail de **Livro de Endereços do Windows**/**Pastas do Outlook Express** para o **Microsoft Outlook**/**Outlook Express** / **Windows Mail** seleccione a opção apropriada do menu expansível**Importar endereços de e-mail de**.

Para o **Microsoft Outlook Express / Windows Mail** uma nova janela aparecerá onde você poderá selecionar a pasta que contém os endereços de e-mail que você deseja adicionar a **Lista de amigos**. Escolha os endereços e clique em **Selecionar**.

Em ambos os casos os e-mails aparecerão na lista de importação. Escolha os endereços desejados e clique em para incluí-los na **Lista de Amigos**. Se você clicar em todos os e-mails serão inclusos na lista.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

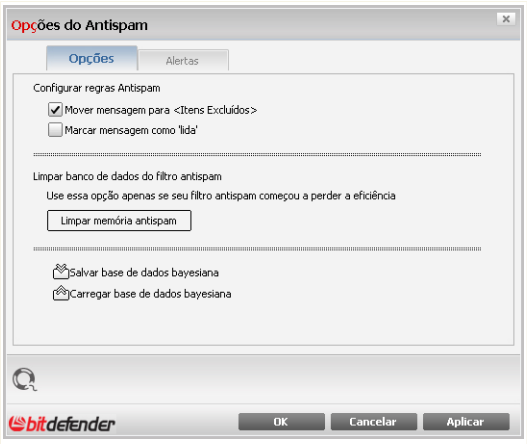
Use os botões **Salvar**/ **Carregar** para salvar / carregar a **Lista de amigos** num local desejado. O arquivo terá a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota
Nós recomendamos que você adicione os nomes e e-mails de seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos que estão na lista, portanto, adicionar amigos ajuda a fazer com que mensagens legítimas sejam recebidas.

Clique em **Aplicar** e **OK** para salvar e fechar a **Lista de amigos**.

- **Opções** - abre a janela **Opções** onde você pode especificar algumas opções para o módulo **Anti-spam**.



Opções

As seguintes opções estão disponíveis:

- **Mover mensagens para Itens Excluídos** - para mover Spam para a pasta **Itens Excluídos** (apenas para o Microsoft Outlook Express / Windows Mail);
- **Marcar mensagens como 'lida'** - para marcar todo Spam como lido para não ser perturbado quando chegarem novos spams.

Se seu filtro antispam está muito impreciso, você pode ter que limpar a base de dados do filtro Bayesiano. Clique em **Limpar dados antispam** se você quer apagar a base de dados Bayesiana.

Use os botões **Salvar Bayes**/ **Carregar Bayes** para salvar/carregar a lista de Base de Dados Bayesiana para o local desejado. O arquivo terá uma extensão `.dat`.

Clique na barra **Alertas** se você quiser acessar a seção onde você pode desativar a aparição das janelas de confirmação para os botões **Incluir spammer** e **Incluir amigo**.

Nota

Na janela de **Alertas** pode activar/desactivar a aparição do alerta **Por favor seleccione um e-email** . Este alerta surge quando selecciona um grupo em vez uma mensagem de e-mail.

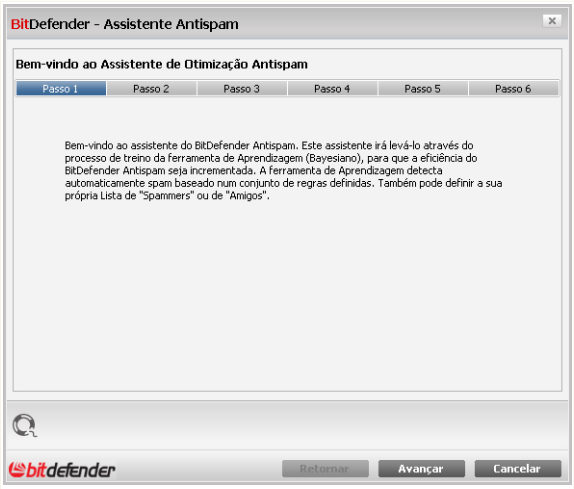
- **Assistente** - abre o wizard tque irá guiá-lo pelo processo de treino do filtro Bayesiano, para que a eficiência do BitDefender Antispam seja maior ainda. Você pode também incluir endereços de seu **Catálogo de endereços** em sua **Lista de amigos** / **Lista de Spammers**.
- **Antispam BitDefender** - abre o interface do usuário BitDefender.

5.7.2. Assistente de Configuração Antispam

A primeira vez que você executar o cliente de mail após ter instalado o BitDefender, um assistente irá aparecer para ajudá-lo a configurar a sua Lista de Amigos e a Lista de Spammers e treinar o Filtro Bayesiano para que seja possível aumentar a eficiência dos filtros Anti-spam.

Nota
O assistente pode ser executado a qualquer altura que deseje clicando no botão **Assistente** na Barra de tarefas Antispam.

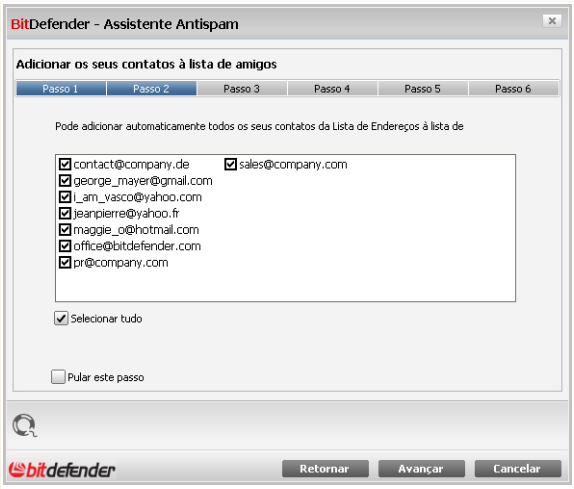
Passo 1/6 - Janela de Boas-vindas



Janela de Boas-Vindas

Clique em **Próximo**.

Passo 2/6 - Preencher a Lista de Amigos



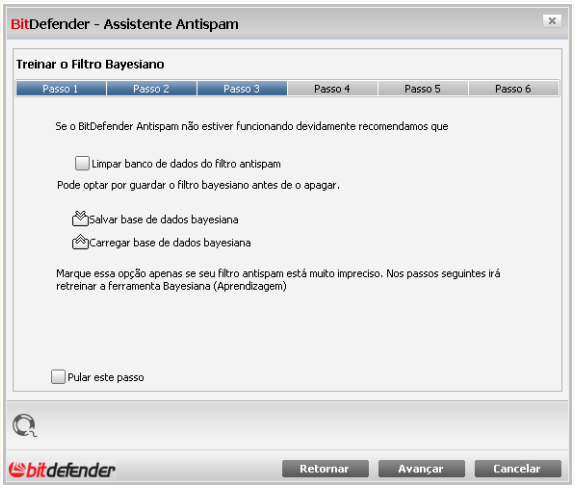
Preencher a Lista de Amigos

Aqui você pode ver todos os endereços de seu **Catálogo de Endereços**. Por favor escolha os que você deseja incluir na **Lista de Amigos** (recomendamos selecionar todos). Você receberá todos os e-mails desses endereços, não importando qual o conteúdo.

Para adicionar todos os seus contactos à lista de Amigos, seleccione **Seleccionar todos**.

Escolha **Pular este passo** se você quer pular esse passo. Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

Passo 3/6 - Apagar a Base de Dados Bayesiana



Apagar a Base de Dados Bayesiana

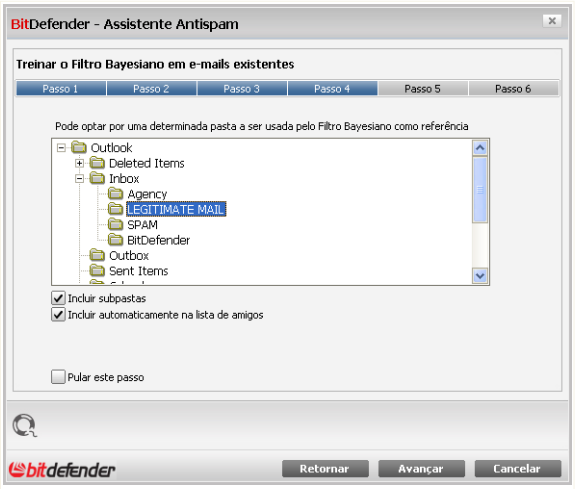
Você pode achar que seu filtro Antispam começou a perder eficiência. Isso pode ser devido a um treino indevido (Ex: se você marcou erroneamente algumas mensagens legítimas como Spam, ou vice-versa). Se seu filtro está muito impreciso, você pode ter que limpar a base de dados do filtro e treiná-lo novamente seguindo os próximos passos do assistente.

Selecione **Limpar banco de dados do filtro Antispam** se você quer limpar a base de dados Bayesiana.

Use os botões **Salvar base de datos bayesiana**/ **Carregar base de datos bayesiana** parar salvar/carregar a lista de Base de Dados Bayesiana para o local desejado. O arquivo terá uma extensão `.dat`.

Escolha **Pular este passo** se você quer pular esse passo. Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

Passo 4/6 - Treine o filtro Bayesiano com e-mails legítimos



Treine o filtro Bayesiano com e-mails legítimos

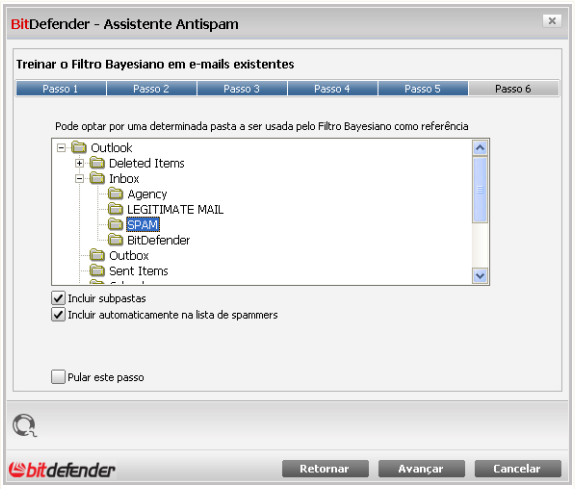
Por favor escolha uma pasta que contenha e-mails legítimos. Essas mensagens serão usadas para treinar o filtro Bayesiano.

Existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir subpastas** - para incluir a subpasta de sua escolha.
- **Incluir automaticamente na lista de amigos** - para incluir os remetentes na **lista de Amigos**.

Escolha **Pular este passo** se você quer pular esse passo. Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

Passo 5/6 - Treine o filtro Bayesiano com SPAM



Treine o filtro Bayesiano com SPAM

Por favor escolha uma pasta que contém mensagens Spam. Essas mensagens serão usadas para treinar o Filtro Bayesiano.

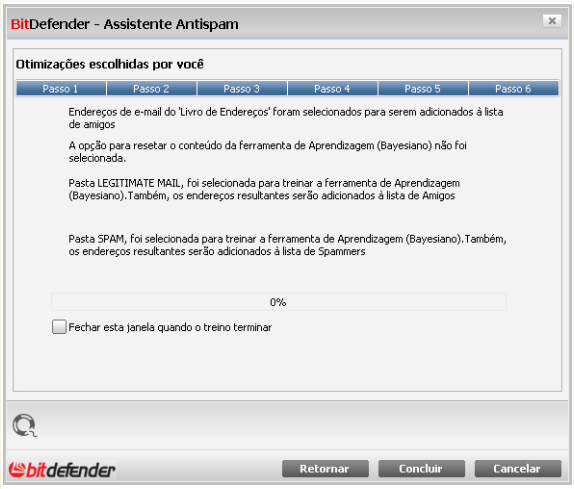
Importante
Por favor assegure-se de que não há nenhuma mensagem legítima na pasta escolhida, senão a performance do filtro Antispam será consideravelmente.

Existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir subpastas** - para incluir a subpasta de sua escolha.
- **Incluir automaticamente na lista de spammers** - para incluir os remetentes na **lista de Spammers**.

Escolha **Pular este passo** se você quer pular esse passo. Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

Passo 6/6 - Conclusão



Sumário

Nessa tela você pode ver todas as opções para o assistente de configuração e pode fazer qualquer mudança, retornando ao passo anterior (**Voltar**).

Se você não quiser fazer quaisquer modificações, clique em **Finalizar** para finalizar o assistente.

5.8. Integração com Exploradores web

BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet. Analisa os sites web que acede e alerta-o no caso de haver alguma ameaça de phishing. Uma Lista Branca de sites web que não serão analisados pelo BitDefender pode ser configurada.

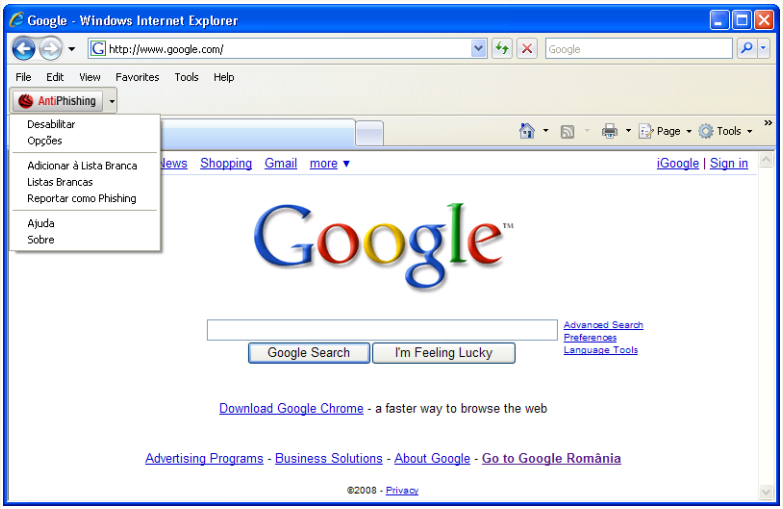
BitDefender integra-se directamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes exploradores da Internet:

- Internet Explorer
- Mozilla Firefox

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada num dos exploradores da internet acima.

A barra de ferramentas antiphishing representado pelo **icone do BitDefender**, está localizado no lado superior do Explorador da Internet. Clique nele de forma a abrir o menu da barra de ferramentas.

Nota
Se não consegue ver a barra de ferramentas, abra o menu **Ver** siga para **Barras de ferramentas** e seleccione **Barra de Ferramentas BitDefender**.



Barra de Ferramentas do Antiphishing

Os seguintes comandos estão disponíveis no menu da barra de ferramentas:

- **Activar/Desactivar** - activa/desactiva a barra de ferramentas Antiphishing do BitDefender.

Nota
Se escolher desactivar a a barra de ferramentas antiphishing, não ficará mais protegido contra as tentativas de phishing.

- **Configuração** - abre uma janela onde pode especificar as definições da barra de ferramentas do antiphishing.

  As seguintes opções estão disponíveis:
  - **Activar Análise** - activa a análise antiphishing.
  - **Avisar antes adicionar à lista branca** - será consultado antes de ser adicionado um site web à Lista Branca.
- **Adicionar à Lista Branca** - adiciona o actual site web à Lista Branca.

  Nota
  Adicionar um site à Lista Branca significa que o BitDefender não irá mais analisar esse site em busca de tentativas de phishing. Recomendamos que adicione à Lista Branca apenas os sites em que confia totalmente.

- **Ver Lista Branca** - abre a Lista Branca.

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

  Se deseja remover um site da Lista Branca de forma a que seja notificado acerca de qualquer possibilidade de ameaça de phishing existente nesse site, clique no botão **Remover** ao pé do mesmo.

  Pode adicionar sites à Lista Branca nos quais confia absolutamente, de forma a que eles não sejam mais analisados pelos motores antiphishing. Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.
- **Ajuda** - abre a documentação eletrônica.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

5.9. Integração com Messenger

O BitDefender oferece uma função de proteção que permite cifrar os seus documentos confidenciais e as suas conversas através do Yahoo Messenger e MSN Messenger.

De forma padrão, BitDefender cifra todas as suas sessões de chat desde que:

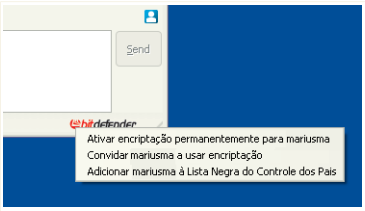
- O seu parceiro de chat tenha instalada uma versão do BitDefender que suporte a cifragem MI e a mesma esteja habilitada para o programa de mensagens usado durante o chat.
- E o seu parceiro de chat esteja a usar quer o Yahoo Messenger ou o Windows Live (MSN) Messenger.

Importante
O BitDefender não vai cifrar uma conversa se o seu parceiro de chat usar um programa de chat, tipo Meebo, ou outro que suporte o Yahoo Messenger ou o MSN.

Pode configurar facilmente a cifragem das mensagens instantâneas usando a barra de ferramentas a partir da janela de chat.

Ao clicar com o botão direito do mouse sobre a barra de ferramentas serão providenciadas as seguintes opções:

- Habilitação/desabilitação permanente da cifragem para um determinado parceiro de chat
- Convidar um determinado parceiro de chat a usar a cifragem
- Remover um determinado parceiro de chat da lista negra do Controle dos Pais

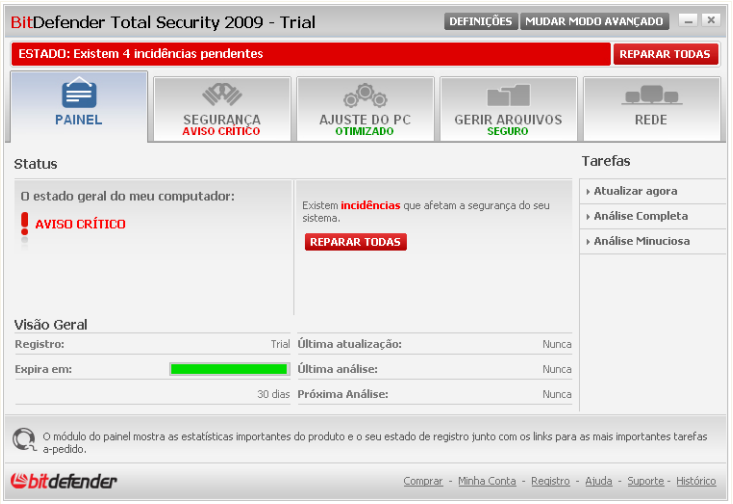


Opções da Cifragem das Mensagens Instantâneas

Clique numa das opções acima de forma a usá-la.

6. 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:

- **Estaísticas** - Mostra informação importante com respeitoà actividade do BitDefender.
- **Visão Geral** - Mostra o estado da actualização, o estado da sua conta, e informação do seu registo e licença.
- **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.
- **Zona Net** - Indica a evolução do tráfego de rede, filtrado pela Firewall do BitDefender. A altura da barra indica a intensidade do tráfego durante esse intervalo de tempo.
- **Tarefas** - Dá-lhe os links para as tarefas de segurança mais importantes: análise completa do sistema, análise minuciosa, actualizar agora.

6.1. Estatísticas

Se deseja manter baixo controle a atividade do BitDefender, um bom lugar para começar é a secção de estatísticas.

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.
Vírus detectados	Indica o número de vírus detectados no seu sistema até ao momento da sua última análise.
Bloquear scan de portas	Indica o número de scans de portas bloqueados pela Firewall do BitDefender. Os scans de portas são frequentemente usados pelos hackers para descobrir portas abertas no seu computador com o objectivo de as explorar. Mantenha a Firewall e o Modo Stealth activados para estar protegido contra os scans de portas.
Tarefas de backup completadas	Indica o número de vezes que fez backup dos seus dados.

6.2. Sumário

Aqui pode ver um resumo das estatísticas respeitantes ao estado da actualização, ao estado da sua conta, registo e informação de licença.

Item	Descrição
Última actualização	Indica a data em que o produto Bitdefender foi actualizado pela última vez. Leve a cabo actualizações regulares de forma a ter um sistema totalmente protegido.
Minha Conta	Indica o endereço de e-mail que pode usar para aceder à sua conta on-line para recuperar a sua chave de licença perdida e beneficiar do suporte BitDefender e de outros serviços personalizados.

Item	Descrição
Registro	Indica o seu tipo de licença e o seu estado. Para manter o seu sistema seguro tem de renovar ou efectuar o upgrade do BitDefender se a sua chave de licença tiver expirado.
Expira em	Indica o número de dias que faltam até que a sua chave de licença expire.

Para actualizar o BitDefender, clique no botaõ **Actualizar Agora** na secção das Tarefas.

Para criar um login para a sua conta BitDefender, siga os seguintes passos.

1. Clique no link **Minha Conta**, localizado no fundo da janela. Uma página web irá abrir.
2. Insira o nome de usuário e a senha e clique no botão **Login**.
3. Para criar uma conta BitDefender, seleccione**Não tem uma conta?** e fornecer a devida informação.

Nota
Os dados que nos fornecer serão mantidos confidenciais.

Para registar o BitDefender Total Security 2009, siga os seguintes passos:

1. Clique no link **Minha Conta** no botão no fundo da janela. Um assistente de um só passo aparecerá.
2. Clique no botão **Registar o produto com uma nova chave** .
3. Insira a nova chave de licença na caixa de texto correspondente.
4. Clique em **Finalizar**.

Para adquirir uma nova chave de licença, siga os seguintes passos.

1. Clique no link **Minha Conta** no botão no fundo da janela. Um assistente de um só passo aparecerá.
2. Clique no link **Renovar a Chave de Licenla BitDefender** . Abrir-se-á uma página web.
3. Clique no botão **Comprar Agora** .

6.3. Tarefas

Aqui é onde pode encontrar os links para as tarefas de segurança mais importantes: Análise completa do sistema, análise minuciosa, actualizar agora.

Estão disponíveis os seguintes botões:

- **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.
- **Análise Minuciosa do Sistema** - inicia uma análise minuciosa ao seu computador.
- **Atualizar agora** - realiza uma atualização imediata.

6.3.1. 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
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.

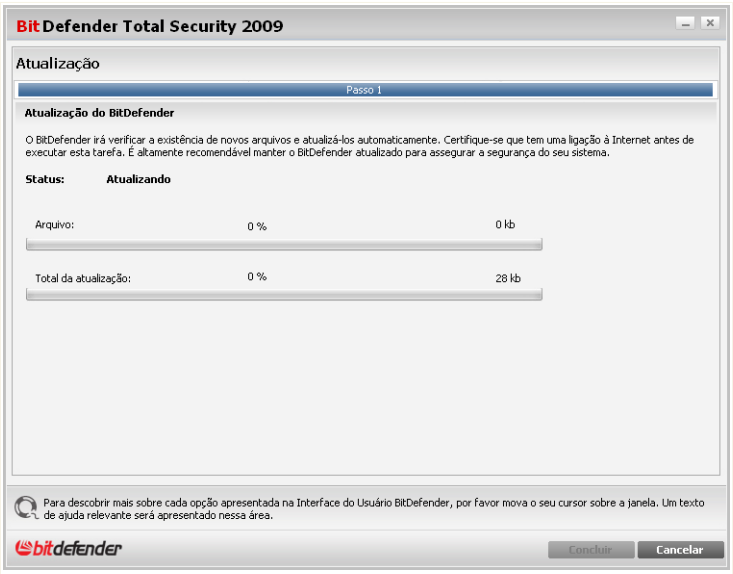
Quando dá início a um processo de análise a-pedido, quer seja uma análise rápida ou completa, o Analisador BitDefender surgirá.

Siga o processo guiado de três passos para completar o processo de análise.

6.3.2. 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 defeito, quando liga o computador o BitDefender verifica se há actualizações e depois disso fá-lo a cada **hora** . 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:

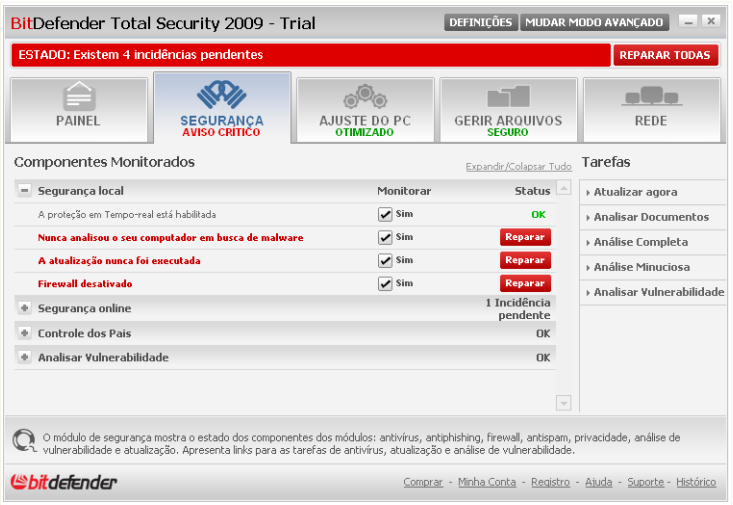
Clique em **Reiniciar** para reiniciar o seu sistema imediatamente.

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

7. Segurança

BitDefender traz consigo um módulo de Segurança que ajuda-o a manter o seu BitDefender actualizado e o seu computador livre de vírus.

Para entrar no módulo de Segurança, clique na barra **Segurança**.



Segurança

O módulo de segurança é composto de duas secções:

- **Componentes Monitorizados** - Permite-lhe ver a lista completa dos componentes monitorizados para cada módulo de segurança. Pode escolher que módulos deseja monitorizar. É recomendável que active a monitorização de todos os componentes.
- **Tarefas** - Aqui é onde pode encontrar os links para as mais importantes tarefas de segurança: análise completa do sistema, análise minuciosa, actualizar agora.

7.1. Componentes Monitorizados

Os componentes monitorizados estão agrupados em diversas categorias:

Categoria	Descrição
Segurança Local	Aqui é onde pode verificar o estado de cada um dos módulos de segurança que estão a proteger o conteúdo do seu computador (arquivos, registo, memória, etc).
Segurança On-line	Aqui é onde pode verificar o estado da cada um dos módulos de segurança que protegem as suas transações on-line e o seu computador enquanto está ligado à Internet.
Segurança de Rede	Aqui é onde pode verificar o estado do módulo de segurança Firewall que o protege contra os hackers.
Controle dos Pais	Aqui é onde pode verificar o estado do Controle dos Pais que lhe permite restringir o acesso das crianças à internet e a determinadas aplicações.
Analisar Vulnerabilidades	Aqui é onde pode verificar se o software crucial para o seu PC está ou não actualizado. As palavras-passe das contas do Windows são verificadas de acordo com as regras de segurança.

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

7.1.1. Segurança Local

Sabemos que é importante ser avisado sempre que há um problema que pode afectar a segurança do seu computador. Ao monitorizar cada módulo de segurança, o BitDefender Total Security 2009 fa-lo-á saber não só quando configura definições que podem afectar a segurança do seu computador, mas também quando se 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	Assegura que todos os arquivos serão analisados, à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.

Incidência	Descrição
Tempo-real está activada	
Você analisou o seu computador em busca de malware hoje	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.
Actualização automatica está activada	Por favor mantenha a actualização automática activada para assegurar que as assinaturas de malware do seu produto BitDefender são actualizadas numa base regular.
Actualizar Agora	A actualização do produto e das assinaturas de malware está a ser levada a cabo.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

7.1.2. Segurança On-line

As incidências que dizem respeito à segurança on-line são descritas em frases bem explicítas. Ao mesmo tempo que a frase, se existe algo que possa ameaçar 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 em Tempo-real para o tráfego web (HTTP) está activada	É recomendável manter a protecção web (HTTP) activada para manter o seu computador protegido contra o malware que se propaga via websites ou através de arquivos descarregados potencialmente infectados.

Incidência	*Descrição*
Protecção em Tempo-real para o tráfego de e-mail está activada	A protecção do tráfego de e-mail assegura que os seus e-mails são analisados em busca de malware e filtrados de spam.
Protecção em Tempo-real para o tráfego IM está activada	É recomendável activar a protecção completa do tráfego de IM para manter o seu computador seguro.
Controle de Identidade ativado	Ajuda-o a manter os seus dados confidenciais seguros ao analisar o tráfego web e de e-mail em busca de palavras-chave. É recomendável que mantenha o Controle de Identidade ativado, para evitar que a sua informação confidencial (endereço de e-mail, IDs de usuário, palavras-passe, números de cartões de crédito, etc) seja roubada.
A encriptação de conversação de IM está activada	Se os seus contactos IM têm o BitDefender 2009 instalado, todas as conversas IM via Yahoo! Messenger e Windows Live Messenger serão encriptadas. É recomendável que tenha a encriptação de conversação IM activada para assegurar que as mesmas se mantém privadas.
A protecção antiphishing Firefox está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.
A protecção antiphishing Internet Explorer está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

7.1.3. Segurança de Rede

Quando o seu computador faz parte de uma rede vai querer definitivamente protegê-los contra os hackers e prevenir quaisquer tentativas de ligação não-autorizadas ao seu sistema.

As incidências que dizem respeito à segurança de rede são descritas em frases bem explicítas. Ao mesmo tempo que cada frase, se existir algo que possa 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*
Firewall activada	Protege o seu computador contra os hackers e os ataques maliciosos vindos do exterior.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

7.1.4. Controle dos Pais

O Controle dos Pais monitoriza o estado dos módulos que lhe permitem restringir o acesso das crianças à internet e a determinadas aplicações.

As incidências que dizem respeito ao módulo do Controle dos Pais são descritas em frases bem explicitas. Ao mesmo tempo que as frases, se existir algo que esteja a afectar a segurança das crianças, verá um botão vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	Descrição
O Controle dos Pais não está configurado	O módulo de Controle dos Pais do BitDefender pode bloquear o acesso a sites na Internet que considere inapropriados, pode bloquear o acesso à Internet durante determinados períodos de tempo e filtrar e-mail, IM e tráfego web por palavras-chave específicas, etc.

Quando o botão de estado está verde, as suas crianças podem navegar na net em segurança. Para colocar os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

7.1.5. Analisar Vulnerabilidades

As incidências com respeito a vulnerabilidades são descritas com frases bem explicitas. Ao mesmo tempo, se existe algo a afectar a segurança do seu computador, verá um botão vermelho de estado denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	Descrição
A verificação de Vulnerabilidades está activada	Monitoriza as actualizações do Microsoft Windows, do Microsoft Windows Office e as palavras-passe das contas Microsoft Windows para assegurar que o seu SO está actualizado e não se encontra vulnerável à quebra de palavras-passe.
Actualizações Criticas da Microsoft	Instala Actualizações Criticas da Microsoft que estejam disponíveis.
Outras Actualizações da Microsoft	Instala Actualizações não-criticas da Microsoft que estejam disponíveis.

Incidência	Descrição
A Actualização Automatica do Windows está activada	Instala novas actualizações de segurança do Windows assim que estejam disponíveis.
Admin (senha forte)	Indica a força de cada senha de usuários específicos

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

7.2. Tarefas

Aqui é onde pode encontrar os links para as tarefas de segurança mais importantes: Análise completa do sistema, análise minuciosa, actualizar agora.

Estão disponíveis os seguintes botões:

- **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.
- **Análise Minuciosa do Sistema** - inicia uma análise minuciosa ao seu computador.
- **Analisar os Meus Documentos** - inicia uma análise rápida à sua pasta Documents and Settings.
- **Atualizar agora** - realiza uma atualização imediata.
- **Análise de Vulnerabilidade**

7.2.1. 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
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.
Analisar Os 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.

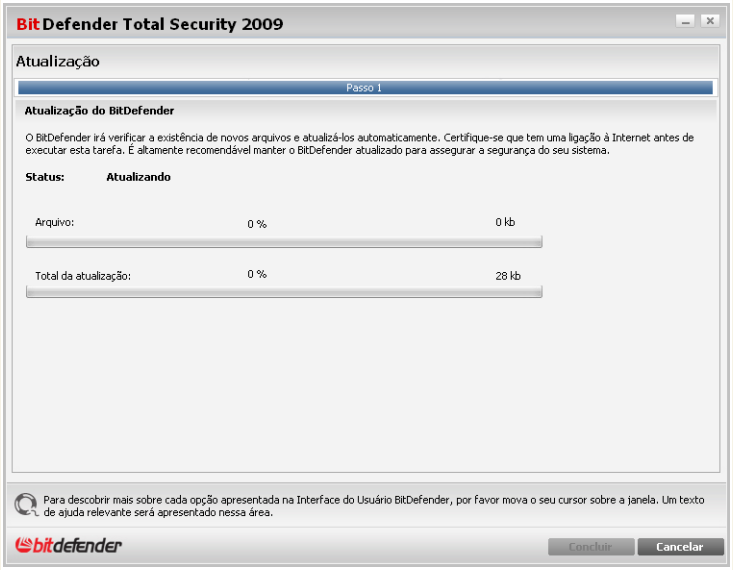
Nota
Um vez que as atrefas **Análise Minuciosa do Sistema** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inactivo.

Quando dá início a um processo de análise a-pedido, quer seja uma análise rápida ou completa, o Analisador BitDefender surgirá. Siga o processo guiado de três passos para completar o processo de análise.

7.2.2. 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 defeito, quando liga o computador o BitDefender verifica se há actualizações e depois disso fá-lo a cada **hora** . 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.

7.2.3. Procurar Vulnerabilidades

A análise de Vulnerabilidade monitoriza as actualizações do Microsoft Windows, do Microsoft Windows Office e as palavras-passe das contas Microsoft Windows para assegurar que o seu SO está actualizado e não se encontra vulnerável à quebra de palavras-passe.

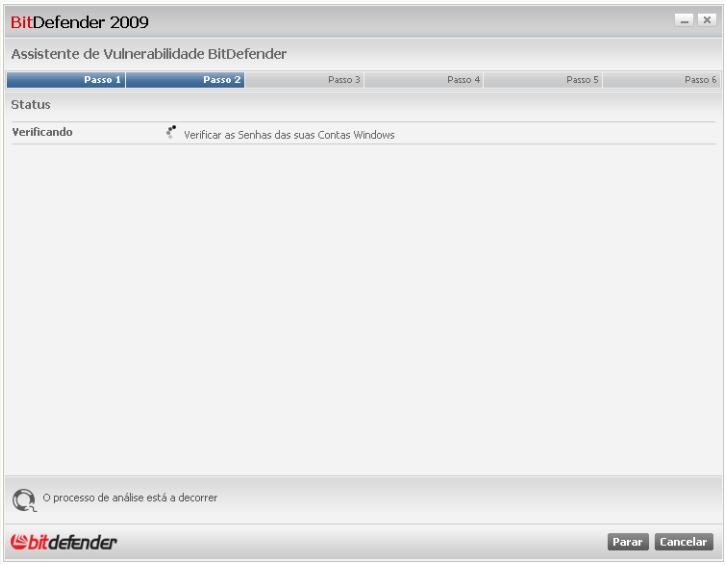
Para verificar as vulnerabilidades do seu computador, clique em **Analisar Vulnerabilidades** e siga o assistente.

Passo 1/6 - Seleccionar Vulnerabilidades a Verificar

Vulnerabilidades

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

Passo 2/6 - Analisar em Busca de Vulnerabilidades



Analisar Vulnerabilidades

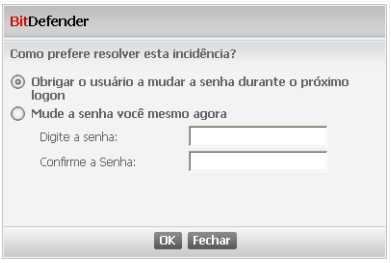
Espere que o BitDefender termine a análise de vulnerabilidades.

Passo 3/6 - Alterar Palvaras-passe Fracas

Senhas do usuário

Pode ver a lista dos usuários de contas Windows configurados no seu computador e o nível de proteção que as suas senhas garantem.

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



Mudar a senha

Seleccionar o método para reparar esta incidência:

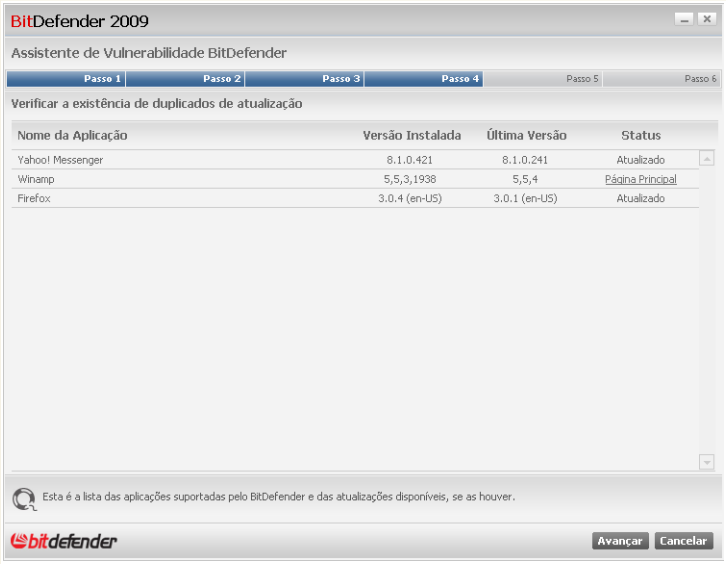
- **Forçar o usuário a mudar a senha no próximo login:** O BitDefender avisará o usuário que tem de alterar a senha da próxima vez que ele entrar no Windows.
- **Mudar a senha do usuário.** Deve inserir a nova senha nos campos editáveis.

> ***Nota***
> Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

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

Clique em **Próximo**.

Passo 4/6 - Actualizar Aplicações

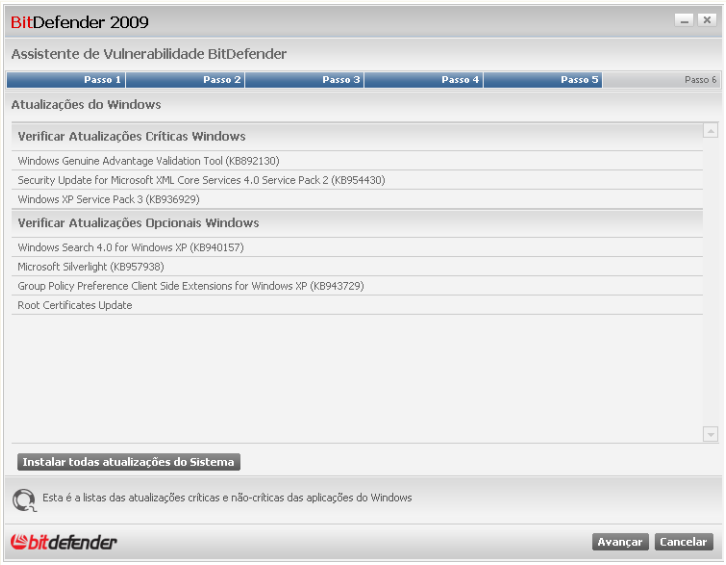


Aplicações

Pode ver a lista de todas as aplicações verificadas pelo BitDefender e se as mesmas estão ou não actualizadas. Se a aplicação não estiver actualizada, clique no link fornecido para descarregar a versão mais recente.

Clique em **Próximo**.

Passo 5/6 - Actualizar Windows



Actualizações Windows

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

Clique em **Próximo**.

Passo 6/6 - Ver Resultados

Resultados

Clique em **Fechar**.

8. TuneUp

BitDefender vem com um módulo de TuneUp que o ajuda a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco rígido.

Para executar operações de manutenção no seu PC, clique na barra **TuneUp** e use as ferramentas disponibilizadas.

Tuneup

O módulo de TuneUp é composto de duas secções:

- **Componentes Monitorizados** - Permite-lhe ver a lista completa das tarefas de tuneup monitorizadas. Pode escolher s tarefas a monitorizar.
- **Tarefas** - Aqui é onde pode encontrar os links para as tarefas de tuneup mais importantes: limpar e recuperar o registo, apagar arquivos permanentemente, apagar os arquivos temporários da Internet e as cookies, apagar arquivos duplicados, desfragmentar os discos locais.

8.1. Componentes Monitorizados

Há um componente monitorizado: Tuneup.

Clique na caixa marcada com o sinal "+" para abrir a categoria de Tuneup ou clique na que está marcada com o sinal "-" para a fechar.

8.1.1. Tuneup

As incidências que possam afectar a capacidade de resposta do seu sistema são descritas em frases bem explicítas. Ao mesmo tempo que cada frase, se existir algo que possa estar a afectar a segurança dos seus dados, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
Nunca levou a cabo uma limpeza do registo	O Limpa Registo analisa o Registo do Windows e apaga as chaves de registo inválidas. Leve a cabo uma limpeza do registo de tempos a tempos para melhorar o desempenho do seu computador.
Nunca levou a cabo um limpeza do seu computador	Levar a cabo uma limpeza do seu computador de tempos a tempos melhora o seu desempenho. Faça-a assim que lhe der jeito.
Nunca executou o Localizador de Duplicados	O localizador de duplicados optimiza o seu espaço em disco ao descobrir arquivos que estão em duplicado no seu sistema. Execute-o assim que lhe der jeito.
Nunca executou o Desfragmentador de Disco	A desfragmentação do disco reorganiza os dados contidos no disco rígido de forma a que as partes constituintes de cada arquivo sejam armazenadas juntas e de forma continua. Leve a cabo uma desfragmentação na altura que mais lhe convier.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

8.2. Tarefas

Estão disponíveis os seguintes botões:

- **Limpar Registo** - inicia o assistente que lhe permite limpar o Registo do Windows.
- **Recuperar Registo** - inicia o assistente que lhe permite recuperar o registo que foi limpo.
- **Destruir arquivos** - inicia o assistente que lhe permite remover arquivos permanentemente do seu computador.
- **Limpar arquivos Internet** - inicia o assistente que lhe permite apagar arquivos temporários da internet e cookies.
- **Encontrar arquivos Duplicados** - inicia o assistente que lhe permite descobrir e apagar arquivos em duplicado.
- **Defrag Discos** - inicia o assistente que lhe permite desfragmentar os discos locais.

8.2.1. Limpar o Registo

O Registo do Windows é uma parte importante dos sistemas operacional baseados no Windows. É uma base de dados que contém informação e definições do hardware e do sistema operacional, das aplicações instaladas, usuários, preferências do seu computador e outros.

Muitas aplicações escrevem chaves no Registo do Windows durante a instalação. Quando remove tais aplicações, algumas das suas chaves de registo associadas poderão não ser apagadas e continuarem no seu Registo do Windows, tornando o seu sistema mais lento e até causando instabilidade no mesmo. O mesmo acontece quando apaga atalhos para ou determinados arquivos das aplicações instaladas no seu sistema, como também no caso de drivers corrompidos.

Para limpar o Registo do Windows e melhorar o desempenho do seu sistema, use o Limpa Registo. O Limpa Registo analisa o Registo do Windows e apaga as chaves de registo inválidas.

Para limpar o Registo do Windows, clique em **Limpa Registo**. Terá de completar de seguida um processo guiado de quatro passos.

Passo 1/4 - Iniciar a Análise

Aqui pode dar início à análise do registo.

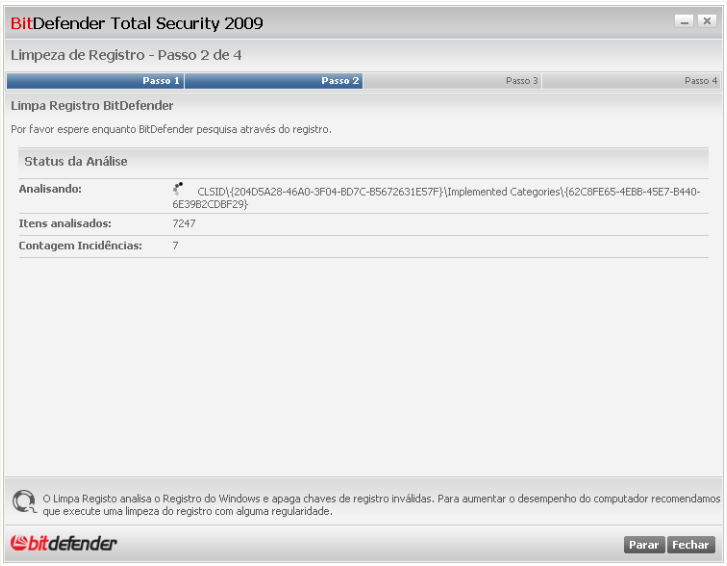
Status

Pode ver quando o Limpa Registo se executou pela última vez e as recomendações do BitDefender.

Clique em **Próximo**.

Passo 2/4 - A analisar...

O Limpa Registo começará a analisar o Registo do Windows.



A analisar...

Pode ver a última chave do registo que foi analisada e as estatísticas relacionadas.

Espere que o Limpa Registo termine a análise do registo. Se deseja cancelar a operação clique em **Cancelar**.

Nota
Se deseja para a análise, apena clique em **Parar**. Saltará de imediato para o próximo passo.

Passo 3/4 - Seleccionar a acção

Após a análise das chaves do registo estar completa, surgirá uma nova janela onde pode ver os resultados.

Nota
Se não forem encontradas quaisquer incidências ou se escolheu parar a análise, saltará este passo.

Ações

Pode ver todas as chaves de registo inválidas ou orfãs detectadas. Informação detalhada é fornecida para cada chave de registo (nome, valor, prioridade, categoria).

As chaves de registo estão agrupadas baseado na sua localização no Registo do Windows:

Categoria	*Descrição*
Localizações do Software	Chaves de registo que contêm informação sobre o caminho para as aplicações instaladas no seu computador. As chaves inválidas têm atribuida uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.
Controles Pessoais	Chaves de registo que contêm informação acerca das extensões dos arquivos registados no seu computador. Estas chaves de registo são normalmente usadas para manter associações de arquivos (para assegurar que o programa correto abre quando abre um arquivo

Categoria	Descrição
	usando o Explorador do Windows). Por exemplo, tal chave de registo permite que o Windows abra um arquivo `.doc` com o Microsoft Word. As chaves inválidas têm atribuida uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.
DLLs partilhadas	As chaves de registo que contêm informação sobre a localização das DLLs (Dynamic Link Libraries) partilhadas. Funções de armazenagem DLLs que são usadas pelas aplicações instaladas para levar a cabo certas tarefas. Podem ser partilhadas por múltiplas aplicações para reduzir os requisitos de espaço em disco e em memória. Estas chaves de registo tornam-se inválidas quando a DLL que apontam é movida para outro local ou completamente removida (isto acontece quando desinstala um programa). As chaves inválidas têm atribuidas uma prioridade média, o que significa que apagá-las pode afectar negativamente o sistema.

Para manusear mais facilmente o processo de limpeza, pode seleccionar a categoria a partir do menu.

Pode escolher apagar todas ou apenas determinadas chaves inválidas de uma categoria específica. Se seleccionou **Apagar todas**, todas as chaves detectadas serão apagadas. Se deseja eliminar somente chaves específicas, seleccione a opção**Apagar** junto da respectiva chave.

Nota
Por defeito, todas as chaves detectadas serão apagadas.

Clique em **Próximo**.

Passo 4/4 - Ver Sumário dos Resultados

Aqui poderá ver os resultados da análise executada pelo Limpa Registo.

Sumário dos Resultados

Se não escolheu apagar todas as chaves de registo, um texto de aviso será apresentado. Recomendamos que reveja as respectivas incidências.

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

8.2.2. Recuperar Limpeza de Registo

Por vezes, após limparmos o registo, poderá notar que o seu sistema não funciona bem ou que algumas aplicações não funcionam bem devido à falta de chaves no registo. Isto pode ser causado devido a chaves de registo partilhadas que foram apagadas durante a limpeza do registo ou por outras chaves apagadas. Para resolver este problema deverá recuperar o registo que foi limpo.

Para recuperar o registo que foi limpo, clique em **Recuperar Registo**. Terá de completar de seguida um procedimento guiado com dois passos.

Importante
Apenas os usuários com direitos de administrador no sistema podem recuperar o registo que foi limpo.

Passo 1/2 - Iniciar Recuperação do Registo

Aqui pode dar início à recuperação da limpeza de registo.

Status

Pode ver uma lista de pontos no tempo em que o Registo do Windows foi limpo. Seleccione o ponto no tempo para restaurar o Registo do Windows.

Se tem a certeza que deseja recuperar a chaves de registo que foram apagadas no ponto de tempo seleccionado, clique em **Seguinte**.

Atenção
A recuperação da limpeza de registo pode sobrescrever as últimas chaves do registo que foram editadas desde a última limpeza do registo.

Passo 2/2 - Ver Resultados

Aqui pode ver se a recuperação foi bem-sucedida.

Resultados

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

8.2.3. Apagar arquivos Permanentemente

Quando apaga um arquivo, o mesmo já não fica acessível por meios normais. No entanto o arquivo continua armazenado no disco rígido até que seja sobrescrito quando copiar para lá novos arquivos.

Mesmo que apague o arquivo, o mesmo pode ser recuperado usando programs especializados. Isto poderá representar uma ameaça à sua privacidade pois poderão ocorrer tentativas maliciosas de se apoderarem da sua informação privada.

Para evitar que informação sensível seja recuperada após a apagar, pode usar o BitDefender para apagar permanentemente aqueles dados removendo-os fisicamente do seu disco rígido.

Para apagar permanentemente os arquivos, clique em **Destruir arquivos**. Depois terá de completar um procedimento guiado de três passos.

Passo 1/3 - Seleccionar Alvo

Aqui pode especificar os arquivos ou pastas que deseja apagar permanentemente.

Alvo

Clique em **Adicionar Alvo**, e seleccione o arquivo ou pasta que deseja apagar e clique em **OK**. O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela.

Nota
Pode seleccionar um ou vários locais.

Clique em **Próximo**.

Passo 2/3 - A eliminar os arquivos...

O BitDefender apagará permanentemente os arquivos dos locais especificados.

A apagar...

Espere que a operação de eliminação dos arquivos termine. Se deseja cancelar a operação clique em **Cancelar**.

Passo 3/3 - Ver Sumário de Resultados

Após os arquivos terem sido removidos, uma nova janela aparecerá onde poderá ver os resultados.

Sumário dos Resultados

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

8.2.4. Limpar arquivos da Internet

Cada vez que visita uma página web, são criados arquivos temporários da Internet de forma a permitir que lhe aceda mais rapidamente da próxima vez.

Apesar de serem apelidados de temporários, estes arquivos não são apagados quando desliga o seu browser de internet. Isto poderá resultar numa questão de privacidade porque estes arquivos podem ser vistos por qualquer pessoa que tenha acesso ao seu computador. E mais ainda, estes arquivos ao fim de algum tempo atingem um tamanho considerável, ocupando desnecessariamente espaço do seu disco rígido.

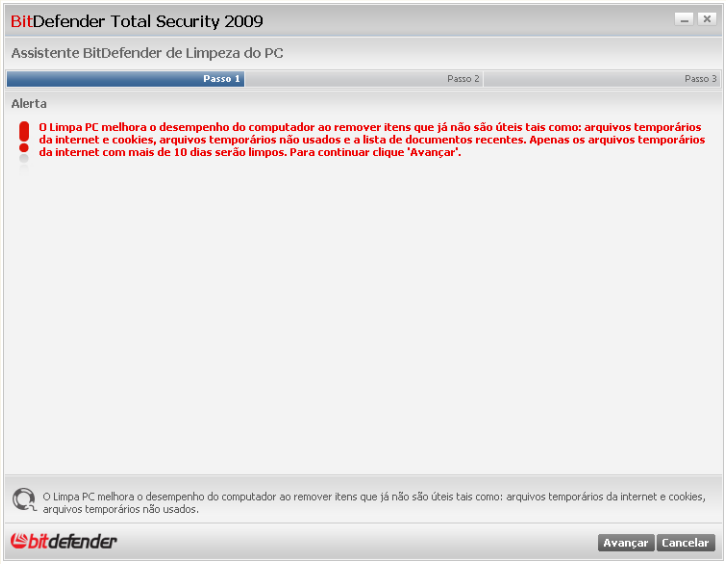
Os cookies também são armazenados na seu computador quando visita uma página web. Os cookies são pequenos arquivos que contém informação sobre as suas preferências de navegação na web. Eles poderão ser vistos também como uma questão de privacidade também, pois eles podem ser analisados e usados por publicitários para rastrear os seus interesses e gostos on-line.

Ao limpar os seus arquivos temporários da internet e os cookies, você liberta espaço em disco e protege a sua privacidade.

Para limpar a pasta dos arquivos Temporários da Internet, onde o Internet Explorer armazena os arquivos temporários da internet e os cookies, clique em **Limpar arquivos Internet**. Seguir-se-á um processo guiado de três passos.

Passo 1/3 - Iniciar a Eliminação

Aqui pode dar início à eliminação dos arquivos temporários da internet e dos cookies.

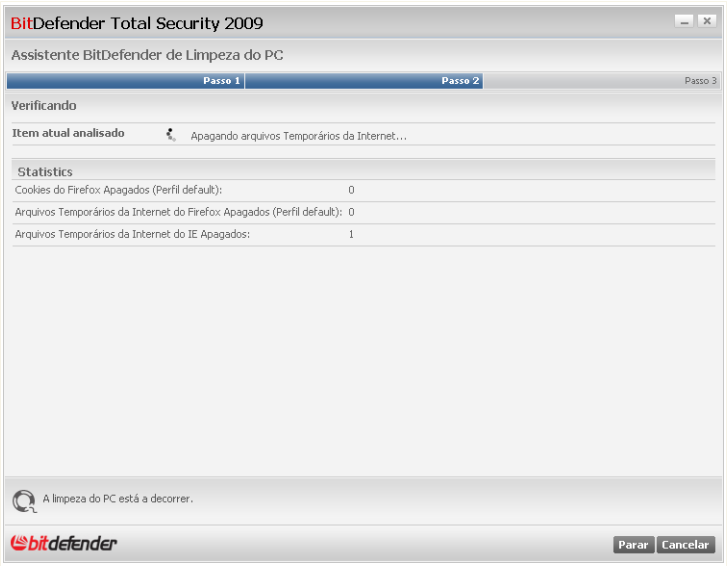


Janela de Boas-Vindas

Clique em **Próximo**.

Passo 2/3 - A eliminar os arquivos...

O eliminador começará a apagar os arquivos temporários da internet e os cookies.



A eliminar os arquivos...

Espere que o Eliminador apague os arquivos temporários da internet e os cookies. Se deseja cancelar a operação clique em **Cancelar**.

Passo 3/3 - Ver Sumário de Resultados

Após o eliminador ter apagados todos os arquivos, uma nova janela surgirá onde poderá ver o sumário de resultados.

