bitdefender
internet security 2010

Manual do Utilizador

BitDefender Internet Security 2010
Manual do Utilizador

Publicado 2009.08.04

Aviso Legal


bitdefender

Índice

Acordo de Licença de Utilizador do Software

SE NÃO CONCORDA COM ESTES TERMOS E CONDIÇÕES NÃO INSTALE O SOFTWARE. AO SELECCIONAR "EU ACEITO", "OK", "CONTINUAR", "SIM" OU AO INSTALAR E USAR O SOFTWARE DE QUALQUER FORMA, ESTÁ A AFIRMAR QUE COMPREENDEU COMPLETAMENTE E ACEITOU OS TERMOS DE ESTE ACORDO.

REGISTO DO PRODUTO. Ao aceitar este Acordo, está a concordar em registar o Seu Software, usando "A Minha Conta BitDefender", como condição do Seu Uso do Software (receber actualizações) e o Seu direito à Manutenção. Este controlo assegura que o Software apenas está a funcionar em computadores devidamente licenciados e que os utilizadores que se encontram devidamente licenciados recebem os serviços de Manutenção. O Registo requer uma chave de licença válida e um endereço de e-mail válido para aviso de renovação e outros avisos legais.

Estes termos abrangem as Soluções e Serviços BitDefender para utilizadores individuais que lhe foram licenciadas, incluindo documentação relacionada, updates (actualizações 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 não concorda com os termos deste acordo, não instale ou use o BitDefender.

Licença BitDefender. O BitDefender está protegido pelas leis de autor e pelos tratados internacionais de reprodução, 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 utilizador. Pode fazer uma cópia adicional para efeitos de back-up (cópia de segurança).

LICENÇA DE UTILIZADOR DE COMPUTADOR INDIVIDUAL. Esta licença aplica-se ao software BitDefender que pode ser instalado num único computador que não providencie serviços de rede. O utilizador primário pode instalar este software num único computador e fazer uma cópia adicional num dispositivo distinto para efeitos

de backup. O número de utilizadores primários permitidos corresponde ao número de utilizadores 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 correctamente 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 utilizadores 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.

DIREITOS DE AUTOR. 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.

EXCEPTO 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, EXACTIDÃO DOS DADOS, EXACTIDÃO DO CONTEÚDO INFORMATIVO, INTEGRAÇÃO DE SISTEMAS, NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS AO FILTRAR, DESACTIVAR OU REMOVER O SOFTWARE DE TERCEIROS, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTOS, PUBLICIDADE OU SEMELHANTE, QUER SURJAM POR ESTATUTO, LEI, NO CURSO DE TRANSAÇÕES, POR COSTUME E HÁBITO, OU USO COMERCIAL.

RENÚNCIA DE DANOS. Qualquer pessoa que use, teste, ou avalie o BitDefender suporta todo o risco pela qualidade e desempenho do BitDefender. A BITDEFENDER não será responsável, em nenhuma circunstância, de qualquer dano de qualquer tipo, incluindo, sem limitação, danos directos ou indirectos provenientes do uso, desempenho, ou entrega do BitDefender, mesmo que a BITDEFENDER tenha sido avisada da existência ou possibilidade de tais danos.

ALGUNS ESTADOS NÃO PERMITEM A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE DE INCIDENTES OU DANOS CONSEQUENTES, POR ISSO A LIMITAÇÃO ACIMA INDICADA PODERÁ NÃO SE APLICAR A SI.

EM NENHUM CASO O RISCO DA BITDEFENDER PODERÁ EXCEDER O PREÇO QUE PAGOU PELO BITDEFENDER. As renúncias e limitações, estabelecidas acima, aplicar-se-ão independentemente se aceita usar, avaliar ou testar o BitDefender.

AVISO IMPORTANTE AOS UTILIZADORES. ESTE SOFTWARE NÃO É À PROVA DE FALHAS E NÃO ESTÁ DESENHADO PARA USO INTENCIONAL EM AMBIENTES DE RISCO QUE REQUEREM UMA PERFORMANCE À PROVA DE FALHAS. ESTE SOFTWARE NÃO ESTÁ INDICADO PARA SER USADO EM OPERAÇÕES DE NAVEGAÇÃO AÉREA, EM INSTALAÇÕES NUCLEARES, OU SISTEMAS DE COMUNICAÇÕES, SISTEMAS DE ARMAMENTO, DIRECTA OU INDIRECTAMENTE EM SISTEMAS DE APOIO À VIDA, CONTROLO DE TRÁFEGO AÉREO, OU QUALQUER APLICAÇÃO OU INSTALAÇÃO, ONDE A FALHA PODE RESULTAR EM MORTE, DANOS FISÍCOS GRAVES OU DANOS DE PROPRIEDADE.

CONSENTIMENTO DE COMUNICAÇÕES ELECTRÓNICAS. A BitDefender poderá ter necessidade de enviar-lhe avisos legais e outras comunicações acerca do Software e dos serviços de subscripção e Manutenção ou usar a informação que nos envia ("Comunicações"). BitDefender enviar-lhe-á Comunicações via avisos do produto ou via e-mail para o endereço de e-mail do utilizador primário registado, ou colocará Comunicações nos seu Sites. Ao aceitar este Acordo, está a consentir receber todas as Comunicações através deste meios electrónicos e acusar a recepção e demonstrar que pode aceder às Comunicações nos Sites.