Sumário dos Resultados

Pode ver as estatística com respeitos aos objectos apagados.

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

8.2.5. Localizar arquivos Duplicados

Os arquivos duplicados comem o seu espaço em disco. Imagine ter o mesmo arquivo `.mp3` aramazenado em três diferentes locais.

Para detectar e apagar arquivo duplicados no seu computador, pode usar o Localizador de Duplicados. Desta forma pode melhorar a gestão do espaço livre nos seus discos rígidos.

Para encontrar duplicados, clique em **Localizar arquivos Duplicados**. Terá de completar um processo guiado de quatro passos.

Passo 1/4 – Seleccionar o Alvo da Procura

Aqui pode especificar onde deseja procurar duplicados.

Alvo da Procura

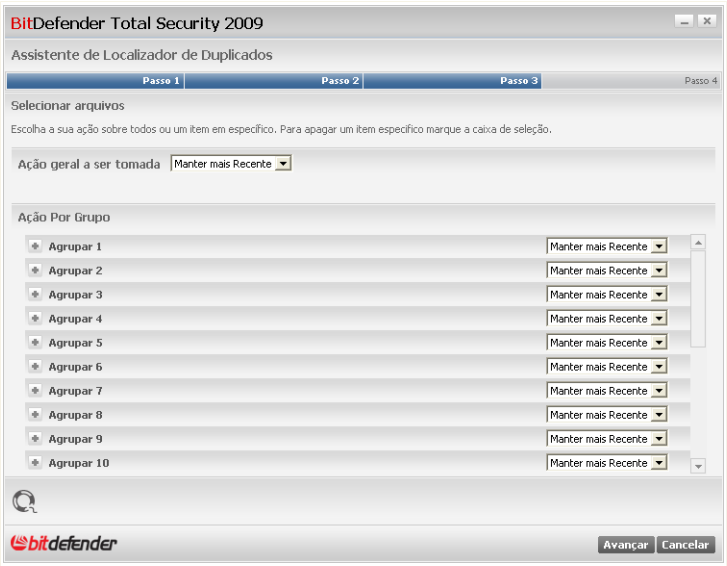
Clique em **Adicionar Alvo**, e selecione o local onde o Localizador de Duplicados deve de procurar por arquivos duplicados. O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela.

Nota
Pode seleccionar um ou vários locais.

Clique em **Próximo**.

Passo 2/4 - A procurar...

O Localizador de Duplicados começará à procura de arquivos duplicados.



A procurar...

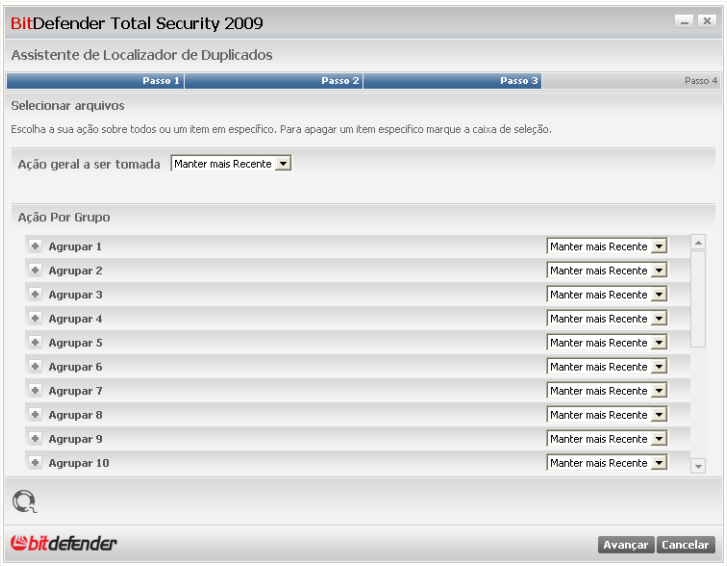
Pode ver o estado da procura e as estatísticas.

Espere que o Localizador de Duplicados complete a sua procura de arquivos duplicados. Se deseja cancelar a operação clique em **Cancelar**.

Passo 3/4 - Seleccionar a acção

Após a procura estar terminada, uma nova janela aparecerá onde pode especificar que ações devem ser tomadas sobre os arquivos duplicados detectados.

Nota
Se não forem encontrados arquivos duplicados, saltará este passo.



Ações

Os arquivos duplicados detectados são organizados e mostrados em grupos. Se clicar em ⊞ junto de um grupo, pode ver info detalhada acerca dos arquivos duplicados (caminho, tamanho, data de criação e modificação).

Pode escolher a acção geral a ser tomada em todos os arquivos duplicados encontrados ou pode escolher ações a serem tomadas em grupos de arquivos duplicados. As seguintes acções estão disponíveis no menu:

Ação	*Descrição*
Manter Recente	O duplicado mais recente será mantido, enquanto que os outros duplicados serão apagados.
Manter Antigo	O duplicado mais antigo será mantido, enquanto que os outros duplicados serão apagados
Nenhuma Acção>	Nenhuma ação será executada sobre os arquivos duplicados.

Se deseja aplicar uma ação geral a todos os objetos de um grupo, selecione a ação desejada do menu correspondente. Se apena deseja especificar arquivos do grupo a serem apagados, selecione a opção **Apagar** ao pé dos respectivos arquivos.

Nota
A ação geral não sobrescreverá a ação escolhida para os arquivos ou grupos especificados. Isto significa, por exemplo que se define **Manter Recente** como a ação geral, mas escolhe não tomar ação sobre um grupo em particular, então a ação geral será aplicada a todos menos a esse grupo em particular.

Clique em **Próximo**.

Passo 4/4 - Ver Sumário dos Resultados

Aqui pode ver os resultados da análise do Localizador de Duplicados.

Sumário dos Resultados

Clique em **Repetir** para iniciar uma nova procura de arquivos duplicados ou clique em **OK** para fechar a janela.

8.2.6. Desfragmentar Volumes de Discos Duros

Quando copia um arquivo que excede o tamanho do maior bloco de espaço livre no disco rígido, a fragmentação do arquivo ocorre. Porque não existe suficiente espaço livre para guardar o arquivo de forma contínua, o mesmo é armazenado em diversos blocos. Quando o arquivo framentado é acedido, os seus dados têm de ser lidos de diversos locais diferentes.

A fragmentação dos arquivos torna mais lento o acesso aos mesmo e diminui o desempenho do sistema. Também acelera o desgaste do seu disco rígido.

Para reduzir a fragmentação de arquivos, deve de desfragmentar os seus discos periodicamente. A desfragmentação do disco reorganiza os dados contidos no disco rígido de forma a que as partes constituintes de cada arquivo sejam armazenadas juntas e de forma continua. Também tenta criar área de espaço livre maiores de forma a evitar que os arquivos sejam mais tarde fragmentados.

É recomendável que desfragmente o seu disco rígido de forma a que:

- acesse mais rápido aos arquivos.
- melhore o desempenho do sistema em geral.
- aumente o tempo de duração do seu disco rígido.

Para desfragmentar o disco rígido, clique em **Defrag Discos**. Será de seguida guiado através de um processo completo de três passos.

Nota
A desfragmentação poderá demorar algum tempo uma vez que involve o mover de porções de dados armazenados de um lugar para o outro do disco rígido. Recomendamos que execute a desfragmentação quando não está a usar o seu computador.

Passo 1/3 - A analisar...

O Desfragmentador do Disco irá analisar o disco rígido para determinar se o mesmo necessita ou não de ser desfragmentado.

A analisar

Espere que o Desfragmentador do Disco termine a análise. Se deseja cancelar a operação clique em **Cancelar**.

Passo 2/3 - Ver o Relatório da Análise

Após a análise estar completa, uma nova janela surgirá onde poderá ver os resultados e iniciar a desfragmentação do disco se necessário.

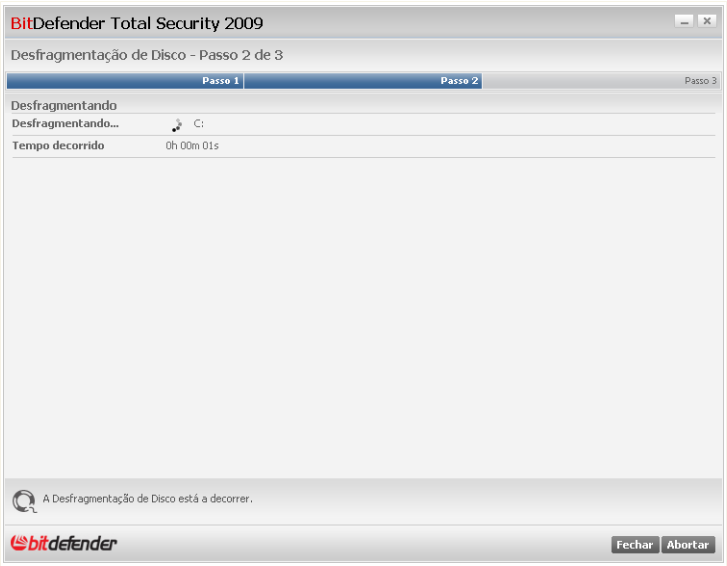
Relatório da Análise

Verificar o relatório da análise.

Se nenhum dos volumes do disco necessita de ser desfragmentado, clique em **Fechar** para fechar a janela. Caso contrário, seleccione a opção **Defrag** correspondente ao volume do disco que necessita de ser desfragmentado e clique em **Executar** para o desfragmentar.

Nota

O Desfragmentador do Disco necessita de 15% de espaço livre no disco a desfragmentar de forma a funcionar correctamente. Se não existir suficiente espaço livre no volume a desfragmentar, a desfragmentação será abortada.



A Desfragmentar

Espere que a desfragmentação do disco termine. Pode cancelar a desfragmentação do disco a qualquer altura clicando em **Abortar**.

Passo 3/3 - Ver Relatório de Desfragmentação

Após a desfragmentação do disco se completar, surgirá uma nova janela onde pode ver as estatísticas de desfragmentação.

Relatório de Desfragmentação

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

9. Gestor de arquivos

BitDefender traz consigo um módulo de Gestor de arquivos que o ajuda a manter os seus dados não apenas seguros, mas também confidenciais. Para atingir este objectivo, faça backup dos seus arquivos e use o cofre de arquivos.

Backup. A protecção antivírus sózinha já não é suficiente para proteger os seus dados valiosos. Por exemplo, o seu computador encontra-se limpo de vírus mas por qualquer razão o mesmo vai abaixo quando necessita mais dele. É aqui que a secção de Backup dos seu módulo de Gestor de arquivos vem mesmo a calhar. Pode, de forma segura, fazer backup dos seus dados com o BitDefender.

Cofre de arquivos. Certamente que quererá que os seus ficheiros mais sensíveis sejam mantidos fora da vista de outros. É aqui que a secção do Cofre de arquivos no módulo de Gerir arquivos, vem mesmo a calhar.

- O cofre de arquivos é um espaço de armazenamento seguro de informação pessoal ou de arquivos considerados sensíveis.
- O cofre de arquivos é um arquivo encriptado no seu computador com a extensão `bvd`.
- Como se encontra encriptado, os dados contidos no mesmo são invulneráveis ao roubo ou a uma quebra de segurança.
- Quando monta o arquivo `bvd`, uma nova partição lógica (nova drive) surge. Será mais fácil compreender este processo se pensar em algo similar: montar uma imagem ISO como um CD virtual.

Abra o Meu Computador e verá uma nova drive baseada no cofre de arquivos. Será capaz de fazer operações com arquivos nele (copiar, apagar, alterar, etc.). Os arquivos estão protegidos na medida em que estejam residentes nesta drive (porque é necessária uma senha para a operação de montagem). Quando terminar, fechar (desmontar) o seu cofre de forma a iniciar a protecção do seu conteúdo.

Para entrar no módulo de Gestor de arquivos, clique na barra **Gestor arquivos**.

Gestor de arquivos

O módulo de Gestor de arquivos é composto de duas seções:

- **Componentes Monitorizados** - Permite-lhe ver a lista completa dos componentes monitorizados para cada módulo. Pode escolher quais os módulos a serem monitorizados. É recomendável activar a monitorização de todos os componentes.
- **Tarefas** - Aqui é onde pode encontrar os links para as tarefas de segurança mais importantes: backup local e restauro, adicionar, ver e apagar cofres de arquivos.

9.1. Componentes Monitorizados

Os componentes monitorizados estão agrupados em diversas categorias:

Os componentes monitorizados são os seguintes:

Categoria	Descrição
Cofre de arquivos	O cofre de arquivos é um espaço de armazenamento seguro de informação pessoal ou de arquivos considerados sensíveis. É mantido localmente, no seu computador. Como se encontra

Categoria	Descrição
	encriptado, os dados contidos no mesmo são invulneráveis ao roubo ou a uma quebra de segurança.
Backup	Ajuda-o a fazer cópias de reserva de quaisquer dados valiosos do seu sistema. É recomendável usar esta ferramenta para armazenar em segurança os seus dados mais importantes.

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

9.1.1. Cofre de arquivos

As incidências que poderão afectar a privacidade dos seus dados são descritas em frases bem explicítas. Ao mesmo tempo, se existir algo que que possa afectar a privacidade dos seus dados, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	Descrição
Apenas o **O Cofre de arquivos está ativo**	O Cofre de arquivos mantém os seus documentos privados ao encriptá-los em drives de cofre especiais.

Quando o botão de estado está verde, o risco de segurança para o seus dados é miníma. Para colocar os botões verdes, siga estes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

9.1.2. Backup

As incidências que poderão estar a afectar o seu sistema são descritas em frases bastantes explicítas. Ao mesmo tempo que cada frase, se existir algo que possa estar

a afectar a segurança dos seus dados, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
Levou a cabo um backup offline no seu computador há x dias atrás	O módulo de backup offline ajuda-o a fazer cópias de reserva de quaisquer dados valiosos do seu sistema.

Quando o botão de estado está verde, o risco de segurança para o seus dados é miníma. Para colocar os botões verdes, siga estes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

9.2. Tarefas

Estão disponíveis os seguintes botões:

- **Backup Local** - Inicia o assistente que o ajuda a fazer cópias de reserva de quaisquer dados valiosos no seu computador, num CD, num local de rede ou noutra drive de disco.
- **Restauro Local** - Inicia o assistente que o ajuda a restaurar os dados que foram backup no seu computador, num CD, num local de rede ou noutra drive de disco.
- **Configuração Backup** - aqui é onde pode definir e executar operações de backup em detalhe.

> ***Nota***
> Para mais informação, por favor consulte o "*Backup Avançado*" (p. 295).

- **Adicionar ao Cofre** - inicia o assistente que lhe permite armazenar de forma privada os seus arquivos / documentos importantes ao encriptá-los em drives de cofre especiais.

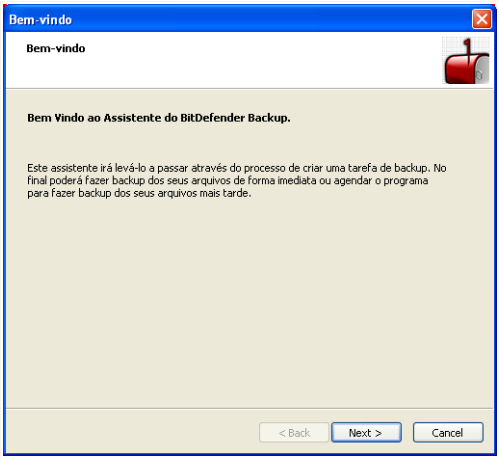
- **Remover do Cofre** - inicia o assistente que lhe permite apagar dados do cofre de arquivos.
- **Ver cofre** - inicia o assistente que lhe permite ver o conteúdo do cofre de arquivos.
- **Fechar cofre** - inicia o assistente que lhe permite fechar o cofre de forma a dar início à protecção do seu conteúdo.

9.2.1. Fazer Backup Local de Dados

Ao clicar em **Backup Local** um assistente irá levá-lo através do processo de criar uma tarefa de backup local. No final do processo será capaz de fazer backup dos seus dados na hora ou agendar o produto para o fazer mais tarde.

Passo 1/5 - Janela de Boas-vindas

Esta é uma página de boas-vindas.

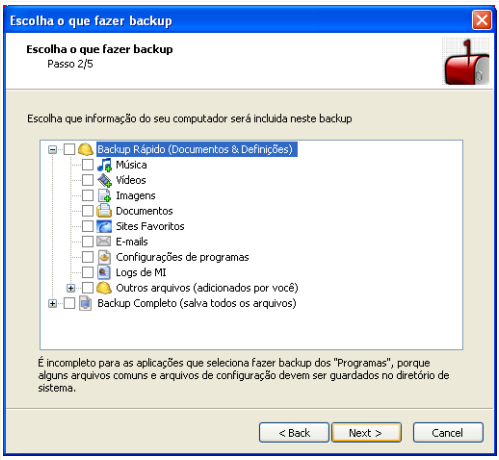


Janela de Boas-Vindas

Clique em **Próximo**.

Passo 2/5 - Escolher do que fazer Backup

Aqui pode escolher que dados do seu computador deseja fazer backup.



Escolher do que fazer backup

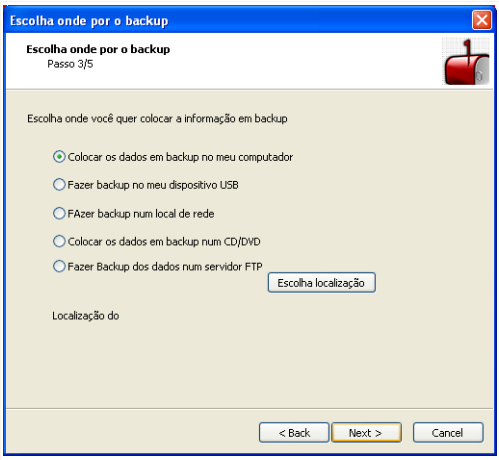
Pode escolher fazer **Backup Rápido** (a sua música, videos, imagens, e-mails, definições de aplicações, etc.) ou **Backup Completo** (todas as partições).

Clique em **Outros ficheiros**, para adicionar outros arquivos do seu Ambiente de Trabalho ao **Backup Rápido**. O **Backup Completo** pode também ser facilmente personalizado ao selecionar que diretórios de um determinada partição deseja fazer backup.

Clique em **Próximo**.

Passo 3/5 - Escolher para onde fazer Backup

Aqui pode seleccionar o local onde guardar os dados do backup.



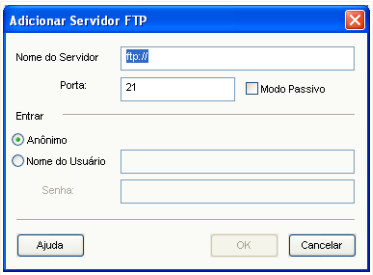
Escolha para onde fazer backup

As seguintes opções estão disponíveis:

- **Fazer Backup dos meus dados no meu computador**
- **Fazer o Backup para a minha drive USB**
- **Fazer o Backup para um local de rede**
- **Fazer o Backup para o CD/DVD**
- **Fazer Backup num Servidor FTP**

Se decidir fazer backup para o seu computador, a sua drive USB ou num local de rede, clique em **Escolher Local** e seleccione o local onde deseja guardar os dados.

Se você deseja efetuar um backup de seus dados em um servidor FTP, clique **Escolha o Local** e adicione o servidor FTP. Uma nova janela irá aparecer.



Adicionar Servidor FTP

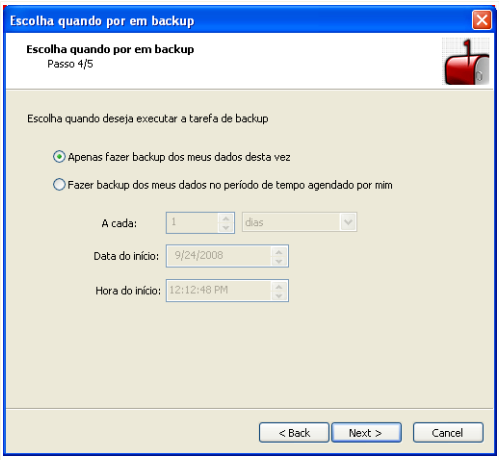
Você precisa determinar as configurações de conexão do servidor FTP como segue:

1. Digite o nome do servidor FTP no campo correspondente.
2. Se o servidor FTP usar uma porta diferente da porta padrão 21, digite-a no campo correspondente.
3. Para usar o modo passivo (o servidor FTP inicia a conexão), selecione **Modo Passivo** selecione opção.
4. Se o servidor permite acessos anônimos, você pode deixar a opção **Anônimo** selecionada. Caso contrário, selecione **Nome de Usuário** e digite o nome do usuário e senha de uma conta reconhecida pelo servidor FTP.
5. Clique em **OK**.

Clique em **Próximo**.

Passo 4/5 - Escolher quando fazer o Backup

Aqui pode seleccionar quando deseja fazer o backup dos dados.



Escolher quando fazer o backup

As seguintes opções estão disponíveis:

- **Fazer Backup dos dados só esta vez**
- **Fazer Backup dos dados numa data agendada por mim**

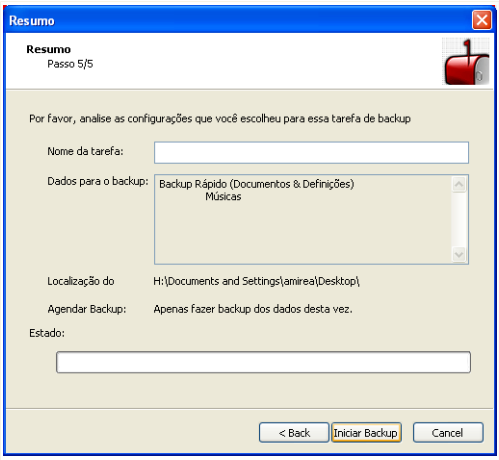
Para fazer backup dos arquivos na hora clique em **Fazer Backup dos dados só esta vez**, para agendar o produto para fazer backup mais tarde, clique **Fazer Backup dos dados numa data agendada por mim**.

Se seleccionar **Fazer Backup dos dados numa data agendada por mim**, pode especificar com que frequência a tarefa agendada será executada: diariamente ou semanalmente. Pode também especificar a data e a hora.

Clique em **Próximo**.

Passo 5/5 - Sumário

Aqui você pode rever as configurações do trabalho de backup e iniciar o backup.



Sumário

Deve inserir um nome de tarefa no campo correspondente. Você pode efetuar qualquer mudança, bastando voltar aos passos anteriores (clique **Voltar**).

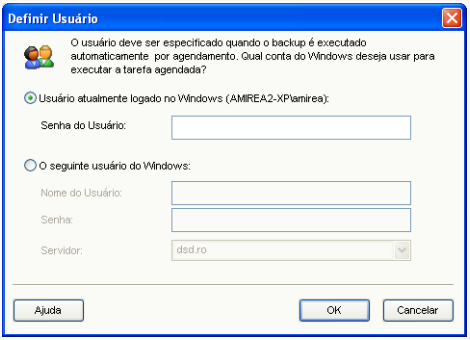
Clique em **Iniciar backup** se estiver satisfeito com as suas definições. Espere até que o BitDefender complete o backup e então clique **Finalizar**.

Nota

A primeira vez que você determinar o agendamento de um trabalho de backup, você será orientado a especificar a conta do Windows usada para executar o trabalho.

Para usar a conta de usuário atual, basta digitar a senha deste usuário no campo correspondente. Se você deseja executar o backup usando uma conta diferente, selecione **O seguinte usuário do Windows** e preencha nos campos.

- **Nome do Usuário** - digite o nome da conta do Windows.
- **Senha** - a senha do usuário da conta especificado anteriormente.
- **Servidor** - digite o nome do domínio do servidor.



Definir Usuário

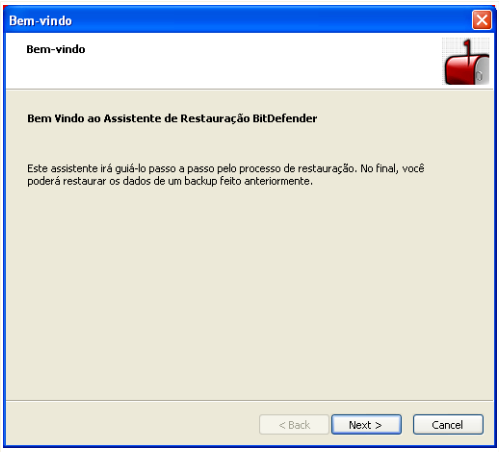
Clique **OK** para continuar.

9.2.2. Restauro Local dos Dados em Backup

Ao clicar em **Restauro Local** um assistente irá levá-lo através do processo de restaurar o seu backup local.

Passo 1/4 - Janela de Boas-vindas

Esta é uma página de boas-vindas.

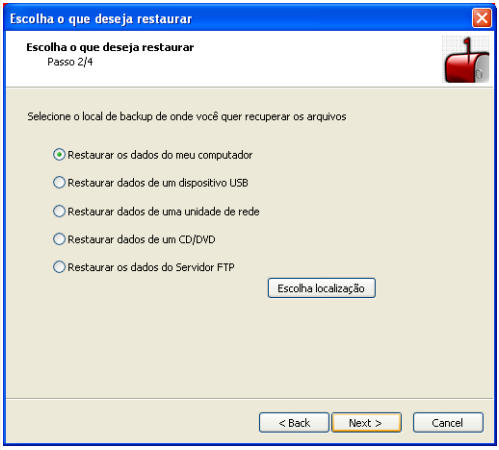


Janela de Boas-Vindas

Clique em **Próximo**.

Passo 2/4 - Escolha de onde deseja restaurar o Backup

Aqui pode selecionar um local de onde deseja restaurar os arquivos.



Escolha de onde deseja restaurar o Backup

As seguintes opções estão disponíveis:

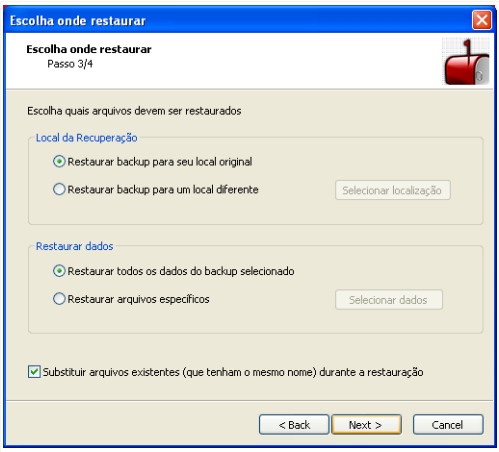
- **Restaurar os dados do meu computador**
- **Restaurar backup de uma drive USB**
- **Restaurar backup de um local de rede**
- **Restaurar backup de um CD/DVD**
- **Restaurar backup de um servidor FTP**

Após selecionar uma opção, clique **Escolha o local** e selecione o arquivo de backup o qual você deseja restaurar.

Clique em **Próximo**.

Passo 3/4 - Escolher o Local e os arquivos de Restauro

Aqui é onde pode escolher que arquivos específicos a restaurar e para onde os restaurar.



Escolher o local e os arquivos de restauro

As seguintes opções estão disponíveis:

- **Restaurar o backup ao seu local de origem**
- **Restaurar o backup para um local diferente**
- **Restaurar todos os dados do local de backup seleccionado**
- **Restaurar arquivos específicos**
- **Sobrescrever os arquivos existentes quando restaurar**

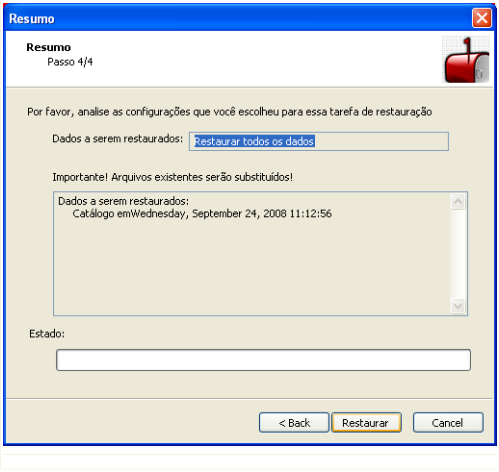
Se deseja restaurar dados para outro local ou apenas arquivos específicos, selecione o local e os dados clicando no botão correspondente.

Para evitar sobreescrever o arquivo existente durante o restauro, limpe a caixa de seleção **Sobrescrever os arquivos existentes quando restaurar**.

Clique em **Próximo**.

Passo 4/4 - Sumário

Aqui você pode rever as configurações do trabalho de restauração e iniciar o processo.



Clique em **Restaurar** se estiver satisfeito com as suas definições. Espere até que o BitDefender restaure os dados selecionados e então clique **Finalizar**.

9.2.3. Adicionar arquivos ao Cofre

O cofre de arquivos é um sitio especial que é usado para armazenar coisas valiosas em condições segura. Os documentos dentro de um cofre de arquivos são encriptados.

Ao clicar em **Adicionar ao cofre** um assistente irá levá-lo através do processo de criar um cofre e adicionar-lhe documentos.

Passo 1/6 - Seleccionar Alvo

Aqui pode especificar os arquivos ou pastas a serem adicionados ao cofre.

Alvo

Clique em **Adicionar Alvo**, selecione o arquivo ou pasta que deseja adicionar e clique em **OK**. O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela.

Nota
Pode seleccionar um ou vários locais.

Clique em **Próximo**.

Passo 2/6 - Seleccionar cofre

Aqui é onde pode criar um novo cofre ou escolher um já existente.

Seleccionar cofreSelecione portas

Se selecionar **Explorar Cofre de arquivos**, deve de clicar **Explorar** e seleccionar o cofre de arquivos. Irá de seguida para o passo 5 se o cofre seleccionado estiver aberto (montado) ou para o passo 4 se estiver fechado (desmontado).

Se clicar em **selecionar um Cofre existente**, deve de clicar no nome do cofre que deseja. Irá de seguida para o passo 5 se o cofre seleccionado estiver aberto (montado) ou para o passo 4 se estiver fechado (desmontado).

Seleccione **Criar um Novo Cofre de arquivos** se nenhum dos existentes satisfizer as suas necessidades. Irá de seguida para o passo 3.

Clique em **Próximo**.

Passo 3/6 - Criar Cofre

Aqui é onde pode especificar informação do novo cofre.

Criar Cofre

Para completar a informação relacionada com o cofre de arquivos, siga estes passos:

1. Clique em **Explorar** e escolha uma localização para o arquivo `bvd`.

   Nota
   Lembre-se que o cofre de arquivos é um arquivo encriptado com a extensão `bvd` que se encontra no seu computador.

2. Selecione a letra da drive para o novo cofre de arquivos a partir do menu drop-down correspondente.

   Nota
   Lembre-se que quando monta o arquivo `bvd` uma nova partição lógica (nova drive) irá aparecer.

3. Insira a senha do cofre de arquivos no campo correspondente.

Nota
A senha deve ter pelo menos oito caracteres em tamanho.

4. Confirmar senha
5. Defina o tamanho do cofre de arquivos (em MB) ao inserir o número no campo correspondente.

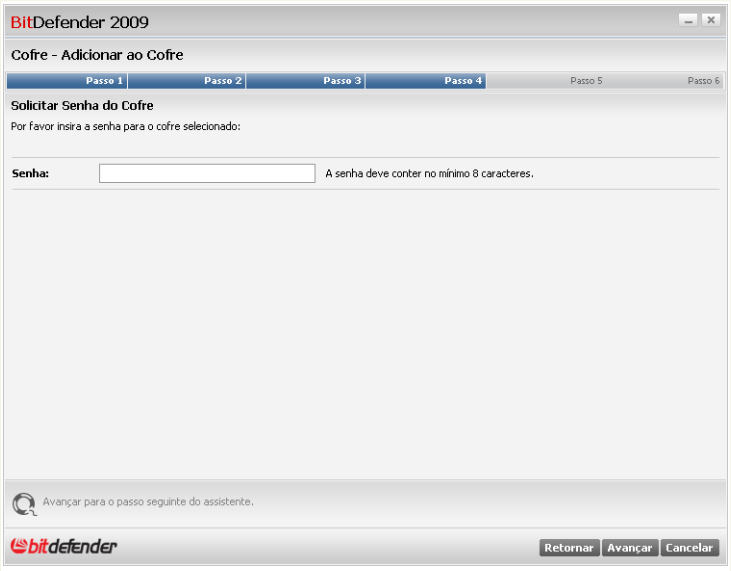
Nota
O tamanho deve de conter apenas dígitos.

Clique em **Próximo**.

Irá para o passo 5.

Passo 4/6 - Senha

Aqui é onde lhe será solicitada a senha para o cofre seleccionado.



Confirmar senha

Insira a senha no campo correspondente e depois clique em **Seguinte**.

Passo 5/6 - Resumo

Aqui é onde pode rever as operações escolhidas.

Sumário

Clique em **Próximo**.

Passo 6/6 - Resultados

Aqui é onde pode ver o conteudo do cofre.

Resultados

Clique em **Finalizar**.

9.2.4. Remover arquivos do Cofre

Ao clicar em **Remover Cofre de arquivos**, um assistente irá levá-lo através do processo de remover arquivos de um determinado cofre.

Passo 1/5 - Seleccionar Cofre

Aqui é onde pode selecionar o cofre de onde deseja remover arquivos.

Seleccionar cofreSelecione portas

Se selecionar **Explorar um Cofre de arquivos**, deve de clicar em **Explorar** e seleccionar o cofre de arquivos. Irá de seguida para o passo 3 se o cofre selecionado estiver aberto (montado) ou para o passo 2 se estiver fechado (desmontado).

Se clicar em **Selecionar um Cofre de arquivos existente**, deve de clicar no nome do cofre desejado. Irá de seguida para o passo 3 se o cofre selecionado estiver aberto (montado) ou para o passo 2 se estiver fechado (desmontado).

Clique em **Próximo**.

Passo 2/5 - Senha

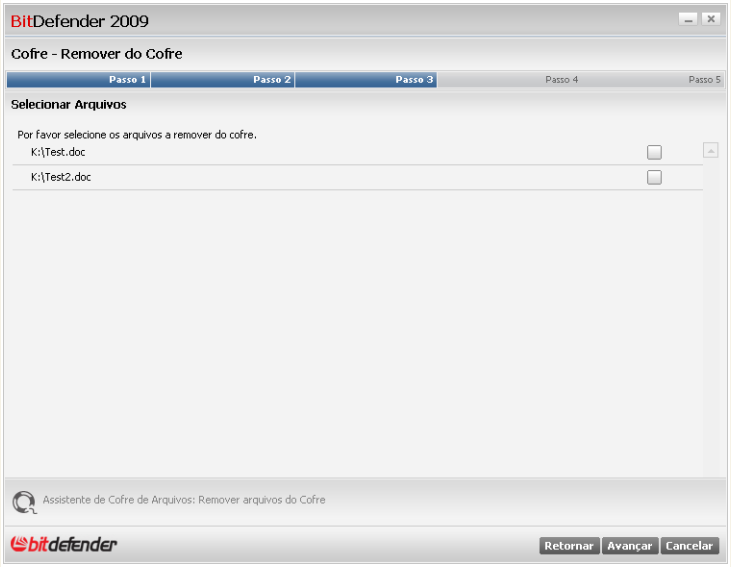
Aqui é onde lhe será solicitada a senha para o cofre seleccionado.

Confirmar senha

Insira a senha no campo correspondente e depois clique em **Seguinte**.

Passo 3/5 - Seleccionar arquivos

Aqui é onde lhe será fornecida a lista dos arquivos do cofre previamente selecionado.

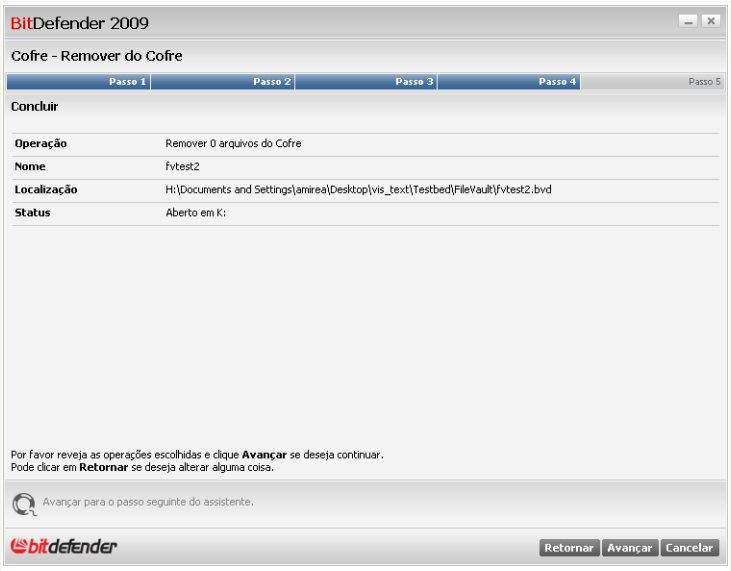


Selecionar arquivos

Selecione os arquivos a serem removidos e clique **Seguinte**.

Passo 4/5 - Sumário

Aqui é onde pode rever as operações escolhidas.



Sumário

Clique em **Próximo**.

Passo 5/5 - Resultados

Aqui é onde poder ver o resultado da operação.

Resultados

Clique em **Finalizar**.

9.2.5. Ver arquivos do Cofre

Ao clicar em **Ver Cofre**, um assistente irá levá-lo através do processo de ver os arquivos de um determinado cofre.

Passo 1/4 - Seleccionar Cofre

Aqui é onde pode selecionar o cofre de onde deseja ver os arquivos.

Seleccionar cofreSelecione portas

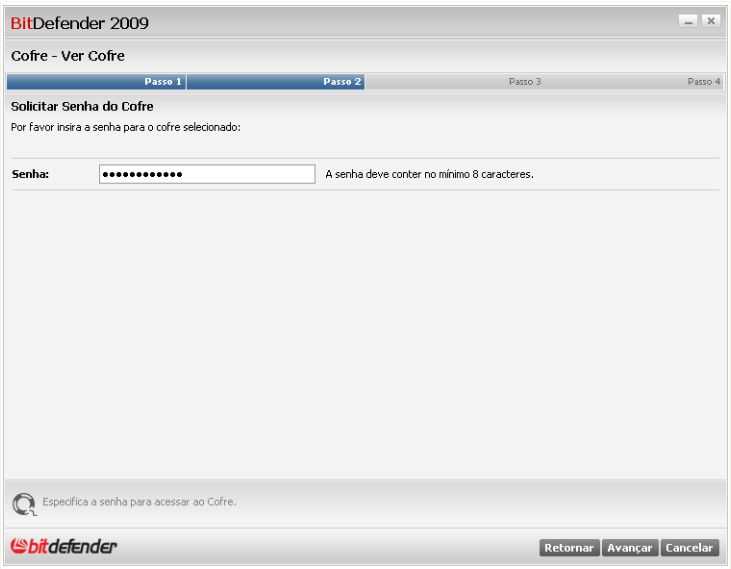
Se selecionar **Explorar um Cofre de arquivos**, deve de clicar em **Explorar** e seleccionar o cofre de arquivos. Irá de seguida para o passo 3 se o cofre selecionado estiver aberto (montado) ou para o passo 2 se estiver fechado (desmontado).

Se clicar em **Selecionar um Cofre de arquivos existente**, deve de clicar no nome do cofre desejado. Irá de seguida para o passo 3 se o cofre selecionado estiver aberto (montado) ou para o passo 2 se estiver fechado (desmontado).

Clique em **Próximo**.

Passo 2/4 - Senha

Aqui é onde lhe será solicitada a senha para o cofre seleccionado.

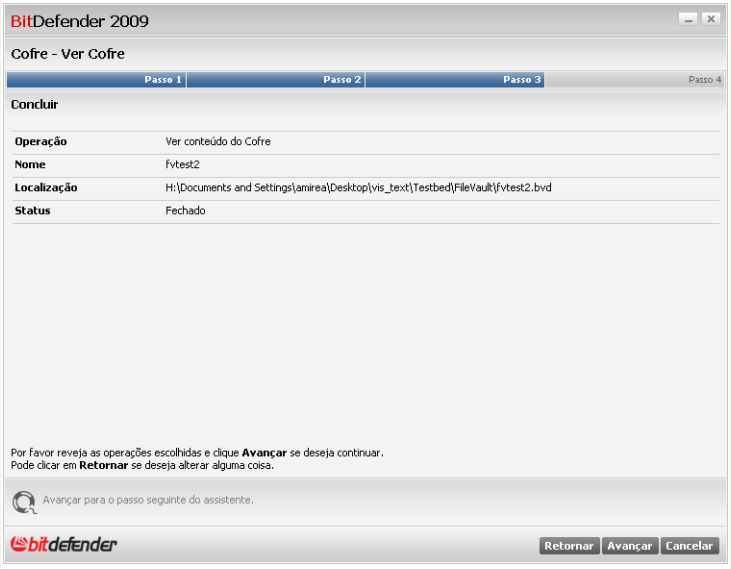


Confirmar senha

Insira a senha no campo correspondente e depois clique em **Seguinte**.

Passo 3/4 - Sumário

Aqui é onde pode rever as operações escolhidas.



Sumário

Clique em **Próximo**.

Passo 4/4 - Resultados

Aqui é onde pode ver os arquivos do cofre.

Resultados

Clique em **Finalizar**.

9.2.6. Fechar o Cofre

Como já sabe, um cofre é um arquivo encriptado com extensão `bvd` que está no seu computador. O cofre pode ser aberto (montado) ou fechado (desmontado).

Para melhor entender este processo, pense num cofre de banco verdadeiro - a sua caixa-forte pode ser aberta ou fechada. No entanto, o conteúdo do cofre só está protegido quando está fechado. Ao mesmo tempo, o seu conteúdo só pode ser acedido quando o mesmo se encontra aberto.

Ao clicar em **Fechar Cofre** um assistente irá levá-lo através do processo de fechar (desmontar) um determinado cofre.

Passo 1/3 - Seleccionar Cofre

Aqui é onde pode especificar o cofre a fechar.

Seleccionar cofreSelecione portas

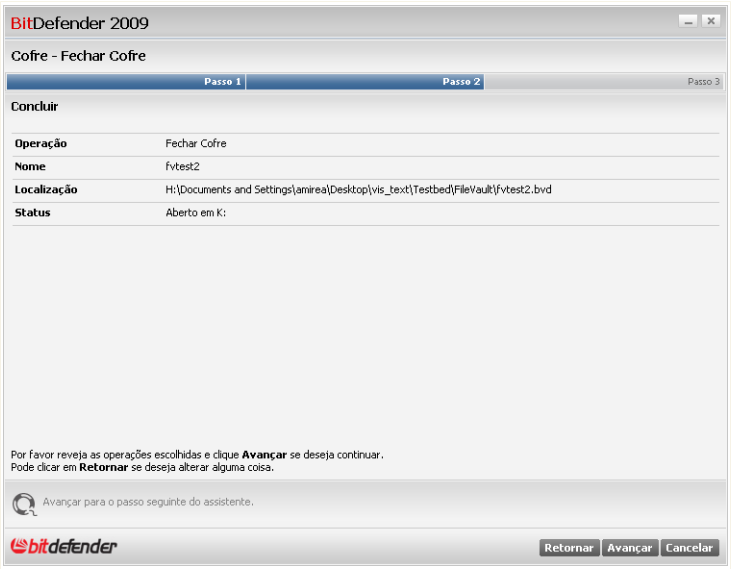
Se selecionar **Explorar Cofre de arquivos**, deve de clicar em **Explorar** e selecionar o cofre de arquivos.

Se clicar em **Seleccionar um Cofre existente**, então deverá clicar no nome do cofre desejado.

Clique em **Próximo**.

Passo 2/3 - Sumário

Aqui é onde pode rever as operações escolhidas.



Sumário

Clique em **Próximo**.

Passo 3/3 - Resultados

Aqui é onde poder ver o resultado da operação.

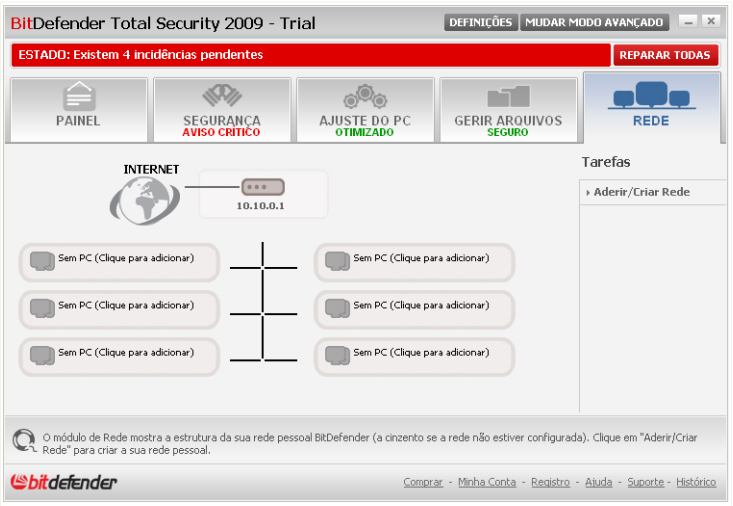
Resultados

Clique em **Finalizar**.

10. Rede

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador.

Para entrar no módulo de Rede, clique na barra **Gestor Arquivos**.



Rede

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

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

10.1. Tarefas

Inicialmente só um botão está disponível.

- **Aderir/Criar Rede** permite-lhe definir a senha de rede, e de seguida entrar na mesma.

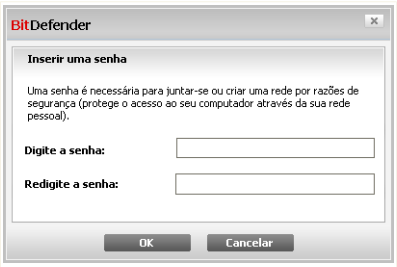
Após aderir à rede, mais botões irão surgir.

- **Sair da rede** - permite-lhe sair da rede.
- **Gerir Rede** - permite-lhe adicionar computadores à sua rede.
- **Analisar Todos** - permite-lhe analisar ao mesmo tempo todos os computadores geridos.
- **Actualizar Todos** - permite-lhe actualizar ao mesmo tempo todos os computadores geridos.
- **Registar Todos** - permite-lhe registar ao mesmo tempo todos os computadores geridos.

10.1.1. Aderir à Rede BitDefender

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

1. Clique em**Aderir/Criar Rede**.>. Será notificado para configurar a senha de gestão de rede pessoal.



Configurar senha

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

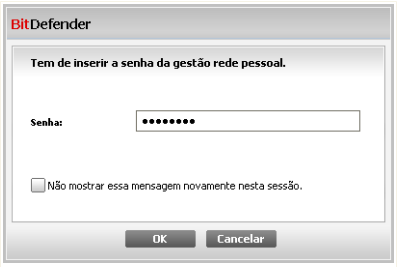
Pode ver o nome do computador a aparecer no mapa de rede.

10.1.2. Adicionar Computadores à Rede BitDefender

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

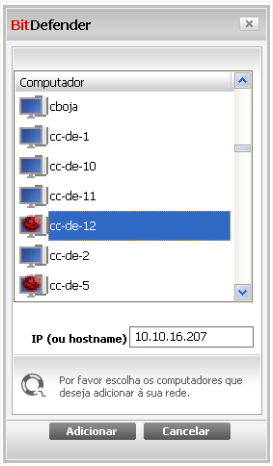
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

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



Inserir senha

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

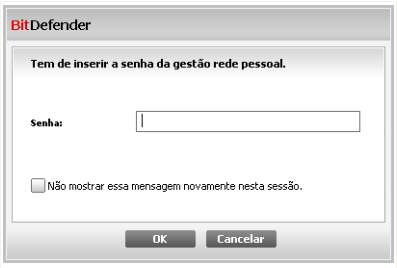


Adicionar Computador

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

- Indica um computador on-line sem produtos BitDefender instalados.
- Indica um computador on-line com o BitDefender instalado.
- Indica um computador offline com o BitDefender instalado.

3. Faça uma das coisas seguintes:
   - Seleccione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
4. Clicando **Adicionar**. Será notificado para inserir a sua senha de gestão de rede pessoal do respectivo computador.



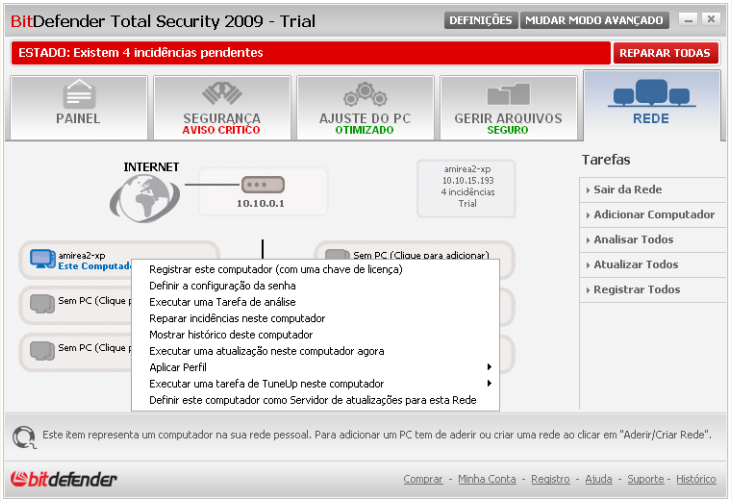
Autenticar

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

Nota
Pode adicionar até cinco computadores neste mapa de rede.

10.1.3. Gerir a Rede BitDefender

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



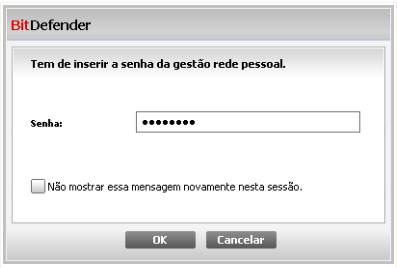
Mapa de Rede

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

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

- **Registar este computador**
- **Definir senha definições**
- **Executar uma tarefa de análise**
- **Reparar incidências neste computador**
- **Mostrar histórico deste computador**
- **Levar a cabo uma actualização neste computador agora**
- **Aplicar Perfil**
- **Levar a cabo uma tarefa de Tuneup neste computador**
- **Definir este computador como Servidor de Actualizações desta Rede**

Antes de levar a cabo uma tarefa num computador específico, será notificado para inserir a senha de gestão de rede pessoal local.



Inserir senha

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

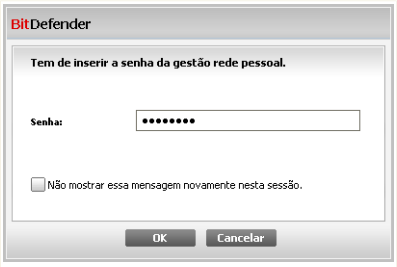
Nota

Se planeia levar a cabo várias tarefas, seleccione **Não me mostrem mais esta mensagem durante esta sessão**. Ao selecionar esta opção, não será notificado novamente pela senha durante esta sessão.

10.1.4. Analisar Todos os Computadores

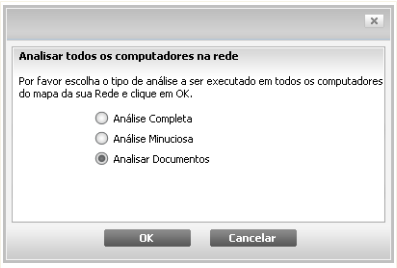
Para analisar todos os computadores geridos, siga estes passos:

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



Inserir senha

2. Seleccione o tipo de análise.
   - **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.
   - **Análise Minuciosa do Sistema** - inicia uma análise minuciosa ao seu computador.
   - **Analisar os Meus Documentos** - inicia uma análise rápida à sua pasta Documents and Settings.



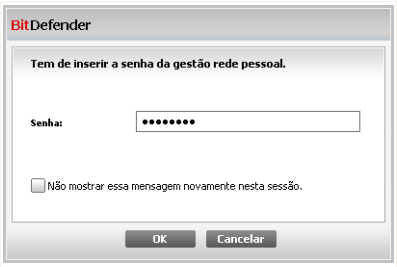
Seleccionar o Tipo de Análise

3. Clique em **OK**.

10.1.5. Actualizar Todos os Computadores

Para actualizar todos os computadores, siga estes passos:

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



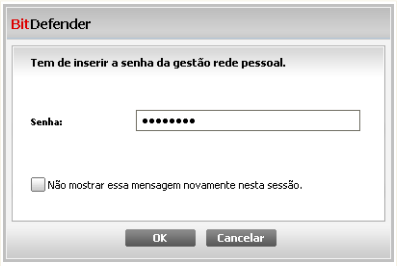
Inserir senha

2. Clique em **OK**.

10.1.6. Registar Todos os Computadores

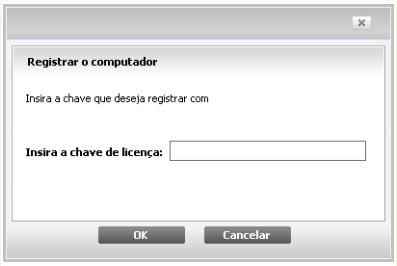
Para registar todos os computadores geridos, siga estes passos:

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



Inserir senha

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



Registar Todos

3. Clique em **OK**.

11. Definições Básicas

O módulo de Definições Básicas é o lugar onde pode activar ou desactivar facilmente os módulos de segurança importantes.

Para entrar no módulo de Definições Básicas, clique no botão **Definições** , localizado na parte superior do Modo Básico.

Definições Básicas

Os módulos de segurança disponíveis estão agrupados em diversas categorias.

Categoria	Descrição
Segurança Local	Aqui é onde pode activar/desactivar a protecção de arquivos em tempo-real ou a actualização automática.
Segurança On-line	Aqui é onde pode activar/desactivar a protecção em tempo-real do e-mail e da web.
Definições do Controle dos Pais	Aqui é onde pode ativar / desativar o Controle dos Pais.
Segurança de Rede	Aqui é onde pode activar / desactivar a firewall.

Categoria	Descrição
Definições do Cofre de arquivos	Aqui é onde pode ativar / desativar o cofre de arquivos.
Configuração Geral	Aqui é onde pode activar/desactivar o modo de jogo, o modo de portátil, palavras-passe, a barra da actividade da análise e mais.

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

11.1. 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 actualização automática assegura que os produtos e as assinaturas mais recentes são descarregados da Internet e instalados automaticamente numa base regular.
Verificação Automática de Vulnerabilidades	A Verificação Automática de Vulnerabilidades assegura que o software crucial no seu PC está actualizado.

11.2. Segurança On-line

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

Módulo de Segurança	Descrição
Antivírus em Tempo-Rea, Antispam & Protecção Antiphishing de e-mail	A protecção em Tempo-real assegura que os seus e-mails são filtrados de spam e analisados em busca de tentativas de phishing.
Antivírus Tempo-real& Protecção Web Antispyware	A proteção Web em tempo-real assegura que os arquivos descarregados via HTTP são analisados em busca de vírus e spyware.
Protecção Antiphishing Web em Tempo-real	A Protecção Antiphishing Web em Tempo-real assegura que todos os arquivos descarregados via HTTP são analisados em busca de tentativas de phishing.
Controle de Identidade	O Controle de Identidade ajuda-o a manter segura a sua informação confidencial ao analisar todo o tráfego de e-mail e web em busca de strings específicas.
Encriptação IM	Se os seus contactos IM tiverem o BitDefender 2009 instalado, todas as conversações via Yahoo! Messenger e Windows Live Messenger serão encriptadas.

11.3. Definições do Controle dos Pais

Aqui é onde pode ativar / desativar o módulo do Controle dos Pais com um só click.

O Controle dos Pais pode bloquear o acesso a páginas web inapropriadas, à internet durante determinados períodos de tempo e pode filtrar o tráfego de e-mail, IM e web baseado em determinadas palavras-chave.

11.4. Definições de rede

Aqui é onde pode activar / desactivar o módulo da Firewall com um só click.

A Firewall protege o seu computador contra os hackers e os ataques maliciosos externos.

11.5. Definições do Cofre de arquivos

Pode ativar / desativar o módulo do Cofre de arquivos com um só click.

O Cofre de arquivos mantém os seus documentos privados ao encriptá-los em drives de cofre especiais.

11.6. Configurações Gerais

Pode activar/desactivar itens relacionados com a segurança apenas com um clique.

Item	Descrição
Modo de Jogo	O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema durante os jogos.
Modo de Portátil	O Modo de Portátil modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no tempo de vida da bateria do seu portátil.
Senha de Configuração	Isto assegura que as definições do BitDefender só podem ser modificadas pela pessoa que conhece esta senha.
Senha do Controle dos Pais	Ao ativar esta opção, a proteção das definições fica a cargo do módulo do Controle dos Pais. Isto assegura que as definições do Controle dos Pais BitDefender apenas podem ser alteradas por alguém que saiba esta senha.
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 de Produtos	Ao activar esta opção, irá receber alertas de informação.
Barra de Actividade de Análise	A Barra de Actividade de Análise é uma pequena e transparente barra que indica o progresso da actividade de análise do BitDefender. As linhas verdes fluidas mostram a actividade da análise no seu sistema local. As linhas vermelhas fluidas mostram a actividade da análise na sua ligação à Internet.

Item	Descrição
Carregar o BitDefender ao iniciar o Windows	Ao ativar esta opção o interface BitDefender do usuário é carregado no iniciar o sistema. Esta opção não afeta o nível de proteção.
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 qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

12. Barra de Estado

Como pode ver facilmente, na parte superior da janela do BitDefender Total Security 2009 existe um barra de estado que mostra o número de incidências pendentes. Clique no botão **Reparar Todas** para facilmente remover qualquer ameaça à segurança do seu computador. Uma janela de estado de segurança aparecerá.

O estado de segurança mostra uma lista de vulnerabilidades de segurança sistematicamente organizada e de fácil gestão do seu computador. O BitDefender Total Security 2009 irá informá-lo sempre que exista um problema que possa afectar a segurança do seu computador.

Barra de Estado

12.1. Segurança Local

Sabemos que é importante ser avisado sempre que há um problema que pode afectar a segurança do seu computador. Ao monitorizar cada módulo de segurança, o BitDefender Total Security 2009 fa-lo-á saber não só quando configura definições que podem afectar a segurança do seu computador, mas também quando se 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 analisou o seu computador em busca de malware hoje	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.
Actualização automatica está activada	Por favor mantenha a actualização automática activada para assegurar que as assinaturas de malware do seu produto BitDefender são actualizadas numa base regular.
Actualizar Agora	A actualização do produto e das assinaturas de malware está a ser levada a cabo.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.2. Segurança On-line

As incidências que dizem respeito à segurança on-line são descritas em frases bem explicítas. Ao mesmo tempo que a frase, se existe algo que possa ameaçar 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 em Tempo-real para o tráfego web (HTTP) está activada	É recomendável manter a protecção web (HTTP) activada para manter o seu computador protegido contra o malware que se propaga via websites ou através de arquivos descarregados potencialmente infectados.
Protecção em Tempo-real para o tráfego de e-mail está activada	A protecção do tráfego de e-mail assegura que os seus e-mails são analisados em busca de malware e filtrados de spam.
Protecção em Tempo-real para o tráfego IM está activada	É recomendável activar a protecção completa do tráfego de IM para manter o seu computador seguro.
Controle de Identidade ativado	Ajuda-o a manter os seus dados confidenciais seguros ao analisar o tráfego web e de e-mail em busca de palavras-chave. É recomendável que mantenha o Controle de Identidade ativado, para evitar que a sua informação confidencial (endereço de e-mail, IDs de usuário, palavras-passe, números de cartões de crédito, etc) seja roubada.
A encriptação de conversação de IM está activada	Se os seus contactos IM têm o BitDefender 2009 instalado, todas as conversas IM via Yahoo! Messenger e Windows Live Messenger serão encriptadas. É recomendável que tenha a encriptação de conversação IM activada para assegurar que as mesmas se mantém privadas.
A protecção antiphishing Firefox está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.
A protecção antiphishing Internet Explorer está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.3. Segurança de Rede

Quando o seu computador faz parte de uma rede vai querer definitivamente protegê-los contra os hackers e prevenir quaisquer tentativas de ligação não-autorizadas ao seu sistema.

As incidências que dizem respeito à segurança de rede são descritas em frases bem explicítas. Ao mesmo tempo que cada frase, se existir algo que possa 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*
Firewall activada	Protege o seu computador contra os hackers e os ataques maliciosos vindos do exterior.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.4. Controle dos Pais

O Controle dos Pais monitoriza o estado dos módulos que lhe permitem restringir o acesso das crianças à internet e a determinadas aplicações.

As incidências que dizem respeito ao módulo do Controle dos Pais são descritas em frases bem explicitas. Ao mesmo tempo que as frases, se existir algo que esteja a afectar a segurança das crianças, verá um botão vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
O Controle dos Pais não está configurado	O módulo de Controle dos Pais do BitDefender pode bloquear o acesso a sites na Internet que considere inapropriados, pode bloquear o acesso à Internet durante determinados períodos de tempo e filtrar e-mail, IM e tráfego web por palavras-chave específicas, etc.

Quando o botão de estado está verde, as suas crianças podem navegar na net em segurança. Para colocar os botões verdes, siga os seguintes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.5. Cofre de arquivos

As incidências que poderão afectar a privacidade dos seus dados são descritas em frases bem explicítas. Ao mesmo tempo, se existir algo que que possa afectar a privacidade dos seus dados, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
Apenas o **O Cofre de arquivos está ativo**	O Cofre de arquivos mantém os seus documentos privados ao encriptá-los em drives de cofre especiais.

Quando o botão de estado está verde, o risco de segurança para o seus dados é miníma. Para colocar os botões verdes, siga estes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.6. Tuneup

As incidências que possam afectar a capacidade de resposta do seu sistema são descritas em frases bem explicítas. Ao mesmo tempo que cada frase, se existir algo que possa estar a afectar a segurança dos seus dados, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
Nunca levou a cabo uma limpeza do registo	O Limpa Registo analisa o Registo do Windows e apaga as chaves de registo inválidas. Leve a cabo uma limpeza do registo de tempos a tempos para melhorar o desempenho do seu computador.
Nunca levou a cabo um limpeza do seu computador	Levar a cabo uma limpeza do seu computador de tempos a tempos melhora o seu desempenho. Faça-a assim que lhe der jeito.
Nunca executou o Localizador de Duplicados	O localizador de duplicados optimiza o seu espaço em disco ao descobrir arquivos que estão em duplicado no seu sistema. Execute-o assim que lhe der jeito.
Nunca executou o Desfragmentador de Disco	A desfragmentação do disco reorganiza os dados contidos no disco rígido de forma a que as partes constituintes de cada arquivo sejam armazenadas juntas e de forma continua. Leve a cabo uma desfragmentação na altura que mais lhe convier.

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

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

2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.7. Backup

As incidências que poderão estar a afectar o seu sistema são descritas em frases bastantes explicítas. Ao mesmo tempo que cada frase, se existir algo que possa estar a afectar a segurança dos seus dados, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
Levou a cabo um backup offline no seu computador há x dias atrás	O módulo de backup offline ajuda-o a fazer cópias de reserva de quaisquer dados valiosos do seu sistema.

Quando o botão de estado está verde, o risco de segurança para o seus dados é miníma. Para colocar os botões verdes, siga estes passos:

1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

12.8. Analisar Vulnerabilidades

As incidências com respeito a vulnerabilidades são descritas com frases bem explicitas. Ao mesmo tempo, se existe algo a afectar a segurança do seu computador, verá um botão vermelho de estado denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

Incidência	*Descrição*
A verificação de Vulnerabilidades está activada	Monitoriza as actualizações do Microsoft Windows, do Microsoft Windows Office e as palavras-passe das contas Microsoft Windows para assegurar que o seu SO está actualizado e não se encontra vulnerável à quebra de palavras-passe.
Actualizações Criticas da Microsoft	Instala Actualizações Criticas da Microsoft que estejam disponíveis.
Outras Actualizações da Microsoft	Instala Actualizações não-criticas da Microsoft que estejam disponíveis.
A Actualização Automatica do Windows está activada	Instala novas actualizações de segurança do Windows assim que estejam disponíveis.
Admin (senha forte)	Indica a força de cada senha de usuários específicos

Quando os botões de estado estão verdes, o risco de segurança do seu computador é minímo. Para por os botões verdes, siga os seguintes passos:

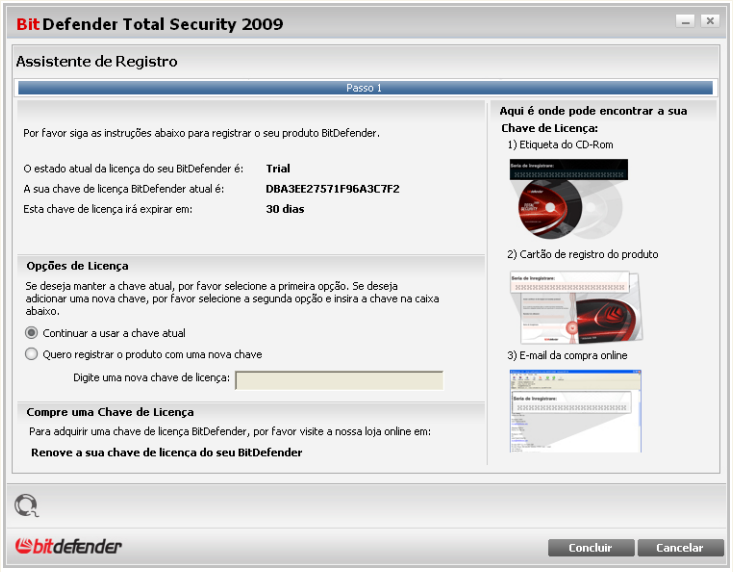
1. Clique no botão **Reparar** para reparar as vulnerabilidades de segurança uma a uma.
2. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Se deseja excluir uma incidência da monitorização, apena limpe a caixa **Sim, monitorizar este componente**.

13. Registro

O BitDefender Total Security 2009 vem com um período de teste de 30 dias. Se deseja registar o BitDefender Total Security 2009, para alterar a chave de licença ou criar uma conta BitDefender, clique no link **Registar**, localizado no fundo da janela BitDefender. O assistente de registo aparecerá.

13.1. Passo 1/1 - Registar o BitDefender Total Security 2009



Registro

Pode ver o estado do registo do BitDefender, a actual chave de licença e quantos dias faltam para a licença expirar.

Para registar o BitDefender Total Security 2009:

1. Seleccione **Desejo registar o produto com uma nova chave**.

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

Nota

Pode encontrar a sua chave de licença:

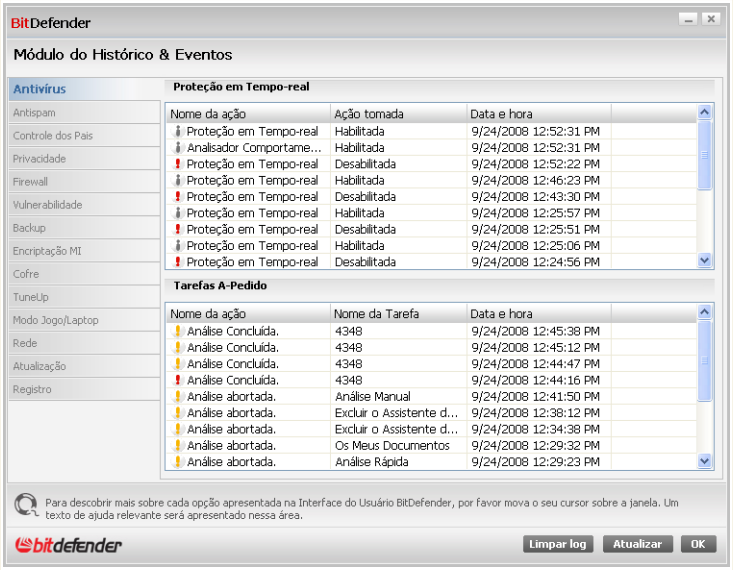
- Na bolsa do CD.
- ou no cartão de registo do produto.
- no e-mail da sua compra on-line.

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

Clique em **Finalizar**.

14. Histórico

O link **Histórico** no fundo da janela do Centro de Segurança BitDefender abre uma outra janela com o histórico & dos eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança. Por exemplo, pode verificar facilmente se a actualização foi levada a cabo 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**
- **Firewall**
- **Antispam**
- **Controle Privacidade**
- **Controle dos Pais**
- **Actualização**

- **Tune Up**
- **Backup**
- **Rede**
- **Encriptação IM**
- **Cofre de arquivos**

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.

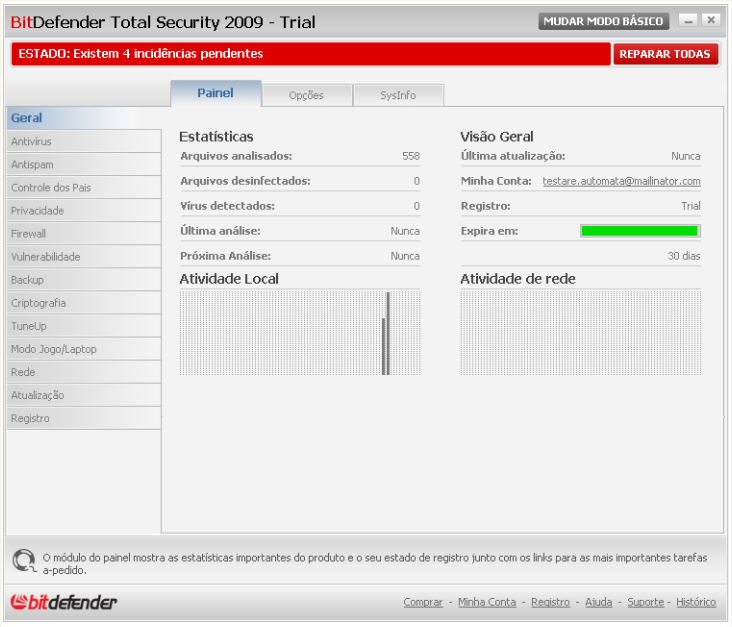
Administração Avançada

15. 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.

15.1. 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 é composto de várias secções:

- **Estaísticas** - Mostra informação importante com respeitoà actividade do BitDefender.
- **Visão Geral** - Mostra o estado da actualização, o estado da sua conta, e informação do seu registo e licença.

- **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.
- **Zona Net** - Indica a evolução do tráfego de rede, filtrado pela Firewall do BitDefender. A altura da barra indica a intensidade do tráfego durante esse intervalo de tempo.

15.1.1. Estatísticas

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

Item	Descrição
Arquivos analisados	Indica o número de arquivos que foram analisados até ao momento da sua última análise.
Arquivos Desinfectados	Indica o número de arquivos que foram desinfectados até ao momento da sua última análise.
Vírus detectados	Indica o número de vírus detectados no seu sistema até ao momento da sua última análise.
Bloquear scan de portas	Indica o número de scans de portas bloqueados pela Firewall do BitDefender. Os scans de portas são frequentemente usados pelos hackers para descobrir portas abertas no seu computador com o objectivo de as explorar. Mantenha a Firewall e o Modo Stealth activados para estar protegido contra os scans de portas.
tarefas de backup completadas	Indica o número de vezes que fez backup dos seus arquivos.

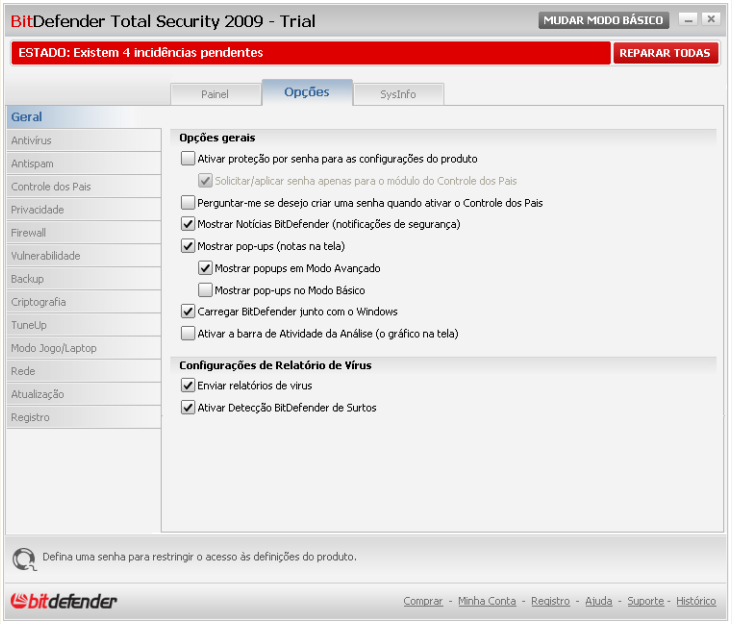
15.1.2. Sumário

Aqui pode ver um resumo das estatísticas respeitantes ao estado da actualização, ao estado da sua conta, registo e informação de licença.

Item	Descrição
Última actualização	Indica a data em que o produto Bitdefender foi actualizado pela última vez. Leve a cabo actualizações regulares de forma a ter um sistema totalmente protegido.
Minha conta	Indica o endereço de e-mail que pode usar para aceder à sua conta on-line para recuperar a sua chave de licença perdida e beneficiar do suporte BitDefender e de outros serviços personalizados.
Registro	Indica o seu tipo de licença e o seu estado. Para manter o seu sistema seguro tem de renovar ou efectuar o upgrade do BitDefender se a sua chave de licença tiver expirado.
Expira em	Indica o número de dias que faltam até que a sua chave de licença expire.

15.2. Opções

Para efectuar as configurações gerais no BitDefender e gerir as suas definições, vá para **Geral>Definições** no Modo Avançado.



Configurações Gerais

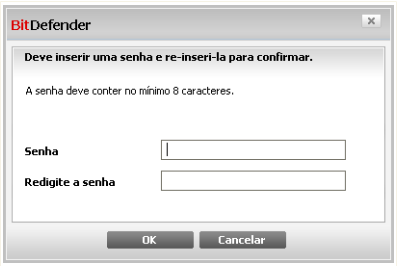
Aqui você pode ajustar o comportamento integral do BitDefender. Por padrão, o BitDefender é carregado na inicialização do Windows e então roda minimizado na área de notificação.

15.2.1. 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.

Se desejar ser notificado para inserir a senha apenas quando configurar o Controle dos Pais, deverá também seleccionar **Perguntar/aplicar senha apenas para o módulo do Controle dos Pais**. Por outro lado, se uma senha for definida apenas para o Controle dos Pais e deseleccionar essa opção, a senha respectiva será requisitada quando configurar qualquer opção do BitDefender.

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

- **Solicitar senha quando activar o Controle dos Pais** - se esta opção estiver activada e nenhuma senha estiver definida, ser-lhe-á solicitado que a defina quando activar o Controle dos Pais. Ao definir uma senha, irá prevenir que outros usuários com direitos administrativos possam mudar as suas definições do Controle dos Pais que configurou para um determinado usuário.
- **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 BitDefender junto com o Windows** - inicia automaticamente o BitDefender na inicialização do sistema. 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.

Nota
Esta opção pode ser configurada apenas para a atual conta de usuário Windows.

15.2.2. 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.

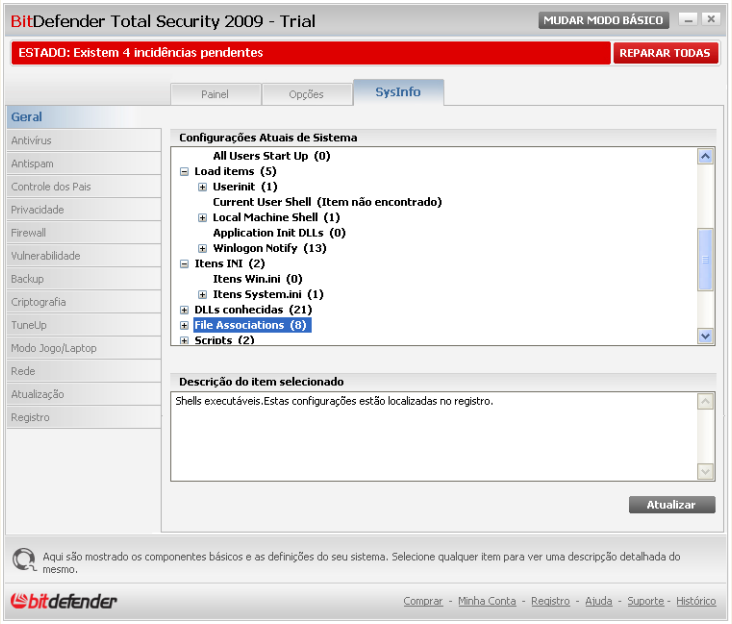
- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  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.

15.3. 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**.

16. 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, BitDefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

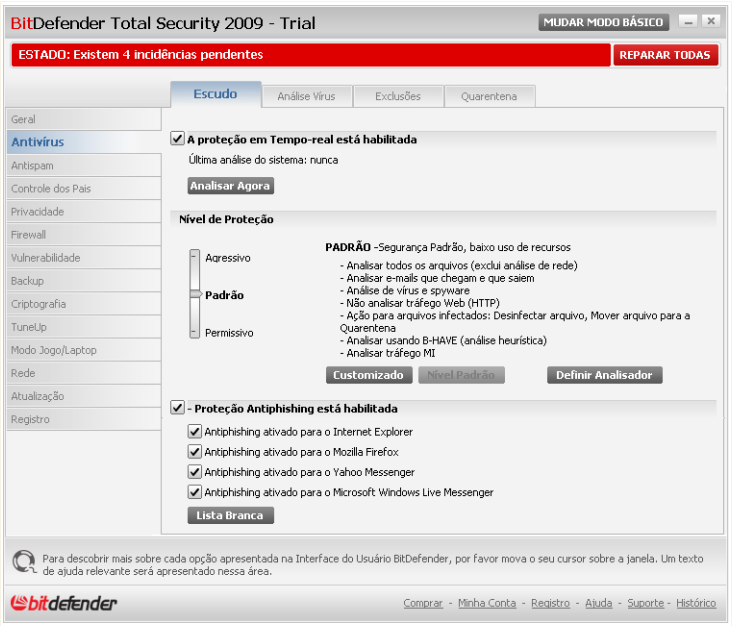
  Nota
  A proteção em Tempo-real, também referida como análise no acesso - os arquivos são analisados à medida que os usuários lhes acessem.

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

16.1. Protecção em Tempo-real

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

Para configurar a protecção em tempo-real e o BitDefender Antiphishing, clique em **Antivírus>Escudo** 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**.

16.1.1. 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:

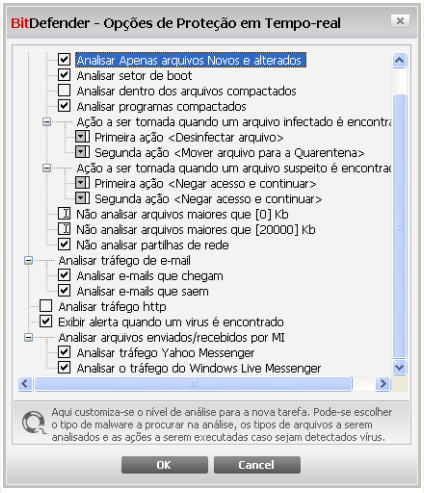
Nível de Protecção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Programas e mensagens de e-mail de entrada são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em arquivos infectados são as seguintes: limpar arquivo/negar acesso.
Por Defeito	Oferece segurança standard. O nível de consumo de recursos é baixo. Todos os arquivos e mensagens de e-mail de entrada e saída são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em arquivos infectados são as seguintes: limpar arquivo/negar acesso.
Agressivo	Oferece uma segurança elevada. O nível de consumo de recursos é moderado. Todos os arquivos, mensagens de e-mail de entrada e saída e tráfego web são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em arquivos infectados são as seguintes: limpar arquivo/negar acesso.

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

16.1.2. 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.

Pode personalizar **Protecção em Tempo-real** ao clicar **Nível personalizado**. A seguinte janela aparecerá:



Configurações do Escudo

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

Nota

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

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

Opção		*Descrição*
Analisar arquivos acedidos	**Verificar todos os arquivos**	Todos os arquivos acessados serão verificados, não importando o tipo.

Opção		Descrição
	Verificar apenas os arquivos de programas	Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Verificar as extensões definidas pelo usuário	Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";".
	Analisar 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 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.
	Negar acesso e continuar	Caso um arquivo infectado seja detectado, o acesso a ele será negado.

Opção		Descrição
	Limpar arquivo	Desinfecta os arquivos infectados.
	Apagar arquivo	Apaga o arquivo infectado imediatamente, sem avisar.
	Mover o arquivo para a quarentena	Move os arquivos infectados para a quarentena.
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.
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.

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

  As seguintes opções estão disponíveis:

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

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

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

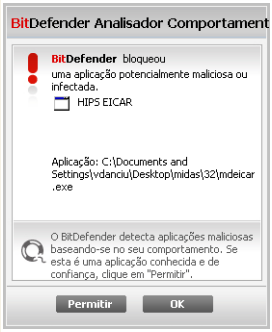
  Caso um arquivo suspeito é detectado você pode executar um assistente que o ajudará a mandar este arquivo para o Laboratório BitDefender para uma melhor análise. Você pode digitar o seu endereço de e-mail para receber informação sobre este relatório.
- **Analisar arquivos recebidos/enviados por MI.** Para analisar todos os arquivos enviados ou recebidos via Yahoo Messenger ou Windows Live Messenger, selecione a correspondente caixa.

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

16.1.3. Configurar o Analisador Comportamental

O Analisador Comportamental fornece uma camada de protecção contra as novas ameaças para as quais ainda não foram desenvolvidas assinaturas. Monitoriza constantemente o comportamento das aplicações que estão a correr no seu computador e alerta-o se uma aplicação apresentar um comportamento suspeito.

O Analisador Comportamental alerta-o sempre que uma aplicação apresentar um comportamento suspeito e malicioso e solicita a sua acção.

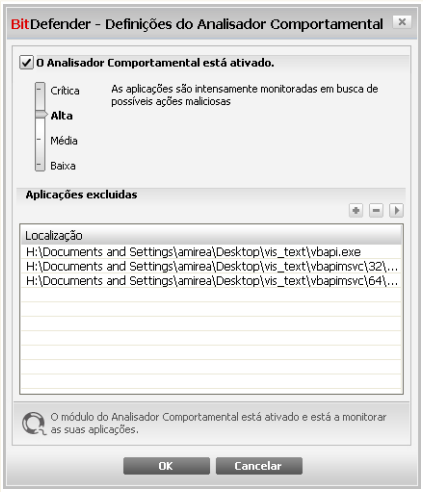


Alerta do Analisador Comportamental

Se conhece e confia na aplicação detectada, clicque em **Permitir**. O Analisador Comportamental não voltará a analisá-la em busca de possível comportamento malicioso.

Se deseja fechar imediatamente a aplicação, clique em **OK**.

Para configurar O Analisador Comportamental, clique em **Configuração**.



Configurações do Analisador Comportamental

Se deseja desactivar o Analisador Comportamental limpe a caixa **Activar Analisador Comportamental** .

Importante
Mantenha o Analisador Comportamental activado de forma a estar protegido contra vírus desconhecidos.

Configurar Nível de Protecção

O nível de protecção do Analisador Comportamental muda automaticamente quando define um novo nível de protecção em tempo-real. Se não está satisfeito com o nível por defeito, pode configurar o nível de protecção manualmente.

Nota
Lembre-se que se alterar o nível de protecção actual da protecção em tempo-real, o nível de protecção do Analisador Comportamental irá mudar também.

Arraste o marcador ao longo da escala para definir o nível de protecção que considera apropriado para as suas necessidades de segurança.

Nível de Protecção	*Descrição*
Crítico	As aplicações são estritamente monitorizadas para possíveis acções maliciosas.
Elevado	As aplicações são intensamente monitorizadas para possíveis acções maliciosas.
Médio	As aplicações são moderadamente monitorizadas para possíveis acções maliciosas.
Baixo	As aplicações são monitorizadas para possíveis acções maliciosas.

Gerir Aplicações Excluidas

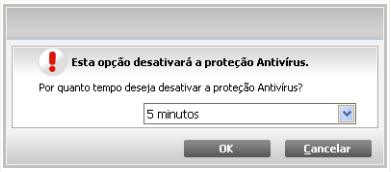
Pode configurar o Analisador Comportamental para não analisar determinadas aplicações. As aplicações que não são analisadas pelo Analisador Comportamental estão listadas na tabela **Aplicações Excluidas**.

Para gerir as aplicações excluidas, pode usar os botões colocados no topo da tabela:

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.
- **Edit** - edit an application path.

16.1.4. 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.

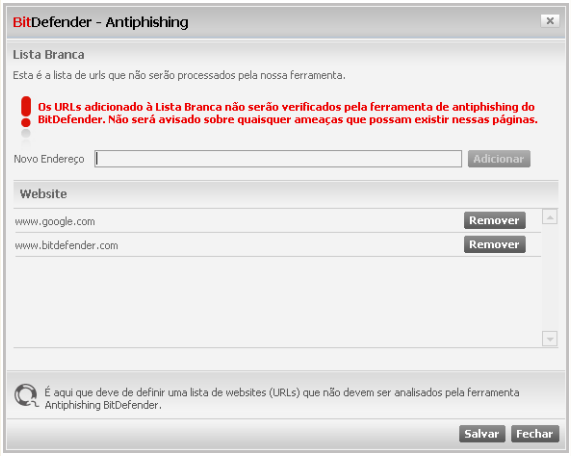
16.1.5. Configurar Protecção Antiphishing

O BitDefender dá-lhe uma protecção Antiphishing em tempo-real para:

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

Pode desactivar a protecção Antiphishing completamente ou somente para determinadas aplicações.

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



Lista Branca do AntiPhishing

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

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

Nota

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada no Internet Explorer.

Para remover um site web da lista branca, seleccione-a e clique **Remover**.

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

16.2. Análise A-pedido

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

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

Para configurar e iniciar uma análise a-pedido, clique **Antivírus>Análise** 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

16.2.1. 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. 182).

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.

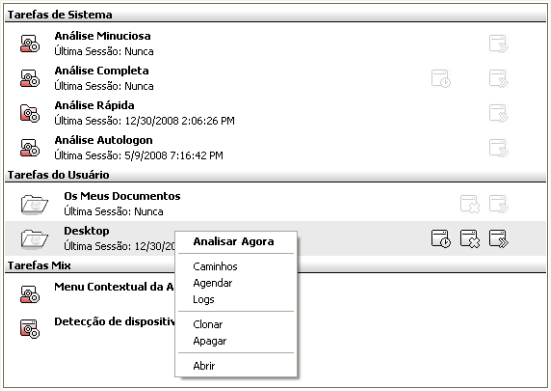
- **Analisar Agora** - executa a tarefa seleccionada dando início a uma análise imediata.

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

16.2.2. 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.

Os seguintes comandos estão disponíveis no menu de atalho:



Menú de Atalho

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.
- **Caminhos** - abre a janela **Propriedades**, Aba Caminhos, 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**, Abs Agenda, onde você poderá agendar a tarefa selecionada.
- **Logs** - abre a janela **Propriedades**, Aba Logs, 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.

16.2.3. 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.

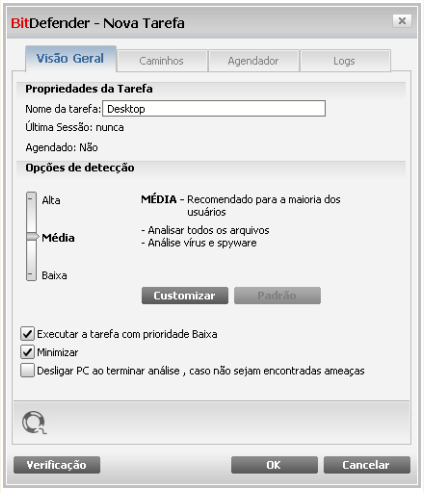
16.2.4. Configurar Tarefas de Análise

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. 201).

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 assinaturas, 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 assinaturas, 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:

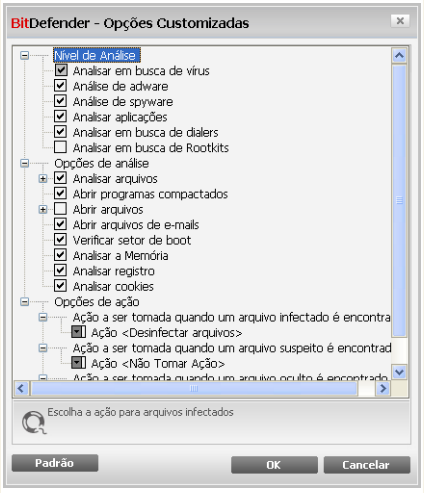
- **Executar a análise com Baixa prioridade.** Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação.
- **Minimizar a janela de análise no inicío para a barra de tarefas.** Minimiza a janela de verificação para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

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

Personalizar o Nível de Análise

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

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



Opções de Análise

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	Todos os arquivos compactados serão verificados. 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.

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

Ação	Descrição
Nenhum (objetos de log)	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.

Ação	Descrição
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
Nenhum (objetos de log)	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
Nenhum (objetos de log)	Nenhuma acção será levada a cabo sobre os arquivos ocultos. Estes arquivos aparecerão no arquivo de relatório.
Mover arquivos para a quarentena	Move os arquivos ocultos para a quarentena. O arquivos em quarentena não podem ser executados

Ação	Descrição
	ou abertos; logo o risco de infectarem o seu computador desaparece.
Tornar visível	Revela arquivos ocultos de forma a que os possa ver.

- **Opções de acção sobre arquivos arquivados.** Analisar e manusear arquivos dentro de arquivos comprimidos são acções limitadas. Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha. Dependendo do formato do arquivo (tipo), o BitDefender poderá não conseguir desinfectá-los, isolá-los ou apagar arquivos arquivados infectados. Configurar as acções a serem levadas a cabo sobre os arquivos comprimidos detectados usandos as opções apropriadas da categoria **Opções de acção sobre arquivos comprimidos**.
  - Seleccione a acção a ser tomada sobre o arquivo infectado. As seguintes opções estão disponíveis:

Ação	Descrição
Não Tomar Acção	Apenas manter registo dos arquivos comprimidos infectados no relatório da análise. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.
Desinfetar arquivos	Remover o código de malware dos arquivos infectados detectados. A desinfecção pode falhar nalguns casos, tais como quando o arquivo infectado se encontra dentro de um arquivo de correio específico.
Apagar arquivos	Apaga o arquivo infectado imediatamente, sem avisar.
Mover arquivos para a quarentena	Mover os arquivos infectados da sua localização original para a Quarentena O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

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

Ação	Descrição
Não Tomar Acção	Apenas manter registo dos arquivos comprimidos suspeitos no relatório da análise. 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.

- Seleccione a ação a ser tomada sobre os arquivos detectados protegidos por senha. As seguintes opções estão disponíveis:

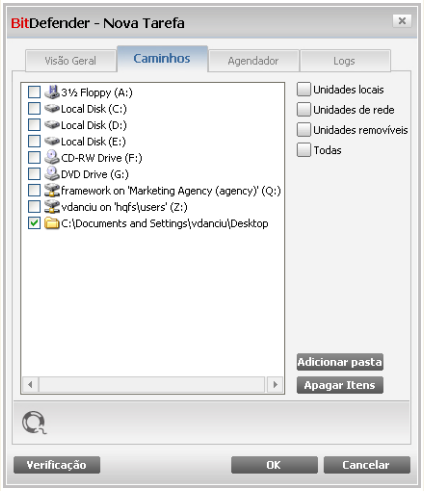
Ação	Descrição
Log não analisou	Apenas manter registo dos arquivos comprimidos protegidos por senha no relatório da análise. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.
Solicitar senha	Quando é detectado um arquivo protegido por senha, pedir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

Nota
Se escolher ignorar os arquivos detectados ou se a acção escolhida falhar, terá de escolher uma acção no assistente de análise.

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.

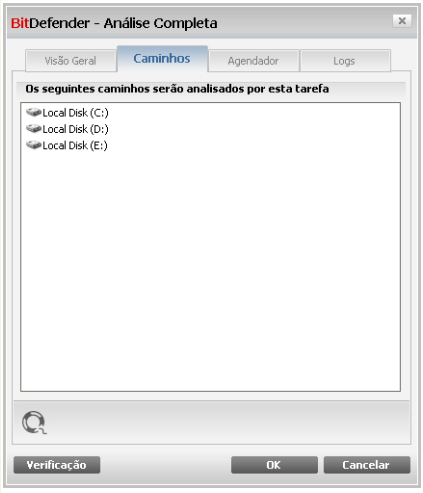
Nota
Se você quer verificar todo o seu computador contra vírus selecione a caixa correspondente a **Todas**.

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

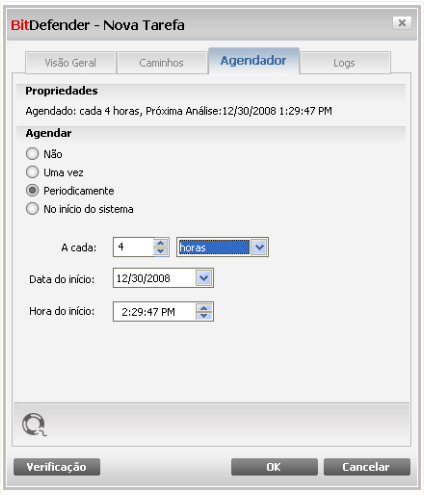
Análise Completa do Sistema e **Análise Minuciosa do Sistema** analisarão todas as drives locais, enquanto **Análise Rápida do Sistema** apenas analisará as pastas `Windows` e `Programas`.

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**.

16.2.5. Analisar objectos

Antes de inciar um processo de análise, deveria certificar-se que o BitDefender está actualizado com as assinaturas de malware mais recentes. Analisar o seu computador usando assinaturas desactualizadas pode impedir que o BitDefender detecte novo malware encontrado desde a última actualização. Para verificar quando a última actualização foi feita, clique em **Actualização>Actualização** nas definições da consola.

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.

Métodos de Análise

O BitDefender permite quatro tipos de verificação solicitada:

- Análise imediata - executa uma tarefa de análise das tarefas do sistema/usuário.
- Verificação contextual - clique com o botão direito em um arquivo ou pasta e escolha BitDefender Antivirus 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.

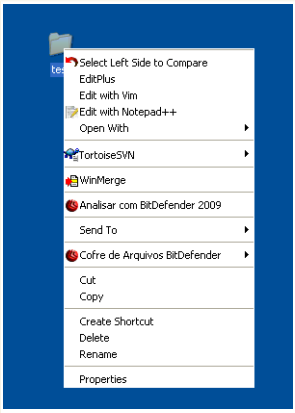
Para executar uma tarefa de análise, use um dos seguintes métodos:

- 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 Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção "*Analisador BitDefender*" (p. 197).

Verificação contextual

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



Verificação Contextual

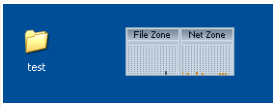
Clique com o botão direito do mouse sobre o arquivo ou pasta que pretende analisar e selecione **BitDefender Antivirus 2009**.

O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção "*Analisador BitDefender*" (p. 197).

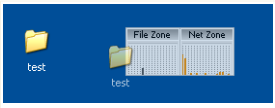
Pode modificar as opções de análise e ver os relatórios ao aceder à janelas das **Propriedades** da tarefa **Análise de Menu Contextual**.

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

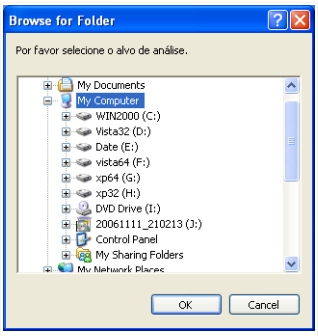
O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção "*Analisador BitDefender*" (p. 197).

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 Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção "*Analisador BitDefender*" (p. 197).

Analisador BitDefender

Quando iniciar o processo de análise a-pedido, o Analisador BitDefender irá surgir. Siga o processo guiado de três passos para completar o processo de 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).

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

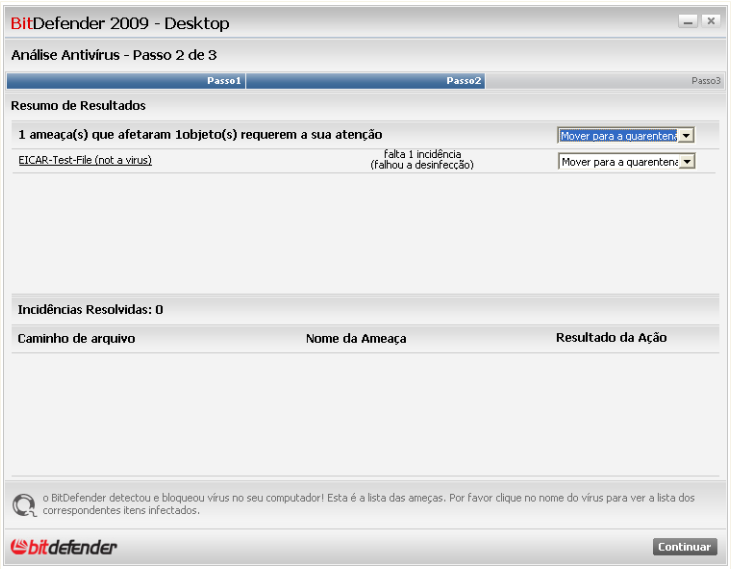
Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá directamente para o último passo do assistente.

Espere que o BitDefender termine 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.

As seguintes opções podem aparecer no menu:

Ação	*Descrição*
Não Tomar Acção	Nenhuma ação será tomada em arquivos detectados.
Desinfetar	Desinfecta os arquivos infectados.
Apagar	Apaga os arquivos detectados.
Desocultar	Torna visíveis objectos ocultos.

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. Clicar **Mostrar Relatório** para ver o relatório da análise.

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

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

BitDefender Não Pode Resolver Algumas Incidências

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

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

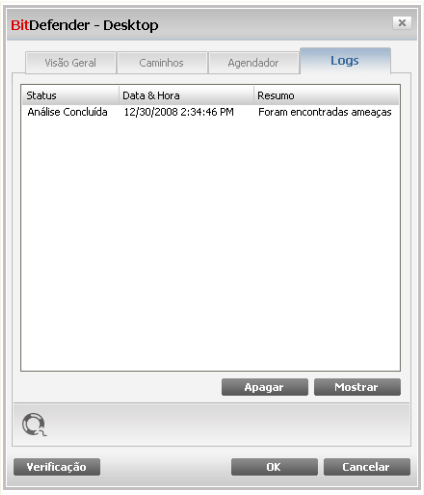
BitDefender Detectou Arquivos Suspeitos

Arquivos suspeitos são arquivos detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura 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.

16.2.6. 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:

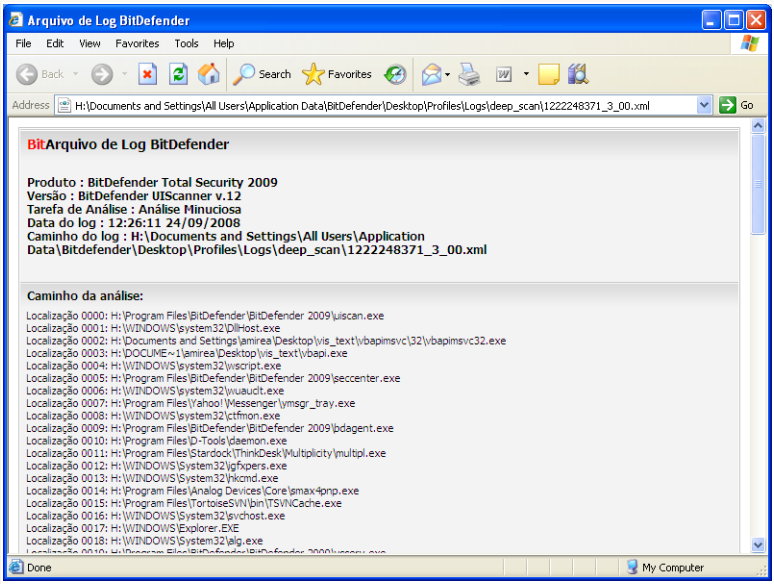
- **Apagar** - apaga o relatório selecionado.
- **Mostrar** - abre o relatório selecionado. O relatório da análise será aberto no seu explorador da internet.

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.

16.3. 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.

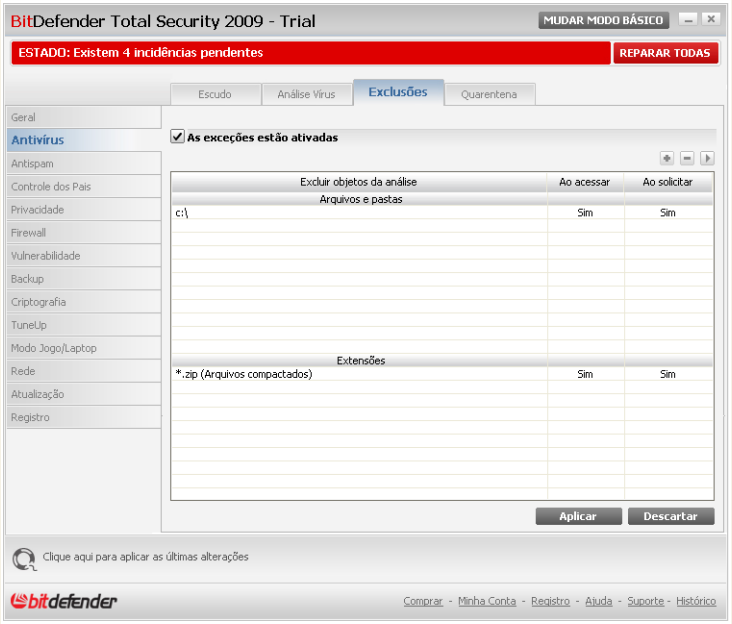
BitDefender permite-lhe excluir objectos da análise no-acesso e da análise a-pedido, ou de ambas. Esta definição tem o propósito de diminuir o tempo de análise e evitar interferência com o seu trabalho.

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.

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**.

16.3.1. 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.

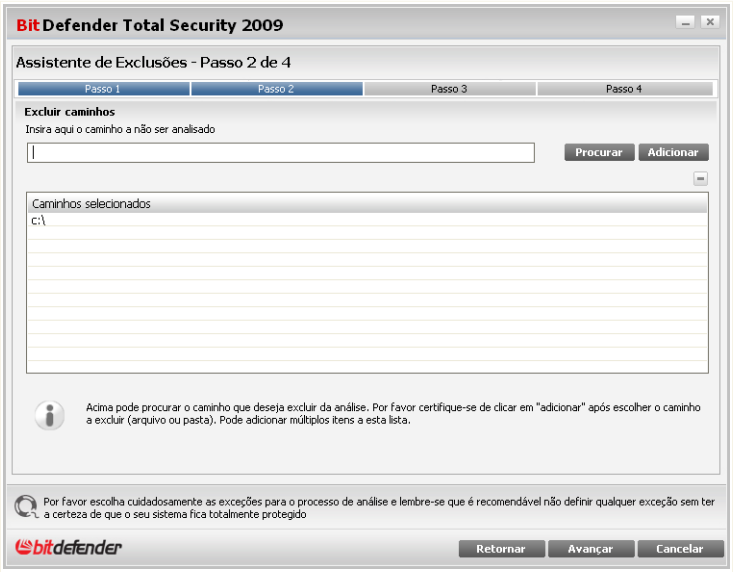
Passo 1/4 - Seleccionar o Tipo de Objecto

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**.

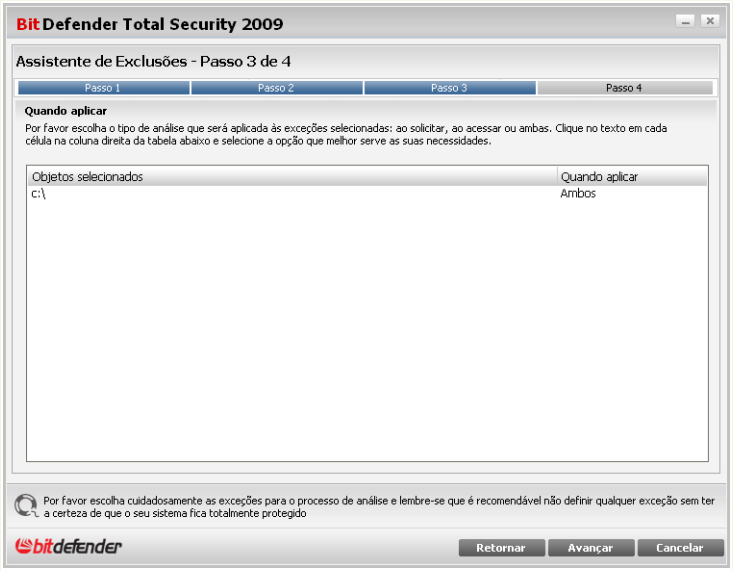
> ***Nota***
> Se o caminho inserido não existe, uma mensagem de erro surgirá. Clique em **OK** e verifique se o caminho é válido ou não.

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.

16.3.2. 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.

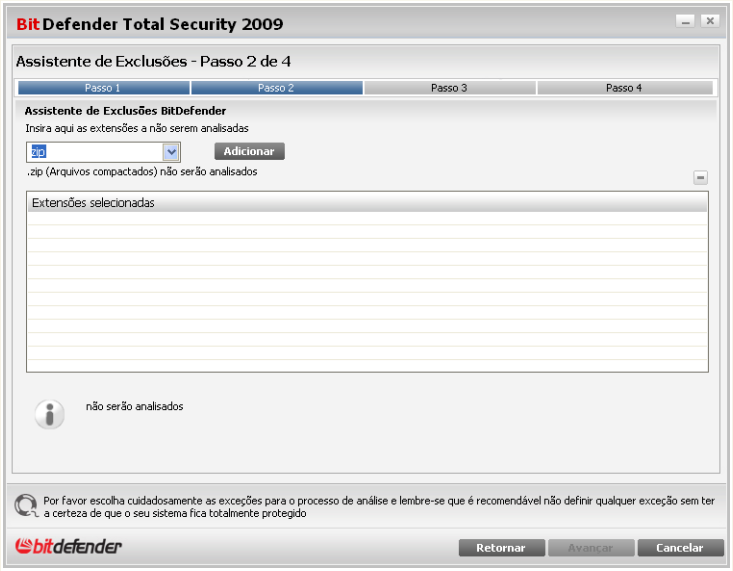
Passo 1/4 - Seleccionar o Tipo de Objecto

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.

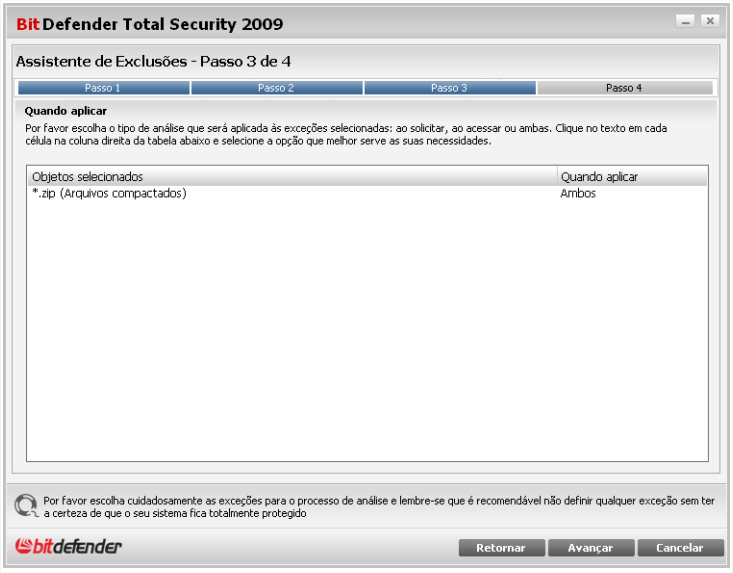
- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

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

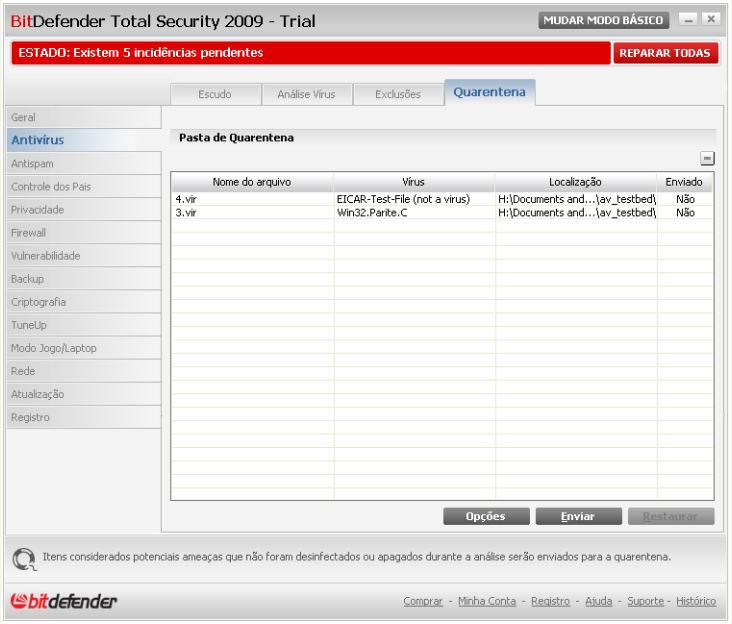
Clique em **Finalizar**.

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

16.4. 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.

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.

16.4.1. Gerir arquivos em Quarentena

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**.

Pode enviar qualquer arquivo selecionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**.

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.

16.4.2. 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.

17. Antispam

O BitDefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam padrão para limpar o spam antes de o mesmo chegar à caixa de correio A receber do usuário.

17.1. Compreender o Antispam

Spam é um problema crescente, tanto para usuários quanto para empresas. Não é bonito, você não gostaria que seus filhos vissem, pode fazer você perder o emprego (por desperdiçar muito tempo ou por receber e-mails impróprios no e-mail do escritório) e você não pode impedir as pessoas de enviá-lo. A melhor coisa a fazer é, obviamente, parar de recebê-los. Infelizmente, spams chegam em inúmeras formas e tamanhos, e em grandes quantidades.

17.1.1. Filtros Anti-spam

O Motor Antispam do BitDefender Antispam incorpora sete filtros distintos, os quais asseguram que a sua Caixa de Entrada de correio se mantenha livre de SPAM: Lista Amigos, Lista Spammers, Filtro caracteres, Filtro de Imagem, Filtro URL, Filtro NeuNet (Heurístico) e Filtro Bayesiano.

Nota
Pode activar/desactivar cada um destes filtros na secção da Configuração no módulo de **Antispam**.

Lista de Spammers / Amigos

A maioria das pessoas se comunica regularmente com um grupo de pessoas ou mesmo recebe mensagens de empresas e organizações do mesmo domínio. Usando as **listas de amigos ou spammers**, você pode facilmente classificar de quais pessoas você quer receber e-mails (amigos) não importa o que a mensagem contenha, ou de quais pessoas você nem quer ouvir falar (spammers).

A lista de Amigos/Spammers pode ser administrada do Modo Avançado ou da barra Antispam integrada a alguns dos clients de email mais comumente utilizados.

Nota
Nós recomendamos que você adicione os nomes e e-mails de seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos que estão na lista, portanto, adicionar amigos ajuda a fazer com que mensagens legítimas sejam recebidas.

Filtro de Caracteres

A maioria das mensagens Spam é escrita em caracteres Cirílicos e/ou Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-as como SPAM.

Filtro de Imagem

Evitar a detecção de um filtro heurístico se tornou um grande desafio, então hoje em dia as caixas de e-mail estão cheias de mais e mais mensagens contendo uma imagem com conteúdo não solicitado. Para lidar com este crescente problema, o BitDefender introduziu o **Filtro de Imagem** que compara as assinaturas das imagens do e-mail com a base de dados BitDefender. Em caso de similaridade o e-mail será marcado como SPAM.

Filtro de URL

A maioria das mensagens de Spam contém links para vários locais da web. Estes locais por sua vez contém mais publicidade e a possibilidade de comprar coisas, e por vezes, são usados para phishing.

O BitDefender mantém uma base de dados de tais links. O filtro URL verificas cada link URL numa mensagem e compara-o com a sua base de dados. Se existir uma correspondência, a mensagem é marcada como SPAM.

Filtro NeuNet (Heurístico)

O **Filtro NeuNet (Heurístico)** executa uma série de testes nos componentes da mensagem (por ex., não só o cabeçalho mas também todo o corpo da mensagem, seja em formato HTML ou em texto), procurando palavras, frases, links ou outras características de SPAM. Baseado nos resultados da análise, adiciona uma marca de SPAM à mensagem.

O filtro também detecta mensagens marcadas como `SEXUALMENTE EXPLÍCITO:` no assunto e marca-as como SPAM.

Nota
A partir de 19 de Maio de 2004, Spams com conteúdo erótico orientado a adultos deverão conter o aviso `SEXUALMENTE EXPLÍCITO:` no assunto, ou poderá sofrer multas por violação de leis federais.

Filtro Bayesiano

O **Filtro Bayesiano** classifica mensagens de acordo com estatísticas sobre a quantidade em que palavras específicas aparecem em mensagens classificadas Spam quando comparadas com aquelas declaradas não-spam (por você ou pelo filtro Heurístico).

Iso significa, por exemplo, que se uma certa palavra de quatro letras aparece mais freqüentemente em Spam, é natural supor que há uma probabilidade maior que a próxima mensagem que a inclua É Spam. Todas as palavras relevantes em uma mensagem são levadas em conta. Sintetizando as estatísticas, a probabilidade total de que a mensagem seja Spam é computada.

Esse módulo apresenta outra característica interessante: é treinável. Ele se adapta rapidamente ao tipo de mensagem recebida por um certo usuário, e grava informações sobre tudo. Para funcionar efetivamente, o filtro deve ser treinado , ou seja, apresentado a exemplos de Spam e mensagens legítimas, bem como um cão de caça que deve seguir uma pista. Às vezes, o filtro deve ser corrigido também – para se ajustar quando tomar uma decisão errada.

Importante
Pode corrigir o módulo Bayesiano ao usar os botões **É Spam** e **Não é Spam** da Barra de tarefas Antispam.

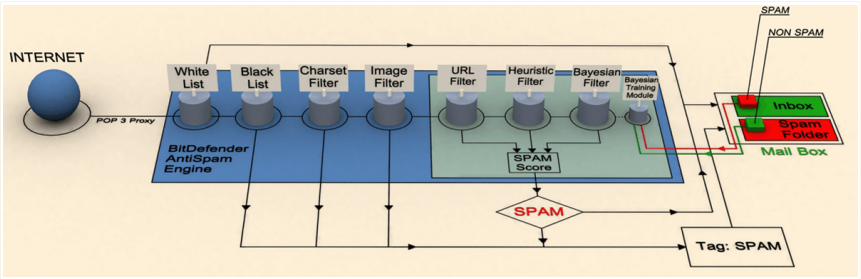
Nota
Cada vez que executa uma actualização:

- novas assinaturas de imagens serão adicionadas ao **Filtro de Imagem**.
- novos links serão adicionados ao **Filtro URL**.
- novas regras serão adicionadas ao **Filtro Neunet (Heurístico)**.

Isso ajudará a aumentar a eficácia de seus mecanismos Antispam.
Para proteger você contra spammers, o BitDefender pode executar atualizações automáticas. Mantenha a opção **Atualização Automática** habilitada.

17.1.2. Operação Antispam

O esquema a seguir mostra como o BitDefender funciona.



Operação Antispam

Os filtros anti-spam do esquema acima (Lista Amigos, Lista Spammers, Filtro de caracteres, Filtro de Imagem, Filtro de URL, Filtro Neunet (Heurístico) e Filtro Bayesiano) são usados em conjunto pelo módulo BitDefender Antispam, para determinar quando um certo e-mail deve entregue a você na **Caixa de entrada** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Amigos / Lista Spammers. Se o endereço do remetente se encontrar na Lista Amigos, o e-mail é movido directamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista Spammers irá apoderar-se do seu e-mail para verificar se o endereço do remetente se encontra na lista. O e-mail será marcado como SPAM e movido para a pasta de **Spam** (localizado no Microsoft Outlook) se houver uma correspondência.

Em seguida, o Filtro de caracteres checa se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Caso esteja o e-mail será marcado como SPAM e movido para a pasta **Spam**.

Se ele não estiver escrito em Asiático ou Cirílico, passará para o Filtro de Imagem. O **Filtro de Imagem** detectará todas as mensagens de e-mail com imagens anexadas com conteúdo spam.

O Filtro de URL vai procurar por links e comparará os links achados com os da base de dados do BitDefender. Caso eles combinem será adicionada uma pontuação de Spam ao e-mail.

O Filtro NeuNet (Heurístico) irá apoderar-se do e-mail e irá executar uma série de testes aos componentes da mensagem, procurando palavras, frases, links e outras características de SPAM. E o e-mail, dependendo do resultado será ou não marcado como SPAM.

Nota
Se o e-mail é marcado como SEXUALLY EXPLICIT na linha do assunto, o BitDefender vai considerá-lo SPAM.

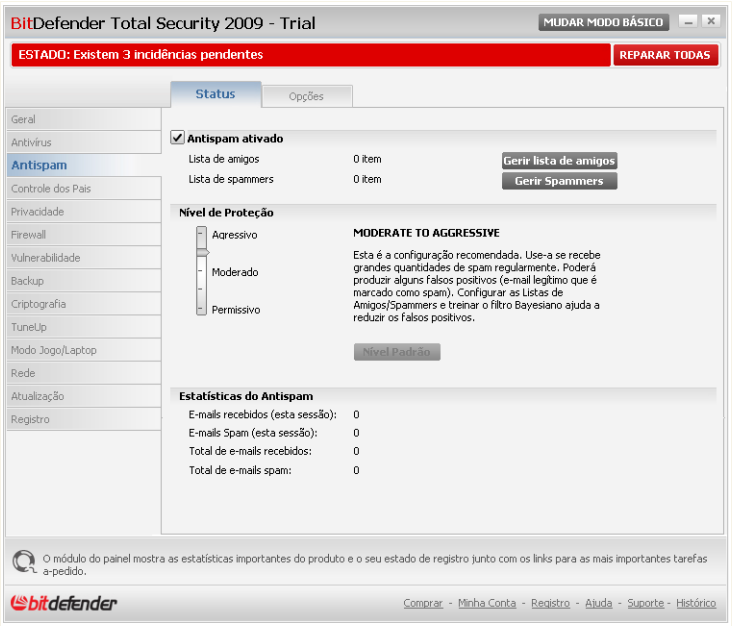
O módulo Filtro Bayesiano então analisará a mensagem, de acordo com estatísticas sobre a quantidade em que palavras específicas aparecem em mensagens classificadas Spam quando comparadas com aquelas declaradas não-spam (por você ou pelo filtro Heurístico). Uma pontuação Spam será adicionada ao e-mail.

Se a pontuação agregada (URL + heurística + Bayesiana) exceder a pontuação SPAM para uma mensagem (ajustada pelo usuário na seção Status como nível de tolerância), a mensagem é considerada SPAM.

Importante
Se você está usando outro cliente de e-mail que não o Microsoft Outlook ou Microsoft Outlook Express você deve criar uma regra para mover as mensagens marcadas como SPAM pelo BitDefender para uma pasta de quarentena. O BitDefender anexa o prefixo `[SPAM]` no assunto das mensagens consideradas SPAM.

17.2. Status

Para configurar a protecção Antispam, clique em **Antispam>Estado** no Modo Avançado.



Status do Antispam

Pode ver se o Antispam está activado ou desactivado. Se deseja alterar o estado do Antispam, limpe ou seleccione a caixa correspondente.

Importante
Para prevenir Spam de entrar em sua **Caixa de entrada**, mantenha o **filtro Anti-spam** ativado.

Na seção **Estatísticas** você pode ver as estatísticas sobre o módulo . Os resultados são apresentados por sessão (desde que você iniciou seu computador) ou você pode ver um resumo da atividade antispam desde a instalação do filtro Anti-spam.

17.2.1. Definir 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 5 níveis de protecção:

Nível de Protecção	Descrição
Permissivo	Oferece protecção às contas que recebem uma grande quantidade de e-mails comerciais legítimos. O filtro irá deixar passar a maior parte dos e-mails, mas poderá produzir falsos negativos (spam classificado como e-mail legítimo).
Permissivo a Moderado	Oferece protecção às contas que recebem alguns e-mails comerciais legítimos. O filtro irá deixar passar a maior parte dos e-mails, mas poderá produzir falsos negativos (spam classificado como e-mail legítimo).
Moderado	Oferece protecção às contas regulares. O filtro bloqueará a maioria do spam, enquanto evita falsos positivos.
Moderado a Agressivo	Oferece protecção às contas que recebem uma grande quantidade de spam regularmente. O filtro irá deixar passar muito pouco spam, mas produzirá falsos positivos (e-mail legítimo marcado incorrectamente como spam). Configura as **Listas de Amigos/Spammers** e treina o **Motor de Aprendizagem (Bayesiano)** de forma a reduzir o número de falsos positivos.
Agressivo	Oferece protecção a contas que recebem um volume muito elevado de spam regularmente. O filtro irá deixar passar muito pouco spam, mas produzirá falsos positivos (e-mail legítimo marcado incorrectamente como spam). Adicione os seus contactos à **Lista de Amigos** de forma a reduzir o número de falsos positivos.

Para definir o nível de protecção por defeito (**Moderado a Agressivo**) clique em **Nível por Defeito**.

17.2.2. Configurar a Lista de Amigos

Lista de amigos é uma lista de todos os e-mails de quem você sempre quer receber mensagens, independente de seu conteúdo. Mensagens de seus amigos não são marcadas como Spam, mesmo se o conteúdo se assemelhe a Spam.

Nota
Qualquer mensagem vinda de um endereço contido na **Lista de amigos**, será automaticamente entregue em sua Caixa de entrada sem mais processamentos.

Para configurar a lista de Amigos clique em **Gerir Amigos** (ou clique no botão **Amigos** da barra de ferramentas Antispam).

Lista de amigos

Aqui você pode incluir ou remover entradas da **Lista de amigos**.

Se você quer incluir um endereço de e-mail marque o campo **E-mail** digite-o e clique no botão . O endereço aparecerá na **Lista de amigos**.

Importante
Syntax: nome@domínio.com.

Se você quer incluir um domínio marque o campo **Domínio** digite-o e clique no botão . O domínio aparecerá na **Lista de amigos**.

Importante
Syntax:

- @domínio.com, *domínio.com e domínio.com - todos os e-mails vindos de domínio.com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;
- *domínio* - todos os e-mails vindos de domínio (não importa quais os sufixos do domínio) chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;
- *com - todos os e-mails contendo o sufixo de domínio com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Salvar**/ **Carregar** para salvar / carregar a **Lista de amigos** num local desejado. O arquivo terá a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota
Nós recomendamos que você adicione os nomes e e-mails de seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos que estão na lista, portanto, adicionar amigos ajuda a fazer com que mensagens legítimas sejam recebidas.

Clique em **Aplicar** e **OK** para salvar e fechar a **Lista de amigos**.

17.2.3. Configurar a lista de Spammers

Lista de Spammers é uma lista de todos os endereços de quem você não quer receber mensagens, não importa qual o conteúdo.

Nota
Qualquer mensagem vinda de um e-mail na **Lista de Spammers** será marcado como Spam, sem pais processamentos.

Para configurar a lista de Spammers clique em **Gerir Spammers** (ou clique no botão **Spammers** da barra de ferramentas Antispam).

Lista de Spammers

Aqui você pode incluir ou remover entradas da **Lista de Spammers**.

Se quiser adicionar um endereço de email seleccione a opção **E-mail**, insira o endereço e clique no botão . O endereço irá aparecer na **Lista de spammers** .

Importante
Syntax: nome@domínio.com.

Se pretende adicionar um domínio seleccione a opção**Domínio**, insira-o e clique no botão . O domínio irá aparecer na **Lista de spammers**.

Importante
Syntax:

- @domínio.com, *domínio.com e domínio.com - todos os e-mails vindos de domínio.com serão marcados como Spam;
- *domínio* - todos os e-mails vindos de domínio (não importa quais os sufixos do domínio) serão marcados como Spam;
- *com - todos os e-mails contendo o sufixo de domínio com serão marcados como Spam.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Salvar**/ **Carregar** para salvar / carregar a **Lista de Spammers** num local desejado. O arquivo terá a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique em **Aplicar** e **OK** para salvar e fechar a **Lista de Spammers**.

Importante
Se você quiser reinstalar o BitDefender é uma boa idéia salvar as listas de **Amigos** / **Spammers** antes, e após a reinstalação você pode carregá-las.

17.3. Opções

Para configurar as definições de antispam e filtros, clique em **Antispam>Definições** no Modo Avançado.

Configurações de Antispam

Encontram-se disponíveis três categorias de opções (**Configuração de Antispam**, **Filtros básicos de Antispam** e **Filtros avançados de Antispam**) organizadas num menu expansível, semelhante aos do Windows.

Nota

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

Para ativar/desativar uma opção selecione/limpe a caixa correspondente.

Para aplicar as configurações por defeito, clique em **Por Defeito**.

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

17.3.1. Configurações de Antispam

- **Marcar spams no assunto** - todas as mensagens de e-mail consideradas spam serão marcadas com SPAM no campo assunto.
- **Marcar as mensagens de phishing no assunto** - todas as mensagens de e-mail consideradas phishing serão marcadas com SPAM no campo assunto.

17.3.2. Filtros Antispam Básicos

- **Listas de amigos/spammers** - filtra mensagens de e-mail usando as Listas de amigos/spammers;
  - **Adicionar automaticamente à lista de Amigos** - para adicionar os destinatários de e-mails enviados à Lista de Amigos.
  - **Incluir automaticamente à lista de amigos** - quando você clicar no **Not Spam** botão da Barra Antispam, remetente será incluso automaticamente na lista de Amigos.
  - **Incluir automaticamente à lista de spammers** - quando você clicar no **Is Spam** botão da Barra Antispam, o remetente será incluso automaticamente na lista de Spammers.

> *Nota*
> Os botões **Não-Spam** e **É Spam** são usados para treinar o filtro Bayesiano.

- **Bloquear Asiático** - bloqueia mensagens escritas com Caracteres asiáticos.
- **Bloquear Cirílico** - bloqueia mensagens escritas com Caracteres cirílicos.

17.3.3. Filtros Antispam Avançados

- **Activar Motor de Aprendizagem (bayesiano)** - activa/desactiva o Motor de Aprendizagem (bayesiano);
  - **Limitar o tamanho do dicionário em 200000 palavras** - configura o tamanho do dicionário Bayesiano – menos é mais rápido, maior é mais preciso.

> *Nota*
> O tamanho recomendado é 200.000 palavras.

- **Treinar Motor de Aprendizagem (bayesiano) nos e-mails de saída** - treina o Motor de Aprendizagem (bayesiano) nos e-mails de saída.

- **Filtro de URL** - ativa/desativa o Filtro de URL;
- **Filtro NeuNet (Heurístico)** - activa/desactiva o Filtro NeuNet (Heurístico);
  - **Bloqueia conteúdo explícito** - ativa/desativa a detecção de mensagens com SEXUALMENTE EXPLÍCITO no campo assunto.
- **Filtro de Imagem** - ativa/desativa o Filtro de Imagem.

18. Controle dos Pais

O Controle dos Pais BitDefender permite-lhe controlar o acesso à Internet e a determinadas aplicações para cada conta de usuário no sistema.

Pode configurar o Controle dos Pais para bloquear:

- Páginas web inapropriadas.
- ligação à Internet, durante determinados períodos de tempo (tal como o período de estudo).
- páginas web, mensagens de e-mail e mensagens instântaneas que contenham determinadas palavras-chave.
- aplicações tais como: jogos, programas de partilha de arquivos e outros.
- mensagens instântaneas enviadas por contacto IM para além dos que estão permitidos.

Importante

Apenas os usuários com direitos de administrador no sistema podem aceder e configurar o Controle dos Pais. Para ter a certeza de que só você pode modificar as definições do Controle dos Pais para qualquer usuário, pode protegê-las com uma senha. Ser-lhe-á pedida a senha cada vez que ativar o Controle dos Pais para um determinado usuário.

Para usar com sucesso o Controle dos Pais para restringir as actividades on-line e o computador das crianças, deve de completar estas principais tarefas:

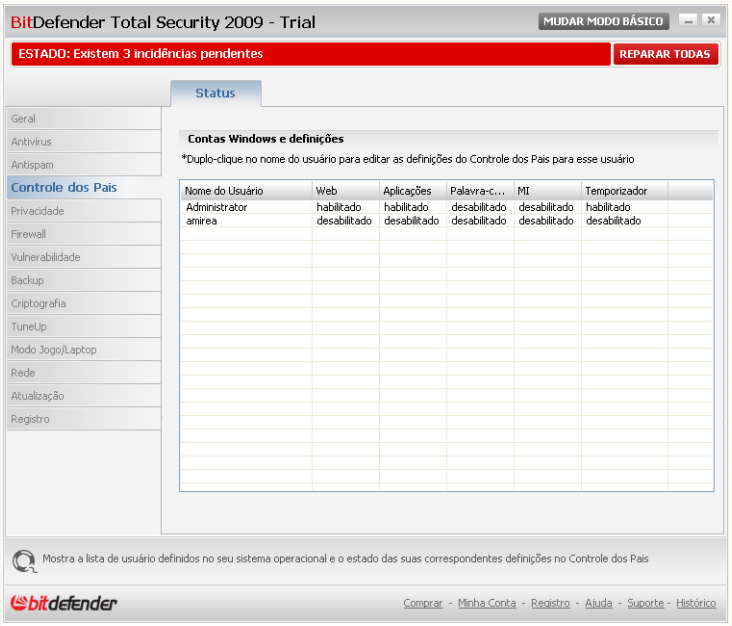
1. Criar uma conta do Windows limitada (standard) para a sua criança usar.

Nota

Para aprender como criar uma conta do Windows, vá ao Centro de Ajuda e Suporte do Windows (no menu Iniciar, clique em **ajuda e suporte**).

2. Configure o Controle dos Pais para as contas de usuário do Windows que as suas crianças utilizam.

Para configurar o Controle dos Pais, clique em **Controle dos Pais** no Modo Avançado.



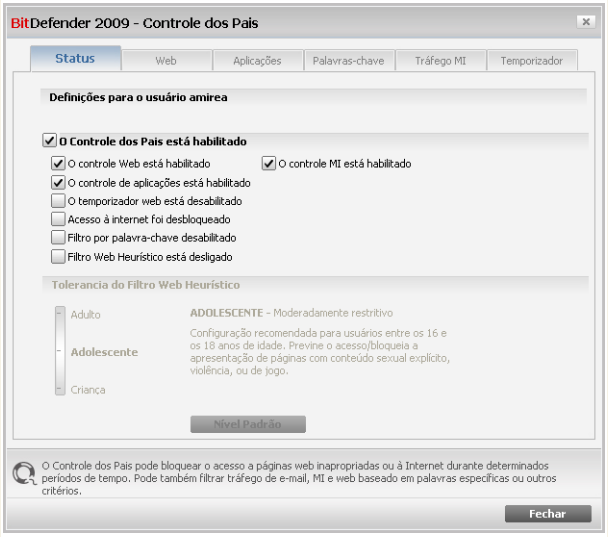
Controle dos Pais

Pode ver o estado das definições do Controle dos Pais configuradas para cada conta de usuário do Windows. Duplo clique sobre o nome do usuário para abrir a janela onde pode configurar o Controle dos Pais para a respectiva conta de usuário.

As seguintes secções dets capítulo apresentam em detalhe as características do Controle dos Pais e a forma de as configurar.

18.1. Definir Estado por usuário

Para configurar o Controle dos Pais para um determinado usuário, faça duplo clique no usuário e clique na barra **Estado**.



Estado do Controle dos Pais

Para configurar o Controle dos Pais para este usuário, siga estes passos:

1. Para ativar o Controle dos Pais para esta usuário marque a caixa de seleção ao pé do **Controle dos Pais**.

   Importante
   Mantenha o **Controle dos Pais** activado de forma a proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.

2. Definir senha para proteger as Definições do Controle dos Pais. Para mais informação, por favor consulte o "*Proteger as Definições do Controle dos Pais*" (p. 233).
3. Marque as caixas correspondentes aos controles de proteção que deseja usar:
   - **Controle Web** - para filtrar a navegação na Internet de acordo com as regras definidas por si na secção Web .
   - **Controle de Aplicações** - para bloquear o acesso às aplicações no seu computador de acordo com as regras definidas por si na seçãoAplicações.

- **Controle Mensagens Instântaneas** - permitir ou bloquear o chat IM de acordo com as regras definidas por si na seção Tráfego IM .
- **Temporizador Web** - para permitir o acesso à web de acordo com a tabela de horário definida por si na secçãoTemporizador .
- **Acesso Web** - para bloquear o acesso a todos os websites (não só apenas aqueles definidos na secção Web).
- **Filtragem Palavra-chave** - para filtrar o acesso à web, ao correio electrónico e às mensagens instântaneas de acordo com as regras definidas por si na secçãoPalavra-chave .
- **Filtro web Heurístico** - para filtrar o acesso à web de acordo com regras pré-estabelecidas baseadas em categorias de idade.

4. De forma a tirar o máximo benefício das características oferecidas pelo Controle dos Pais, deve de configurar os controles selecionados. Para aprender como configurá-los, por favor consulte os seguintes tópicos deste capítulo.

18.1.1. Proteger as Definições do Controle dos Pais

Se não for a única pessoa com direitos administrativos a utilizar este computador, recomendamos que protega as suas configurações do Controle dos Pais com uma senha. Ao definir uma senha, irá prevenir que outros usuários com direitos administrativos possam mudar as suas definições do Controle dos Pais que configurou para um determinado usuário.

BitDefender irá solicitar-lhe por defeito que defina uma senha quando ativar o Controle dos Pais.

Definir Proteção por senha

Para definir protecção por senha, faça o seguinte:

1. Digite a senha na campo **Senha** .
2. Insira de novo a senha no campo **Reinserir Senha** para a confirmar.
3. Clique em **OK** para guardar a senha e fechar a janela.

Uma vez definida a senha, se desejar modificar as definições do Controle dos Pais, ser-lhe-á pedido que insira a senha. Os outros administradores de sistema (se existirem) terão também de inserir a senha de forma a poderem alterar as definições do Controle dos Pais.

Nota
A senha não protege quaisquer outras definições do BitDefender.

Caso não defina uma senha e não queira que a janela para o efeito lhe surja novamente, seleccione **Não solicitar senha quando ativar Controle dos Pais**.

18.1.2. Configurar Filtro Web Heurístico

O filtro web heurístico analisa as páginas web e bloqueia aquelas que correspondem aos modelos de conteúdos potencialmente inapropriados.

De forma a filtrar o acesso à web de acordo com um conjunto de regras (ruleset) de idade, deverá definir um determinado nível de tolerância. Arraste o marcador ao longo da escala para definir o nível de tolerância que considera apropriado para o usuário seleccionado.

Existem 3 níveis de tolerância:

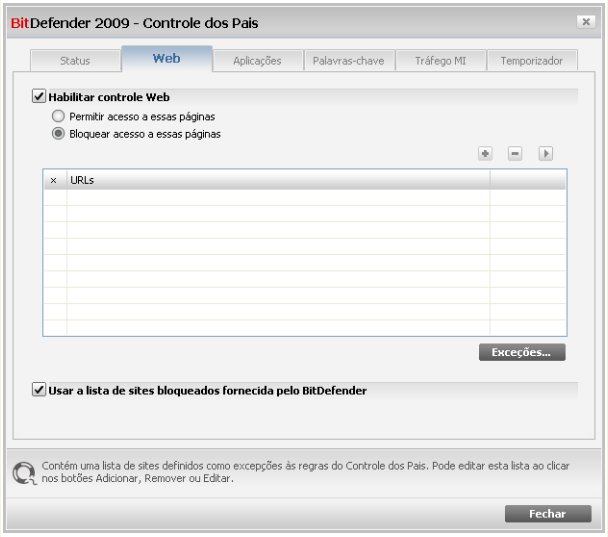
Nível de Tolerância	*Descrição*
Criança	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para usuários menores de 14. São bloqueadas as páginas web com um potencial conteúdo prejudicial para as crianças (porno, sexualidade, drogas, hacking, etc.).
Adolescente	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para usuários entre os 14 e os 18 anos de idade. São bloqueadas as páginas web com um conteúdo sexual, pornográfico ou adulto.
Adulto	Oferece um acesso sem restrições a todas as páginas web independentemente do seu conteúdo.

Clique em **Nível por Defeito** para colocar o marcador no nível por defeito.

18.2. Controle Web

O **Controle Web** ajuda você a bloquear páginas web de conteúdo inapropriado. Uma lista de candidatos para bloquear as páginas ou parte delas será providenciada e atualizada pelo BitDefender, como parte do processo normal de atualização. Páginas contendo referências (links) para páginas web na lista negra também poderão ser bloqueadas.

Para configurar o Controle Web para um determinado usuário, faça duplo clique no mesmo e clique na barra **Web**.



Controle Web

Para habilitar esta proteção marque a caixa correspondente **Habilitar Controle Web**.

Seleccione **Permitir acesso a estas páginas**/**Bloquear acesso a estas páginas** para ver a lista dos sites permitidos/bloqueados. Clique em **Excepções...** para aceder à janela onde pode ver a lista complementar.

As regras devem ser inseridas manualmente. Primeiro que tudo, seleccione **Permitir acesso a estas páginas**/**Bloquear acesso a estas páginas** para permitir/bloquear o acesso aos sites web que irá especificar no assistente. Então clique no botão **Adicionar...** para iniciar o assistente de configuração.

Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para modificar uma regra seleccione-a e clique no botão **Editar...** ou faça duplo-clique sobre ela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

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

18.2.1. Assistente de Configuração

O assistente de configuração é um procedimento de um passo.

Passo 1/1 - Especifique as páginas web

Especifique as páginas web

Introduza o site web para o qual a regra será aplicada e clique em **Terminar**.

Importante
Syntax:

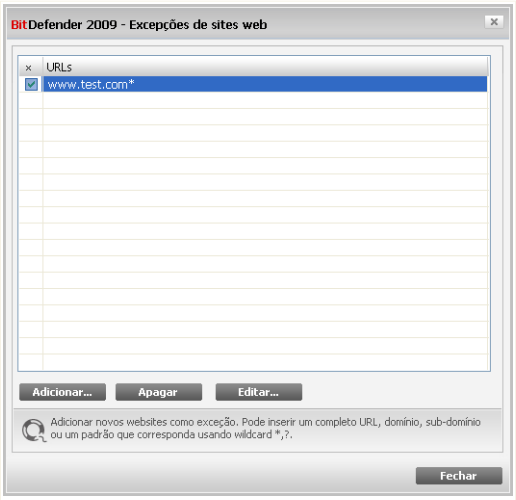
- `*.xxx.com` - a acção da regra será aplicada a todos os sites web que terminam em `.xxx.com`;
- `*porn*` - a acção da regra será aplicada a todos os sites web que contenham `porn` no endereço do site web;
- `www.*.com` - a acção da regra será aplicada a todos os sites web que tenham o sufixo de domínio `com`;
- `www.xxx.*` - a acção da regra será aplicada a todos os sites web que comecem por `www.xxx.` sem importar o sufixo do domínio.

18.2.2. Especifique as exceções

Por vezes necessita de especificar excepções para uma regra em particular. Por exemplo, define uma regra que bloqueia sites que contêm a palavra "hard" no endereço (sintaxe: `*hard*`). Também está consciente da existência de um site denominado `hard-rock` onde os visitantes podem ouvir música on-line. Para abrir uma excepção

à regra previamente criada, aceda à janela **Excepções** e defina uma excepção para a regra.

Clique em **Excepções...**. A seguinte janela irá aparecer:



Especificando as exceções

Clique em **Adicionar...** para especificar excepções. O assistente de configuração aparecerá. Complete o assistente de forma a definir a excepção.

Para apagar uma regra, apenas seleccione-a e clique em **Apagar**. Para modificar uma regra seleccione-a e clique em **Editar...** ou faça um duplo-clique nela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

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

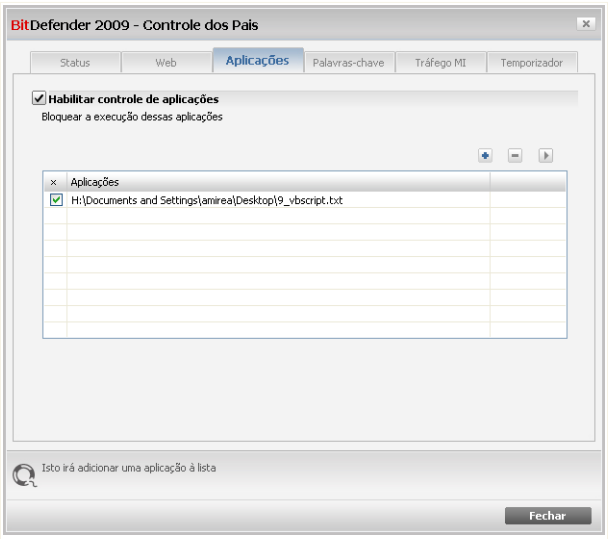
18.2.3. Lista Negra Web BitDefender

De forma a proteger as suas crianças, o BitDefender dá-lhe um lista negra de sites web com conteúdo inapropriado ou possivelmente perigoso. Para bloquear os sites que aparecem nesta lista seleccione **Usar a lista dos sites bloqueados fornecidos por BitDefender**.

18.3. Controle de Aplicações

O **Controle de aplicações** ajuda você a bloquear qualquer aplicação contra execução. Jogos, mídia e software de mensagens, assim como outras categorias de software e malware podem ser bloqueadas desta maneira. Aplicações bloqueadas desta forma também são bloqueadas contra modificação, e não podem ser copiadas ou movidas.

Para configurar o Controle de aplicações para um determinado usuário, faça duplo clique no mesmo e clique na barra **Aplicações**.



Controle de Aplicações

Para habilitar esta proteção selecione a caixa correspondete a **Habilitar Controle de Aplicações**.

As regras devem ser inseridas manualmente. Clique no botão **Adicionar...** para dar início ao assistente de configuração.

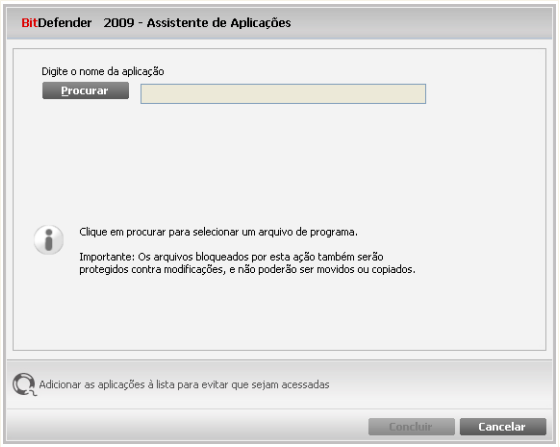
Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para modificar uma regra seleccione-a e clique no botão **Editar...** ou faça duplo-clique sobre ela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

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

18.3.1. Assistente de Configuração

O assistente de configuração é um procedimento de um passo.

Passo 1/1 - Selecionar a aplicação a ser bloqueada



Selecione a aplicação a ser bloqueada

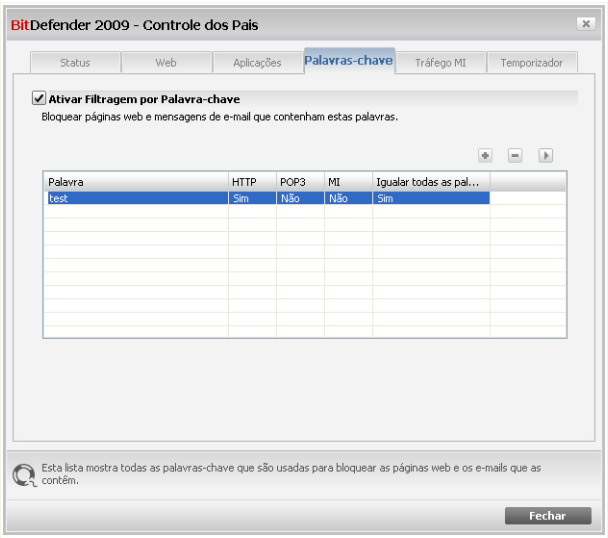
Clique em **Explorar**, seleccione a aplicação a ser bloqueada e clique em **Terminar**.

18.4. Filtragem Palavra-chave

A Filtragem por Palavra-chave ajuda-o a bloquear o acesso dos usuários a mensagens de e-mail, páginas web e mensagens instântaneas que contenham determinadas palavras. Ao usar a Filtragem por Palavra-chave, pode evitar que as crianças vejam palavras ou frases inapropriadas quando estão on-line.

Nota
A Filtragem por Palavra-chave das mensagens instântaneas só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.

Para configurar Filtragem por Palavra-chave para um determinado usuário, faça duplo clique no respectivo usuário e clique na barra **Palavras-chave**.



Filtragem Palavra-chave

Marque a caixa **Activar Filtragem Palavra-chave** se pretende usar esta opção de controle.

Tem de adicionar regras para especificar as palavras-chave a serem bloqueadas. Para adicionar uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para editar uma regra existente faça duplo clique na regra ou clique no botão **Editar** e faça as alterações desejadas na janela de configuração.

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

18.4.1. Janela de configuração

Quando adiciona ou edita regras, a janela de configuração irá aparecer.

Inserir senha

Deve definir os seguintes parâmetros:

- **Palavra-chave** - insira no campo de edição a palavra ou frase que deseja bloquear.
- **Protocolo** - escolha o protocolo que o BitDefender deve analisar para a palavra especificada.

Opção	*Descrição*
POP3	As mensagens de e-mail que contenham a palavra-chave são bloqueadas.
HTTP	As páginas web que contenham a palavra-chave são bloqueadas.
Mensagens Instântaneas	As mensagens instântaneas que contenham a palavra-chave são bloqueadas.

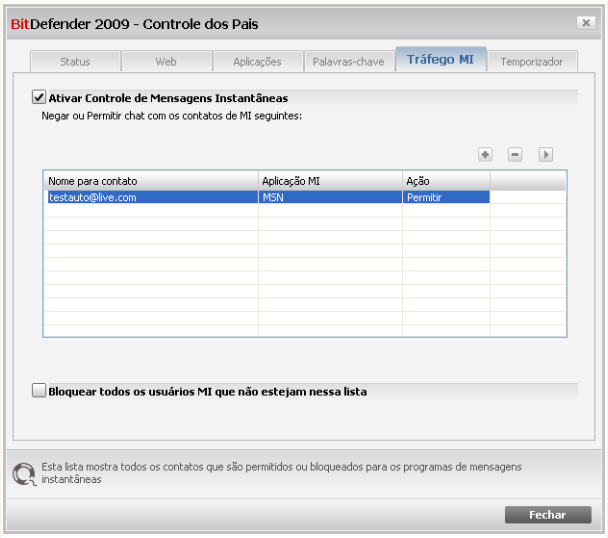
Clique em **Terminar** para adicionar a regra.

18.5. Controle de Mensagens Instântaneas (IM)

O Controle de Mensagens Instântaneas (IM) permite-lhe especificar os contactos IM com os quais a sua criança pode fazer chat.

Nota
O Controle de Mensagens Instântaneas (IM) só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.

Para configurar O Controle de Mensagens Instântaneas (IM) para um determinado usuário, faça duplo clique sobre o mesmo e clique na barra **Tráfego IM**.



Controle de Mensagens Instântaneas

Marque a caixa **Ativar Controle de Mensagens Instântaneas** se deseja utilizar esta opção de controle.

Tem de adicionar regras para especificar que contatos IM o usuário está ou não autorizado a fazer chat. Para adicionar uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

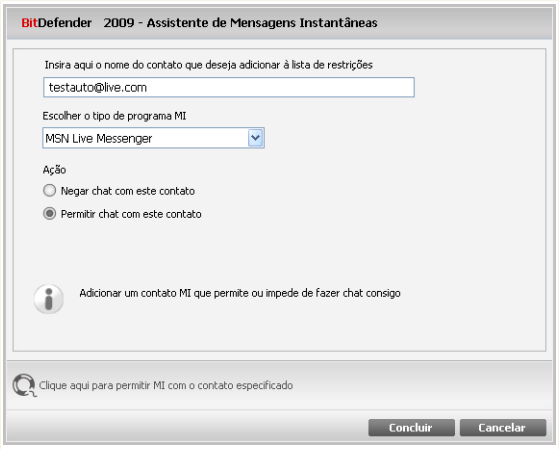
Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para editar uma regra existente faça duplo clique na regra ou clique no botão **Editar** e faça as alterações desejadas na janela de configuração.

Se definiu todos os contatos IM que o usuário está permitido a fazer chat com, selecione **Bloquear todos os contatos IM que não estão nesta lista**. Desta forma, somente os contatos explicitamente autorizados podem enviar mensagens instântaneas ao usuário.

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

18.5.1. Janela de configuração

Quando adiciona ou edita regras, a janela de configuração irá aparecer.



Adicionar contacto IM

Proceder da seguinte forma:

1. Inserir nome de usuário (ID) do contato IM.
2. Escolher o program de IM com o qual o contacto se associa.
3. Seleccionar a acção da regra:
   - **Bloquear chat com este contacto**
   - **Permitir chat com este contacto**

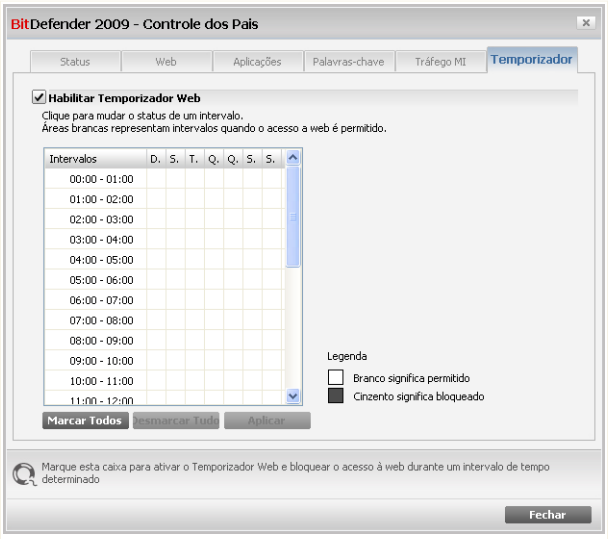
4. Clique em **Terminar** para adicionar a regra.

18.6. Limitador de Horário Web

O **Limitador de Horário Web** ajuda você a permitir ou bloquear o acesso web para usuários e aplicações durante intervalos específicos de tempo.

Nota
O BitDefender irá executar atualizações de hora em hora não importando as configurações do **Limitador de Horário Web**.

O BitDefender efectuará a actualização de hora-a-hora independentemente da configuração do **Temporizador Web**.



Limitador de Horário Web

Para habilitar esta proteção selecione a caixa correspondente a **Limitador de Horário Web**.

Seleccione os intervalos de tempo em que todas as ligações à Internet estarão bloqueadas. Pode clicar em células individuais ou pode clicar e arrastar o ponteiro de forma a cobrir longos períodos de tempo. Também pode clicar em **Marcar Todas**

para seleccionar todas as células, implicitamente, bloqueando todo o acesso à web. Se clicar em **Desmarcar Todas**, as ligações de internet serão sempre permitidas.

Importante
As caixas em cinza representam intervalos em que todas as conexões com a Internet estão bloqueadas.

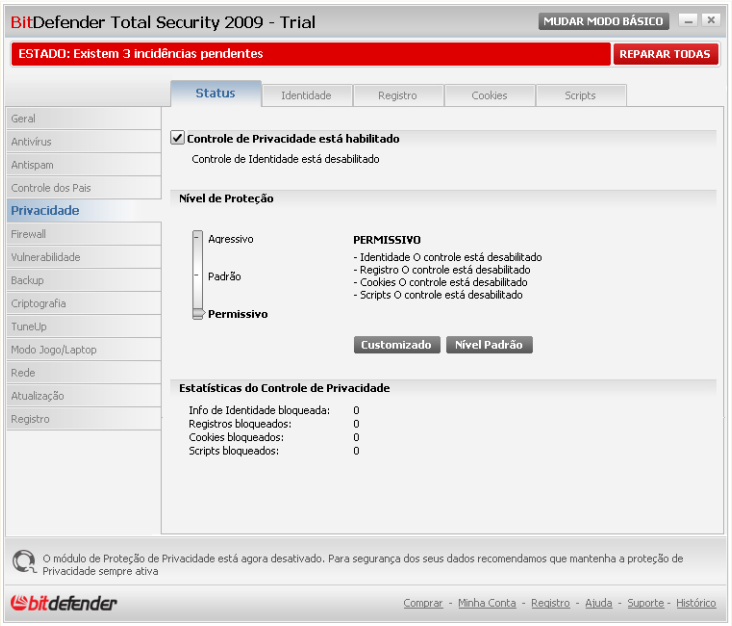
Clique em **Aplicar** para salvar as modificações.

19. Controle Privacidade

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

19.1. Estado do Controle de Privacidade

Para configurar o Controle de Privacidade e ver informação quanto à sua atividade, vá para **Controle de Privacidade>Estado** no Modo Avançado.



Estado do Controle de Privacidade

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

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

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

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

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

19.1.1. Configurar Nível de 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	Apenas o **Controle de Registo** está ativo.
Por Defeito	O **Controle de Registo** e o **Controle de Identidade** estão ativos.
Agressivo	O **Controle de Registo**, o **Controle de Identidade** e o **Controle de Script** estão ativos.

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

Clique em **Nível por Defeito** para colocar o mostrador no nível por defeito.

19.2. Controle de Identidade

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

Quer seja o seu e-mail o seu número de cartão de crédito, quandos eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

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

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária. Suporte multi-usuário é fornecido de forma a que os usuários de diferentes contas do Windows possam configurar e usar as suas próprias regras de identidade. As regras que criou são aplicadas e podem ser acedidas apenas quando entrou com a sua conta no Windows.

Porquê usar o Controle de Identidade?

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

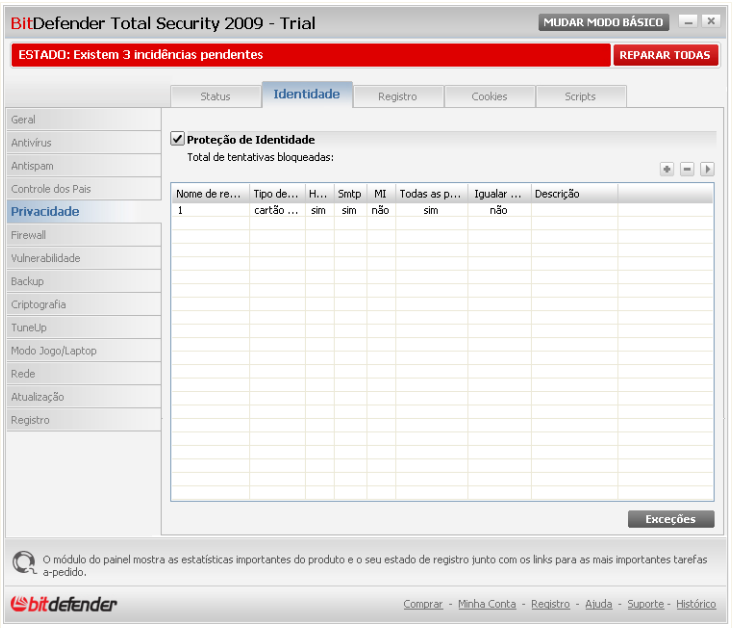
  Supondo que tal aplicação funciona de forma a evitar a detecção antivírus, a mesma não pode enviar os dados roubados por e-mail, web ou mensagens instântaneas se tiver criado as regras de protecção de identidade adequadas.

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

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

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

Para configurar o Controle de Identidade, clique em **Controle Privacidade>Identidade** no Modo Avançado.



Controle de Identidade

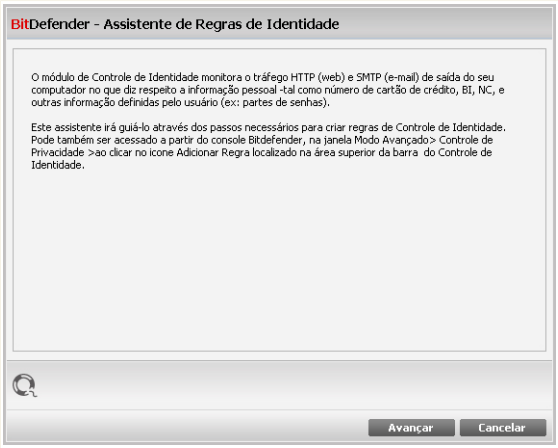
Se deseja usar Controle de Identidade, siga estes passos:

1. Selecione a caixa **Controle de Identidade**.
2. Criar regras para proteger a sua informação sensível. Para mais informação, por favor consulte o "*Criar Regras de Identidade*" (p. 251).
3. Se necessário, defina excepções específicas para as regras que criou. Para mais informação, por favor consulte o "*Definir Excepções*" (p. 254).

19.2.1. Criar Regras de Identidade

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

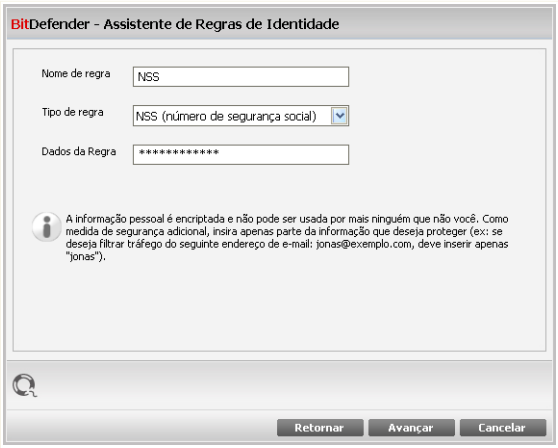
Passo 1/4 - Janela de Boas-vindas



Janela de Boas-Vindas

Clique em **Próximo**.

Passo 2/4 - Definir Tipo de Regra e Dados



Definir Tipo de Regra e Dados

Deve definir os seguintes parâmetros:

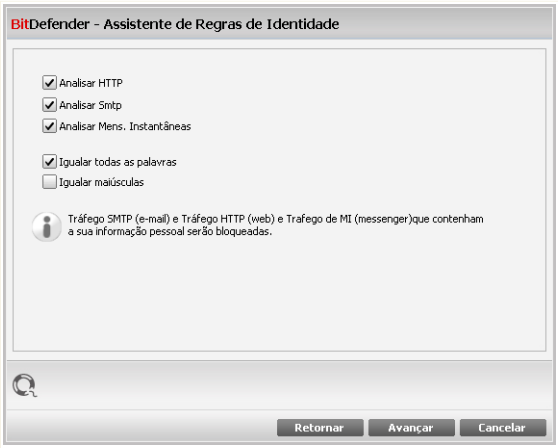
- **Nome Regra** - insira o nome da regra no campo editável.
- **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
- **Dados Regra** - insira os dados que quer proteger com a regra no campo editável. Por exemplo, se deseja proteger o seu número de cartão de crédito,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

> ***Nota***
> Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

Clique em **Próximo**.

Passo 3/4 - Seleccionar Tráfego



Seleccionar Tráfego

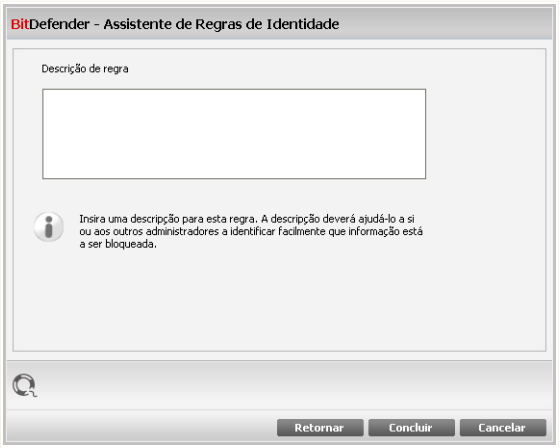
Seleccione o tráfego que quer que o BitDefender analise. As seguintes opções estão disponíveis:

- **Analisar HTTP** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar SMTP** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
- **Analisar Mensagens Instantâneas** - analisa todo o tráfego Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

Clique em **Próximo**.

Passo 4/4 - Descrever Regra



Descrever Regra

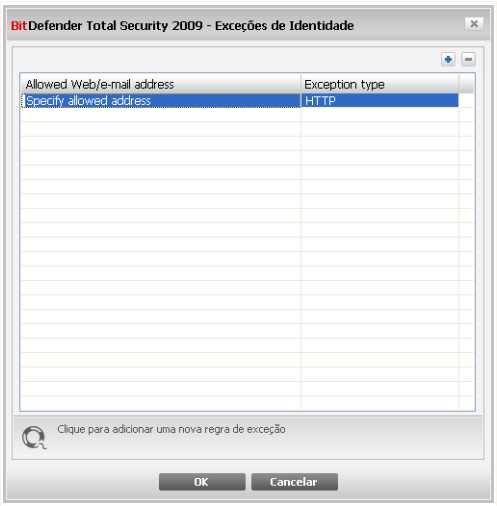
Insira uma breve descrição da regra no campo de edição. Uma vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

Clique em **Finalizar**. A regra aparecerá na tabela.

19.2.2. Definir Excepções

Há casos em que necessita de definir excepções para especificar as regras de identidade. Consideremos o caso em que criou uma regra que evita que o número do seu cartão de crédito seja enviado por HTTP (web). Sempre que o seu cartão de crédito seja submetido num site web a partir da sua conta de utilizador, a respectiva página web é bloqueada. Se deseja por exemplo, pagar uma compra online numa loja virtual (que você sabe ser segura), terá de especificar uma excepção para a respectiva regra.

Para abrir a janela onde pode gerir as excepções, clique em **Excepções**.



Exceções

Para adicionar uma excepção, siga os seguintes passos:

1. Clique **Adicionar** para adicionar uma nova entrada na lista.
2. Duplo-clique em **Especificar endereço permitido** e inserir o endereço web, endereço de e-mail ou o contacto IM que deseja adicionar como excepção.
3. Duplo-clique em**Escolher Tipo** e escolha do menu a opção correspondente ao tipo de endereço que inseriu anteriormente.
   - Se especificou um endereço web, seleccione **HTTP**.
   - Se especificou um endereço de e-mail, seleccione**SMTP**.
   - Se especificou um contacto IM, seleccione**IM**.

Para remover uma excepção da lista, seleccione-a e clique **Remover**.

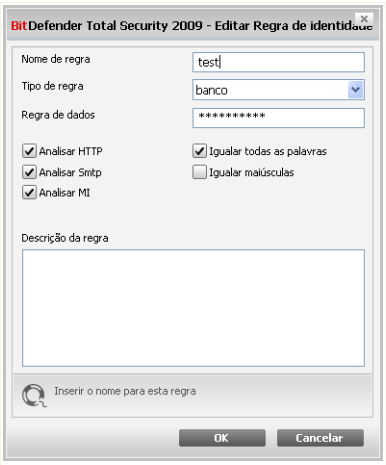
Clique em **OK** para salvar as alterações.

19.2.3. Gerir Regras

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

Para editar uma regra, seleccione-a e clique no botão **Editar** ou faça duplo-clique sobre ela. Uma nova janela irá aparecer.



Editar Regra

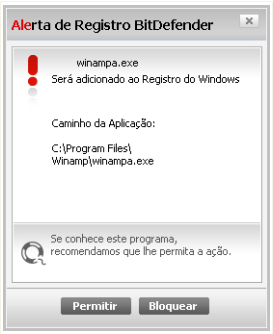
Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

19.3. Controle de Registro

Uma parte muito importante do sistema operacional Windows é chamada de **Registro**. É aqui que o Windows mantém suas configurações, programas instalados, informações de usuário e informações do gênero.

O **Registro** é também usado para definir quais programas deverão ser iniciados automaticamente quando o Windows inicia. Vírus costumam usar isso para serem executados automaticamente quando o usuário reinicia seu computador.

O **Controle de Registro** fica de olho no Registro do Windows – Isso é útil também para detectar Trojans. Você será alertado sempre que um programa tentar modificar uma entrada de registro para ser executado na inicialização do Windows.



Alerta do Registro

Poderá ver o programa que está a tentar alterar o registo do Windows.

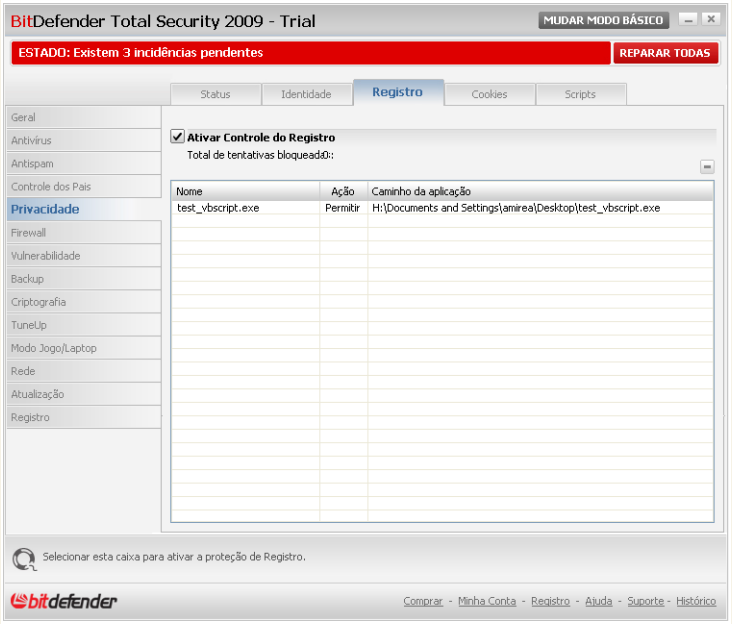
Se não reconhece o programa e lhe parecer suspeito, clique em **Bloquear** para evitar que ele modifique o registo do Windows. De outra forma, clique em **Permitir** para permitir a modificação.

Baseado na sua resposta, a regra é criada e listada na tabela de regras. A mesma acção será aplicada sempre que este programa tentar modificar uma entrada no registo.

Nota

O BitDefender normalmente irá alertá-lo quando você instalar novos programas que precisam rodar após a próxima inicialização de seu computador. Na maioria dos casos, esses programas são legítimos e podem ser confiados.

Para configurar o Controle de Registo, clique em **Controle Privacidade>Registo** no Modo Avançado.



Controle de Registro

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

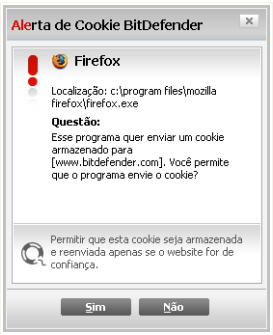
19.4. Controle de Cookie

Cookies são uma ocorrência muito comum na Internet. Eles são pequenos arquivos gravados em seu computador. Websites criam esses cookies para manter controle de informações específicas sobre você.

Cookies normalmente são usados para tornar sua vida mais fácil. Por exemplo, eles podem ajudar o site a lembrar de seu nome e preferências, para que você não tenha que inseri-los a cada visita.

Mas os cookies podem também ser usados para comprometer sua privacidade, vigiando seus padrões de navegação.

É aí que o **Controle de Cookie** ajuda. Quando ativado, o **Controle de Cookie** pedirá sua permissão sempre que um novo site tentar colocar um cookie:



Alerta de cookie

Você pode ver o nome do aplicativo que está tentando enviar o cookie.

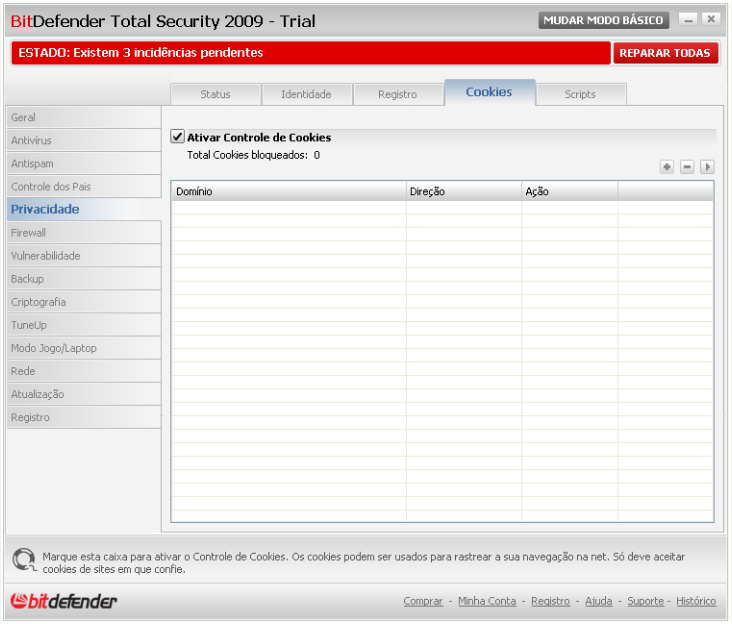
Marque a caixa **Lembrar dessa resposta** e clique em **Sim** ou **Não** e uma regra será criada, aplicada e listada na tabela de regras. Você não será mais notificado quando se conectar a esse site.

Isso ajudará você a escolher quais sites tem ou não sua confiança.

Nota

Por causa do grande número de cookies usados hoje na Internet, o **Controle de Cookie** pode ser bem chato no início. No início, ele fará várias perguntas sobre sites tentando colocar cookies em seu computador. Conforme você adicionar seus sites comuns à lista de regras, surfar na Internet será tão fácil quanto antes.

Para configurar o Controle de Cookies, clique em **Controlo Privacidade>Cookie** no Modo Avançado.



Controle de Cookie

Pode ver as regras criadas até agora listadas na tabela.

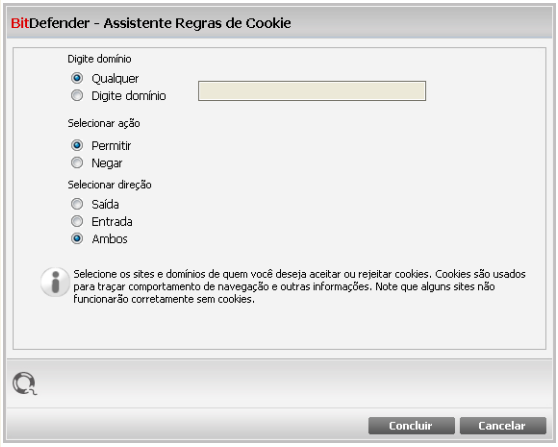
Importante
A prioridade das regras é de baixo para cima, ou seja, a última regra tem a maior prioridade. Arraste & solte regras para mudar a prioridade.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para modificar os parâmetros da regra, faça duplo clique sobre a regra e faça as modificações desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

19.4.1. Janela de configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



Selecione endereço, ação e direção

Você pode configurar parâmetros:

- **Domínio** - digite o domínio em que você quer aplicar a regra.
- **Ação** - selecione a ação da regra.

Ação	*Descrição*
Permitir	Os cookies daquele domínio serão executados.
Negar	Os cookies daquele domínio não serão executados.

- **Direção** - selecione a direção do tráfego.

Tipo	*Descrição*
Saída	A regra será aplicada apenas para os cookies que forem devolvidos para o site conectado.
Entrada	A regra será aplicada apenas para os cookies que forem recebidos do site conectado.
Ambos	As regras valem para as duas direções.

Nota
Você pode aceitar cookies mas nunca devolvê-los definindo a ação como **Negar** e a direção como **Saída**.

Clique em **Finalizar**.

19.5. Controle de Scripts

Scripts e outros códigos tais como Controles ActiveX e Java applets, que são usados para criar páginas da web interativas, podem ter efeitos danosos. Elementos ActiveX , por exemplo, podem ganhar acesso total a seus dados e eles podem ler dados de seu computador, apagar informações, capturar senhas e interceptar mensagens enquanto você esta on-line. Você pode apenas aceitar conteúdo ativo de sites de sua total confiança.

O BitDefender deixa você escolher entre executar estes elementos ou bloquear a execução.

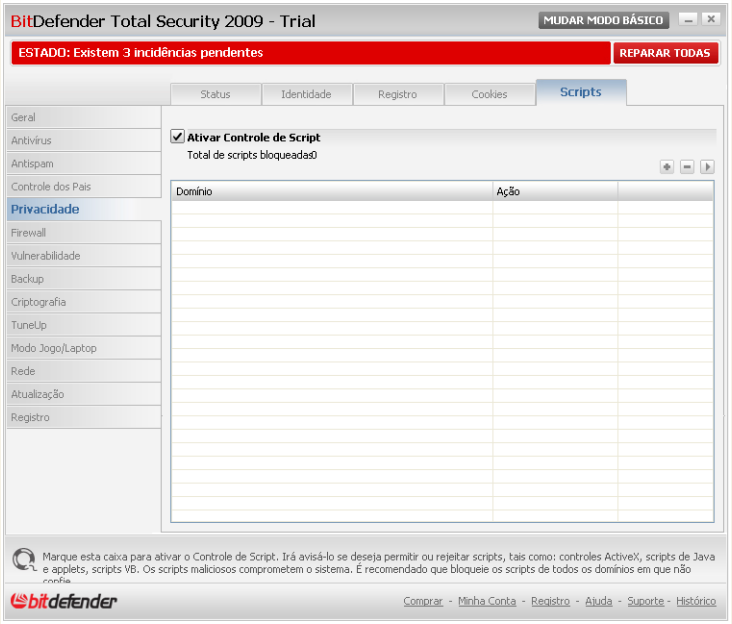
Com o **Controle de Scripts** você será responsável por quais websites você confia ou não. O BitDefender pedra sua permissão sempre que um site tentar ativar um script ou outro conteúdo ativo:

Alerta de script

Você pode ver o nome do recurso.

Marque a caixa **Lembrar dessa resposta** e clique em **Sim** ou **Não** e uma regra será criada, aplicada e listada na tabela de regras. Você não será mais notificado quando esse site tentar lhe enviar conteúdo ativo.

Para configurar o Controle de Script, clique em **Controle Privacidade>Script** no Modo Avançado.



Controle de Scripts

Pode ver as regras criadas até agora listadas na tabela.

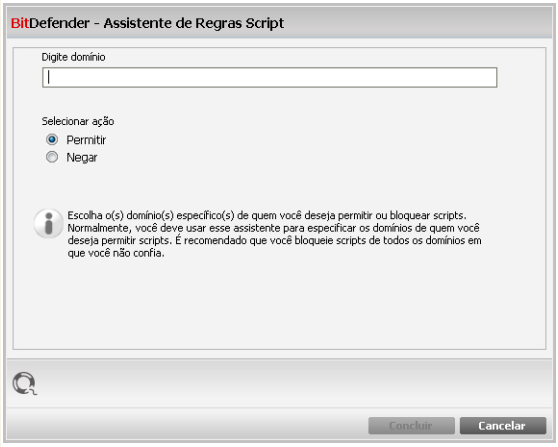
Importante
A prioridade das regras é de baixo para cima, ou seja, a última regra tem a maior prioridade. Arraste & solte regras para mudar a prioridade.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para modificar os parâmetros da regra, faça duplo clique sobre a regra e faça as modificações desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

19.5.1. Janela de configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



Selecione endereço e ação

Você pode configurar parâmetros:

- **Domínio** - digite o domínio em que você quer aplicar a regra.
- **Ação** - selecione a ação da regra.

Ação	*Descrição*
Permitir	Os scripts daquele domínio serão executados.
Negar	Os scripts daquele domínio não serão executados.

Clique em **Finalizar**.

20. Firewall

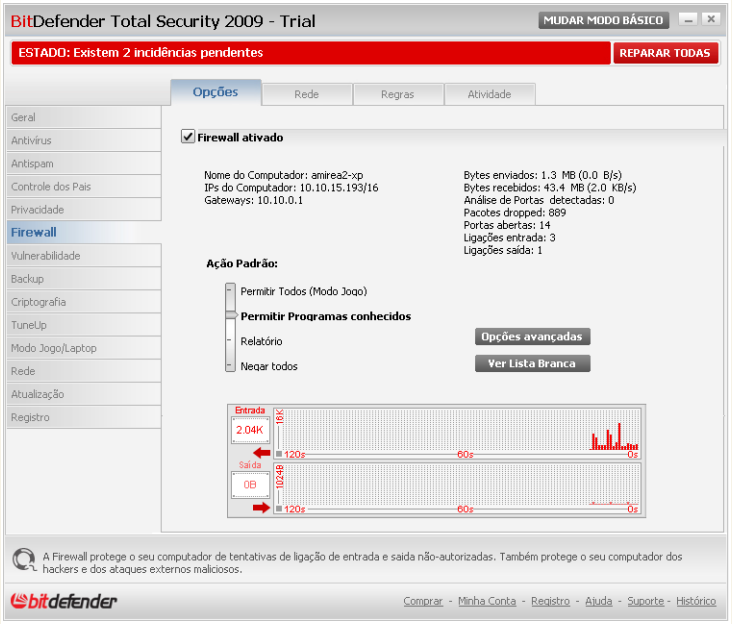
A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.

Nota
Um firewall é essencial se você estiver usando uma conexão banda-larga ou DSL.

Em Modo Stealth o seu computador fica “escondido” do software maligno e dos hackers. O módulo da firewall é capaz de detectar e proteger automaticamente o seu computador contra os scans de portas (conjunto de pacotes enviados para uma máquina de forma a encontrar "pontos de acesso", frequentemente como modo de preparação para um ataque).

20.1. Opções

Para configurar a protecção firewall, clique em **Firewall>Definições** no Modo Avançado.



Definições da Firewall

Aqui é onde pode ver se a Firewall BitDefender se encontra activada ou desactivada. Se deseja alterar o estado da firewall, limpe ou seleccione a caixa correspondente.

Importante
Para estar protegido contra ataques de Internet mantenha o **Firewall** habilitado.

Existem duas categorias de informação:

- **Configuração de Rede Breve.** Pode ver o nome do seu computador, o seu endereço IP e a sua gateway por defeito. Se tem mais do que um adaptador de rede (significando que está ligado a mais do que uma rede), verá o endereço IP e a gateway configurada para cada adaptador de rede.
- **Estatísticas.** Pode ver as várias estatísticas com respeito à actividade da firewall:
  - número de bytes enviados.

- número de bytes recebidos.
- número de scans de portas detectados e bloqueados pelo BitDefender. Os scans de portas são frequentemente usados pelos hackers para descobrir portas abertas no seu computador com o objectivo de as explorar.
- número de pacotes deixados cair.
- número de portas abertas.
- número de ligações de entrada activas.
- número de ligações de saída activas.

Para ver as ligações activas e as portas abertas, vá até à barra Actividade.

Ao fundo e ao lado desta secção pode ver as estatísticas do BitDefender com respeito ao tráfego de entrada e de saída. O gráfico mostra-lhe o volume de tráfego da Internet durante os últimos dois minutos.

Nota
O gráfico aparece mesmo que o **Firewall** esteja desabilitado.

20.1.1. Definir a Acção por Defeito

Por defeito o BitDefender permite automaticamente que todos os programas conhecidos da sua lista branca acedam aos serviços da rede e à Internet. Para todos os outros programs o BitDefender consulta-o através de uma janela de alerta para que decida a acção a tomar. A acção que determinar será aplicada cada vez que a respectiva aplicação solicite o acesso à rede/internet.

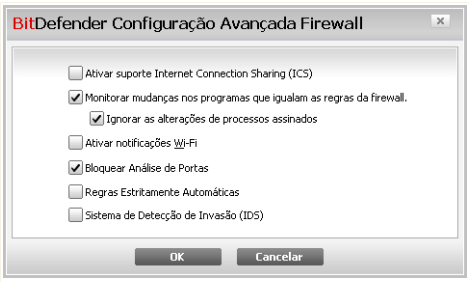
Arraste o marcador ao longo da escala para definir a acção a ser levada a cabo para as aplicações que solicitem acesso à rede/Internet. Estão disponíveis as seguintes acções por defeito:

Acção por Defeito	Descrição
Permitir Todos	Aplica as regras actuais e permite as tentativas de tráfego que não correspondem com nenhuma das regras actuais sem o consultar. Esta política é muito desaconselhada, mas poderá ser útil para administradores de redes e jogadores.
Permitir Programas Conhecidos	Aplica as regras actuais e permite todas as tentativas de ligação de saída dos programas que BitDefender

Acção por Defeito	Descrição
	considera como legítimos (lista branca) sem o consultar. Para as restantes tentativas de ligação, Bitdefender solicitará a sua permissão. Programas da Lista Branca são as aplicações mais usadas e comuns a nível mundial. Incluem os mais conhecidos browsers de internet, audio&video players, programas de chat e filesharing, como também as aplicações de cliente servidor e do sistema operacional.
Relatório	Aplica as regras actuais e consulta-o acerca das tentativas de tráfego que não correspondem com nenhuma das regras actuais.
Bloquear Todos	Aplica as regras actuais e bloqueia todas as tentativas de tráfego que não correspondem com nenhuma das regras actuais.

20.1.2. Configuração Avançada da Firewall

Clique em **Avançada** para configurar as definições avançadas da firewall.



Configuração Avançada da Firewall

As seguintes opções estão disponíveis:

- **Activar Suporte de Internet Connection Sharing (ICS)** - activa o suporte para Internet Connection Sharing (ICS).

Nota
Esta opção não ativa automaticamente o ICS no seu sistema, mas apenas permite este tipo de ligação em caso de a ativar no seu sistema operacional.

O Internet Connection Sharing (ICS) permite que elementos da sua rede de área local se liguem à Internet através do seu computador. Isto é útil quando benefecia de uma ligação à Internet especial/particular (ex:- ligação wireless) e a quer partilhar com outros membros da sua rede.

Partilhar a sua ligação à Internet com membros da sua rede de área local leva a um elevado consumo de recursos e pode envolver algum risco. Também lhe retira algumas portas (aquelas abertas pelos membros que estão a usar a sua ligação à Internet).

- **Monitorizar mudanças em arquivos de programas que igualam as regras da firewall** - Verifica cada tentativa de ligação à Internet das aplicações para ver se elas mudaram desde que a regra que controla o seu acesso foi criada. Se a aplicação foi alterada, um aviso de alerta surgirá para que permita ou bloquei o acesso da aplicação à Internet.

  Normalmente as aplicações são alteradas pelas actualizações. Mas, existe um risco que elas sejam alteradas por aplicações malware, com o propósito de infectar o seu computador e outros computadores na rede.

  Nota
  Recomendamos que mantenha esta opção seleccionada e permita acesso apenas àquelas aplicações que espera que tenham mudado após a regra que controla o seu acesso ter sido criada.

  Aplicações assinadas são suposta serem fiáveis e de um alto nível de segurança. Pode escolher **Ignorar mudanças em processos assinados** de forma a permitir que aplicações assinadas que se alteraram se liguem à Internet sem ser alertado acerca deste evento.

- **Activar notificações wireless** - se estiver ligado a uma rede wireless, mostra janelas informativas com respeito aos eventos de rede (por exemplo, quando um novo computador foi ligado à rede).

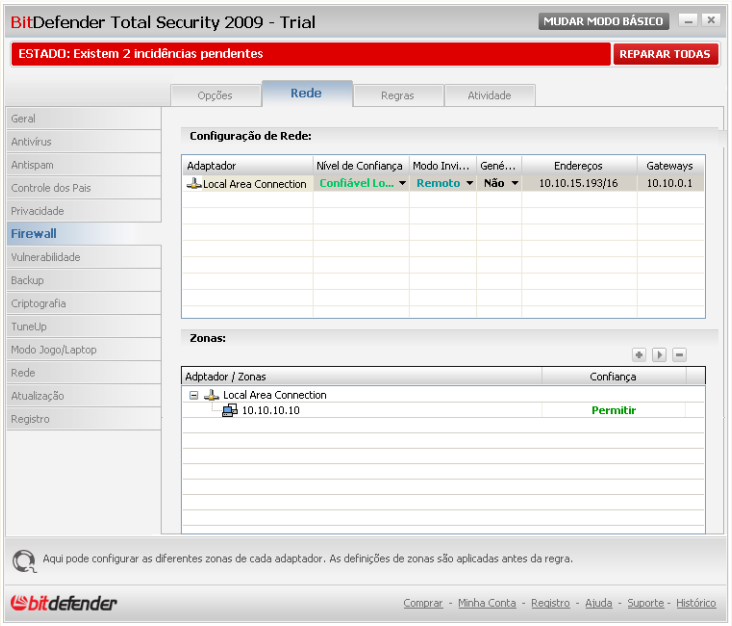
- **Bloquear scans de portas** - detecta e bloqueia todas as tentativas de descobrir que portas se encontram abertas.

  Os scans de portas são frequentemente usados pelos hackers para descobrir que portas se encontram abertas no seu computador. Então eles poderão entrar no seu computador se descobrirem uma porta menos segura ou vulnerável.

- **Regras automáticas estritas** - cria regras estritas usando a janela de alerta da firewall. Com esta opção seleccionada. o BitDefender consulta-lo-á para tomar uma acção e criar regras para cada diferente processo que abre a aplicação que está a solicitar o acesso à rede ou à Internet.
- **Sistema de detecção de Intrusão (IDS)** - activa a monitorização heurística das aplicações que estão a tentar aceder aos serviços de rede ou à Internet.

20.2. Rede

Para configurar a protecção firewall, clique em **Firewall>Rede** no Modo Avançado.



Rede

As colunas na tabela de **Configuração de Rede** dão-lhe informação detalhada da rede à qual se encontra ligado:

- **Adaptador** - o adaptador de rede que o seu computador usa para se ligar à rede ou à Internet.

- **Tipo** - o nível de confiança atribuido ao adaptador de rede. Dependendo da configuração do dispositivo de rede, o BitDefender pode automaticamente atribuir ao dispositivo um nível de confiança ou solicitar-lhe mais informação.
- **Stealth** - para não ser detectado por outros computadores.
- Prima **Genérico** - se regras genéricas são aplicadas a esta ligação.
- **Endereços** - o endereço IP configurado no dispositivo.
- **Gateways** - O endereço IP que o seu computador usa para se ligar à Internet.

20.2.1. Alterar o Nível de Confiança

BitDefender atribui a cada dispositivo de rede um nível de confiança. O nível de confiança atribuido ao adaptador indica quão fiável a respectiva rede é.

Baseado no nível de confiança, determinadas regras são criadas para o adaptador independentemente de como os processo do sistema e do BitDefender acedem à rede ou à Internet.

Pode ver o nível de confiança configurado para cada adaptador na tabela de **Configuração de Rede** debaixo da coluna **Tipo** . Para alterar o nível de confiança, clique na seta da coluna **Tipo** e escolha o nível desejado.

Nível de Confiança	Descrição
Confiança Total	desactiva a firewall para o respectivo dispositivo.
Local Fiável	Permite o tráfego entre o seu computador e os computadores na rede local.
Segura	Permite partilhar recursos entre computadores numa rede local. Este nível é automaticamente definido para redes locais (casa ou escritório).
Insegura	Impede que os computadores de rede ou da Internet se liguem ao seu. Este nível é automaticamente definido para redes públicas (se recebe um endereço IP de um ISP (Internet Service Provider)).
Bloquear Local	Bloqueia todo o tráfego entre o seu computador e os computadores na rede local, enquanto mantém o acesso à Internet. Este nível de confiança é automaticamente definido para redes wireless inseguras (abertas).

Nível de Confiança	Descrição
Bloqueado	Bloqueia completamente o tráfego de rede e de Internet através do respectivo adaptador.

20.2.2. Configurar o Modo Stealth

O Modo Stealth torna o seu computador invisível na rede ou na internet ao software malicioso e aos hackers. Para configurar o Modo Stealth, clique na seta ▾ da coluna **Stealth** e seleccione a opção desejada.

Opção Stealth	Descrição
Ligado.	O Modo Stealth está ligado. O seu computador deixa de ser visível a partir da rede local e da Internet.
Desligado	O Modo Stealth está desligado. Qualquer pessoa da rede local ou da Internet pode fazer ping e detectar o seu computador.
Remoto	O seu computador não pode ser detectado da Internet. As redes locais podem fazer ping e detectar o seu computador.

20.2.3. Configurar Definições Gerais

Se o endereço IP de um adaptador é alterado, o BitDefender modifica o nível de confiança de acordo com a alteração. Se deseja manter o mesmo nível de confiança, clique na seta ▾ da coluna **Genérico** e seleccione **Sim**.

20.2.4. Zonas de Rede

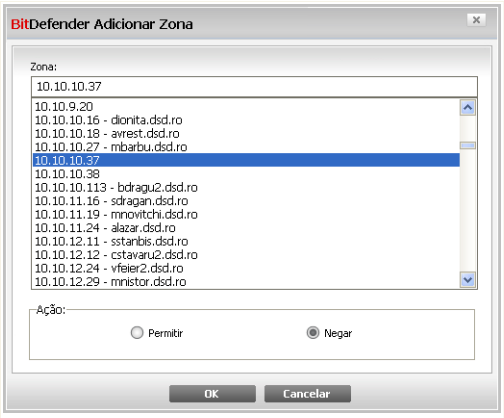
Pode adicionar computadores autorizados ou bloqueados a uma determinado adaptador.

Uma zona fiável é um computador em que confia totalmente. Todo o tráfego entre o seu computador e o computador fiável é permitido. Para partilhar recursos com determinados computadores numa rede wireless insegura, adicione-os como computadores autorizados.

Uma zona bloqueada é um computador que você não quer de forma alguma que comunique com o seu.

A tabela **Zonas** mostra as actuais zonas de rede por dispositivo.

Para adicionar uma zona, clique no botão **Adicionar** .



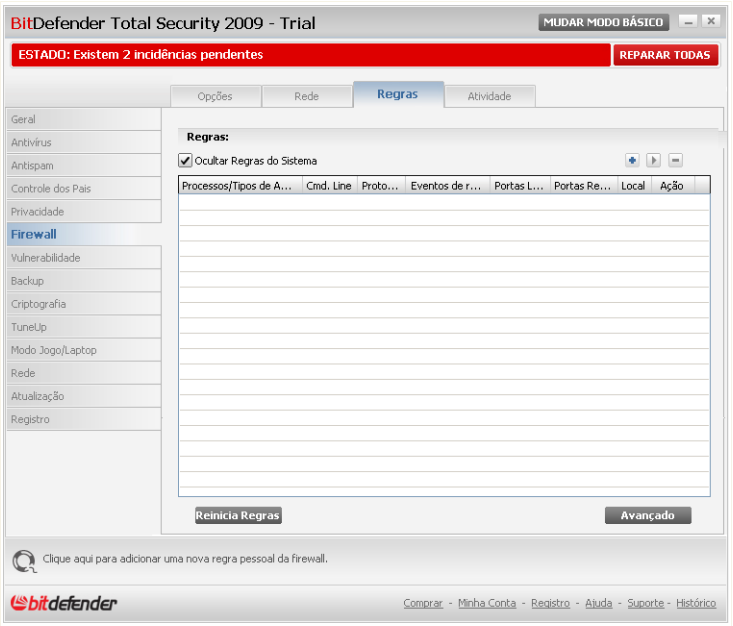
Adicionar Zona

Proceder da seguinte forma:

1. Seleccione o endereço IP do computador que pretende adicionar.
2. Seleccionar a acção:
   - **Permitir** - para autorizar o tráfego entre o seu computador e o computador seleccionado.
   - **Negar** - para bloquear o tráfego entre o seu computador e o computador seleccionado.
3. Clique em **OK**.

20.3. Regras

Para gerir as regras da firewall que controlam o acesso das aplicações aos recursos de rede e à Internet, clique em **Firewall>Regras** no Modo Avançado.



Regras da Firewall

Pode ver as aplicações (processos) para os quais as regras de firewall foram criadas. Limpe a caixa de selecção correspondente a **Ocultar processos de sistema** para poder ver as regras que dizem respeito aos processos de sistema e do BitDefender.

Para ver as regras criadas para uma aplicação especifíca, clique na caixa + ao pé da respectiva aplicação. Pode aprender info detalhada sobre cada regra, como indicada na tabela de colunas:

- **Processo/Tipos Adaptador** - o processo e os tipos de adaptador de rede aos quais a regra se aplica. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de uma aplicação através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **Linha de comando** - o comando (**cmd**) usado para iniciar o processo no interface de linha de comando do Windows.

- **Protocolo** - o protocolo IP aos quais as regras se aplicam. Pode ver um dos seguintes:

Protocolo	Descrição
Todas	Inclui todos os protocolos IP.
TCP	Transmission Control Protocol - TCP possibilita dois computadores a estabelecer uma conexão e trocar dados. O TCP garante a entrega de dados e também que pacotes serão entregues na mesma ordem que foram enviados.
UDP	User Datagram Protocol - UDP é um transporte baseado em IP concebido para alta performance. Jogos e outros aplicativos baseados em vídeo usam UDP.
Um número	Representa um protocolo IP específico (outro que não TCP e UDP). Pode encontrar a lista completa de números IP atribuidos em www.iana.org/assignments/protocol-numbers.

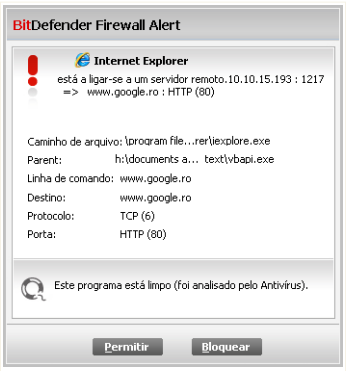
- **Eventos de Rede** - os eventos de rede aos quais a regra se aplica. Os seguintes eventos podem ser tidos em consideração:

Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma. Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação peer.

- **Portas Locais** - as portas no seu computador em que a regra se aplica.
- **Portas Remotas** - as portas nos computadores remotos em que a regra se aplica.
- **Local** - se a regra só se aplica a computadores na rede local.
- **Acção** -se à aplicação será permitido ou negado o acesso à rede ou Internet nas circunstâncias determinadas.

20.3.1. Adicionar Regras Automaticamente

Com a **Firewall** activada, o BitDefender pedirá a sua permissão sempre que uma tentativa de ligação à Internet seja feita:



Alerta da Firewall

Pode ver o seguinte: a aplicação que se está a tentar ligar à internet, o caminho do arquivo da aplicação, o destino, o protocolo usado e a porta na qual a aplicação se está a tentar ligar.

Clique **Permitir** para permitir o tráfego (entrada e saída) gerado por esta aplicação a partir do local host para qualquer destino, no respectivo protocolo IP protocol e em todas as portas. Se clicar em **Bloquear**, será negado completamente o acesso à Internet por parte da aplicação no respectivo protocolo IP.

Baseado na sua resposta, uma regra será criada, aplicada e listada na tabela. A próxima vez que a aplicação se tentar ligar, esta regra será aplicada por defeito.

Importante
Permitir tentativas de ligação de entrada apenas de IP's ou domínios em que confia totalmente.

20.3.2. Apagar Regras

Para apagar uma regra, seleccione-a e clique no botão **Apagar Regra**. Pode seleccionar e apagar várias regras de uma só vez.

Para eliminar todas as regras criadas para uma especifica aplicação, seleccione-a da lista e clique no botão **Remover regra**.

20.3.3. Criar e Modificar Regras

Criar novas regras manualmente e modificar as regras existentes consiste em configurar os parâmetros da regra na janela de configuração.

Criar regras. Para criar regras manualmente, siga estes passos:

1. Clique no botão **Adicionar Regra** . A janela de configuração irá aparecer.

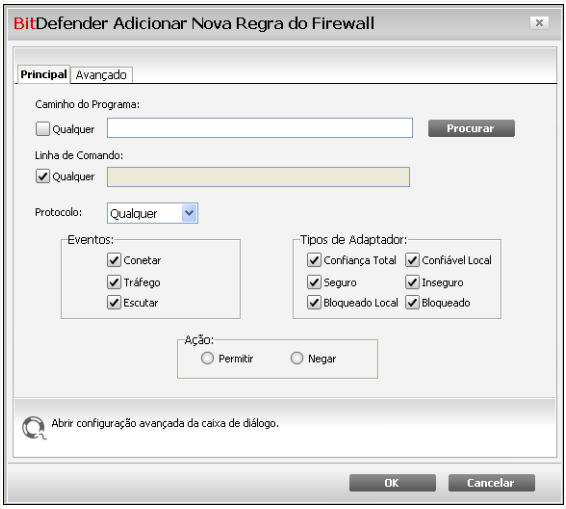
2. Configure os parâmetros principais e avançados quanto seja necessário.
3. Clique em **OK** para adicionar a nova regra.

Modificar regras. Para modificar uma regra existente, siga os seguintes passos:

1. Clique no botão **Editar Regra** ou faça duplo-clique sobre ela. A janela de configuração irá aparecer.
2. Configure os parâmetros principais e avançados quanto seja necessário.
3. Clique em **OK** para salvar as alterações.

Configurar os Parâmetros Principais

A barra **Principal** da janela de configuração permite configurar os principais parâmetros da regra.



Parâmetros Principais

Pode configurar os seguintes parâmetros:

- **Caminho do Programa.** Clique em **Explorar** para seleccionar a aplicação à qual a regra se aplica. Se deseja que a regra se aplique a todas as aplicações, apenas seleccione **Todas**.

- **Linha de comando.** Se deseja que a regra se aplique apenas quando a aplicação é aberta com um comando especifico na linha de comandos do Windows, limpe a caixa **Todas** e insira o respectivo comando no campo de edição.
- **Protocolo.** Seleccione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, seleccione **Todos**.
  - Se deseja que a regra se aplique a um determinado protocolo, seleccione **Outro**. Um campo de edição irá aparecer. Insira no campo de edição o número atribuido ao protocolo que deseja filtrar.

Nota

Os números dos protocolos IP são atribuidos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuidos em www.iana.org/assignments/protocol-numbers.

- **Eventos.** Dependendo dos protocolo seleccionado, escolha os eventos de rede aos quais a regra se aplica. Os seguintes eventos podem ser tidos em consideração:

Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma. Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação peer.

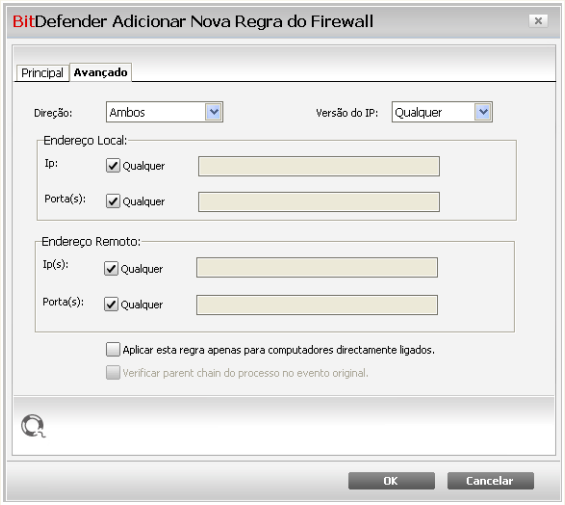
- **Nível de Confiança.** Seleccione os níveis de confiança aos quais a regra se aplica.
- **Ação.** Seleccione uma das seguintes acções disponíveis:

Ação	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.

Ação	Descrição
Negar	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

Configurar Parâmetros Avançados

A barra**Avançada** da janela de configuração permite-lhe configurar parâmetros avançados da regra.



Parâmetros Avançados

Pode configurar os seguintes parâmetros avançados:

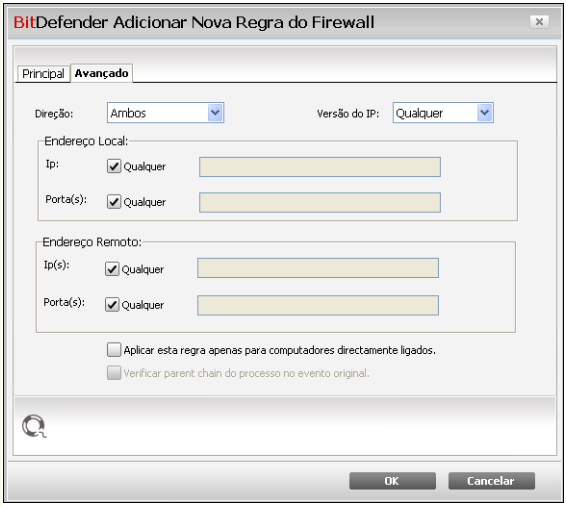
- **Direcção.** Seleccione do menu a direcção do tráfego ao qual a regra se aplica.

Direcção	Descrição
Saída	As regras valem apenas para tráfego de saída.
Entrada	As regras valem apenas entrada.
Ambos	As regras valem para as duas direções.

- **versão IP.** Seleccione do menu a versão do IP (IPv4, IPv6 ou qualquer) ao qual a regra se aplica.
- **Endereço Local.** Especifique o endereço IP local e a porta aos quais a regra se aplica da seguinte forma:
  - Se tem mais de um adaptador de rede, pode limpar a caixa **Todos** e inserir um endereço IP específico.
  - Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.
- **Endereço Remoto.** Especifique o endereço IP remoto e a porta aos quais a regra se aplica da seguinte forma:
  - Para filtrar o tráfego entre o seu computador e um determinado computador, limpe a caixa **Todos** e insira o endereço IP do outro computador.
  - Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.
- **Aplicar esta regra apenas a computadores ligados directamente.** Seleccione esta opção quando deseja que a regra se aplique apenas às tentativas de tráfego locais.
- **Verificar o processo parent chain pelo evento original.** Apenas pode alterar este parâmetro se tiver seleccionado **Regras estritamente automáticas** (vá para a barra Definições e clique **Configuração Avançada**). Regras estritas significa que o BitDefender consulta-o para que tome uma acção quando a aplicação requer acesso à rede/Internet de cada vez que o processo parent é diferente.

20.3.4. Gestão Avançada de Regras

Se necessita de controle avançado sobre as regras da firewall, clique em **Avançadas**. Uma nova janela irá aparecer.



Gestão Avançada de Regras

Pode ver as regras da firewall listadas pela ordem em que são verificadas. A tabela de colunas dá-lhe uma informação completa sobre cada regra.

Nota

Quando uma tentativa de ligação é feita (seja de entrada ou saída), o BitDefender aplica a acção da primeira regra que corresponda a essa respectiva ligação. Logo, a ordem pela qual as regras são verificadas é muito importante.

Para apagar uma regra, seleccione-a e clique no botão **Apagar Regra**.

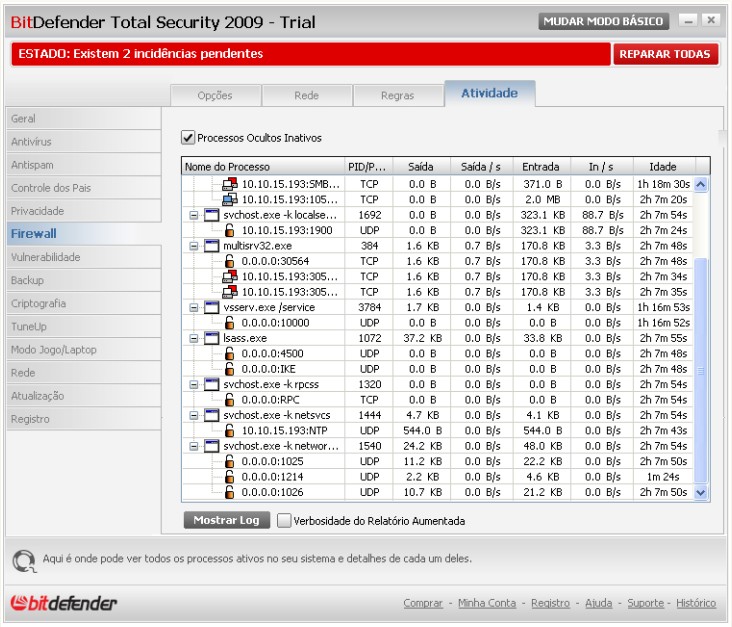
Para editar uma regra, seleccione-a e clique no botão **Editar Regra** ou faça duplo-clique sobre ela.

Pode aumentar ou diminuir a prioridade de uma regra. Clique no botão **Subir na Lista** para aumentar um nível a prioridade da regra seleccionada, ou clique no botão **Descer na Lista** para diminuir um nível a prioridade da regra seleccionada. Para atribuir a máxima prioridade a uma regra, clique no botão **Subir Topo**. Para atribuir a uma regra a miníma prioridade, clique no botão **Descer Fundo** .

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

20.4. Controle de Conexão

Para monitorizar a rede actual / actividade Internet (em TCP e UDP) por aplicação e abrir o log da Firewall BitDefender, clique em **Firewall>Actividade** no Modo Avançado.



Controle de Conexão

Pode ver todo o tráfego por aplicação. Para cada aplicação, pode ver as ligações e as portas abertas, como também as estatísticas com respeito à velocidade de tráfego de saída & entrada e o montante total de dados enviados / recebidos.

Se deseja ver também os processos inactivos, limpe a caixa **Ocultar processos inactivos**.

O significado dos ícones é o seguinte:

- Indica uma ligação aberta no seu computador.
- Indica uma porta aberta no seu computador.

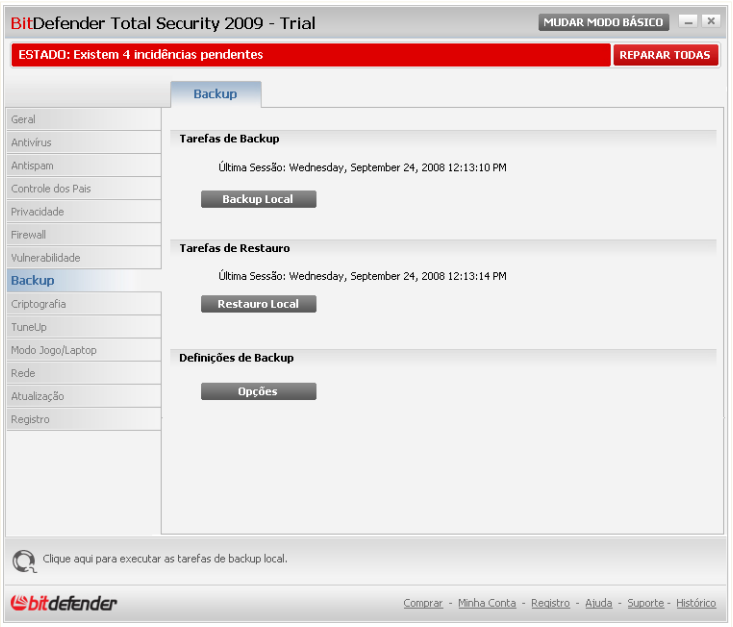
A janela apresenta em tempo-real a actividade da actual rede / Internet. À medida que as ligações e portas são fechadas, pode ver que as estatísticas correspondentes são diminuidas e que, eventualmente, desaparecerão. A mesma coisa acontece a todas as estatísticas correspondentes a uma aplicação que gera tráfego ou que tem portas abertas que você fecha.

Para obter uma lista mais completa de eventos com respeito ao uso do módulo da Firewall (ativar/desativar a firewall, bloquear tráfego, modificar configurações) ou gerado pelas actividades detectadas por ela (scan de portas, bloqueio de tentativas de ligação ou de tráfego de acordo com as regras) consulte o arquivo de relatório da Firewall do BitDefender que pode ser visualizado clicando em **Mostrar Relatório**. O arquivo está localizado na pasta de Arquivos Comuns do usuário atual do Windows, no caminho: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Se deseja que o relatório contenha mais informação, seleccione **Aumentar verbosidade do relatório**.

21. Tarefas de Backup

BitDefender vem com um módulo de Backup que o ajuda a fazer cópias de reserva de todos os dados valiosos no seu sistema. Pode fazer backup para o seu computador, discos amovíveis ou para uma localização de rede para se certificar que os pode restaurar quando necessário. O restauro dos seus dados é um processo muito fácil.



Tarefas de Backup

Estão disponíveis os seguintes botões:

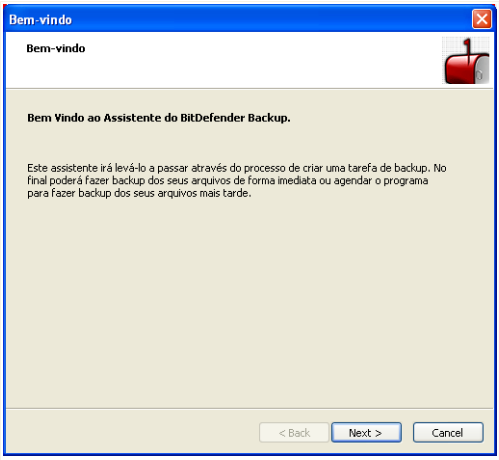
- **Backup Local** - inicia um procedimento de cinco passos para fazer um backup dos seus dados localmente.
- **Restauro Local** - inicia um procedimento de quatro passos para restaurar os seus dados localmente.
- **Configuração** - abre o BitDefender Backup, que lhe permite definir e executar operações de backup em detalhe.

21.1. Fazer Backup Local de Dados

Ao clicar em **Backup Local** um assistente irá levá-lo através do processo de criar uma tarefa de backup local. No final do processo será capaz de fazer backup dos seus dados na hora ou agendar o produto para o fazer mais tarde.

21.1.1. Passo 1/5 - Janela de Boas-vindas

Esta é uma página de boas-vindas.

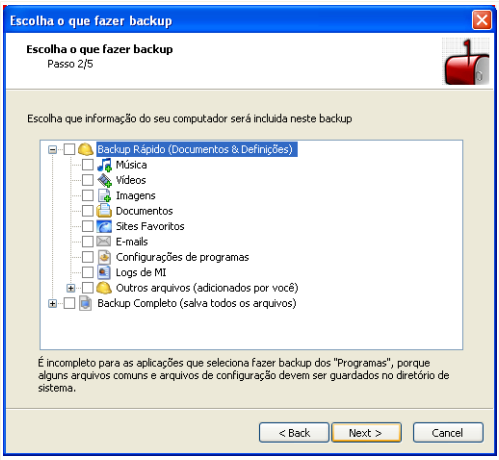


Janela de Boas-Vindas

Clique em **Próximo**.

21.1.2. Passo 2/5 - Escolher do que fazer Backup

Aqui pode escolher que dados do seu computador deseja fazer backup.



Escolher do que fazer backup

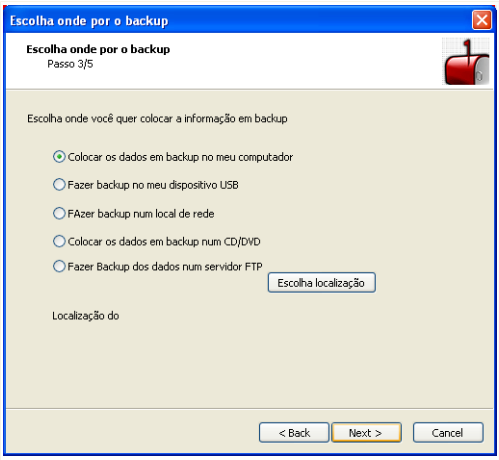
Pode escolher fazer **Backup Rápido** (a sua música, videos, imagens, e-mails, definições de aplicações, etc.) ou **Backup Completo** (todas as partições).

Clique em **Outros ficheiros**, para adicionar outros arquivos do seu Ambiente de Trabalho ao **Backup Rápido**. O **Backup Completo** pode também ser facilmente personalizado ao selecionar que diretórios de um determinada partição deseja fazer backup.

Clique em **Próximo**.

21.1.3. Passo 3/5 - Escolher para onde fazer Backup

Aqui pode seleccionar o local onde guardar os dados do backup.



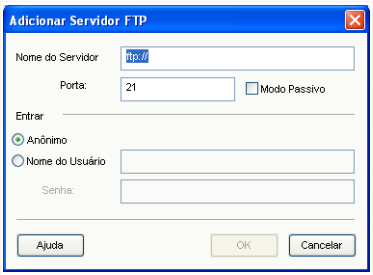
Escolha para onde fazer backup

As seguintes opções estão disponíveis:

- **Fazer Backup dos meus dados no meu computador**
- **Fazer o Backup para a minha drive USB**
- **Fazer o Backup para um local de rede**
- **Fazer o Backup para o CD/DVD**
- **Fazer Backup num Servidor FTP**

Se decidir fazer backup para o seu computador, a sua drive USB ou num local de rede, clique em **Escolher Local** e seleccione o local onde deseja guardar os dados.

Se você deseja efetuar um backup de seus dados em um servidor FTP, clique **Escolha o Local** e adicione o servidor FTP. Uma nova janela irá aparecer.



Adicionar Servidor FTP

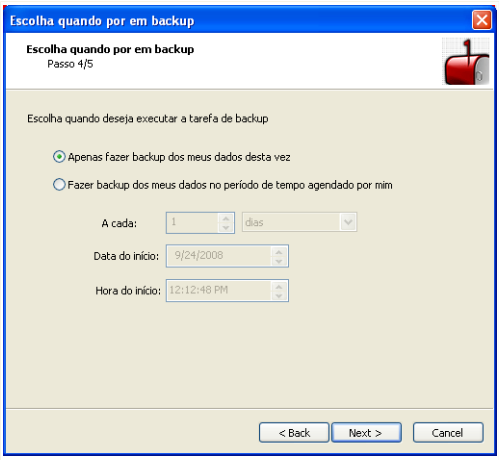
Você precisa determinar as configurações de conexão do servidor FTP como segue:

1. Digite o nome do servidor FTP no campo correspondente.
2. Se o servidor FTP usar uma porta diferente da porta padrão 21, digite-a no campo correspondente.
3. Para usar o modo passivo (o servidor FTP inicia a conexão), selecione **Modo Passivo** selecione opção.
4. Se o servidor permite acessos anônimos, você pode deixar a opção **Anônimo** selecionada. Caso contrário, selecione **Nome de Usuário** e digite o nome do usuário e senha de uma conta reconhecida pelo servidor FTP.
5. Clique em **OK**.

Clique em **Próximo**.

21.1.4. Passo 4/5 - Escolher quando fazer o Backup

Aqui pode seleccionar quando deseja fazer o backup dos dados.



Escolher quando fazer o backup

As seguintes opções estão disponíveis:

- **Fazer Backup dos dados só esta vez**
- **Fazer Backup dos dados numa data agendada por mim**

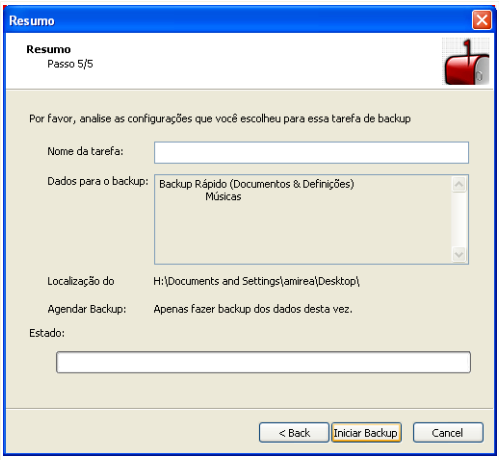
Para fazer backup dos arquivos na hora clique em **Fazer Backup dos dados só esta vez**, para agendar o produto para fazer backup mais tarde, clique **Fazer Backup dos dados numa data agendada por mim**.

Se seleccionar **Fazer Backup dos dados numa data agendada por mim**, pode especificar com que frequência a tarefa agendada será executada: diariamente ou semanalmente. Pode também especificar a data e a hora.

Clique em **Próximo**.

21.1.5. Passo 5/5 - Sumário

Aqui você pode rever as configurações do trabalho de backup e iniciar o backup.



Sumário

Deve inserir um nome de tarefa no campo correspondente. Você pode efetuar qualquer mudança, bastando voltar aos passos anteriores (clique **Voltar**).

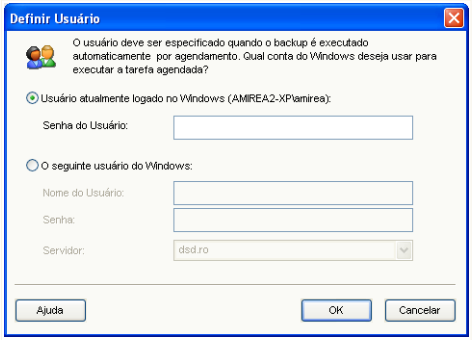
Clique em **Iniciar backup** se estiver satisfeito com as suas definições. Espere até que o BitDefender complete o backup e então clique **Finalizar**.

Nota

A primeira vez que você determinar o agendamento de um trabalho de backup, você será orientado a especificar a conta do Windows usada para executar o trabalho.

Para usar a conta de usuário atual, basta digitar a senha deste usuário no campo correspondente. Se você deseja executar o backup usando uma conta diferente, selecione **O seguinte usuário do Windows** e preencha nos campos.

- **Nome do Usuário** - digite o nome da conta do Windows.
- **Senha** - a senha do usuário da conta especificado anteriormente.
- **Servidor** - digite o nome do domínio do servidor.



Definir Usuário

Clique **OK** para continuar.

21.2. Restaurar dados num Backup Local

Ao clicar em **Restauro Local** um assistente irá levá-lo através do processo de restaurar o seu backup local.

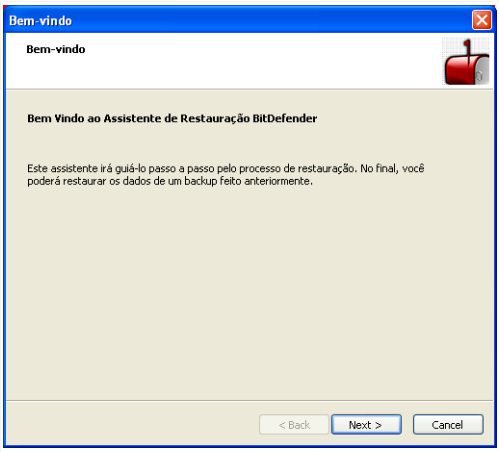
Nota

Antes de restaurar qualquer dado, certifique-se que o equipamento onde você efetuou o backup esta disponível. Dependendo do equipamento usado, você poderá efetuar uma destas ações:

- Insira o equipamento USB de backup na porta USB.
- Insira o CD ou DVD de backup no drive.
- Verifique se você pode se conectar ao local de rede ou servidor FTP onde os dados foram armazenados.

21.2.1. Passo 1/4 - Janela de Boas-vindas

Esta é uma página de boas-vindas.

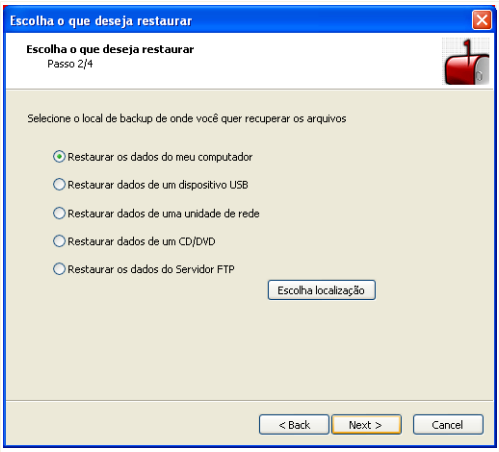


Janela de Boas-Vindas

Clique em **Próximo**.

21.2.2. Passo 2/4 - Escolha de onde deseja restaurar o Backup

Aqui pode selecionar um local de onde deseja restaurar os arquivos.



Escolha de onde deseja restaurar o Backup

As seguintes opções estão disponíveis:

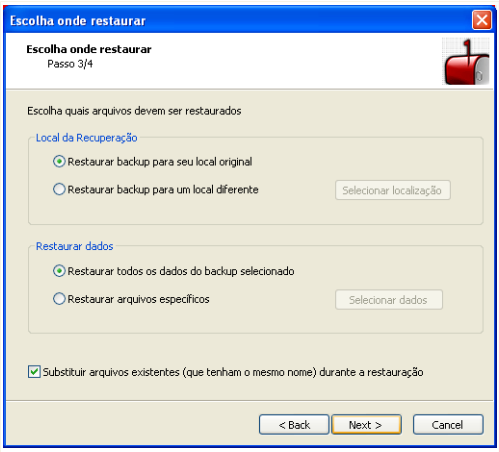
- **Restaurar os dados do meu computador**
- **Restaurar backup de uma drive USB**
- **Restaurar backup de um local de rede**
- **Restaurar backup de um CD/DVD**
- **Restaurar backup de um servidor FTP**

Após selecionar uma opção, clique **Escolha o local** e selecione o arquivo de backup o qual você deseja restaurar.

Clique em **Próximo**.

21.2.3. Passo 3/4 - Escolher o Local e os arquivos de Restauro

Aqui é onde pode escolher que arquivos específicos a restaurar e para onde os restaurar.



Escolher o local e os arquivos de restauro

As seguintes opções estão disponíveis:

- **Restaurar o backup ao seu local de origem**
- **Restaurar o backup para um local diferente**
- **Restaurar todos os dados do local de backup seleccionado**
- **Restaurar arquivos específicos**
- **Sobrescrever os arquivos existentes quando restaurar**

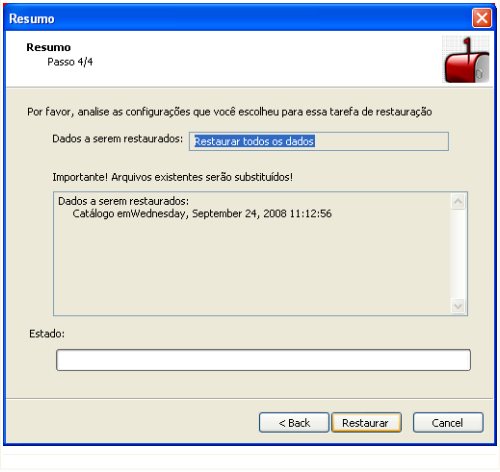
Se deseja restaurar dados para outro local ou apenas arquivos específicos, selecione o local e os dados clicando no botão correspondente.

Para evitar sobreescrever o arquivo existente durante o restauro, limpe a caixa de seleção **Sobrescrever os arquivos existentes quando restaurar**.

Clique em **Próximo**.

21.2.4. Passo 4/4 - Sumário

Aqui você pode rever as configurações do trabalho de restauração e iniciar o processo.



Clique em **Restaurar** se estiver satisfeito com as suas definições. Espere até que o BitDefender restaure os dados selecionados e então clique **Finalizar**.

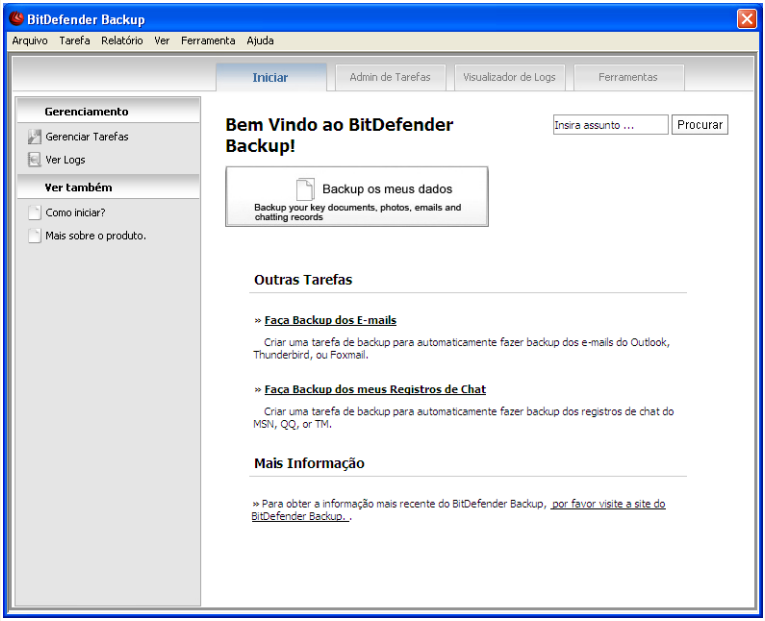
21.3. Backup Avançado

Se necessita de levar a cabo uma operação de backup e restauro mais complexa, pode usar a solução do BitDefender Backup com todas as opções. O Backup BitDefender oferece:

- uma variedade de opções de backup, tais como compressão, encriptação, e filtragem de arquivos para backup ou definir a velocidade de backup.
- controle refinado no restauro de arquivos (por exemplo, pode restaurar dados dos quais fez um backup num determinado ponto do tempo).
- capacidade de agendamento avançada (por exemplo, pode escolher iniciar o seu backup durante o arranque do sistema ou quando o computador estiver ianctivo).
- um visualizador de relatório que o ajuda a manter um registo das operações de backup e restauro que levou a cabo e assim reparar eventuais erros.

Nesta secção ser-lhe-á dada informação detalhada sobre o interface gráfico e as características do Backup Bitdefender.

Para abrir o módulo de Backup BitDefender clique em **Configuração Backup**.

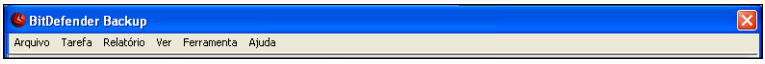


Backup BitDefender

Existem duas formas como pode estabelecer e executar operações de backup. Ou acede à **Barra de Menu** superior, ou clica numa determinada barra a partir da **Barra de Navegação**.

21.3.1. Barra de Menu

Existem seis menus que pode usar para executar todas as funções oferecidas pela solução de backup BitDefender.



Barra de Menu

Arquivo

- **Criar Nova tarefa:** Mostra uma caixa de diálogo de forma a criar uma nova tarefa de backup ou outra tarefa.
- **Abrir o Backup Set:** - Mostra uma caixa de diálogo de forma a abrir o backup set ou o catalog set para restauro.
- **Sair:** Permite sair da secção de backup BitDefender.

Tarefa

- **Backup:** Executa o backup de uma tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Restaurar arquivo:** Restaura a tarefa selecionada. Se existe mais do que uma tarefa selecionada, executa todas as tarefas selecionadas .
- **Restaurar Dados em Ponto-Tempo:** Restaura a tarefa seleccionada para um determinado ponto do tempo. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Agendar:** Cria a tarefa agendada ou modifica a que já existe.
- **Apagar Agendar:** - Elimina o agendamento da tarefa agendada.
- **Apagar:** - elimina a tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Apagar Todas** - Elimina todas as tarefas no gestor de tarefas.
- **Explorar Destino:** Permite ver os dados do backup do destino da tarefa seleccionada.
- **Modificar Opções:** Modifica opções das tarefas seleccionadas.
- **Propriedades:** - PErmite modificar as propriedades de uma tarefa seleccionada, incluindo a fonte dos dados, nome, destino, etc, da tarefa.

Relatório

- **Ver Relatório:** Se a tarefa seleccionada contém definições de segurança, esta opção permite ver os conteúdos do relatório da tarefa.
- **Guardar como:** Guarda o conteúdo do relatório selecionado para um determinado arquivo.
- **Imprimir:** Imprime o conteúdo do relatório seleccionado.
- **Apagar Tudo:** - Apaga o conteúdo do relatório da tarefa seleccionada.
- **Actualizar:** Actualiza o conteúdo do relatório da tarefa seleccionada.

Ver

- **Introdução:** Se a janela da introdução não estiver a ser mostrada, esta opção permite abri-la.
- **Gestor de Tarefa:** Se a janela do gestor de tarefa não estiver a ser mostrada, esta opção permite abri-la.
- **Ver Log:** Se a janela do visualizador de logs não estiver a ser mostrada, esta opção permite abri-la.

- **Toolbox:** Se a janela não estiver a ser mostrada, esta opção permite abri-la.
- **Mostrar Barra de Menu:** Esconde a Barra de Menu. Para a mostrar, apenas prima **ALT**.
- **Mostrar Linha de Grelha:** Mostra ou esconde a linha de grelha. Aplica-se ao visualizador de logs e ao gestor de tarefas windows.

Ferramenta

- **Assistente de Backup:** Inicia o assistente de backup.
- **Assistente de Restauro** - Inicia o assistente de restauro.
- **Gravar:** Inicia a ferramenta de gravação de CD/DVD/ISO ou a ferramenta de gestão da gravação.
  - **Gravar CD/DVD**
  - **Gravar arquivos ISO**
  - **Ver Info Gravador**
- **Exportar todas Tarefas:** Exporta todas as tarefas criadas para um arquivo específico.
- **Importar Tarefas:** Importa tarefas de um arquivo `.JOB`, um arquivo `.TXT` , ou um arquivo `.XML`.
- **Exportar Logs:** Exporta logs para um arquivo `.TXT` ou um arquivo `.XML` .
  - Para um arquivo `TXT`
  - Para um arquivo `XML`
- **Importar Logs:** Importa logs de um arquivo `.TXT` ou de um arquivo `.XML` .
  - De um arquivo `TXT`
  - De um arquivo `XML`
- **Opções:** Modifica as suas opções gerais de backup.
  - **Geral**
  - **Relatórios & Log**
  - **Agendar Tarefa**

Ajuda

- **Tópico de Ajuda:** Mostra tópicos de ajuda.
- **Procurar:** Permite procurar tópicos de ajuda baseado nas palavras chave inseridas ou seleccionadas.
- **BitDefender no Website:** Permite aceder à página da Internet do BitDefender e aceder às notícias BitDefender e ao suporte online.
- **Acerca do Backup BitDefender :** Mostra o copyright, versão, e edição da info relacionada com o Backup BitDefender.

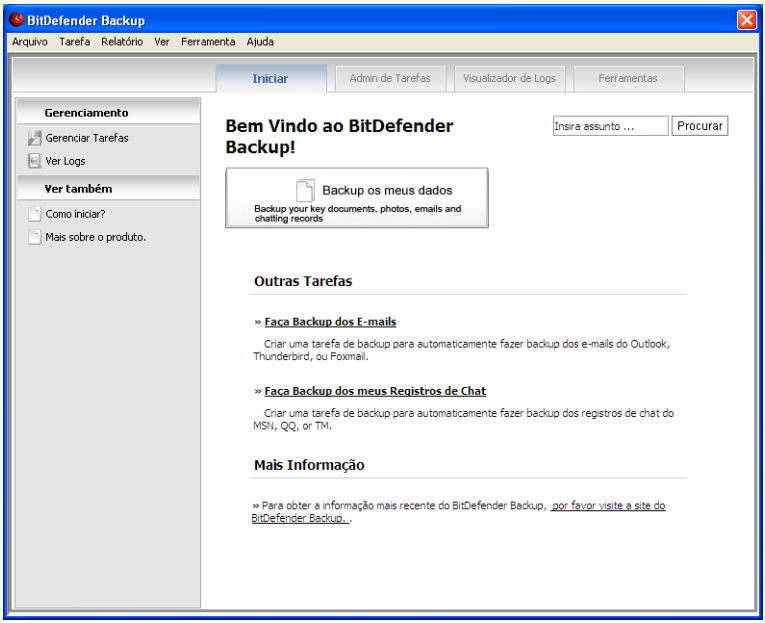
21.3.2. Barra de Navegação

A **Barra de Navegação**, mostrada na parte superior da janela principal e por debaixo da **Barra de Menu**, dá acesso a quatro secções:

- **Introdução**
- **Gestor Tarefas**
- **Visualizador Log**
- **Toolbox**

Introdução

A área de **Introdução** ajuda-o a fazer facilmente backups dos seus e-mails, registos de chat e dados.



Introdução

Pode mudar para a **Introdução** fazendo o seguinte:

- Clique em **Introdução** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Introdução**.
- Use um atalho premindo as teclas **CTRL+Alt+S**.

Para fazer backup dos seus documentos chave, fotos, e-mails e registos de chat durante a mesma tarefa, clique no botão **Fazer Backup Dados** e siga o procedimento de três passos.

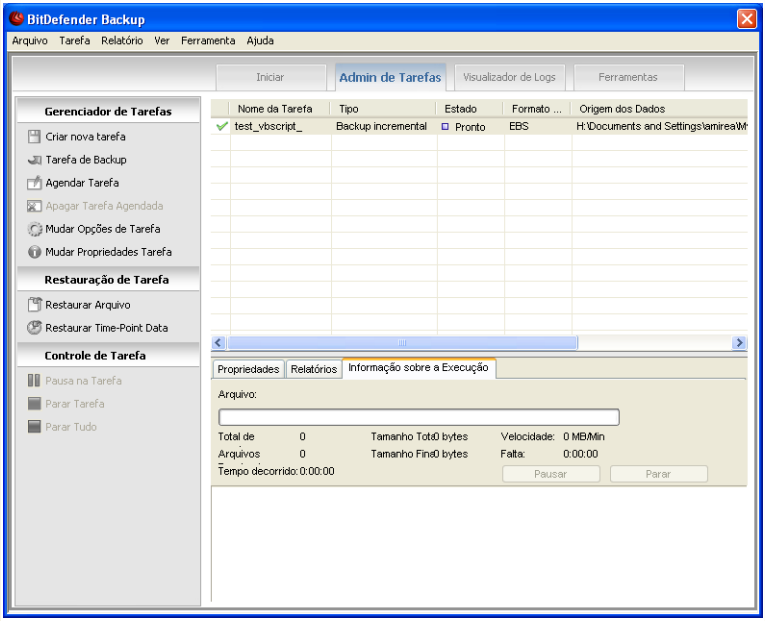
Para fazer backup apenas dos seus e-mails clique no botão **Fazer Backup E-mails** e siga o procedimento de três passos.

Para fazer backup apenas dos seus registos de chat, clique no botão **Fazer Backup do Chat** e siga o procedimento de três passos.

Nota
O procedimento de três passos é também descrito na secção Criar Nova Tarefa .

Gestor de Tarefa

Gestor de Tarefa é usado para ver e gerir tarefas de backup, ver propriedades das tarefas e os relatórios das tarefas como também monitorizar a velocidade de execução da mesma. **Gestor de Tarefa** permite verificar as propriedades da tarefa e o seu estado actual, modificando as definições da tarefas como também executando a tarefa de backup ou restauro.



Gestor de Tarefa

Pode mudar para o **Gestor de Tarefa** fazendo o seguinte:

- Clique em **Gestor de Tarefa** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Gestor de Tarefa**.
- Use um atalho premindo as teclas **CTRL+Alt+M**.

À esquerda, poderá ver uma lista de links de operações rápidas, como se seguem:

Gestão de Tarefa

- **Criar Nova Tarefa**
- **Tarefa de Backup**
- **Tarefa Agendada**
- **Apagar Tarefa Agendada**
- **Modificar Opções de Tarefa**
- **Modificar Propriedades de Tarefa**

Restaurar Tarefa

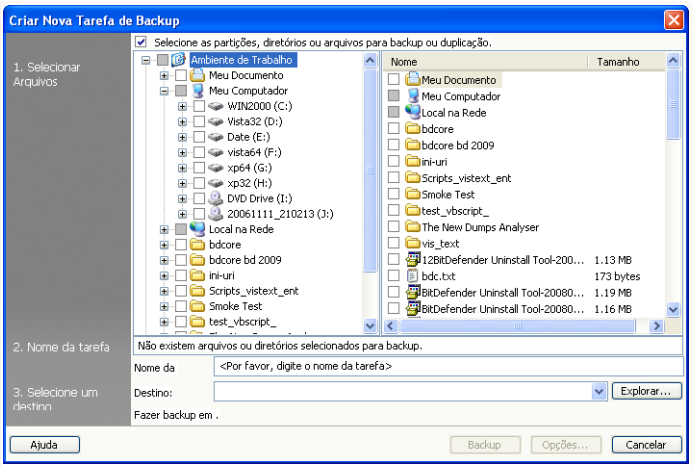
- **Restaurar arquivo**
- **Restaurar Dados Ponto-Tempo**

Controle Tarefa

- **Pausa na Tarefa**
- **Parar Tarefa**
- **Parar Todas**

Criar Nova Tarefa

Para fazer backup dos seus documentos chave, fotos, e-mails e registos de chat durante a mesma tarefa, clique no botão**Criar Nova Tarefa** e siga os próximos três passos.



Criar Nova Tarefa

1. Clique na caixa de seleção para selecionar partições, diretórios, ou arquivos para backup.

   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo será mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Insira um nome para a sua tarefa de backup ou aceite o nome por defeito da mesma.

O nome por defeito da tarefa é automaticamente gerado quando os arquivos ou os diretórios são selecionados para serem backup, mas pode ser modificado.

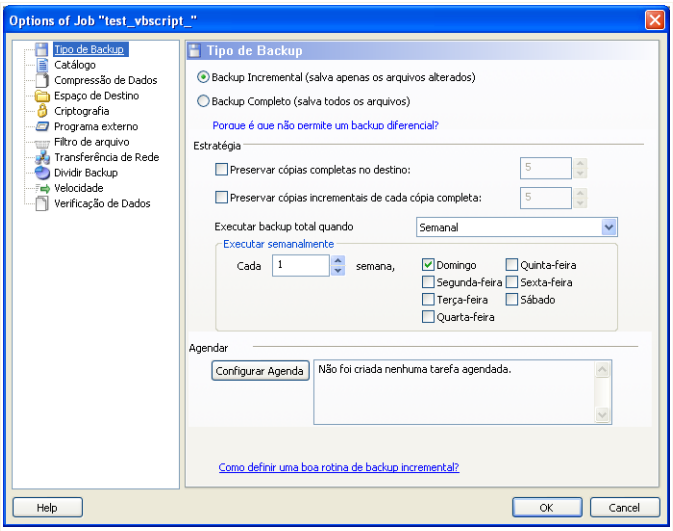
3. Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota

Não se esqueça de clicar em **Backup** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Backup

Existem diversas sub-opções na caixa de diálogo das **Opções**.



Caixa de Diálogo Opções de Backup

Tipo de Backup

O Backup BitDefender suporta dois tipos de backup.

- **Backup Total:** Faz um backup completo de fonte de dados seleccionada para o backup set no destino especificado. Quando executar um backup total, o Backup BitDefender não fará backup dos dados modificados mas sim de toda a fonte de dados.
- **Backup Incremental:** Quando executar pela primeira o Backup Incremental é o mesmo que o Backup Total porque faz um backup completo de toda a fonte

de dados para o backup set no destino especificado. Mais tarde, apenas faz backup dos novos arquivos ou dos arquivos modificados. Sempre que um Backup Incremental Backup é executado um backup catalog set é criado.

O Backup Incremental e o Total podem também combinar-se num **Backup de Rotação**. Por exemplo, pode definir um Backup Incremental do trabalho enquanto definie um Backup Total uma vez por semana, digamos ao Domingo. Eis como é feito: Seleccione **Semanal** do menu drop-down, `1` do campo**Cada Semana** e seleccionar Domingo. Este Backup Total ao Domingo substituirá todos os backups anteriores e será a base para o novo Backup Incremental trabalhar.

Catalog Set

É usado para indexar toda a informação de arquivos de cada backup, e é a base do processos de Backup Incremental e Restauração. O catalog set (`*.ecs`) contém uma série de catálogos que representam um índice de todos os ficheiros e diretórios existente no backup set. Tal índice inclui os dados da data do backup, diretório de backup, nome do arquivo e propriedades. Os dados podem ser restaurados a partir do catalog set.

Um nome de arquivo de catalog set é gerado automaticamente por destino de tarefa. Para modificar o catalog set de uma tarefa faça o seguinte:

1. Clique em **Catalog Set**.
2. Insira um nome de arquivo no campo correspondente.
3. Clique em **Explorar** para selecionar o diretório onde guardar os arquivos do Catalog set.
4. Clique em **OK**.

Compressão de Dados

O Backup BitDefender permite a comprimir e guardar os dados para o backup set quando executa um backup para poupar espaço. Suporta Compressão Rápida, Compressão Standard, Compressão Alta Intensidade. Por exemplo, para iniciar a compressão standard a uma velocidade de compressão média, siga os seguintes passos:

1. Clique em **Compressão de Dados**.
2. Clique em **Compressão Standard**.
3. Clique em **OK**.

Span de Destino

O Backup BitDefender permite a distribuição do backup set para um destino diferente. neste caso, mesmo que um determinado destino não tenha suficiente espaço livre, a execução do backup dos dados prosseguirá.

Pode adicionar um ou mais destinos para continuar o backup, modificá-lo ou mesmo removê-lo, da seguinte forma:

1. Clique em **Span de Destino**.
2. Clique em **Adicionar** para seleccionar um novo destino para guardar os dados de backup.
3. Clique em **Editar** para modificar o destino de backup seleccionado.
4. Clique em **Apagar** para apagar o destino de backup seleccionado.
5. Clique em **Apagar Todos** para apagar todos os destinos de backup.
6. Clique em **OK**.

Encriptação

O Backup BitDefender mantém os dados backup mais seguros ao encriptá-los antes de os guardar no backup set. As definições de segurança de uma tarefa inclui proteção por senha.

Para encriptar os dados antes do backup, siga estes passos:

1. Clique em **Encriptação**.
2. Seleccione um tipo de encriptação a partir do menu drop-down.
3. Insira a sua senha no campo correspondente.
4. Reinsira a sua senha no campo correspondente.
5. Clique em **OK**.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa**.
3. Clique em **Explorar** para selecionar os arquivos de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa**.
3. Clique em **Explorar** para selecionar os arquivos de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do usuário atual** quando o backup terminar.
7. Clique em **OK**.

Nota
Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de arquivos

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir arquivos específicos, tipos de arquivos ou diretórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de arquivos especificados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de arquivos nos pop-ups das caixas de diálogo ao selecionar as opções **Incluir apenas tipos de arquivos selecionados** ou **Excluir tipos de arquivos selecionados**
4. Se necessário, insira outro tipo de arquivo no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um arquivo especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Filtrar arquivo**.
3. Exclua ou inclua arquivos específicos nos pop-ups das caixas de diálogo selecionando as opções **Incluir apenas os arquivos especificados por regra** ou **Excluir os arquivos especificados** .
4. Clique em **Explorar** e selecione o arquivo. O caminho da localização do arquivo será automaticamente adicionado no campo **Aplicar aos seguintes diretórios** . Para incluir ou excluir o respectivo arquivo da sua localização, clique em **Aplicar a todos os diretórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .

4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:
1. Clique em**Filtro de arquivos**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:
1. Clique em**Filtro de arquivos**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

Transferência de Rede

O Backup BitDefender permite fazer backup e restaurar dados partilhados em grupos de trabalho de rede minuciosamente. Se a rede não estiver acessível, tentará fazer backup dos dados de vez em quando. Para especificar com que frequência ou quantas vezes deseja tentar o backup, siga os seguintes passos:
1. Clique em **Transferência de Rede**.
2. Clique em **Quando falhar em ler arquivos de rede devido a desconexão, tentar conectar de novo**.
3. Insira com que frequência deseja tentar de novo o backup dos dados (em segundos).
4. Insira quantas vezes deseja tentar de novo o backup dos dados.
5. Clique em **OK**.

Nota

Para evitar ser esmagado por informação de erros de rede, clique em **Não é gerado relatório de erro quando a rede não está disponível**.

Dividir Backup Set

O backup set gerado pode ser dividido em diveros outros backup sets, de forma a que o backup possa ser executado normalmente mesmo quando o destino ou o sistema de arquivos é limitado. O Backup BitDefender dá-lhe dois métodos de divisão: auto-divisão e divisão-definida.

As definições de divisão da tarefa de backup podem ser modificadas da seguinte forma:

1. Clique em **Dividir Backup Set**.
2. Seleccionar **Divisão Automática por Espaço no Destino**.
3. Ou seleccione **Especificar tamanho para dividir** e escolha o tamanho desejado no menu drop down.
4. Clique em **OK**.

Velocidade

O Backup BitDefender suporta três tipos de velocidade. Quanto maior a velocidade, mais CPU será ocupado

A velocidade de Backup pode ser especificada seguindo estes passos.

1. Clique em **Velocidade**.
2. Seleccione velocidade**Rápida**, **Média** ou **Baixa** .
3. Clique em **OK**.

Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Tarefa de Backup

Uma vez que a tarefa tenha sido criada, o backup é executado automaticamente. No entanto, pode entrar em **Gestor de Tarefa** para executar backup ao seleccionar a tarefa criada e clicar no menu **Tarefa de Backup** .

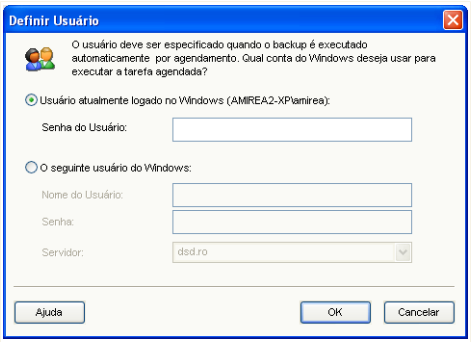
De forma a receber os detalhes do backup quando restaurar os arquivos, deve de inserir uma breve descrição na janela de pop-up que se abre. Clique em **Cancelar** para ignorar a janela de pop-up ou **OK** para continuar. A tarefa de backup pode ser cancelada ao clicar no botão **Cancelar Backup** .

Nota

Para informação detalhada, uma boa ideia seria ver as **Propriedades**, **Relatórios** e **Info Execução** da tarefa a partir da janela da barra de estado.

Agendar Tarefa

Aqui é onde poderá agendar a tarefa de backup para uma altura que seja conveniente. Pode agendar a tarefa para ser executada diariamente, semanalmente, mensalmente ou a qualquer altura que deseje (por exemplo durante o arranque do sistema). **Agendar Tarefa** é a base para o backup automático.



Agendar Tarefa

Se o seu computador é membro de um domínio de rede, uma série de passos extra são necessários para agendar uma tarefa.

1. Seleccione a tarefa e depois clique em **Agendar Tarefa**.
2. A caixa de diálogo de **Usuário de Execução** aparecerá. Se é um usuário do domínio, por favor insira a senha do domínio.
3. De outra forma selecione **Executar como o seguinte usuário Windows**.
4. Insira o nome do usuário, senha e o nome do servidor de domínio.
5. Clique em **OK**.

Uma vez que defina o usuário de execução, o Backup BitDefender mostrará a caixa de diálogo **Agendar** de forma a que possa definir uma altura conveniente para executar a tarefa.

É aqui onde pode especificar a frequência com que as tarefas agendadas se executam: diariamente, semanalmente, mensalmente, uma vez, no arranque do sistema, no login, quando o computador está em descanso. Se a tarefa é agendada diariamente, semanalmente, mensalmente, uma só vez, pode também especificar a hora de início. Pode também seleccionar com que frequência a tarefa agendada é executada (expresso como o número de dias ou semanas, o dia do mês ou a data). Outra definição possível é a duração (em minutos) do período de descanso após o qual a tarefa agendada se inicia.

É também possível configurar múltiplos agendamentos para uma tarefa clicando em **Mostrar múltiplos agendamentos**. Ao clicar **Avançado** pode definir opções adicionais de agendamento. Por exemplo, pode definir a data de início e fim da tarefa.

Para refinar ainda mais a tarefa agendada, clique na barra **Definições** . Três sub-opções estão disponíveis.

- **Tarefa Agendada Terminada**
  - Apague a tarefa se não estiver agendada para se executar novamente.

    Esta tarefa é útil para tarefas agendadas para se executarem uma só vez.
  - Parar a tarefa se se executa para:

    Especifique por quanto tempo após a tarefa ter sido iniciada deverá ser parada.
- **Tempo de Descanso**
  - Apenas inicia a tarefa se o computador estiver em descanso há pelo menos:

    Especifique quanto tempo (em minutos) deve passar sem usar o rato ou o teclado antes de a tarefa agendada se iniciar.
  - Se o computador não estiver estado em descanso tanto tempo, tentar de novo com:

    Especifique quanto tempo (em minutos) a tarefa deve continuar a verificar se o computador está em descanso.
  - Parar a tarefa se o computador deixar de estar em descanso.

    Especifique se a tarefa deve ser parada se você começar a usar o computador enquanto a tarefa estive a decorrer.
- **Gestor de Energia**
  - Não inicie a tarefa se o seu computador estiver a funcionar a bateria.

    Especifique se a tarefa deve ser impedida de inciar enquanto o seu computador está a funcionar a bateria. Ao seleccionar esta caixa de selecção pode aumentar a duração da sua bateria.
  - Parar a tarefa se o modo de bateria iniciar.

    Especifique se a tarefa deve ser parada quando o seu computador começar a funcionar a bateria.
  - Desperte o computador para executar esta tarefa.

    Especifica se o computador deve executar a tarefa agendada mesmo que esteja no modo de Hibernação.

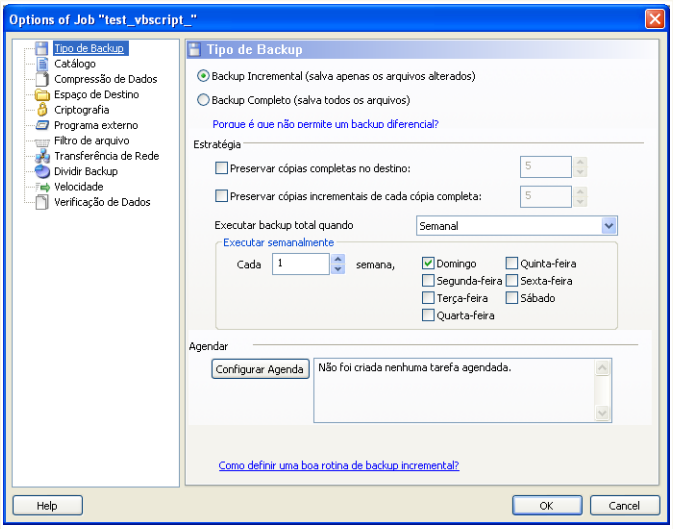
Apagar Tarefa Agendada

Para apagar uma tarefa agendada, seleccione-a e clique em**Apagar Tarefa Agendada** na secção**Gestão de Tarefas** .

Se a tarefa não está agendada, **Apagar Tarefa Agendada** será mostrada a cinzento, significando que não é usada.

Modificar Opções da Tarefa

Para modificar opções da tarefa, seleccione-a e clique em **Modificar Opções da Tarefa** na secção **Gestão de Tarefas** .

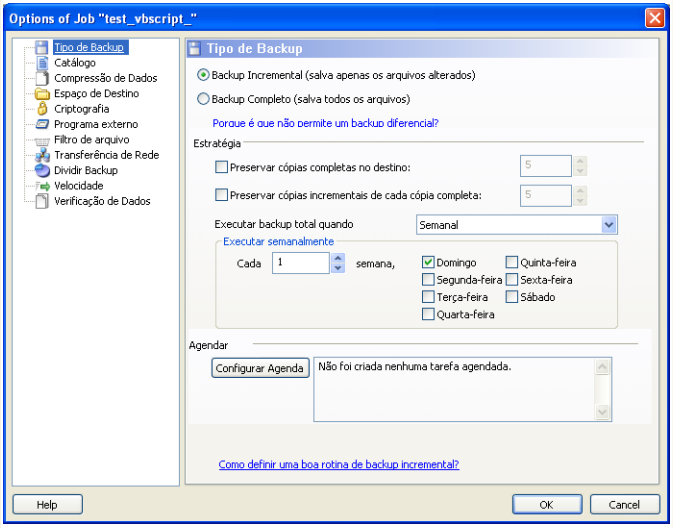


Modificar Opções da Tarefa

A tarefa seleccionada pode ser um backup ou uma gravação. Vamos pegar numa de cada vez.

Caixa de Diálogo Opções de Backup

Existem diversas sub-opções na caixa de diálogo das **Opções**.



Caixa de Diálogo Opções de Backup

Tipo de Backup

O Backup BitDefender suporta dois tipos de backup.

- **Backup Total:** Faz um backup completo de fonte de dados seleccionada para o backup set no destino especificado. Quando executar um backup total, o Backup BitDefender não fará backup dos dados modificados mas sim de toda a fonte de dados.
- **Backup Incremental:** Quando executar pela primeira o Backup Incremental é o mesmo que o Backup Total porque faz um backup completo de toda a fonte de dados para o backup set no destino especificado. Mais tarde, apenas faz backup dos novos arquivos ou dos arquivos modificados. Sempre que um Backup Incremental Backup é executado um backup catalog set é criado.

O Backup Incremental e o Total podem também combinar-se num **Backup de Rotação**. Por exemplo, pode definir um Backup Incremental do trabalho enquanto definie um Backup Total uma vez por semana, digamos ao Domingo. Eis como é feito: Seleccione **Semanal** do menu drop-down, 1 do campo**Cada Semana** e seleccionar Domingo. Este Backup Total ao Domingo substituirá todos os backups anteriores e será a base para o novo Backup Incremental trabalhar.

Catalog Set

É usado para indexar toda a informação de arquivos de cada backup, e é a base do processos de Backup Incremental e Restauração. O catalog set (`*.ecs`) contém uma série de catálogos que representam um índice de todos os ficheiros e diretórios existente no backup set. Tal índice inclui os dados da data do backup, diretório de backup, nome do arquivo e propriedades. Os dados podem ser restaurados a partir do catalog set.

Um nome de arquivo de catalog set é gerado automaticamente por destino de tarefa. Para modificar o catalog set de uma tarefa faça o seguinte:

1. Clique em **Catalog Set**.
2. Insira um nome de arquivo no campo correspondente.
3. Clique em **Explorar** para selecionar o diretório onde guardar os arquivos do Catalog set.
4. Clique em **OK**.

Compressão de Dados

O Backup BitDefender permite a comprimir e guardar os dados para o backup set quando executa um backup para poupar espaço. Suporta Compressão Rápida, Compressão Standard, Compressão Alta Intensidade. Por exemplo, para iniciar a compressão standard a uma velocidade de compressão média, siga os seguintes passos:

1. Clique em **Compressão de Dados**.
2. Clique em **Compressão Standard**.
3. Clique em **OK**.

Span de Destino

O Backup BitDefender permite a distribuição do backup set para um destino diferente. neste caso, mesmo que um determinado destino não tenha suficiente espaço livre, a execução do backup dos dados prosseguirá.

Pode adicionar um ou mais destinos para continuar o backup, modificá-lo ou mesmo removê-lo, da seguinte forma:

1. Clique em **Span de Destino**.
2. Clique em **Adicionar** para seleccionar um novo destino para guardar os dados de backup.
3. Clique em **Editar** para modificar o destino de backup seleccionado.
4. Clique em **Apagar** para apagar o destino de backup seleccionado.
5. Clique em **Apagar Todos** para apagar todos os destinos de backup.
6. Clique em **OK**.

Encriptação

O Backup BitDefender mantém os dados backup mais seguros ao encriptá-los antes de os guardar no backup set. As definições de segurança de uma tarefa inclui proteção por senha.

Para encriptar os dados antes do backup, siga estes passos:

1. Clique em **Encriptação**.
2. Seleccione um tipo de encriptação a partir do menu drop-down.
3. Insira a sua senha no campo correspondente.
4. Reinsira a sua senha no campo correspondente.
5. Clique em **OK**.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa**.
3. Clique em **Explorar** para selecionar os arquivos de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa**.
3. Clique em **Explorar** para selecionar os arquivos de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do usuário atual** quando o backup terminar.
7. Clique em **OK**.

Nota

Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de arquivos

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir arquivos específicos, tipos de arquivos ou diretórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de arquivos especificados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de arquivos nos pop-ups das caixas de diálogo ao selecionar as opções **Incluir apenas tipos de arquivos selecionados** ou **Excluir tipos de arquivos selecionados**
4. Se necessário, insira outro tipo de arquivo no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um arquivo especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Filtrar arquivo**.
3. Exclua ou inclua arquivos específicos nos pop-ups das caixas de diálogo selecionando as opções **Incluir apenas os arquivos especificados por regra** ou **Excluir os arquivos especificados** .
4. Clique em **Explorar** e selecione o arquivo. O caminho da localização do arquivo será automaticamente adicionado no campo **Aplicar aos seguintes diretórios** . Para incluir ou excluir o respectivo arquivo da sua localização, clique em **Aplicar a todos os diretórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

Transferência de Rede

O Backup BitDefender permite fazer backup e restaurar dados partilhados em grupos de trabalho de rede minuciosamente. Se a rede não estiver acessível, tentará fazer backup dos dados de vez em quando. Para especificar com que frequência ou quantas vezes deseja tentar o backup, siga os seguintes passos:

1. Clique em **Transferência de Rede**.
2. Clique em **Quando falhar em ler arquivos de rede devido a desconexão, tentar conectar de novo**.
3. Insira com que frequência deseja tentar de novo o backup dos dados (em segundos).
4. Insira quantas vezes deseja tentar de novo o backup dos dados.
5. Clique em **OK**.

Nota

Para evitar ser esmagado por informação de erros de rede, clique em **Não é gerado relatório de erro quando a rede não está disponível**.

Dividir Backup Set

O backup set gerado pode ser dividido em diveros outros backup sets, de forma a que o backup possa ser executado normalmente mesmo quando o destino ou o sistema de arquivos é limitado. O Backup BitDefender dá-lhe dois métodos de divisão: auto-divisão e divisão-definida.

As definições de divisão da tarefa de backup podem ser modificadas da seguinte forma:

1. Clique em **Dividir Backup Set**.
2. Seleccionar **Divisão Automática por Espaço no Destino**.
3. Ou seleccione **Especificar tamanho para dividir** e escolha o tamanho desejado no menu drop down.
4. Clique em **OK**.

Velocidade

O Backup BitDefender suporta três tipos de velocidade. Quanto maior a velocidade, mais CPU será ocupado

A velocidade de Backup pode ser especificada seguindo estes passos.

1. Clique em **Velocidade**.
2. Seleccione velocidade**Rápida**, **Média** ou **Baixa** .

3. Clique em **OK**.

Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Modificar Opções da Tarefa de Gravação

Várias sub-opções estão disponíveis na caixa de diálogo da tarefa de gravação.

Gravar

Aqui é onde pode definir que o disco seja ejetado após a gravação ter terminado (se deseja partilha-lo com outros) ou escrito usando o arquivo de sistema Joliet (menos restrições no nome do arquivo).

Se deseja agendar a tarefa, clique em **Definir Agendar**.

Aqui é onde poderá agendar a tarefa de backup para uma altura que seja conveniente. Pode agendar a tarefa para ser executada diariamente, semanalmente, mensalmente ou a qualquer altura que deseje (por exemplo durante o arranque do sistema). **Agendar Tarefa** é a base para o backup automático.

Se o seu computador é membro de um domínio de rede, uma série de passos extra são necessários para agendar uma tarefa.

1. Seleccione a tarefa e depois clique em **Agendar Tarefa**.
2. A caixa de diálogo de **Usuário de Execução** aparecerá. Se é um usuário do domínio, por favor insira a senha do domínio.
3. De outra forma selecione **Executar como o seguinte usuário Windows**.
4. Insira o nome do usuário, senha e o nome do servidor de domínio.
5. Clique em **OK**.

Uma vez que defina o usuário de execução, o Backup BitDefender mostrará a caixa de diálogo **Agendar** de forma a que possa definir uma altura conveniente para executar a tarefa.

É aqui onde pode especificar a frequência com que as tarefas agendadas se executam: diariamente, semanalmente, mensalmente, uma vez, no arranque do sistema, no login, quando o computador está em descanso. Se a tarefa é agendada diariamente, semanalmente, mensalmente, uma só vez, pode também especificar a hora de início. Pode também seleccionar com que frequência a tarefa agendada é executada (expresso como o número de dias ou semanas, o

dia do mês ou a data). Outra definição possível é a duração (em minutos) do período de descanso após o qual a tarefa agendada se inicia.

É também possível configurar múltiplos agendamentos para uma tarefa clicando em **Mostrar múltiplos agendamentos**. Ao clicar **Avançado** pode definir opções adicionais de agendamento. Por exemplo, pode definir a data de início e fim da tarefa.

Para refinar ainda mais a tarefa agendada, clique na barra **Definições** . Três sub-opções estão disponíveis.

- **Tarefa Agendada Terminada**
  - Apague a tarefa se não estiver agendada para se executar novamente.

    Esta tarefa é útil para tarefas agendadas para se executarem uma só vez.
  - Parar a tarefa se se executa para:

    Especifique por quanto tempo após a tarefa ter sido iniciada deverá ser parada.
- **Tempo de Descanso**
  - Apenas inicia a tarefa se o computador estiver em descanso há pelo menos:

    Especifique quanto tempo (em minutos) deve passar sem usar o rato ou o teclado antes de a tarefa agendada se iniciar.
  - Se o computador não estiver estado em descanso tanto tempo, tentar de novo com:

    Especifique quanto tempo (em minutos) a tarefa deve continuar a verificar se o computador está em descanso.
  - Parar a tarefa se o computador deixar de estar em descanso.

    Especifique se a tarefa deve ser parada se você começar a usar o computador enquanto a tarefa estive a decorrer.
- **Gestor de Energia**
  - Não inicie a tarefa se o seu computador estiver a funcionar a bateria.

    Especifique se a tarefa deve ser impedida de inciar enquanto o seu computador está a funcionar a bateria. Ao seleccionar esta caixa de selecção pode aumentar a duração da sua bateria.
  - Parar a tarefa se o modo de bateria iniciar.

    Especifique se a tarefa deve ser parada quando o seu computador começar a funcionar a bateria.
  - Desperte o computador para executar esta tarefa.

    Especifica se o computador deve executar a tarefa agendada mesmo que esteja no modo de Hibernação.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa**.
3. Clique em **Explorar** para selecionar os arquivos de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa**.
3. Clique em **Explorar** para selecionar os arquivos de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do usuário atual** quando o backup terminar.
7. Clique em **OK**.

Nota

Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de arquivos

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir arquivos específicos, tipos de arquivos ou diretórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de arquivos especificados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de arquivos nos pop-ups das caixas de diálogo ao selecionar as opções **Incluir apenas tipos de arquivos selecionados** ou **Excluir tipos de arquivos selecionados**
4. Se necessário, insira outro tipo de arquivo no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um arquivo especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Filtrar arquivo**.
3. Exclua ou inclua arquivos específicos nos pop-ups das caixas de diálogo selecionando as opções **Incluir apenas os arquivos especificados por regra** ou **Excluir os arquivos especificados** .
4. Clique em **Explorar** e selecione o arquivo. O caminho da localização do arquivo será automaticamente adicionado no campo **Aplicar aos seguintes diretórios** . Para incluir ou excluir o respectivo arquivo da sua localização, clique em **Aplicar a todos os diretórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:

1. Clique em**Filtro de arquivos**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

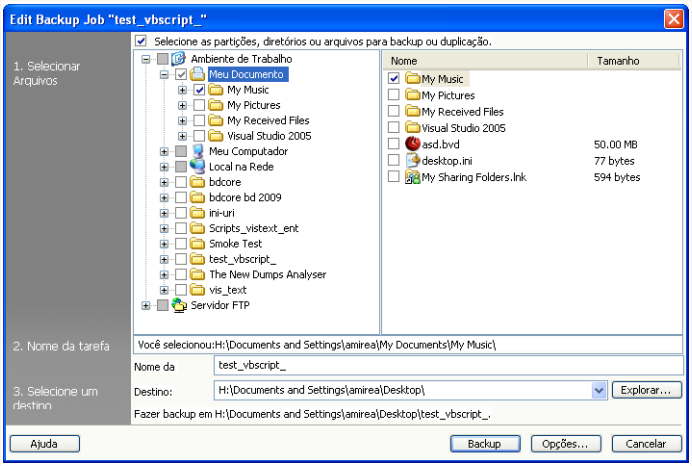
Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Modificar Propriedades da Tarefa

Para modificar as propriedades da tarefa, seleccione a tarefa em questão e depois clique em **Modificar Propriedades da Tarefa** na secção **Gestão de Tarefa**.



Modificar Propriedades da Tarefa

1. Clique na caixa de seleção para selecionar partições, diretórios, ou arquivos para backup.

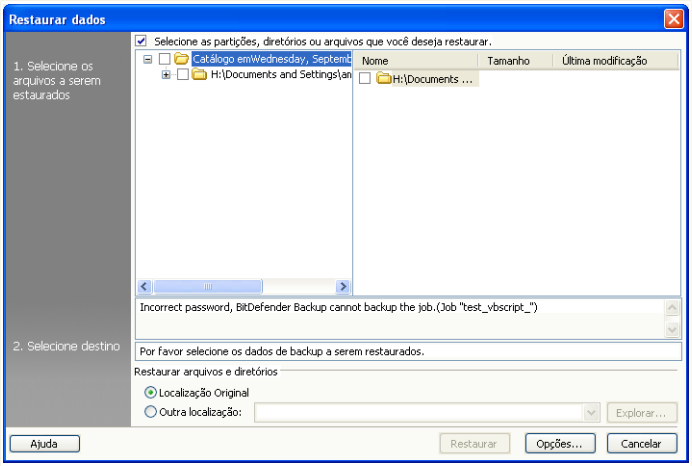
   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo será mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Insira um nome para a sua tarefa de backup ou aceite o nome por defeito da mesma.

   O nome por defeito da tarefa é automaticamente gerado quando os arquivos ou os diretórios são selecionados para serem backup, mas pode ser modificado.
3. Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Backup** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Restaurar arquivo

Para restaurar o backup dos seus dados, selecione a tarefa da qual deseja restaurar os dados, e clique em **Restaurar arquivo** no menu **Restaurar Tarefa** e depois siga estes passos.



Restaurar arquivo

1. Seleciones as caixas de seleção perto das partições, diretórios, ou arquivos selecionados para serem restaurados.

   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo é mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Na janela **Selecionar Local de Restauro**, pode usar o local original sem quaisquer mudanças, ou especificar outro local para onde restaurar o arquivo.

   Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota

Não se esqueça de clicar em **Restaurar** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Restaurar

As opções de restaurar permitem especificar se os arquivos a serem restaurados já existem no destino na altura do restauro em si, e se atualiza a data modificada de cada arquivo restaurado.

Quando os arquivos a restaurar já existem

- **Ignorar arquivos** O BitDefender ignora os arquivos respectivos.
- **Perguntar Usuário** O BitDefender pergunta se deve ou não substituir os arquivos existentes.
- **Substituir Directo** O BitDefender substitui os arquivos sem perguntar.
- **Substituir Antigos** O BitDefender substitui apenas os arquivos antigos. Os arquivos antigos são determinados baseado na data em que foram modificados.

Data de Modificação do arquivo

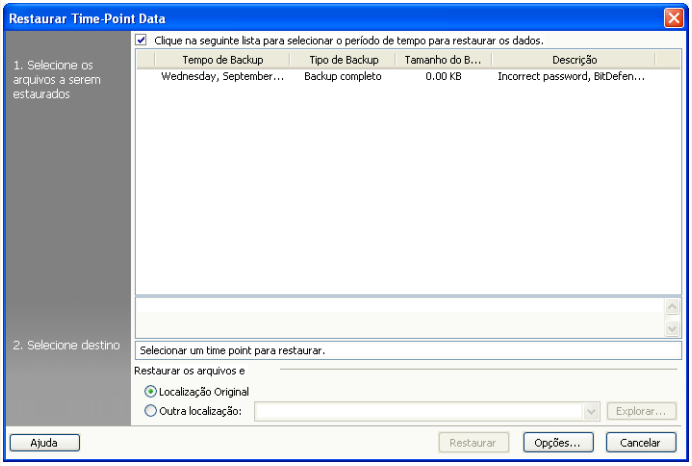
Se a opção for selecionada, o BitDefender usa a data atual para indicar a data em que os arquivos ou diretórios foram restaurados. Se não, o BitDefender usa a data de modificação do arquivo ou diretório de quando eles foram backup.

Estrutura de Directório

Só se torna activa quando escolhe outro local para onde restaurar os dados. Pode também preservar a estrutura de directório dos seus dados.

Restaurar Dados do Ponto do Tempo

Para restaurar os dados de um backup de um determinado ponto do tempo, selecciona a tarefa da qual deseja restaurar os dados, e clique em **Restaurar Dados do Ponto do Tempo** no menu **Restaurar Tarefa** e então siga os seguintes passos.



Restaurar Dados do Ponto do Tempo

1. Seleccione o backup set de um determinado ponto do tempo da lista. Comentários serão mostrados por debaixo dele.
2. Na janela **Selecionar Local de Restauro** , pode usar quer o local original, sem quaisquer alterações, ou especificar outro local para o qual restaurar o arquivo.

   Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Restaurar** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Restaurar

As opções de restaurar permitem especificar se os arquivos a serem restaurados já existem no destino na altura do restauro em si, e se atualiza a data modificada de cada arquivo restaurado.

Quando os arquivos a restaurar já existem

- **Substituir Antigos** O BitDefender substitui apenas os arquivos antigos. Os arquivos antigos são determinados baseado na data em que foram modificados.

Data de Modificação do arquivo

Se a opção for selecionada, o BitDefender usa a data atual para indicar a data em que os arquivos ou diretórios foram restaurados. Se não, o BitDefender usa a data de modificação do arquivo ou diretório de quando eles foram backup.

Estrutura de Directório

Só se torna activa quando escolhe outro local para onde restaurar os dados. Pode também preservar a estrutura de directório dos seus dados.

Controle de Tarefa

Existem três formas de monitorizar uma tarefa: pausar a tarefa, parar a tarefa e parar todas.

Pausa

Para por em pausa um backup que está a decorrer ou uma tarefa de restauro, clique no botão **Pausar Tarefa** no menu **Controle de Tarefa** .

Parar

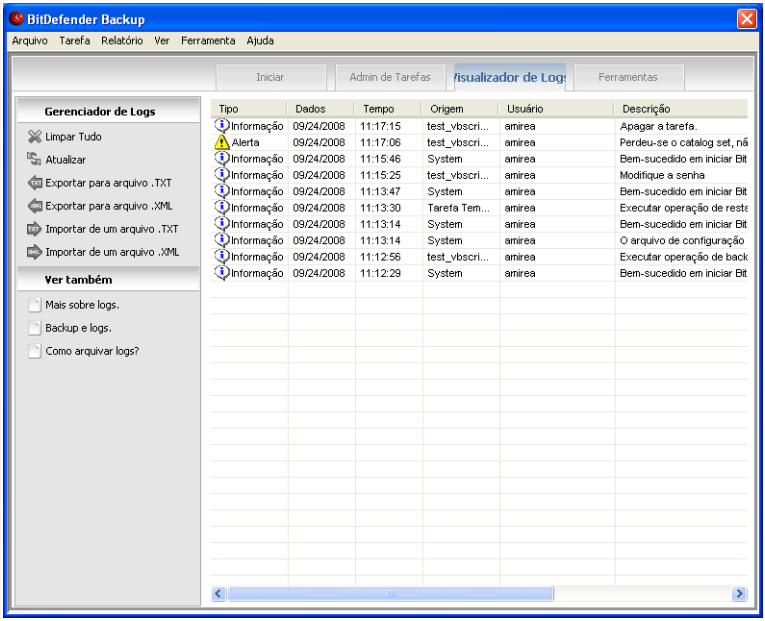
Para parar um backup que está a decorrer ou uma tarefa de restauro, clique no botão **Parar Tarefa** no menu **Controle de Tarefa** .

Parar Todas

Se existe mais do que uma tarefa de backup ou restauro a decorrer, não há necessidade de as parar uma a uma. Clique no botão **Parar Todas** no menu **Controle de Tarefa** para as parar todas de uma só vez.

Visualizar Log

Esta secção mostra-lhe como ver, importar, exportar e limpar logs. A opção de Logs ajuda-o a lembrar do que fez backup ou restaurou e quando o fez e também mostra os avisos de erro das operações. Por exemplo, se um erro ocorreu quando um arquivo foi lido durante a execução, o BitDefender regista-a como uma mensagem de aviso.



Visualizar Log

Pode mudar para **Visualizar Log** ao fazer uma das coisas seguintes:

- Clique em **Visualizador do histórico** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Visualizar Log**.
- Use um atalho ao premir as seguintes teclas **CTRL+Alt+L**.

Ver Logs

A opção de visualização de logs permite rastrear a sua operação, e descobrir a razão para a mesma ter falhado.

A descripção de um item de um log do Backup BitDefender contém os seguintes elementos:

Tipo

Uma classificação da severidade do item no log. Existem quatro graus de severidade no Backup BitDefender:

- **Fatal:** Um problema significativo que previne que o Backup BitDefender de decorrer normalmente. Por exemplo, o arquivo de configuração do Backup BitDefender foi danificado.
- **Erro:** Um problema que leva a uma falha da operação. Por exemplo, uma tarefa que é backup num servidor, mas o servidor não pode ser acedido.
- **Aviso:** um problema que não afeta uma operação, mas que pode mais tarde ser classificado como um evento. Por exemplo, um arquivo que não pode ser lido durante o backup.
- **Informação:** Descreve uma operação bem-sucedida. Por exemplo, uma tarefa foi apagada com sucesso.

Data
A data em que o item do log ocorreu.

Hora
A hora local em que o item do log ocorreu.

Fonte
A fonte que fez o log do respectivo item, que pode ser uma tarefa ou a aplicação do Backup BitDefender. Por exemplo, um item de sistema marcado indica que foi posto no log pela aplicação do Backup BitDefender. Outras possíveis marcas são os nomes das tarefas do Backup BitDefender terem feito log do respectivo item.

Usuário
O nome do usuário conforme com a ação do item que foi log.

Descripção
Apresenta o conteúdo detalhado do item que foi log.

Limpar Logs

O Backup BitDefender fornece duas formas de limpar logs: automaticamente e manualmente.

Importante
Uma vez que o registo de log tenha sido limpo, não pode mais ser recuperado. Logo é melhor exportar os logs para um arquivo e preservá-los para futura consulta.

Limpar Automaticamente
Quando o Backup BitDefender inicia, compara o tamanho do log existente com o tamanho do log por defeito. O Backup BitDefender limpa automaticamente todos os arquivos de log que excedam o tamanho por defeito.

Nota
Para saber mais ou modificar o tamanho por defeito do log siga os seguintes passos:
1. Clique em **Ferramenta** na **Barra de Menu**.
2. Clique em **Opções**, e depois seleccione **Relatórios & Log**.
3. Insira a desejada limitação de tamanho (em MB) no campo correspondente. Quando o arquivo de log o atingir como limite, o Backup BitDefender limpará todos os logs.

Limpar Manualmente

Siga estes passos para limpar logs manualmente.
1. Clique em **Limpar Todos** no menu **Gestão de Logs** .
2. Clique em **OK** para exportar certos logs antes de limpar os outros, ou clique **Não** se não desejar preservar quaisquer logs.

Importar e Exportar Logs

O Backup BitDefender suporta atualmente importação e exportação de arquivos em dois formatos: `.TXT` e `.XML`

Nota
Recomendamos que exporte e guarde o log para um arquivo antes de o limpar.

Para exportar os logs para um arquivo especificado, siga estes passos:

1. Clique em **Exportar para arquivo .TXT** ou **Exportar para arquivo .TXT** no menu **Gestão de Logs** .
2. Insira o nome do arquivo e selecione o local para onde guardar o arquivo.
3. Clique em **Guardar**.

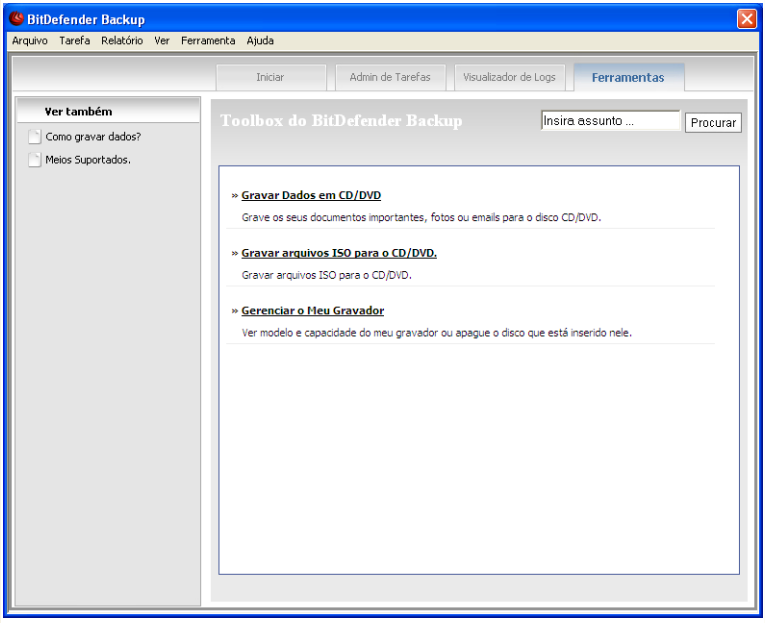
Para importar logs de um arquivo específico, siga estes passos:

1. Clique em **Importar para arquivo .TXT** ou **Importar para arquivo .TXT** no menu **Gestão de Logs** .
2. Encontrar o seu arquivo.
3. Clique em **Abrir**.

Nota
Clique no botão **Actualizar** no menu **Gestão de Logs** para ter a certeza que vê os logs mais recentes.

Toolbox

Esta secção mostra como usar o Backup BitDefender para gravar dados num CD/DVD ou para gravar um arquivo de imagem ISO. Abrange assuntos tais como gravar um CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL e preservar dados em backup offline.



Toolbox

Pode mudar para **Toolbox** fazendo uma das coisas seguintes:

- Clique em **Toolbox** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Toolbox**.
- Use um atalho premindo as teclas **CTRL+Alt+T**.

Gravar para CD/DVD

Para gravar manualmente num CD/DVD, siga estes passos:

1. Clique em **Gravar dados no CD/DVD**.

2. Clique em **Apagar** se deseja reutilizar um disco regravável. Se deseja apagar o seu conteúdo rapidamente, clique em **Rápido**. Se necessita de apagar a informação de gravação completamente, clique em **Completa**, mas esta levará algum tempo.
3. Clique em **Gravar com Diálogo**.

   Aqui é onde pode definir que o disco seja ejetado após a gravação ter terminado (se deseja partilha-lo com outros) ou escrito usando o arquivo de sistema Joliet (menos restrições no nome do arquivo).
4. Clique em **Arquivo** ou **Diretório** nos pop-ups da caixa de diálogo para adicionar dados que deseja gravar.
5. Após os dados terem sido adicionados, seleccione o gravador e insira o nome do disco onde vai gravar os dados, e depois clique em **Gravar**.

Gravar um arquivo de imagem ISO para um CD/DVD

Para gravar um arquivo de imagem ISO para um CD/DVD siga estes passos:

1. Clique em **Gravar um arquivo de imagem ISO para um CD/DVD**.
2. Clique em **Apagar** se deseja reutilizar um disco regravável. Se deseja apagar o seu conteúdo rapidamente, clique em **Rápido**. Se necessita de apagar a informação de gravação completamente, clique em **Completa**, mas esta levará algum tempo.
3. Clique em **Gravar com Diálogo**.

   É aqui que pode definir ejetar o seu disco após gravação, finalizar o disco (se desja partilhá-lo com outros) ou escrever os dados usando o arquivo de sistema Joliet (menos restrições de nome do arquivo).
4. Clicando **Adicionar**.
5. Selecione um arquivo de imagem ISO para gravar e clique em **Abrir**.
6. Clique em **Gravar**.

Gerir o Meu Gravador

Isto ajuda-o a gerir e ver o dispositivo de gravação e de media do sistema actual. Contém os seguintes links:

- **Ejectar Dispositivo** Ejecta o dispositivo de gravação seleccionado.
- **Fechar Dispositivo** Fecha o dispositivo de gravação seleccionado.
- **Infos de Media** Permite visualizar a informação de Media do dispositivo de gravação.
- **Infos de Dispositivo** Permite visualizar a informação do dispositivo de gravação.
- **Capacidades** Permite visualizar as capacidades de gravação de media.
- **Apagar Media** Apaga o conteúdo do disco.

22. Encriptação

O BitDefender oferece uma função de proteção que permite cifrar os seus documentos confidenciais e as suas conversas através do Yahoo Messenger e MSN Messenger.

22.1. Encriptação de Mensagens Instantâneas (IM)

De forma padrão, BitDefender cifra todas as suas sessões de chat desde que:

- O seu parceiro de chat tenha instalada uma versão do BitDefender que suporte a cifragem MI e a mesma esteja habilitada para o programa de mensagens usado durante o chat.
- E o seu parceiro de chat esteja a usar quer o Yahoo Messenger ou o Windows Live (MSN) Messenger.

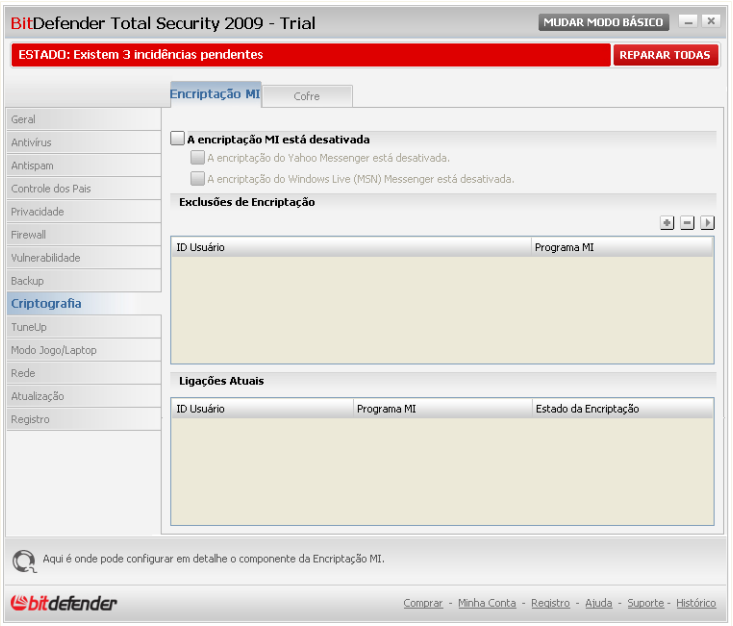
Importante

O BitDefender não vai cifrar uma conversa se o seu parceiro de chat usar um programa de chat, tipo Meebo, ou outro que suporte o Yahoo Messenger ou o MSN.

Para configurar a encriptação de Mensagens Instantâneas, clique em **Encriptação>Encriptação IM** no Modo Avançado.

Nota

Pode configurar facilmente a cifragem das mensagens instantâneas usando a barra de ferramentas a partir da janela de chat. Para mais informação, por favor consulte a seção "*Integração com Messenger*" (p. 51).



Encriptação de Mensagens Instantâneas

Por defeito, a Encriptação de Mensagens Instantâneas está activada para o Yahoo Messenger e o Windows Live (MSN) Messenger. Pode escolher desactivar a encriptação de Mensagens Instantâneas para apenas uma aplicação de chat ou para todas.

São mostradas duas tabelas:

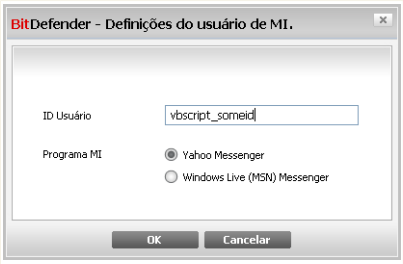
- **Exclusões da Encriptação** - lista os IDs dos usuários e o programa de IM associado para os quais a encriptação está desativada. Para remover um contacto da lista , seleccione-o e clique no botão **Remover**.
- **Ligações Atuais** - lista as atuais ligações de mensagens (IDs dos usuários e o programa de IM associado) e se devem ou não ser encriptadas. Uma ligação poderá não ser encriptada pelas seguintes razões:
  - Desactivou explicitamente a encriptação para o respectivo contacto.

- O seu contacto não tem instalado uma versão do BitDefender que suporte a encriptação IM.

22.1.1. Desativar a Encriptação para usuários Específicos

Para desativar a encriptação para um determinado usuário, siga estes passos:

1. Clique no botão **Adicionar** para abrir a janela de configuração.



Adicionar Contactos

2. Insira no campo de edição o ID do usuário do seu contato.
3. Seleccione a aplicação de mensagens instântaneas associada ao contacto.
4. Clique em **OK**.

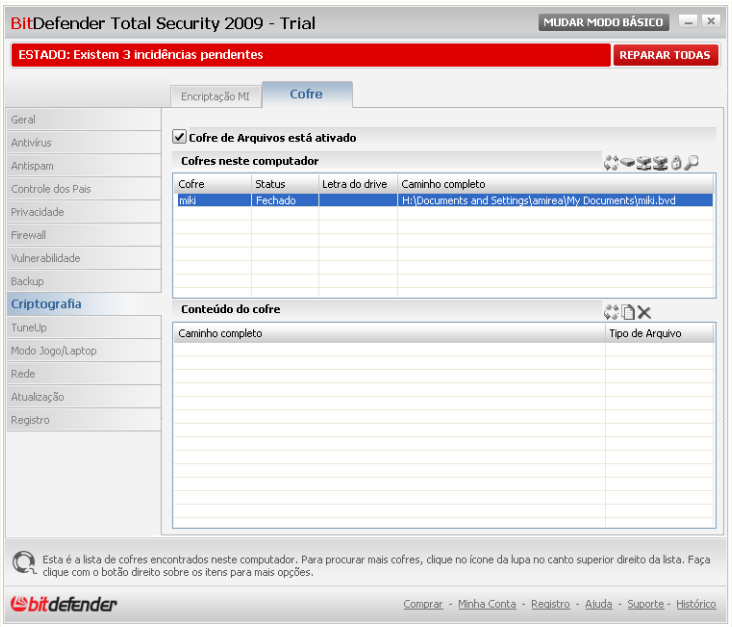
22.2. Cofre de arquivos

O Cofre de arquivos BitDefender permite-lhe criar drives lógicas encriptadas, e protegidas por senha (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis. Os dados armazenados nos cofres apenas podem ser acessados pelos usuários que sabem a senha.

A senha permite-lhe abrir, armazenar dados no cofre e fechá-lo ao mesmo tempo que o mantém seguro. Quando um cofre é aberto, pode adicionar-lhe arquivos, aceder aos que lá estão ou alterá-los.

Fisicamente, o cofre é um arquivo armazenado no seu disco rígido local com a extensão `.bvd`. Apesar dos arquivoos físicos que representam as drives de cofre poderem ser acessados a partir de um sistema operacional diferente (tal como Linux), a informação armazenada não pode ser lida por estar encriptada.

Para gerir os cofres no seu computador, clique em **Encriptação>Cofre arquivos** no Modo Avançado.



Cofre de arquivos

Para desativar Cofre de arquivos, limpe a caixa**Cofre de arquivos ativado** e clique em **Sim** para confirmar. Se desativar o Cofre de arquivos, todos os cofres de arquivos serão fechados e não será mais capaz de aceder aos arquivos que eles contêm.

A tabela no topo mostra os cofres de arquivos no seu computador. Pode ver o nome, o estado (aberto / fechado), a letra da drive e o caminho completo para o cofre. A tabela do fundo mostra o conteúdo dos cofre seleccionado.

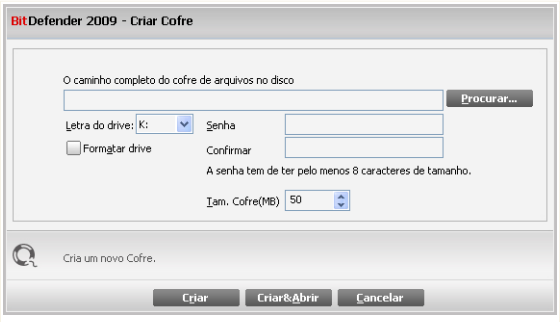
22.2.1. Criar um Cofre

Para criar um cofre, use um dos seguintes métodos:

- Clique **Criar cofre**.
- Clique botão direito do mouse na tabela dos cofres e selecionar **Criar**.

- Clique botão direito do mouse no seu Ambiente de Trabalho ou numa pasta do seu computador, apontar para **Cofre Arquivos BitDefender** e selecionar **Criar**.

Uma nova janela irá aparecer.



Criar Cofre de arquivos

Proceder da seguinte forma:

1. Especificar a localização e o nome do cofre de arquivos.
   - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de arquivos sob o nome desejado.
   - Insira o caminho completo do cofre de arquivos no disco.
2. Escolha a letra da drive a partir do menu. Quando abre o cofre, um disco virtual com a letra seleccionada aparecerá em O Meu Computador.
3. Insira a palavra-passe do cofre no campo **Senha** . Qualquer pessoa que tente abrir o cofre e aceder aos seus arquivos tem de inserir a senha.
4. Seleccione **Formatar drive** para formatar a drive virtual atribuida ao cofre.
5. Se deseja mudar o tamanho por defeito (50 MB) do cofre, insira o valor desejado no campo **Tamanho Cofre** .
6. Clique em **Criar** se deseja criar o cofre na localização seleccionada. Para criar e mostrar o cofre como um disco virtual em O Meu Computador, clique em **Criar&Abrir**.

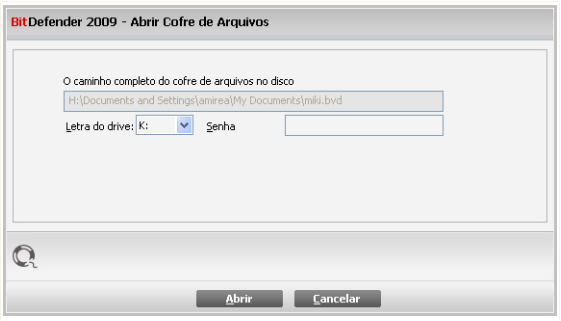
22.2.2. Abrir um Cofre

De forma a poder aceder e trabalhar com os arquivos armazenados no cofre, tem de o abrir. Quando abre o cofre, um disco virtual aparece em O Meu Computador. A drive tem a denominação da letra que atribuiu ao cofre.

Para abrir o cofre, use um dos seguintes métodos:

- Seleccione o cofre da tabela e clique **Abrir cofre**.
- Clique com o botão-direito na tabela e seleccione **Abrir**.
- Clique com o botão-direito no cofre de arquivos no seu computador, aponte para **Cofre arquivos BitDefender** e selecione **Abrir**.

Uma nova janela irá aparecer.



Abrir Cofre de arquivos

Proceder da seguinte forma:

1. Escolha a letra da drive a partir do menu.
2. Insira a palavra-passe do cofre no campo **Senha** .
3. Clique em **Abrir**.

22.2.3. Fechar um Cofre

Quando terminou de trabalhar sobre um cofre de arquivos, deve de o fechar de forma a proteger os seus dados.

Para fechar um cofre, use um dos seguintes métodos:

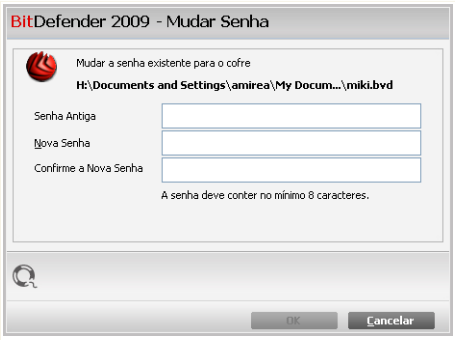
- Seleccione o cofre na tabela e clique em **Fechar cofre**.
- Clique com o botão-direito do mouse no cofre da tabela e selecione **Fechar**.
- Clique com o botão direito do mouse no cofre de arquivos do seu computador, aponte para **Cofre Arquivos BitDefender** e selecione **Fechar**.
- Clique com o botão direito do mouse no correspondente disco virtual em Meu Computador, aponte para **Cofre arquivos BitDefender** e selecione **Fechar**.

22.2.4. Mudar senha do Cofre

Para mudar a senha do cofre, use um dos seguintes métodos:

- Selecione o cofre na tabela e clique em **Alterar senha**.
- Clique com o botão-direito do mouse no cofre da tabela e selecione **Alterar senha**.
- Clique com o botão-direito do mouse no cofre de arquivos do seu computador, aponte para **Cofre arquivos BitDefender** e selecione **Alterar senha do cofre**.

Uma nova janela irá aparecer.



Alterar senha do Cofre

Proceder da seguinte forma:

1. Insira a senha atual do cofre no campo **senha antiga** .
2. Insira a nova senha nos campos **Nova senha** e **Confirmar nova senha** .

Nota

A senha deve ter pelo menos oito caracteres em tamanho. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

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

22.2.5. Adicionar arquivos ao Cofre

Para adicionar arquivos ao cofre, siga os seguintes passos:

1. Clique **Adicionar arquivo**. Uma nova janela irá aparecer.
2. Selecione os arquivos / pastas que deseja adicionar ao cofre.
3. Clique em **OK** para copiar os objectos seleccionados para o cofre.

Nota

Não pode adicionar arquivos de sistema ou de aplicações ao cofre.

22.2.6. Remover arquivos do Cofre

Para remover arquivos do cofre, siga os seguintes passos:

1. Seleccione da tabela de cofres o cofre que contém o arquivo a ser removido.
2. Seleccione o arquivo a ser removido a partir da tabela que mostra o conteúdo do cofre.
3. Clique **Remover arquivo**.

Nota

Se o cofre estiver aberto, pode remover diretamente os arquivos a partir da drive virtual atribuida ao cofre.

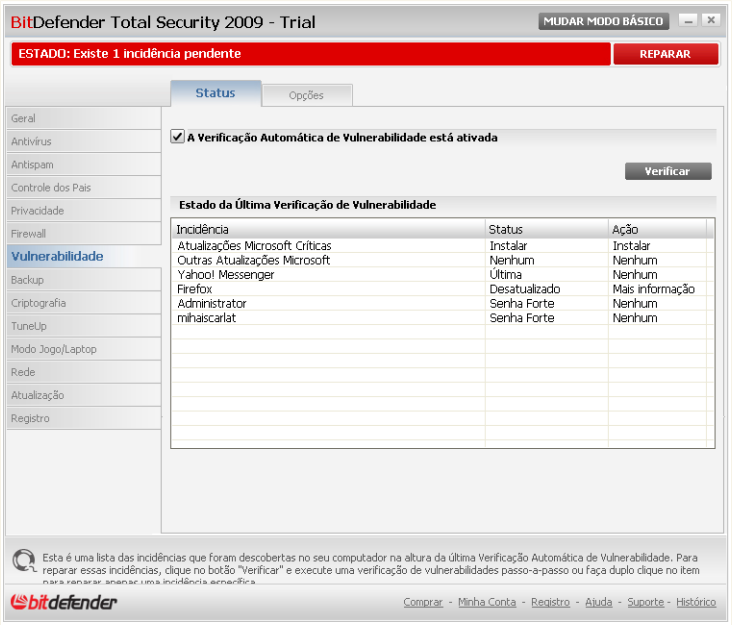
23. Vulnerabilidade

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operacional e as aplicações que usa regularmente. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, senhas fortes (senhasque não são fáceis de adivinhar) devem de ser criadas para cada conta de usuário do Windows.

O BitDefender analisa regularmente o seu sistema em busca de vulnerabilidades e notifica-o das incidências existentes.

23.1. Status

Para configurar a análise automática de vulnerabilidades, ou levar a cabo uma, clique em **Vulnerabilidade>Estado** no Modo Avançado.



Status de Vulnerabilidade

A tabela mostra os problemas cobertos na última análise de vulnerabilidade e o seu estatus. Você pode ver a ação que deve ser tomada para consertar cada situação de vulnerabiliade, caso esta exista. Se a ação é **Nenhuma**, então o ponto detectado não representa um ponto de vulnerabilidade.

Importante
Para ser automaticamente notificado acerca das vulnerabilidades do seu sistema e aplicações, mantenha a **Análise Automática de Vulnerabilidades** activada.

23.1.1. Consertando pontos vulneráveis

Para consertar um ponto vulnerável, clique duas vezes com o mouse e, dependendo do problema, continue como definido a seguir:

- Se houverem atualizações disponíveis do Windows, clique **Instale todas as Atualizações do Sistema** para instalá-las.
- Se um aplicativo estiver desatualizado, use o link **Página Inicial** fornecido para efetuar o download e instalar a versão mais atualizada do aplicativo.
- Se uma conta de usuário do Windows possuir uma senha considerada vulnerável, faça o usuário mudar sua senha no próximo logon ou mude a senha você mesmo.

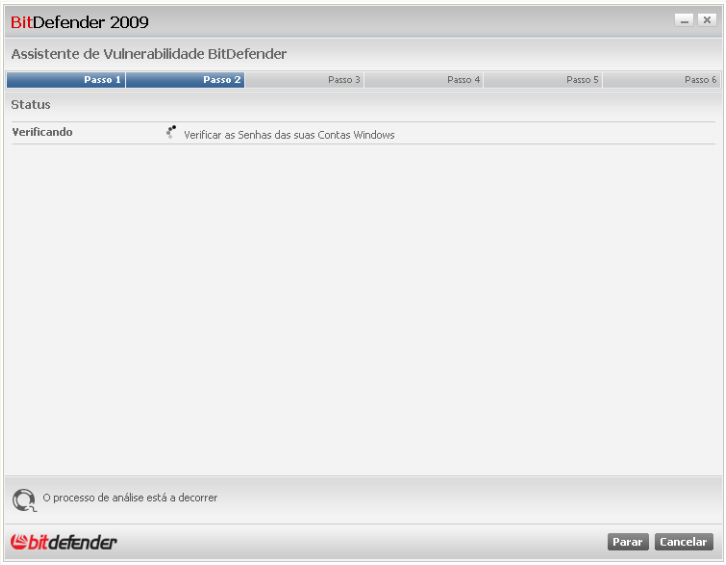
Você pode clicar **Verificar Agora** e seguir as instruções para consertar os pontos vulneráveis passo a passo.

Passo 1/6 - Seleccionar Vulnerabilidades a Verificar

Vulnerabilidades

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

Passo 2/6 - Analisar em Busca de Vulnerabilidades



Analisar Vulnerabilidades

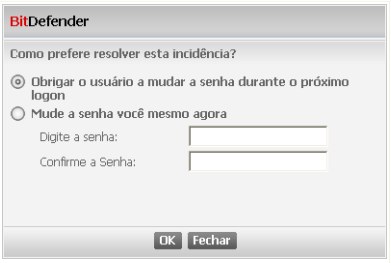
Espere que o BitDefender termine a análise de vulnerabilidades.

Passo 3/6 - Alterar Palvaras-passe Fracas

Senhas do usuário

Pode ver a lista dos usuários de contas Windows configurados no seu computador e o nível de proteção que as suas senhas garantem.

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



Mudar a senha

Seleccionar o método para reparar esta incidência:

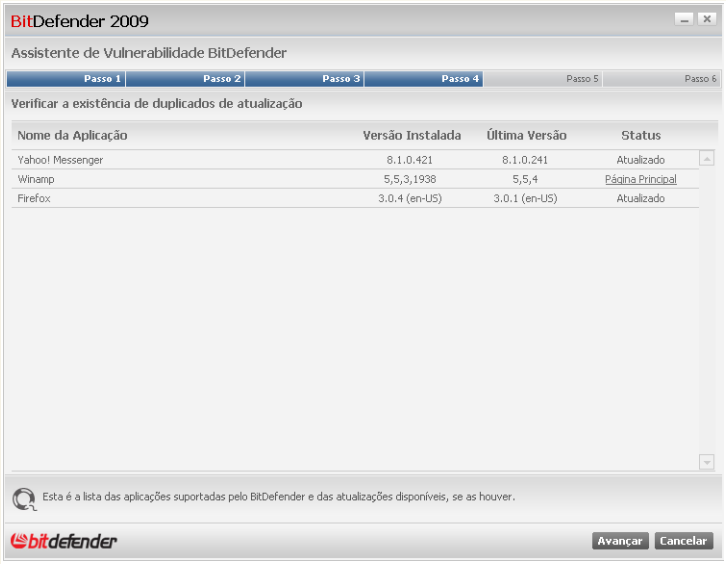
- **Forçar o usuário a mudar a senha no próximo login:** O BitDefender avisará o usuário que tem de alterar a senha da próxima vez que ele entrar no Windows.
- **Mudar a senha do usuário.** Deve inserir a nova senha nos campos editáveis.

> ***Nota***
> Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

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

Clique em **Próximo**.

Passo 4/6 - Actualizar Aplicações

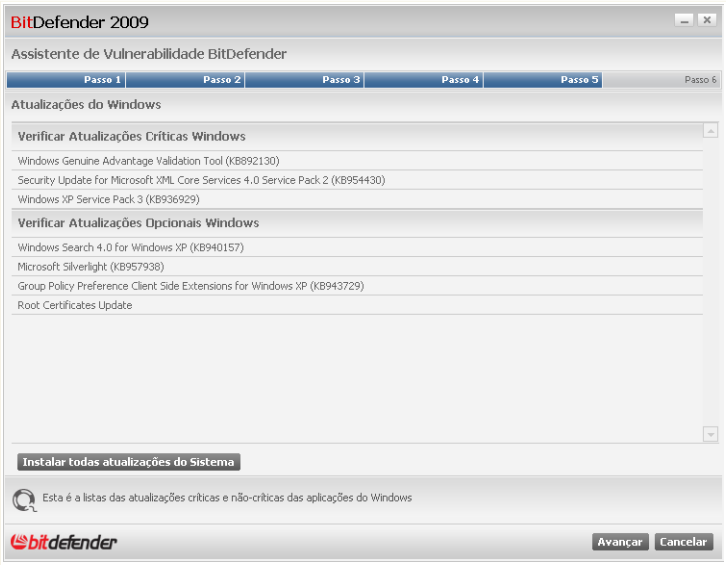


Aplicações

Pode ver a lista de todas as aplicações verificadas pelo BitDefender e se as mesmas estão ou não actualizadas. Se a aplicação não estiver actualizada, clique no link fornecido para descarregar a versão mais recente.

Clique em **Próximo**.

Passo 5/6 - Actualizar Windows



Actualizações Windows

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

Clique em **Próximo**.

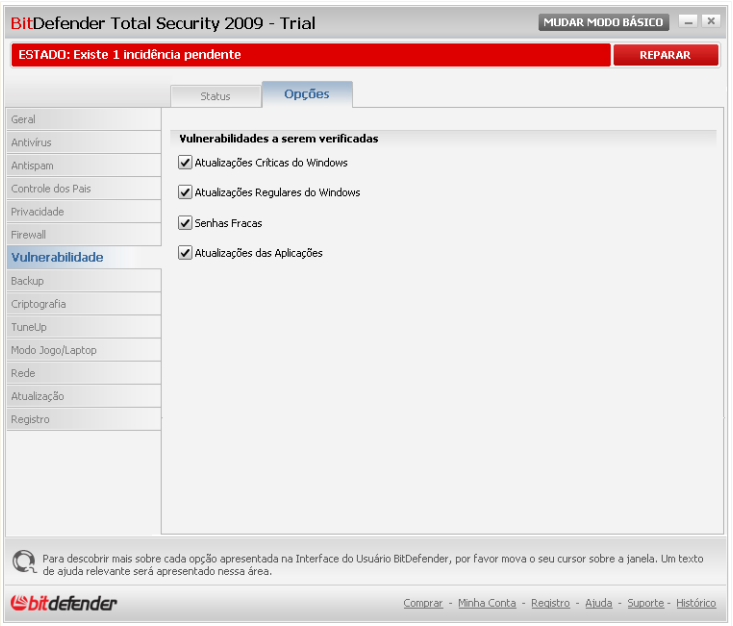
Passo 6/6 - Ver Resultados

Resultados

Clique em **Fechar**.

23.2. Opções

Para configurar as definições da análise automática de vulnerabilidades, clique em **Vulnerabilidade>Configuração** no Modo Avançado.



Definições da Análise Automática de Vulnerabilidades

Seleccione as caixas que correspondem às vulnerabilidades do sistema que deseja que sejam regularmente verificadas.

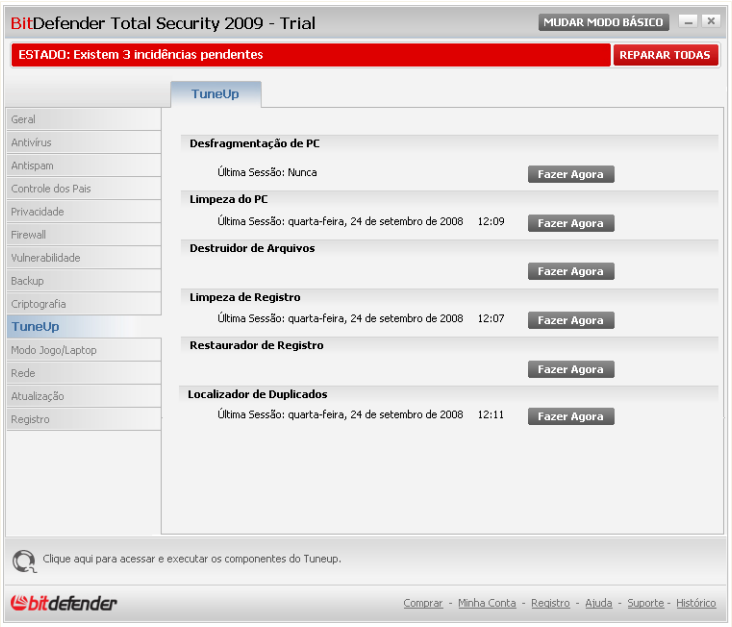
- **Actualizações Críticas do Windows**
- **Actualizações Regulares do Windows**
- **Palavras-passe Fracas** .
- **Actualizações de Aplicações**

Nota
Se limpar a a caixa correspondente a uma determinada vulnerabilidade, o BitDefender não o irá mais notificar acerca das incidências relacionadas.

24. TuneUp

BitDefender vem com um módulo de TuneUp que o ajuda a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco rígido.

Para executar operações de manutenção no seu PC, clique na barra **TuneUp** e use as ferramentas disponibilizadas.



TuneUp

O BitDefender fornece as seguintes ferramentas de tuneup para o PC.

- O desfragmentador PC reorganiza os dados contidos no disco rígido de forma a que as partes constituintes de cada arquivo sejam armazenadas juntas e de forma continua.

- Limpa PC remove os arquivos temporários da Internet e as cookies, os arquivos não utilizados do sistema e os atalhos recentes dos documentos.
- Destruidor arquivos apaga permanentemente os arquivos e os seus vestígios do sistema. Use o Destruidor arquivos para se assegurar que os ficheiros que apaga do seu computador não podem mais ser recuperados.
- Limpa Registo identifica e apaga referências orfãs ou inválidas do Registo do Windows. De forma a manter o Registo do Windows limpo e optimizado, é recomendável que execute o seu Limpa Registo uma vez por mês.
- O Restaurar Registo pode recuperar as chaves de registo previamente apagadas do Registo do Windows no uso do Limpa Registo BitDefender.
- O Localizador de Duplicados encontra e apaga arquivos que se encontram duplicados no seu sistema.

Para usar uma dessas ferramentas, clique no botão correspondente **Executar Agora** e siga o assistente.

24.1. Desfragmentar Volumes de Discos Duros

Quando copia um arquivo que excede o tamanho do maior bloco de espaço livre no disco rígido, a fragmentação do arquivo ocorre. Porque não existe suficiente espaço livre para guardar o arquivo de forma contínua, o mesmo é armazenado em diversos blocos. Quando o arquivo framentado é acedido, os seus dados têm de ser lidos de diversos locais diferentes.

A fragmentação dos arquivos torna mais lento o acesso aos mesmo e diminui o desempenho do sistema. Também acelera o desgaste do seu disco rígido.

Para reduzir a fragmentação de arquivos, deve de desfragmentar os seus discos periodicamente. A desfragmentação do disco reorganiza os dados contidos no disco rígido de forma a que as partes constituintes de cada arquivo sejam armazenadas juntas e de forma continua. Também tenta criar área de espaço livre maiores de forma a evitar que os arquivos sejam mais tarde fragmentados.

É recomendável que desfragmente o seu disco rígido de forma a que:

- acesse mais rápido aos arquivos.
- melhore o desempenho do sistema em geral.
- aumente o tempo de duração do seu disco rígido.

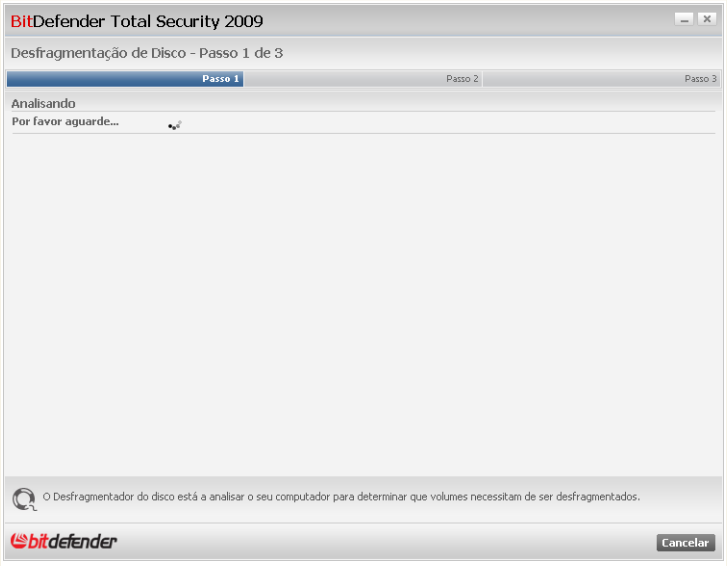
Para desfragmentar o disco rígido, siga estes passos:

1. No Modo Avançado, clique em **TuneUp** no menu da esquerda.
2. Clique em **Executar Agora** correspondente ao desfragmentador de PC.
3. Siga o processo guiado de três passos.

Nota
A desfragmentação poderá demorar algum tempo uma vez que involve o mover de porções de dados armazenados de um lugar para o outro do disco rígido. Recomendamos que execute a desfragmentação quando não está a usar o seu computador.

24.1.1. Passo 1/3 - A analisar...

O Desfragmentador do Disco irá analisar o disco rígido para determinar se o mesmo necessita ou não de ser desfragmentado.



A analisar

Espere que o Desfragmentador do Disco termine a análise. Se deseja cancelar a operação clique em **Cancelar**.

24.1.2. Passo 2/3 - Ver o Relatório da Análise

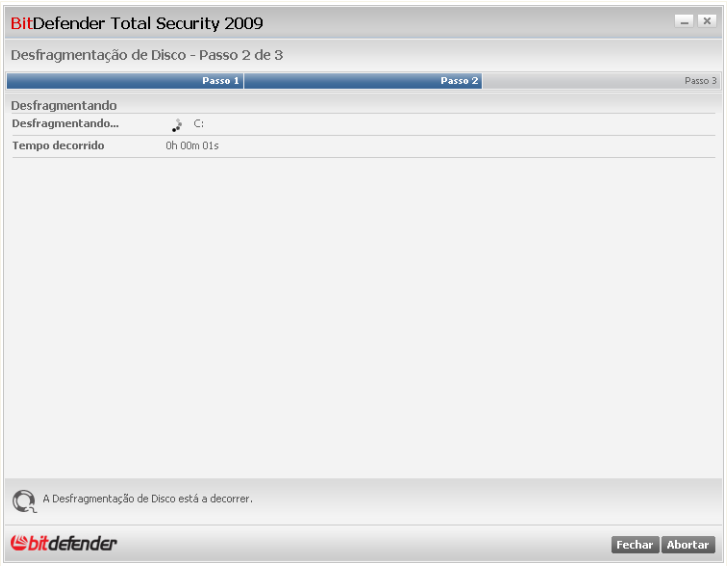
Após a análise estar completa, uma nova janela surgirá onde poderá ver os resultados e iniciar a desfragmentação do disco se necessário.

Relatório da Análise

Verificar o relatório da análise.

Se nenhum dos volumes do disco necessita de ser desfragmentado, clique em **Fechar** para fechar a janela. Caso contrário, seleccione a opção **Defrag** correspondente ao volume do disco que necessita de ser desfragmentado e clique em **Executar** para o desfragmentar.

Nota
O Desfragmentador do Disco necessita de 15% de espaço livre no disco a desfragmentar de forma a funcionar correctamente. Se não existir suficiente espaço livre no volume a desfragmentar, a desfragmentação será abortada.



A Desfragmentar

Espere que a desfragmentação do disco termine. Pode cancelar a desfragmentação do disco a qualquer altura clicando em **Abortar**.

24.1.3. Passo 3/3 - Ver Relatório de Desfragmentação

Após a desfragmentação do disco se completar, surgirá uma nova janela onde pode ver as estatísticas de desfragmentação.

Relatório de Desfragmentação

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

24.2. Limpar o Seu PC

Cada vez que visita uma página web, são criados arquivos temporários da Internet de forma a permitir que lhe aceda mais rapidamente da próxima vez. Apesar de serem apelidados de temporários, estes arquivos não são apagados quando desliga o seu browser de internet. Isto poderá resultar numa questão de privacidade porque estes arquivos podem ser vistos por qualquer pessoa que tenha acesso ao seu computador. E mais ainda, estes arquivos ao fim de algum tempo atingem um tamanho considerável, ocupando desnecessariamente espaço do seu disco rígido.

Os cookies também são armazenados na seu computador quando visita uma página web. Os cookies são pequenos arquivos que contém informação sobre as suas preferências de navegação na web. Eles poderão ser vistos também como uma questão de privacidade também, pois eles podem ser analisados e usados por publicitários para rastrear os seus interesses e gostos on-line.

O Limpa PC ajuda-o a libertar espaço em disco e a proteger a sua privacidade ao apagar arquivos que já não são úteis.

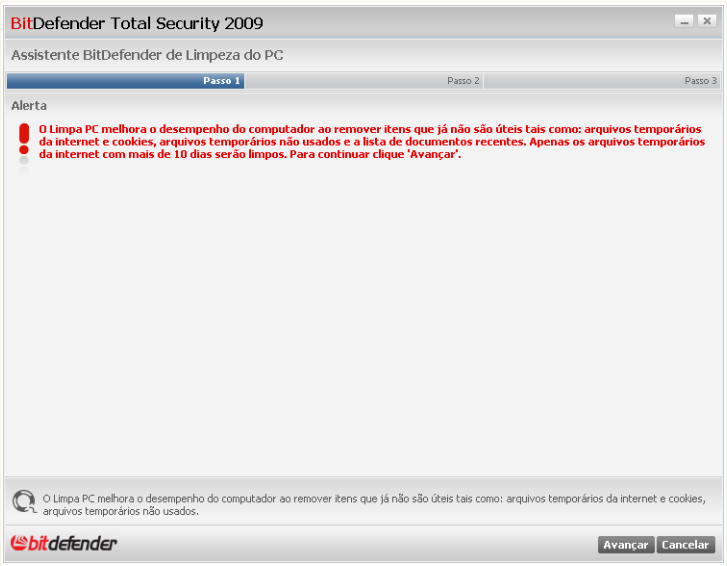
- Arquivos temporários da internet e cookies do Internet Explorer.
- Arquivos temporários da internet e cookies do Mozilla Firefox.
- arquivos temporários do sistema que o Windows cria durante esta operação.
- recentes atalhos de documentos que o Windows cria quando abre um arquivo.

Para limpar o sistema de arquivos temporários da Internet e das cookies, dos arquivos temporários do sistema e dos recentes atalhos de documentos, siga os seguintes passos:

1. No Modo Avançado, clique em **TuneUp** no menu da esquerda.
2. Clique em **Executar** correspondente ao Limpador de PC.
3. Siga o processo guiado de três passos.

24.2.1. Passo 1/3 - Iniciar a Eliminação

Aqui pode dar início à eliminação dos arquivos temporários da internet e dos cookies.

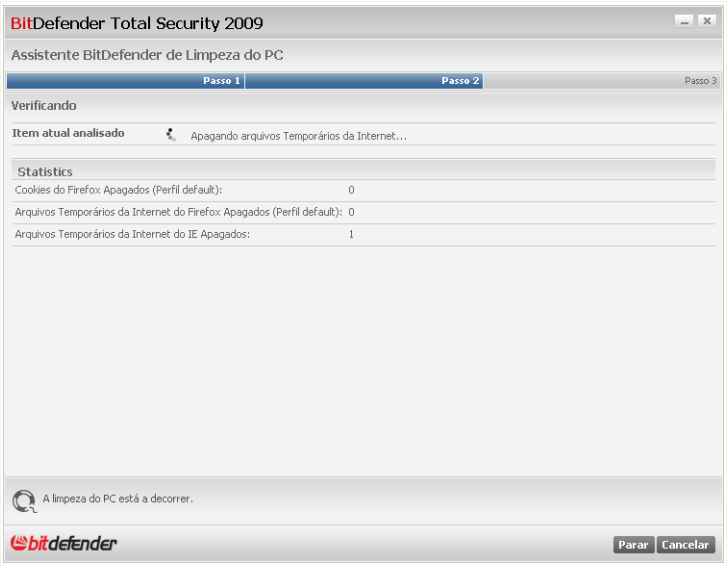


Janela de Boas-Vindas

Clique em **Próximo**.

24.2.2. Passo 2/3 - A eliminar os arquivos...

O eliminador começará a apagar os arquivos temporários da internet e os cookies.



A eliminar os arquivos...

Espere que o Eliminador apague os arquivos temporários da internet e os cookies. Se deseja cancelar a operação clique em **Cancelar**.

24.2.3. Passo 3/3 - Ver Sumário de Resultados

Após o eliminador ter apagados todos os arquivos, uma nova janela surgirá onde poderá ver o sumário de resultados.

Sumário dos Resultados

Pode ver as estatística com respeitos aos objectos apagados.

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

24.3. Apagar arquivos Permanentemente

Quando apaga um arquivo, o mesmo já não fica acessível por meios normais. No entanto o arquivo continua armazenado no disco rígido até que seja sobrescrito quando copiar para lá novos arquivos.

Mesmo que apague o arquivo, o mesmo pode ser recuperado usando programs especializados. Isto poderá representar uma ameaça à sua privacidade pois poderão ocorrer tentativas maliciosas de se apoderarem da sua informação privada.

Para evitar que informação sensível seja recuperada após a apagar, pode usar o BitDefender para apagar permanentemente aqueles dados removendo-os fisicamente do seu disco rígido.

Para remover permanentemente arquivos, siga estes passos:

1. No Modo Avançado, clique em **TuneUp** no menu da esquerda.
2. Clique em **Executar** correspondente ao Destruidor de arquivos.
3. Siga o processo guiado de três passos.

24.3.1. Passo 1/3 - Seleccionar Alvo

Aqui pode especificar os arquivos ou pastas que deseja apagar permanentemente.

Alvo

Clique em **Adicionar Alvo**, e seleccione o arquivo ou pasta que deseja apagar e clique em **OK**. O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela.

Nota
Pode seleccionar um ou vários locais.

Clique em **Próximo**.

24.3.2. Passo 2/3 - A eliminar os arquivos...

O BitDefender apagará permanentemente os arquivos dos locais especificados.

A apagar...

Espere que a operação de eliminação dos arquivos termine. Se deseja cancelar a operação clique em **Cancelar**.

24.3.3. Passo 3/3 - Ver Sumário de Resultados

Após os arquivos terem sido removidos, uma nova janela aparecerá onde poderá ver os resultados.

Sumário dos Resultados

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

24.4. Limpar o Registo do Windows

O Registo do Windows é uma parte importante dos sistemas operacional baseados no Windows. É uma base de dados que contém informação e definições do hardware e do sistema operacional, das aplicações instaladas, usuários, preferências do seu computador e outros.

Muitas aplicações escrevem chaves no Registo do Windows durante a instalação. Quando remove tais aplicações, algumas das suas chaves de registo associadas poderão não ser apagadas e continuarem no seu Registo do Windows, tornando o seu sistema mais lento e até causando instabilidade no mesmo. O mesmo acontece quando apaga atalhos para ou determinados arquivos das aplicações instaladas no seu sistema, como também no caso de drivers corrompidos.

Para limpar o Registo do Windows e melhorar o desempenho do seu sistema, use o Limpa Registo. O Limpa Registo analisa o Registo do Windows e apaga as chaves de registo inválidas.

Para limpar o Registo do Windows, siga os seguintes passos:

1. No Modo Avançado, clique em **TuneUp** no menu da esquerda.
2. Clique no **Executar** correspondente ao Limpador de Registo.
3. Siga o processo guiado de quatro passos.

24.4.1. Passo 1/4 - Iniciar a Análise

Aqui pode dar início à análise do registo.

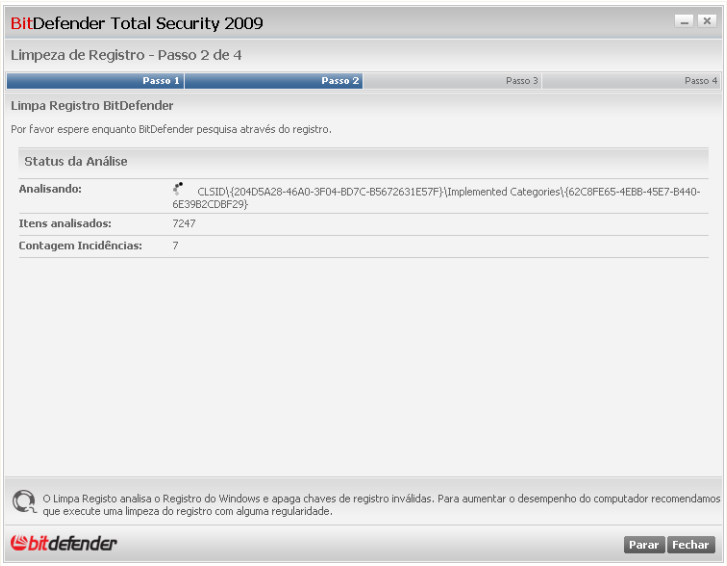
Status

Pode ver quando o Limpa Registo se executou pela última vez e as recomendações do BitDefender.

Clique em **Próximo**.

24.4.2. Passo 2/4 - A analisar...

O Limpa Registo começará a analisar o Registo do Windows.



A analisar...

Pode ver a última chave do registo que foi analisada e as estatísticas relacionadas.

Espere que o Limpa Registo termine a análise do registo. Se deseja cancelar a operação clique em **Cancelar**.

Nota
Se deseja para a análise, apena clique em **Parar**. Saltará de imediato para o próximo passo.

24.4.3. Passo 3/4 - Seleccionar a acção

Após a análise das chaves do registo estar completa, surgirá uma nova janela onde pode ver os resultados.

Nota
Se não forem encontradas quaisquer incidências ou se escolheu parar a análise, saltará este passo.

Ações

Pode ver todas as chaves de registo inválidas ou orfãs detectadas. Informação detalhada é fornecida para cada chave de registo (nome, valor, prioridade, categoria).

As chaves de registo estão agrupadas baseado na sua localização no Registo do Windows:

Categoria	*Descrição*
Localizações do Software	Chaves de registo que contêm informação sobre o caminho para as aplicações instaladas no seu computador. As chaves inválidas têm atribuida uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.
Controles Pessoais	Chaves de registo que contêm informação acerca das extensões dos arquivos registados no seu computador. Estas chaves de registo são normalmente usadas para manter associações de arquivos (para assegurar que o programa correto abre quando abre um arquivo

Categoria	Descrição
	usando o Explorador do Windows). Por exemplo, tal chave de registo permite que o Windows abra um arquivo `.doc` com o Microsoft Word. As chaves inválidas têm atribuida uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.
DLLs partilhadas	As chaves de registo que contêm informação sobre a localização das DLLs (Dynamic Link Libraries) partilhadas. Funções de armazenagem DLLs que são usadas pelas aplicações instaladas para levar a cabo certas tarefas. Podem ser partilhadas por múltiplas aplicações para reduzir os requisitos de espaço em disco e em memória. Estas chaves de registo tornam-se inválidas quando a DLL que apontam é movida para outro local ou completamente removida (isto acontece quando desinstala um programa). As chaves inválidas têm atribuidas uma prioridade média, o que significa que apagá-las pode afectar negativamente o sistema.

Para manusear mais facilmente o processo de limpeza, pode seleccionar a categoria a partir do menu.

Pode escolher apagar todas ou apenas determinadas chaves inválidas de uma categoria específica. Se seleccionou **Apagar todas**, todas as chaves detectadas serão apagadas. Se deseja eliminar somente chaves específicas, seleccione a opção**Apagar** junto da respectiva chave.

Nota
Por defeito, todas as chaves detectadas serão apagadas.

Clique em **Próximo**.

24.4.4. Passo 4/4 - Ver Sumário dos Resultados

Aqui poderá ver os resultados da análise executada pelo Limpa Registo.

Sumário dos Resultados

Se não escolheu apagar todas as chaves de registo, um texto de aviso será apresentado. Recomendamos que reveja as respectivas incidências.

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

24.5. Recuperar Limpeza de Registo

Por vezes, após limparmos o registo, poderá notar que o seu sistema não funciona bem ou que algumas aplicações não funcionam bem devido à falta de chaves no registo. Isto pode ser causado devido a chaves de registo partilhadas que foram apagadas durante a limpeza do registo ou por outras chaves apagadas. Para resolver este problema deverá recuperar o registo que foi limpo.

Para recuperar o registo que foi limpo, siga os seguintes passos:

1. No Modo Avançado, clique em **TuneUp** no menu da esquerda.
2. Clique no **Executar** correspondente ao Restaurador de Registo.
3. Siga o processo guiado de dois passos.

Importante
Apenas os usuários com direitos de administrador no sistema podem recuperar o registo que foi limpo.

24.5.1. Passo 1/2 - Iniciar Recuperação do Registo

Aqui pode dar início à recuperação da limpeza de registo.

Status

Pode ver uma lista de pontos no tempo em que o Registo do Windows foi limpo. Seleccione o ponto no tempo para restaurar o Registo do Windows.

Se tem a certeza que deseja recuperar a chaves de registo que foram apagadas no ponto de tempo seleccionado, clique em **Seguinte**.

Atenção
A recuperação da limpeza de registo pode sobrescrever as últimas chaves do registo que foram editadas desde a última limpeza do registo.

24.5.2. Passo 2/2 - Ver Resultados

Aqui pode ver se a recuperação foi bem-sucedida.

Resultados

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

24.6. Localizar arquivos Duplicados

Os arquivos duplicados comem o seu espaço em disco. Imagine ter o mesmo arquivo `.mp3` aramazenado em três diferentes locais.

Para detectar e apagar arquivo duplicados no seu computador, pode usar o Localizador de Duplicados. Desta forma pode melhorar a gestão do espaço livre nos seus discos rígidos.

Para encontrar arquivos duplicado no seu computador, siga os seguintes passos:

1. No Modo Avançado, clique em **TuneUp** no menu da esquerda.
2. Clique no **Executar** correspondente ao Encontrar arquivos Duplicados.

3. Siga o processo guiado de quatro passos.

24.6.1. Passo 1/4 – Seleccionar o Alvo da Procura

Aqui pode especificar onde deseja procurar duplicados.

Alvo da Procura

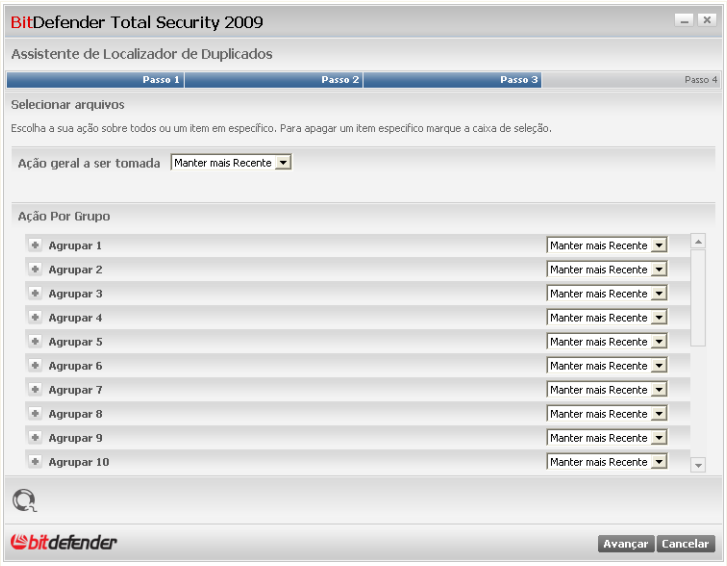
Clique em **Adicionar Alvo**, e selecione o local onde o Localizador de Duplicados deve de procurar por arquivos duplicados. O caminho para o local escolhido aparecerá na coluna **Caminho**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela.

Nota
Pode seleccionar um ou vários locais.

Clique em **Próximo**.

24.6.2. Passo 2/4 - A procurar...

O Localizador de Duplicados começará à procura de arquivos duplicados.



A procurar...

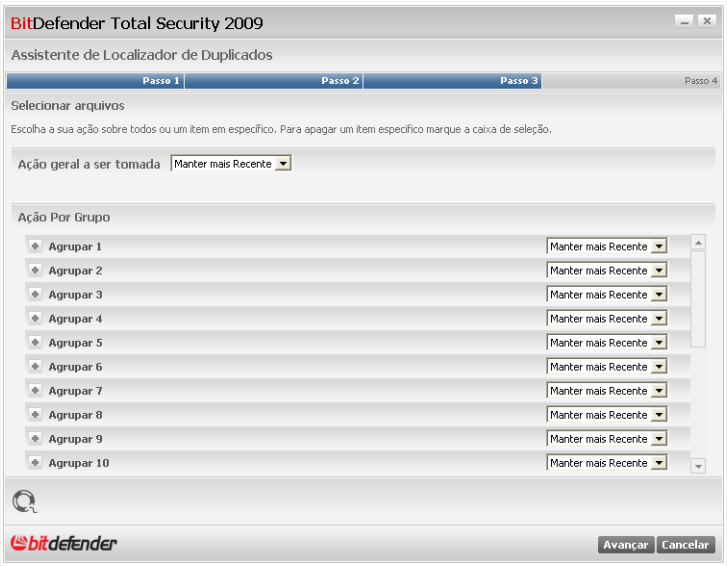
Pode ver o estado da procura e as estatísticas.

Espere que o Localizador de Duplicados complete a sua procura de arquivos duplicados. Se deseja cancelar a operação clique em **Cancelar**.

24.6.3. Passo 3/4 - Seleccionar a acção

Após a procura estar terminada, uma nova janela aparecerá onde pode especificar que ações devem ser tomadas sobre os arquivos duplicados detectados.

Nota
Se não forem encontrados arquivos duplicados, saltará este passo.



Ações

Os arquivos duplicados detectados são organizados e mostrados em grupos. Se clicar em ⊞ junto de um grupo, pode ver info detalhada acerca dos arquivos duplicados (caminho, tamanho, data de criação e modificação).

Pode escolher a acção geral a ser tomada em todos os arquivos duplicados encontrados ou pode escolher ações a serem tomadas em grupos de arquivos duplicados. As seguintes acções estão disponíveis no menu:

Ação	*Descrição*
Manter Recente	O duplicado mais recente será mantido, enquanto que os outros duplicados serão apagados.
Manter Antigo	O duplicado mais antigo será mantido, enquanto que os outros duplicados serão apagados
Nenhuma Acção>	Nenhuma ação será executada sobre os arquivos duplicados.

Se deseja aplicar uma ação geral a todos os objetos de um grupo, selecione a ação desejada do menu correspondente. Se apena deseja especificar arquivos do grupo a serem apagados, selecione a opção **Apagar** ao pé dos respectivos arquivos.

Nota
A ação geral não sobrescreverá a ação escolhida para os arquivos ou grupos especificados. Isto significa, por exemplo que se define **Manter Recente** como a ação geral, mas escolhe não tomar ação sobre um grupo em particular, então a ação geral será aplicada a todos menos a esse grupo em particular.

Clique em **Próximo**.

24.6.4. Passo 4/4 - Ver Sumário dos Resultados

Aqui pode ver os resultados da análise do Localizador de Duplicados.

Sumário dos Resultados

Clique em **Repetir** para iniciar uma nova procura de arquivos duplicados ou clique em **OK** para fechar a janela.

25. Modo de Jogo / Portátil

O módulo do modo de Jogo / Portátil permite-lhe configurar os modos especiais de operação do BitDefender.

- O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema enquanto estiver a jogar.
- O Modo de Portátil evita que as atrefas agendadas sejam executadas quando o seu portátil esteja em modo de bateria de forma a economizar a mesma.

25.1. Modo de Jogo

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

- Todos os alertas e pop-ups do BitDefender são desactivados.
- O nível da protecção em tempo-real do BitDefender é definida como **Permissivo**.
- A Firewall BitDefender está definida para **Permitir todos**. Isto significa que todas as novas ligações (quer de entrada quer de saída) são automaticamente autorizadas, independentemente da porta e do protocolo utilizado.
- As actualizações não são executadas por defeito.

> ***Nota***
> Para mudar esta configuração, vá para Atualizar>Configurações e limpe a **Não atualizar se o Modo Game (Jogo)estiver ativado** selecione a opção.

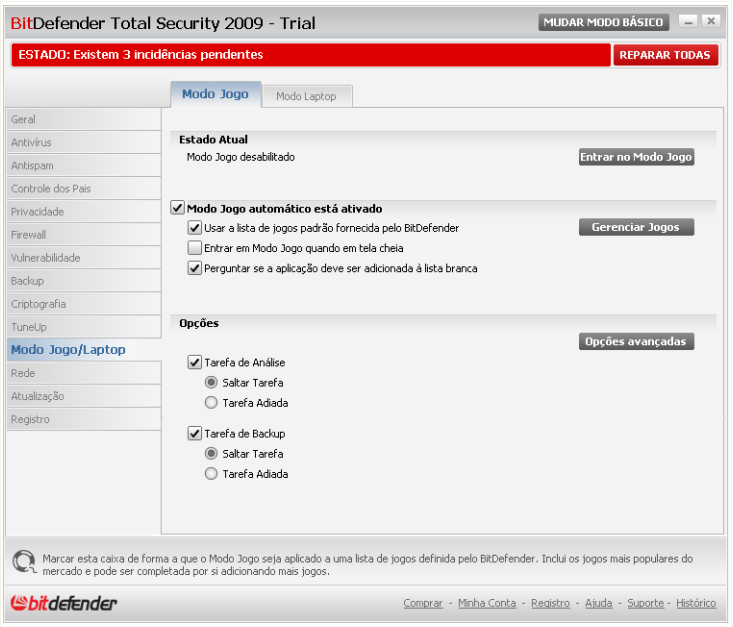
- As tarefas de análise agendadas são desactivadas por defeito.
- As tarefas de backup agendadas são desactivadas por defeito.

Por defeito, o BitDefender entra automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender ou quando uma aplicação entra em Modo de ecrã inteiro. Pode entrar manualmente em Modo de Jogo usando a hotkey por defeito `Ctrl+Alt+Shift+G`. É fortemente recomendado que saia do Modo de Jogo quando acaba de jogar (Pode usar a mesma hotkey por defeito `Ctrl+Alt+Shift+G`).

Nota

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

Para configurar o Modo Jogo, vá para **Modo Jogo/Laptop>Modo Jogo** no Modo Avançado



Modo de Jogo

No topo da secção, pode ver o estado do Modo de Jogo. Clique em **Entrar Modo de Jogo** ou **Sair Modo de Jogo** para alterar o estado actual.

25.1.1. Configurar Modo de Jogo Automático

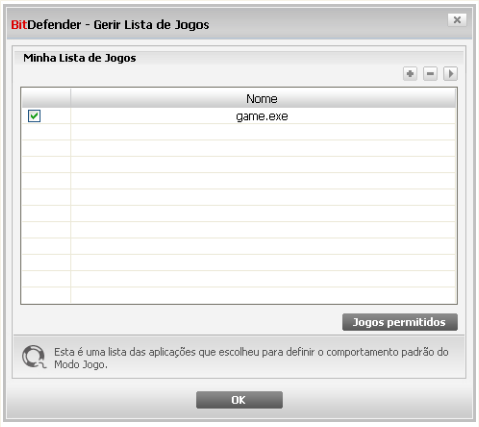
O Modo de Jogo Automático permite que o BitDefender entre automaticamente em Modo de Jogo quando um jogo é detectado. Você pode configurar uma das seguintes opções:

- **Usar por defeito a lista de jogos do BitDefender** - para entrar automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender. Para ver esta lista, cique em **Gerir Jogos** e depois em **Ver Jogos Permitidos**.
- **Entrar em Modo de Jogo quando em ecrã inteiro** - entra automaticamente em Modo de Jogo quando uma aplicação entra em modo de ecrã inteiro.
- **Adicionar a aplicação à lista de jogos?** - para ser notificado a adicionar a nova aplicação à lista de jogos quando deixar o modo de ecrã inteiro. Ao adicionar uma nova aplicação à lista de jogos, da próxima vez que o jogar o BitDefender entrará automaticamente em Modo de Jogo.

Nota
Se não deseja que o BitDefender entre automaticamente em Modo de Jogo, limpe a caixa de selecção **Modo de Jogo Automático**.

25.1.2. Gerir a Lista de Jogos

O BitDefender entra automaticamente em Modo de Jogo quando inicia uma aplicação que se encontra na lista de jogos. Para ver e gerir a lista de jogos, clique em **Gerir Jogos**. Uma nova janela irá aparecer.



Lista de Jogos

Novas aplicações são adicionadas automaticamente à lista quando:

- Inicia um jogo da lista de jogos conhecidos do BitDefender. Para ver esta lista, clique em **Ver Jogos Permitidos**.
- Após sair do modo de ecrã inteiro, pode adicionar a aplicação à lista de jogos a partir da janela de notificação.

Se deseja descativar o Modo de Jogo Automático para uma determinada aplicação da lista, limpe a correspondente caixa de selecção. Deve de desactivar o Modo de Jogo Automático para as aplicações que regularmente entram em modo de ecrã inteiro, tais como os exploradores da Internet e os leitores de filmes.

Para gerir a lista de jogos, pode usar os botões colocados no topo da tabela:

- **Adicionar** - adicionar um novo aplicativo à lista de jogos.
- **Remover** - remover um aplicativo da lista de jogos.
- **Editar** - editar um registro existente na lista de jogos.

Adicionar ou Editar Jogos

Quando adiciona ou edita uma entrada da lista de jogos, a seguinte janela aparecerá:

Adicionar Jogo

Clique em **Explorar** para seleccionar a aplicação e o caminho da mesma no campo de edição.

Se não quiser entrar automaticamente em Modo de Jogo quando a aplicação seleccionada é executada seleccione **Desactivar**.

Clique em **OK** para adicionar a entrada à lista de jogos.

25.1.3. Configurar as Definições do Modo de Jogo

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Tarefa de Análise** - para evitar que as tarefas de análise agendadas se executem enquanto estiver em Modo de Jogo. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executa a tarefa imediatamente após sair do Modo de Jogo.

- **Tarefa de Backup** - evita que a tarefa de backup agendada se execute enquanto o Modo de Jogo estiver ligado. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executa a tarefa imediatamente após sair do Modo de Jogo.

Para desactivar automaticamente a firewall BitDefender enquanto estiver no Modo de Jogo, siga os seguintes passos:

1. Clique em **Configuração Avançada**. Uma nova janela irá aparecer.
2. Marcar a caixa **Não usar firewall** .
3. Clique em **OK** para salvar as alterações.

25.1.4. Mudar a Hotkey do Modo de Jogo

Pode entrar manualmente em Modo de Jogo usando a hotkey por defeito `Ctrl+Alt+Shift+G`. Se deseja mudar a hotkey, siga estes passos:

1. Clique em **Configuração Avançada**. Uma nova janela irá aparecer.

Configurações Avançadas

2. Por baixo da opção **Usar HotKey** , defina a hotkey desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

   Por exemplo, de deseja usar a hotkey `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir `D`.
3. Clique em **OK** para salvar as alterações.

Nota
Remover a selecção ao pé de **Activar HotKey** irá desactivar a hotkey.

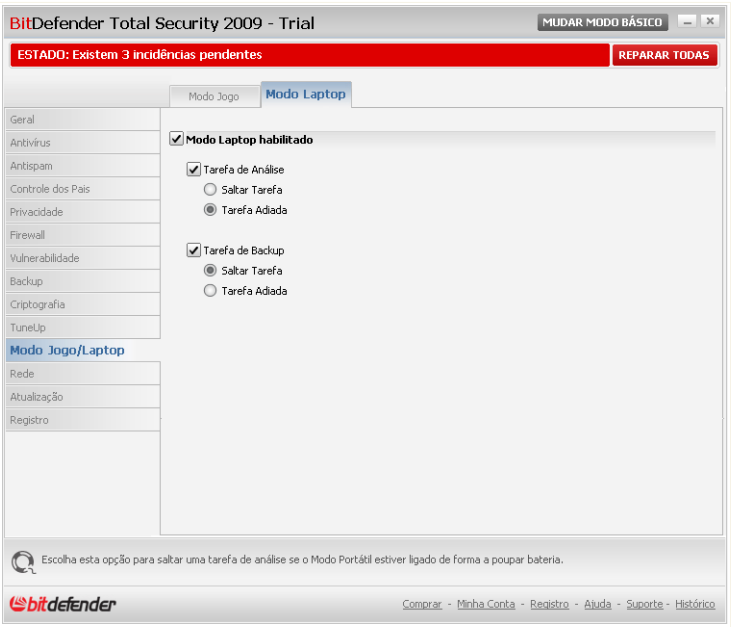
25.2. Modo de Portátil

O Modo Portátil foi especialmente desenhado para os usuários de laptops. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o laptop estiver a funcionar a bateria.

Enquanto estiver em Modo de Portátil, as tarefas agendadas não serão levadas a cabo por defeito.

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

Para configurar o Modo Laptop, vá para **Modo Jogo/Laptop>Modo Laptop** no Modo Avançado



Modo de Portátil

Pode ver se o Modo de Portátil está ou não ligado. Se o Modo de Portátil está ligado, o BitDefender aplicará as definições configuradas para o portátil a funcionar a bateria.

25.2.1. Configurar Definições do Modo de Portátil

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Tarefa de Análise** - para evitar que as tarefas de análise agendadas se executem enquanto estiver em Modo de Portátil. Você pode escolher uma das seguintes opções:

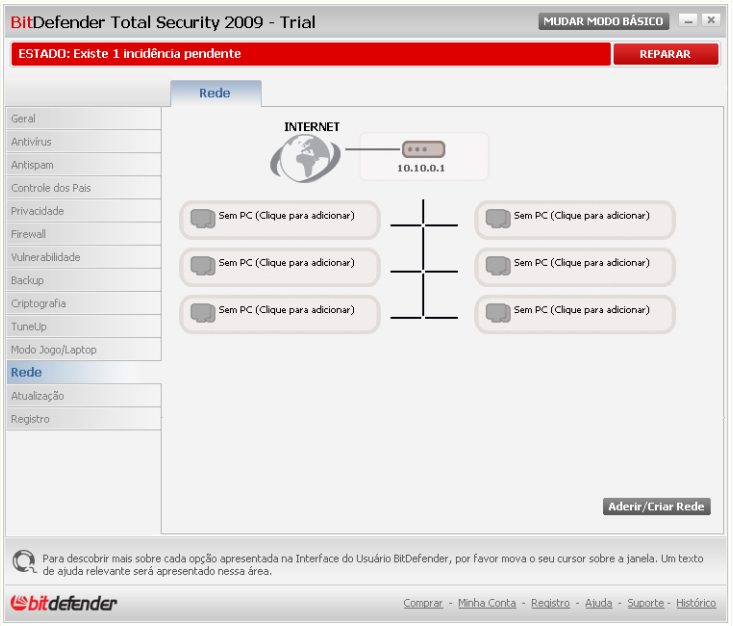
Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada assim que sair do Modo de Portátil.

- **Tarefa de Backup** - evita que a tarefa de backup agendada se execute enquanto o Modo de Portátil estiver ligado. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada assim que sair do Modo de Portátil.

26. Rede

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador.



Mapa de Rede

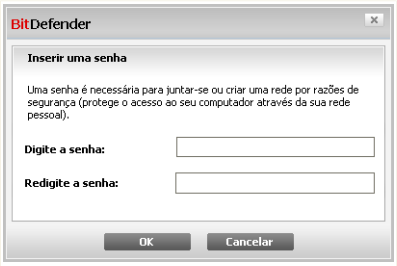
Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

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

26.1. Aderir à Rede BitDefender

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

1. Clique em**Aderir/Criar Rede**.>. Será notificado para configurar a senha de gestão de rede pessoal.



Configurar senha

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

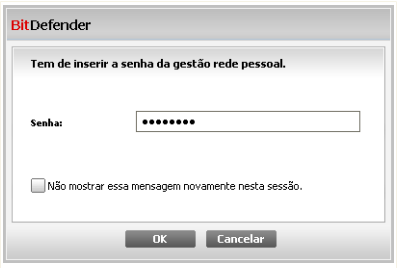
Pode ver o nome do computador a aparecer no mapa de rede.

26.2. Adicionar Computadores à Rede BitDefender

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

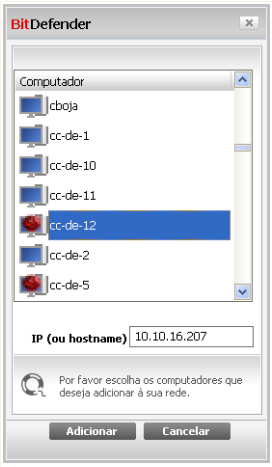
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

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



Inserir senha

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

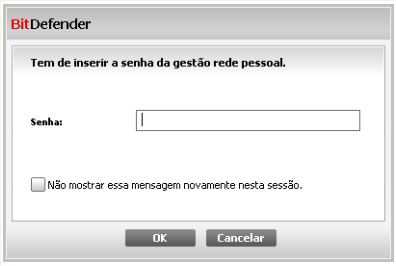


Adicionar Computador

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

- Indica um computador on-line sem produtos BitDefender instalados.
- Indica um computador on-line com o BitDefender instalado.
- Indica um computador offline com o BitDefender instalado.

3. Faça uma das coisas seguintes:
   - Seleccione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
4. Clicando **Adicionar**. Será notificado para inserir a sua senha de gestão de rede pessoal do respectivo computador.



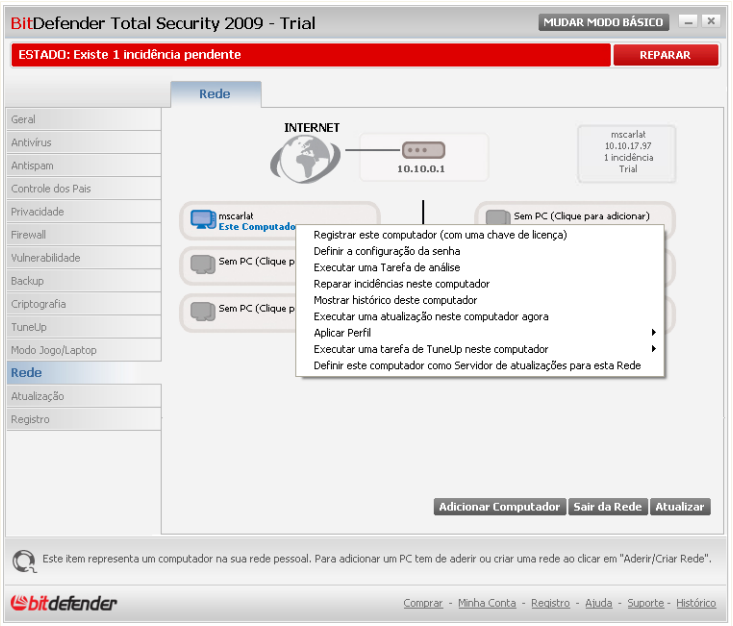
Autenticar

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

Nota
Pode adicionar até cinco computadores neste mapa de rede.

26.3. Gerir a Rede BitDefender

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



Mapa de Rede

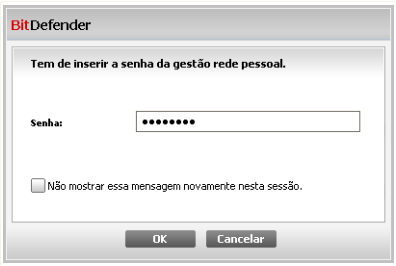
Se mover o curso do seu mouse sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afetar a segurança do sistema, o estado de registo do BitDefender).

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

- **Registar este computador**
- **Definir senha definições**
- **Executar uma tarefa de análise**
- **Reparar incidências neste computador**
- **Mostrar histórico deste computador**
- **Levar a cabo uma actualização neste computador agora**

- **Aplicar Perfil**
- **Levar a cabo uma tarefa de Tuneup neste computador**
- **Definir este computador como Servidor de Actualizações desta Rede**

Antes de levar a cabo uma tarefa num computador específico, será notificado para inserir a senha de gestão de rede pessoal local.



Inserir senha

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

Nota

Se planeia levar a cabo várias tarefas, seleccione **Não me mostrem mais esta mensagem durante esta sessão**. Ao selecionar esta opção, não será notificado novamente pela senha durante esta sessão.

27. Atualização

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

Se você se conectar a Internet através de banda-larga ou DSL, o BitDefender se encarrega da atualização. Ele verifica novas assinaturas de vírus quando você liga o seu computador e toda **hora** depois.

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

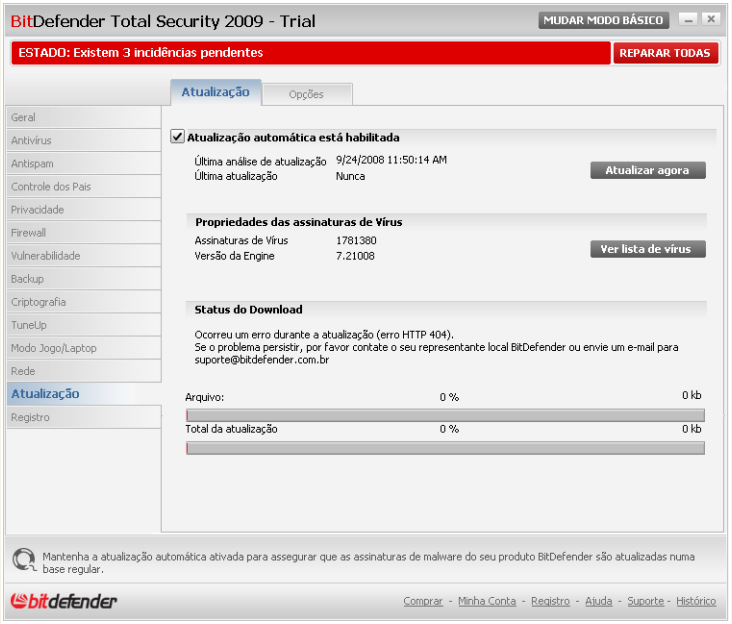
O processo de atualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Atualizações vêm das seguintes formas:

- **Atualização dos mecanismos antivírus** - conforme novas ameaças aparecem, os arquivos contendo as assinaturas de vírus devem ser atualizados para assegurar proteção permanente atualizada contra eles. Esta atualização também é conhecido como **Atualização de Definições de Vírus**.
- **Atualização dos mecanismos Anti-spam** - novas regras serão adicionadas aos filtros heurístico e de URL e novas imagens serão adicionadas ao Filtro de Imagem. Isso ajudará a aumentar a eficácia de seus mecanismos Anti-spam. Esta atualização também é conhecido como **Atualização do Anti-Spam**.
- **Atualizações para os motores anti-spyware** - novas assinaturas de spyware serão adicionadas a base de dados. Esta atualização também é conhecido como **Atualização Anti-spyware**.
- **Atualização do produto** - quando uma nova versão do produto é lançada, novos recursos e técnicas de verificação são introduzidos para aprimorar a performance do produto. Esta atualização também é conhecido como **Atualização de versão do produto**.

27.1. Atualização Automática

Para ver informação relacionada com actualizações e executar actualizações automáticas, clique em **Actualização>Actualização** no Modo Avançado.



Atualização Automática

Aqui poderá ver quando foi feita a última actualização e a última verificação de actualizações, com também a informação da última actualização feita (se bem-sucedida, se ocorreram erros). Também a informação acerca da versão do motor e o número de assinatura 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 assinaturas de malware do seu BitDefender ao clicar **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.

27.1.1. 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**.

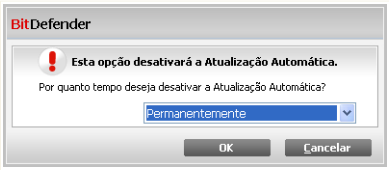
O módulo de **Atualização** irá conectar ao servidor de atualização do BitDefender e verificará se uma atualização está disponível. Caso seja verdadeiro, dependendo das opções configuradas na seção Opções de Atualização Manual você será indagado a confirmar a atualização ou a mesma será feita automaticamente.

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.

27.1.2. Desabilitar Atualização Automática

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



Desabilitar Atualização Automática

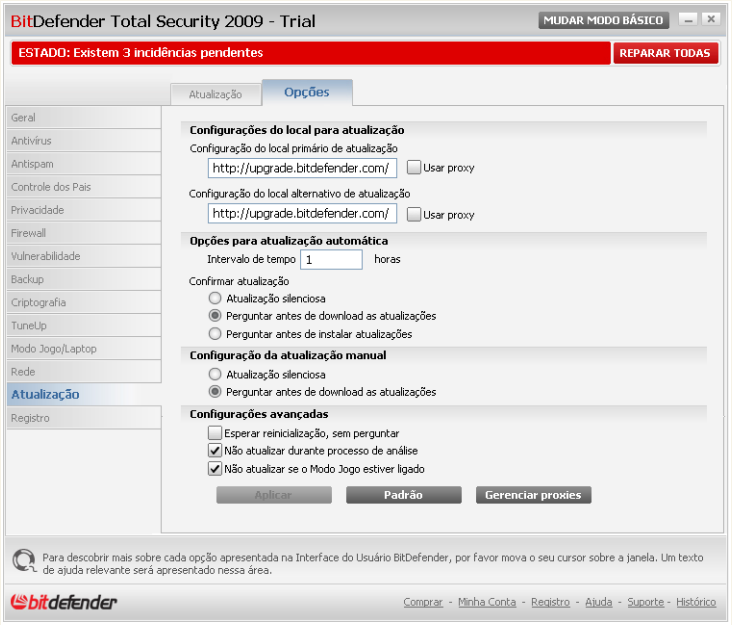
Tem de confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a actualização automática fique desactivada. Pode desactivar a actualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção
Esta é uma incidência de segurança critica. recomendamos que desactive a actualização automática pelo menor tempo possível. Se o BitDefender não for actualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.

27.2. Opções de Actualização

Atualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy. Por defeito, o BitDefender verificará as actualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

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



Opções de Actualização

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.

27.2.1. 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 ligado a uma rede local que armazena localmente as assinaturas 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. 392)

27.2.2. Configurar Atualização Automática

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

Pode definir o intervalo entre duas verificações consecutivasde actualizações no campo **Interval Tempo**. Por defeito, o intervalo de tempo da actualização é de 1 hora.

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.

27.2.3. 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.

27.2.4. 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.

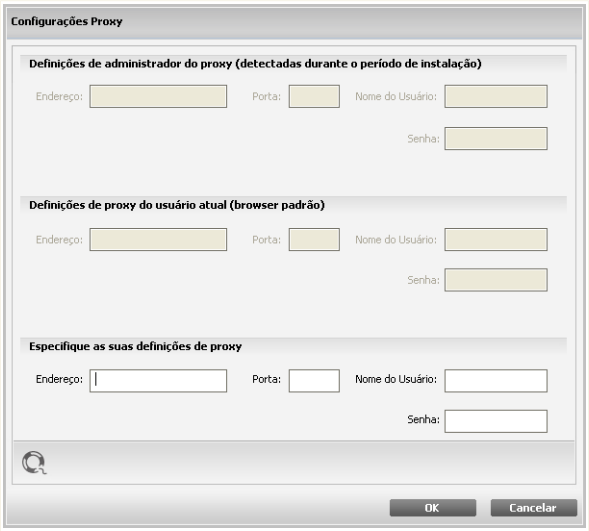
- **Não actualizar se o modo de jogo estiver ligado** - O BitDefender não actualizará se o Modo de Jogo estiver ligado. Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.

27.2.5. 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.

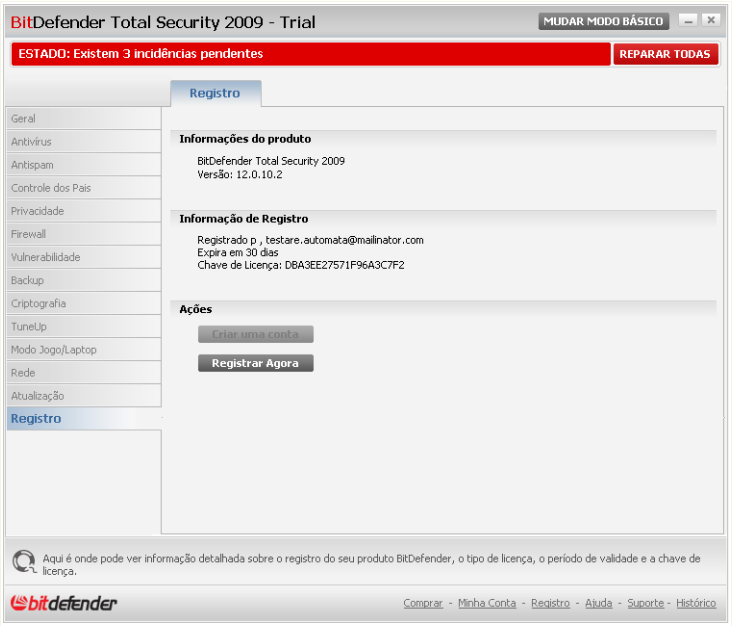
Primeiro, o conjunto que contém as suas definições do proxy será utilizado para ligar a Internet. Se esse não funcionar, as definições de proxy detectadas durante a instalação serão experimentadas logo a seguir. Finalmente se nenhuma dessa funcionar, as definições de proxy do usuário atual serã retiradas 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.

28. Registro

Para saber toda a informação sobre o seu produto BitDefender e o estado do registo, clique em**Registo** no Modo Avançado.



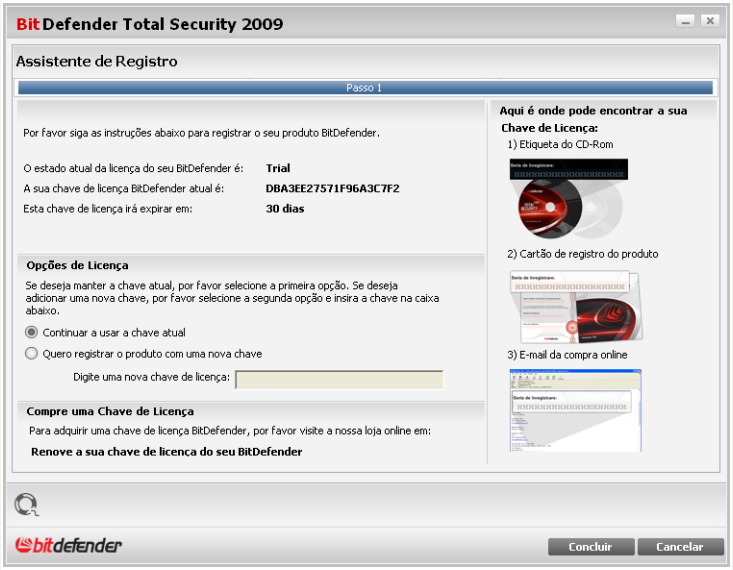
Registro

Esta secção mostra:

- **Informação do Produto** : O produto BitDefender e a sua versão.
- **Informação de Registo** : o endereço de e-mail usado para entrar na sua conta BitDefender (se configurada), a actual chave de licença e o número de dias que faltam para a licença expirar.

28.1. Registar o BitDefender Total Security 2009

Clique em **Registar agora** para abrir a janela de registo do produto.



Registro

Pode ver o estado do registo do BitDefender, a actual chave de licença e quantos dias faltam para a licença expirar.

Para registar o BitDefender Total Security 2009:

1. Seleccione **Desejo registar o produto com uma nova chave**.
2. Insira a chave de licença no campo de edição.

Nota

Pode encontrar a sua chave de licença:

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

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

Clique em **Finalizar**.

28.2. Criar uma conta BitDefender

Como parte do processo de registro, você PRECISA criar sua conta BitDefender. A sua cnta BitDefender lhe oferece acesso às atualizações de virus BitDefender, suporte técnico grátis, além de ofertas e promoções especiais. Se perder a sua chave de licença BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Importante

Você precisa se registrar criando uma conta dentro de 15 dias após ter instalado BitDefender (se você o fizer, o prazo limite se extenderá para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivirus.

Se ainda não criou uma conta BitDefender, clique em **Criar uma conta** para abrir a janela de registo da conta do produto

Criar uma Conta

Se não deseja criar uma conta BitDefender neste momento, seleccione **Saltar o registo** e clique em **Terminar**. De outra forma, actue de acordo com a sua presente situação:

- “Não tenho uma conta BitDefender” (p. 398)
- “Já tenho uma conta BitDefender” (p. 399)

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 pelo menos seis caracteres em 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.

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**

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.

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**

Clique em **Finalizar**.

Ajuda

29. Suporte

Como um fabricante de valor agregado, a BitDefender garante um nível de serviço sem precedentes de suporte rápido e qualificado. O Centro de Suporte (cujo endereço é providenciado em baixo) mantém-se continuamente atualizado contra as ameças mais recentes. É aqui onde obterá respostas e a informação necessária de uma forma rápida.

Com o BitDefender, tem sido sempre a nossa prioridade poupar aos nossos clientes tempo e dinheiro ao fornecer-lhes os produtos mais avançados aos preços mais económicos. Mais ainda, pensamos que um negócio de sucesso é baseado numa boa comunicação e num compromisso de excelência no suporte ao cliente.

Convidamo-lo desde já a colocar as suas questões em suporte@bitdefender.com.br a qualquer altura. Para uma resposta rápida, por favor inclua no seu e-mail o máximo de detalhes que consiga sobre seu BitDefender, seu sistema e uma descrição do problema tão completa e fiel quanto possível.

29.1. BitDefender Knowledge Base

O BitDefender Knowledge Base é um repositório on-line de informação sobre os produtos BitDefender. Ele armazena em formato facilitado relatórios sobre resultados de problemas técnicos e questionamentos sendo analisados pela equipe de suporte e desenvolvimento BitDefender, com artigos de informações gerais sobre prevenção de vírus, gerenciamento das soluções e explicações detalhadas.

O BitDefender Knowledge Base é aberto ao público e gratuito. Este rico meio de informação é outra forma de providenciar aos clientes BitDefender conhecimento técnico e visão necessária. Todas as requisições sobre problemas encontrados por clientes BitDefender eventualmente acabam chagando ao BitDefender Knowledge Base, como relatórios de bugfix e arquivos de ajuda.

O BitDefender Knowledge Base está disponível em http://kb.bitdefender.com.

29.2. Pedir Ajuda

29.2.1. Vá até ao Self-Service Web

Tem uma dúvida? Os nossos peritos em segurança estão disponíveis para o ajudar 24/7 via e-mail ou chat sem custos adicionais.

Por favor siga os seguintes links:

English

http://www.bitdefender.com/site/KnowledgeBase/

German

http://www.bitdefender.com/de/KnowledgeBase/

French

http://www.bitdefender.com/fr/KnowledgeBase/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/

29.2.2. Abrir um ticket de suporte

Se deseja abrir um ticket de suporte e receber ajuda via e-mail, siga os seguintes links:

English: http://www.bitdefender.com/site/Main/contact/1/
German: http://www.bitdefender.de/site/Main/contact/1/
French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

29.3. Informação sobre contato

Comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

29.3.1. Brasil

Telefone: +55-11-5506-8630
Fax: +55-11-5506-8630
Vendas: http://www.bitdefender.com/links/br/2009/buy/total-security.html
Suporte Técnico: http://www.bitdefender.com/links/br/2009/support/total-security.html
Página Web: http://www.bitdefender.com/links/br/homepage.html

CD de Resgate BitDefender

30. Sumário

O BitDefender Total Security 2009 vem num CD de arranque (Cd de Emergência BitDefender), capaz de analisar e desinfectar todos os discos rígidos antes do seu sistema operacional iniciar.

Você deve usar o CD de Resgate BitDefender a qualquer momento que o seu sistema operacional não estiver funcionando corretamente por infecção de vírus. Isto normalmente acontece quando você não usa um produto antivírus.

A atualização das assinaturas de vírus é feita automaticamente, sem a intervenção do usuário quando você executa o CD de Resgate BitDefender.

O CD de Emergência BitDefender é uma distribuição do Knoppix recompilada por BitDefender, que integra a mais recente solução BitDefender de segurança para Linux dentro do CD ao Vivo GNU/Linux Knoppix, que lhe oferece uma protecção instantânea de antivírus que é capaz de analisar e desinfectar discos duros existentes (incluindo partições Windows NTFS. Ao mesmo tempo, o CD de Emergência BitDefender pode ser usado para recuperar a sua preciosa informação quando não consegue arrancar com o Windows.

Nota
O CD de Emergência BitDefender pode ser descarregado a partir deste local na net: http://download.bitdefender.com/rescue_cd/

30.1. Requisitos de Sistema

Antes de arrancar com o CD de Emergência BitDefender, deve em primeiro lugar verificar se o seu sistema possui os seguintes requisitos.

Processador
Compatível com x86, mínimo de 166 MHz. Um processador de geração i686, de 800MHz, seria uma melhor escolha mínima.

Memória
512 MB de memória RAM (1 GB recomendado)

CD-ROM
O CD de Emergência BitDefender, é executado a partir do CD-ROM, logo um CD-ROM e uma BIOS capaz de arrancar a partir do mesmo são necessários.

Conexão a Internet
Apesar de o CD de Emergência BitDefender se executar sem ligação à Internet, os processos de actualização requerem uma ligação HTTP activa, mesmo que seja através de um servidor proxy. Logo, para ter uma protecção actualizada, a Ligação à Internet tem de EXISTIR.

Resolução gráfica
Placa gráfica Standard SVGA compatível.

30.2. Software incluído

O CD de Resgate BitDefender inclui os seguintes pacotes de programas.

Xedit
Este é um arquivo de um editor de texto.

Vim
Este é um poderoso arquivo de um editor de texto, contendo uma sintaxe highlighting, uma GUI e muito mais. Para mais informação consulte a página web da Vim.

Xcalc
Este é uma calculadora.

RoxFiler
RoxFiler é um rápido e poderoso gestor de arquivos gráficos.

Para mais informação, consultar a página internet da RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) um gestor de arquivos em modo de texto.

Para mais informação, consultar apágina internet da MC.

Pstree
Pstree mostra processos que estão a decorrer.

Top
Top mostra as tarefas do Linux.

Xkill
Xkill mata um cliente com os seus recursos X.

Partition Image

Partition Image ajuda-o a guardar partições em arquivos de sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 para um arquivos de imagem. Este programa pode ser útil para propósitos de backup.

Para mais informação, consulte a página web da Partimage.

GtkRecover

GtkRecover é uma versão da GTK da recuperação do prgrama de consola. Ajuda-o a recuperar um arquivo.

Para mais informação, consulte a página web da GtkRecover.

ChkRootKit

ChkRootKit é uma ferramenta que o ajuda a analisar o seu computador em busca de rootkits.

Para mais informação, consulte a página web do ChkRootKit.

Nessus Network Scanner

Nessus um analisador remoto de segurança para Linux, Solaris, FreeBSD, e Mac OS X.

Para mais informação, consulte a página web do Nessus.

Iptraf

Iptraf é um Software de Monitorização de Rede por IP.

Para mais informação, consulte a página web do Iptraf.

Iftop

Iftop mostra num interface o grau de utilização de banda.

Para mais informação, consulte a página web do Iftop.

MTR

MTR é uma ferramenta de diagnóstico de rede.

Para mais informação, consulte a página web da MTR.

PPPStatus

PPPStatus mostra as estatísticas acerca do tráfego TCP/IP de entrada e saída.

Para mais informação, consulte a página web da PPPStatus.

Wavemon

Wavemon uma aplicação de monitorização para dispositivos de redes wireless.

Para mais informação, consulte a página web da Wavemon.

USBView

USBView mostra informação acerca de dispositivos ligados ao USB bus.

Para mais informação, consulte a página web da USBView.

Pppconfig

Pppconfig ajuda-o a definir automaticamente uma ligação por dial up ppp.

DSL/PPPoe

DSL/PPPoe configura uma ligação PPPoE (ADSL).

I810rotate

I810rotate toggles o video output em i810 hardware usando o i810switch(1).

Para mais informação, consulte a página internet da I810rotate.

Mutt

Mutt é um poderoso cliente de e-mail MIME baseado em texto.

Para mais informação, consulte a página internet da Mutt.

Mozilla Firefox

Mozilla Firefox é um browser de internet bastante conhecido.

Para mais informação, consulte a página internet da Mozilla Firefox.

Elinks

Elinks um browser de internet em modo de texto.

Para mais informação, consulte a página internet da Elinks.

31. Como Usar o CD de Emergência BitDefender

Este capítulo comtém informação sobre como começar e parar o CD de Emergência BitDefender, analisar o seu computador em busca de malware como também guardar dados do seu comprometido PC Windows para um dispositivo amovível. No entanto ao usar as aplicações que vem com o CD, pode fazer muita tarefas cuja descripção vai muito para além deste manual de usuário.

31.1. Iniciar CD de Resgate BitDefender

Para iniciar o CD, configure a BIOS do seu computador para iniciar diretamente do CD, coloque o CD no drive e reinicie o computador. Tenha certeza que o seu computador pode iniciar do CD.

Espere até a próxima tela aparecer e siga as instruções na tela para iniciar o CD de Resgate BitDefender.

Nota

Seleccione a linguagem que deseja usar para o CD de Emergência a partir da lista disponível.

Boot Splash Screen

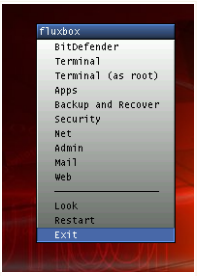
A actualização das assinaturas dos vírus é feita automaticamente, cada vez que arranca com o Cd de Emergência do BitDefender. Isto pode demorar um pouco.

Quando o processo finalizar você verá o próximo desktop. Você pode agora usar o CD de Resgate BitDefender.

O Desktop

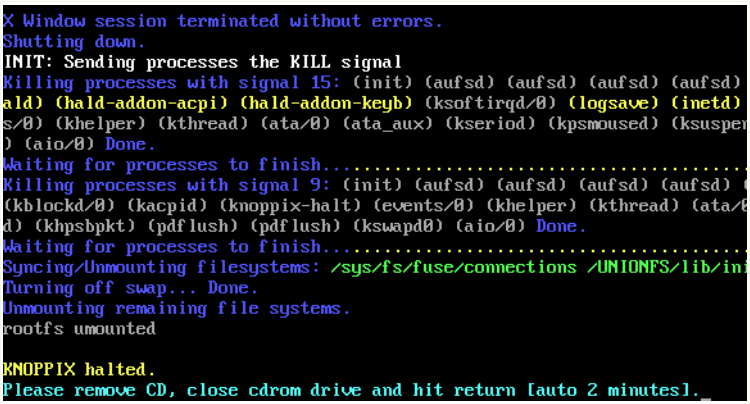
31.2. Parar o CD de Resgate BitDefender

Pode desligar em segurança o seu computador ao seleccionar **Sair** a partir do menu do CD de Emergência BitDefender (clique botão-direito para o abrir) ou ao emitir o comando **halt** num terminal.



Escolha "EXIT"

Quando o CD de Emergência BitDefender fechar com sucesso todos os programas mostra-lhe uma tela como a imagem seguinte. Pode remover o CD de forma a arrancar pelo seu disco rígido. Agora é OK desligar o seu computador ou reiniciá-lo.



Espere por esta mensagem enquanto estiver a desligar

31.3. Como executo uma verificação antivírus?

Um assistente aparecerá quando o processo de arranque terminar e permite-lhe analisar totalmente o seu computador. Tudo o que tem de fazer é clicar no botão **Iniciar** .

Nota
Se a resolução do seu ecrã não for suficiente, ser-lhe-á solicitado que inicie a análise em modo de texto.

Siga o processo guiado de três passos para completar o processo de análise.

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

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

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

   As incidências são mostradas em grupos. Clique na caixa com "+" para abrir um grupo ou na caixa com "-" para fechar um grupo.

Pode escolher uma acção geral a ser tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.

3. Pode ver o sumário dos resultados.

Se deseja analisar uma determinada directoria apenas, faça o seguinte:

Navegue pelas pastas, clique com o botão direito em um arquivo ou pasta e selecione **Enviar**. Então escolha **BitDefender Scanner**.

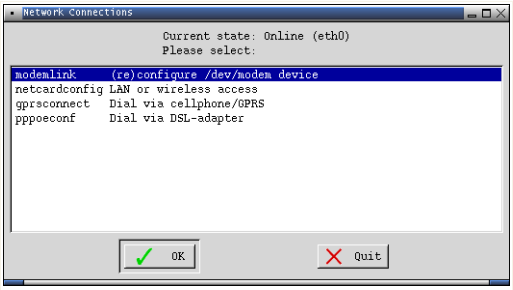
Ou você pode digitar o próximo comando no terminal. O **BitDefender Antivirus Scanner** irá começar pelo arquivo ou pasta selecionada como local padrão de verificação.

```
# bdscan /path/to/scan/
```

31.4. Como posso configurar a Ligação à Internet?

Se você estiver em uma rede DHCP e você tiver uma placa de rede ethernet, uma conexão de Internet já deveria estar detectada e configurada. Para uma configuração manual, siga os próximos passos.

1. Duplo Clique sobre o atalho das Ligações de Rede no Ambiente de Trabalho. A seguinte janela irá aparecer:



Ligações de Rede

2. Seleccione o tipo de ligação que está a usar e clique em OK.

Conexão	Descrição
modemlink	Seleccione este tipo de ligação quando está a usar um modem e uma ligação telefónica para aceder à Internet.
netcardconfig	Seleccione este tipo de ligação quando está a usar uma rede de área local (LAN) para aceder à Internet. É também utilizada para ligações sem fios.
gprsconnect	Seleccione este tipo de ligação quando está a usar uma rede de telemóvel com o protocolo GPRS (General Packet Radio Service). Também pode estar a usar um modem GPRS em vez de um telemóvel.
pppoeconf	Seleccione este tipo de ligação quando estiver a usar um modem DSL (Digital Subscriber Line) para aceder à Internet.

3. Siga as instruções na tela. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.

Importante
Tenha em mente que apenas activou o modem ao seleccionar as opções acima mencionadas. Para configurar a ligação à rede siga estes passos.

1. Clique botão direito do mouse sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
2. Seleccione **Terminal (como raiz)**.
3. Insira os seguintes comandos:

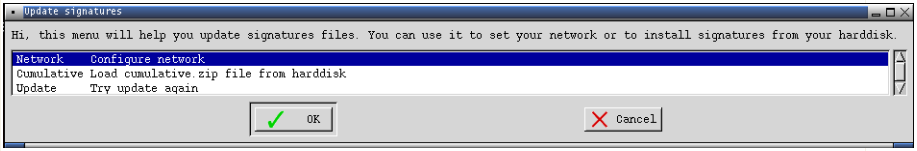
```
# pppconfig
```

4. Siga as instruções na tela. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.

31.5. Como eu posso atualizar o BitDefender?

A actualização das assinaturas dos vírus é feita automaticamente, cada vez que arranca com o Cd de Emergência do BitDefender. Mas se saltar este passo, emtão siga os passos seguinte para actualizar o BitDefender.

1. Duplo clique no atalho da Actualização de assinaturas no Ambiente de Trabalho. A seguinte janela irá aparecer.



Actualização de Assinaturas

2. Faça uma das coisas seguintes:
   - Selecione **Cumulativa** para instalar as assinaturas guardadas no seu disco rigido devido a ter descarregado no seu computador o arquivo `cumulative.zip`.
   - Seleccione **Actualização** para ligar-se imediatamente à internet e descarregar as últimas assinaturas de vírus.
3. Clique em **OK**.

31.5.1. Como posso actualizar o BitDefender através de um proxy?

Se existe um servidor proxy entre o vosso computador e a internet, algumas configurações têm de ser feitas de forma a poder actualizar o seu BitDefender.

Para actualizar o BitDefender através de um proxy, siga os seguintes passos:

1. Clique botão direito do mouse sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
2. Seleccione **Terminal (como raiz)**.
3. Digite o comando: **cd /ramdisk/BitDefender-scanner/etc**.
4. Digite o comando: **mcedit bdscan.conf** para editar este arquivo usando o GNU Midnight Commander (mc).
5. Uncomment a seguinte linha: `#HttpProxy =` (apenas apague o sinal `#`) e especifique o domínio, nome, senha e a porta do servidor proxy. Por exemplo, a linha respectiva deverá parecer-se com o seguinte:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Prima **F2** para guardar o arquivo atual, confirme o guardar, e depois prima **F10** para o fechar.
7. Digite o comando: **bdscan update**.

31.6. Como posso salvar os meus dados?

vamos partir do principio que não consegue arrancar o seu PC em Windows PC devido a incidências desconhecidas. Ao mesmo tempo, você necessita desesperadamente de aceder a alguma informação importante do seu computador. Eis aqui uma situação em que o CD de Emergência BitDefender se revela extremamente útil.

Para guardar os seus dados do computador para um dispositivo amovível, tal como um stick de memória USB, siga os seguintes passos:

1. Coloque o CD de Emergência BitDefender na drive de CDs, e o stick de memória na entrada USB e depois reinicie o computador.

   Nota

   Se conectar o stick de memória mais tarde, tem de montar o dispositivo amovível seguindo os seguintes passos:

   a. Faça duplo-clique com o rato sobre o atalho do Terminal Emulator no Ambiente de Trabalho.
   b. Insira o seguinte comando:

      ```
      # mount  /media/sdb1
      ```

      Lembre-se que dependendo da configuração do seu computador poderá ser `sda1` em vez de `sdb1`.

2. Espere que o CD de Emergência BitDefender termine de arrancar o PC. A seguinte janela irá aparecer.

Ecrã de Ambiente de Trabalho

3. Faça duplo clique sobre a partição onde os dados que deseja salvar se encontram (ex. `[sda3]`).

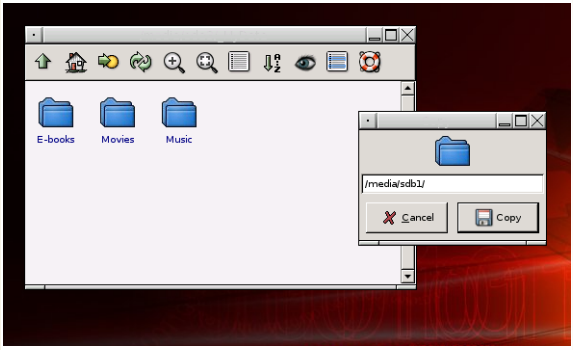
Nota
Quando está a trabalhar com o CD de Emergência BitDefender, estará a lidar com nomes de partições baseado em Linux. Assim, `[sda1]` provavelmente corresponderá à partição Windows `(C:)`, `[sda3]` a `(F:)`, e `[sdb1]` ao stick de memória.

Importante
Se o computador não for desligado correctamente, é possível que certas partições não sejam montadas automaticamente. Para montar uma partição siga estes passos.

a. Faça duplo-clique com o rato sobre o atalho do Terminal Emulator no Ambiente de Trabalho.
b. Insira o seguinte comando:

```
# mount  /media/partition_name
```

4. Explore as suas pastas e abra a directoria que deseja. Por exemplo, `Meus Dados` que contém as sub-directorias`Filmes`, `Música` e `E-books` .
5. Clique botão direito do mouse sobre o diretorio desejado e selecione **Copiar**. A seguinte janela irá aparecer:



Guardar Dados

6. Insira `/media/sdb1/` na correspondente caixa de texto e clique em **Copiar**.

   Lembre-se que dependendo da configuração do seu computador poderá ser `sda1` em vez de `sdb1`.

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.

Atualização

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.