RECOLHA DE DADOS TECNOLOGIA-BitDefender informa que, em certos programas ou produtos podem utilizar tecnologia de recolha de dados para recolher informações técnicas (incluindo os arquivos suspeitos), para melhorar os produtos, a prestação de serviços conexos, para adaptá-las e evitar a utilização ilegal, sem licença de produto ou os danos resultantes de produtos de malware . Aceite que o BitDefender use essas informações como parte dos serviços prestados em relação ao produto e para prevenir e que programas de malware em execução no seu computador.

Reconhece e aceita que o BitDefender pode fornecer atualizações ou complementos para o programa ou produto que serão automaticamente descarregados para o seu computador.

Ao aceitar este Acordo, Aceita fazer upload os ficheiros executáveis com o objectivo de serem analisados pelos servidores da BitDefender. Da mesma forma, para fins de contratação e utilização de programas, poderá ter de fornecer dados pessoais à BitDefender. A BitDefender informa-o que tratará dos seus dados pessoais de acordo com a legislação aplicável e com a Política de Privacidade.

RECOLHA DE DADOS. O acesso ao site do usuário e da aquisição de produtos e serviços ea utilização de instrumentos ou de conteúdo através do site implica o tratamento de dados pessoais. Conformes com a legislação que rege o tratamento de dados pessoais e serviços da sociedade da informação e do comércio electrónico é de extrema importância para a BitDefender. Às vezes, para o acesso a produtos, serviços, conteúdo e ferramentas, será em alguns casos, terá a necessidade de fornecer certas informações pessoais. O BitDefender garante que tais dados sejam tratados confidencialmente e em conformidade com a legislação relativa à protecção dos dados pessoais e da sociedade da informação e comércio electrónico.

A BitDefender cumpre a legislação aplicável à protecção de dados, e tomou as medidas administrativas e técnicas necessárias para garantir a segurança dos dados pessoais que recolhe.

Declara que todos os dados que forneceu são verdadeiros e precisos e compromete-se a informar a BitDefender de quaisquer alterações a esses dados. Tem o direito de se opor ao tratamento de qualquer dos seus dados que não são essenciais para a execução do acordo e à sua utilização, para outros fins, que não a manutenção da relação contratual.

No caso de fornecer detalhes de um terceiro, a BitDefender não deve ser responsabilizada pelo cumprimento dos princípios da informação e consentimento, e deve, portanto, ser você a garantir que informou previamente o terceiro e obteve o seu consentimento, no que se refere à comunicação de tais dados.

A BitDefender e as suas afiliadas e parceiros enviam apenas informações de marketing por e-mail ou outros meios electrónicos a utilizadores que tenham dado o seu consentimento expresso para receber comunicações relativas aos produtos, serviços ou boletins informativos da BitDefender.

A política de privacidade da BitDefender garante-lhe o direito de acesso, rectificação, eliminação e oposição ao tratamento de dados através da notificação por email à BitDefender: juridic@bitdefender.com.

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

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

BitDefender e o Logótipo BitDefender são marcas registadas de BITDEFENDER. Todas as outras marcas registadas usadas no produto ou nos materiais associados ao mesmo são propriedade dos respectivos proprietários.

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 afectará 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.

Contacte BITDEFENDER, em 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucharest, Romania, ou pelo Tel No: 40-21-206.34.70 ou Fax: 40-21-264.17.99, e-mail: office@bitdefender.com.

Prefácio

Este manual é dirigido a todos os utilizadores que escolheram **BitDefender Internet Security 2010** 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 operativo Windows, independentemente do seu nível de conhecimento de informática.

Este livro irá descrever-lhe o BitDefender Internet Security 2010, irá guiá-lo através do processo de instalação, irá mostrar-lhe como configurá-lo. Vai descobrir como usar o BitDefender Internet Security 2010, como fazer actualizações, testes e personalizá-lo. Vai aprender a tirar o melhor partido do BitDefender.

Desejamos-lhe uma leitura proveitosa e agradável.

1. Convenções Usadas neste Manual

1.1. Convenções Tipográficas

Diversos estilos de texto são usados neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela seguinte.

Aparência	Descrição
`sample syntax`	Exemplos de sintaxe são impressos com caracteres `monospace`.
http://www.bitdefender.com	O link URL aponta para um local externo num servidor http ou ftp.
comercial@bitdefender.pt	Endereços de e-mail são inseridos no texto para contactar a solicitar mais informação.
“Prefácio” (p. xvi)	Este é um link interno que o leva para um local dentro do documento.
`filename`	Ficheiros e directorias são impressos usando uma fonte `monospaced`.
option	Todas as opções de produto são impressas usando caracteres a **cheio**.
`sample code listing`	A listagem de código é impressa com caracteres `monospaced`.

1.2. Advertências

As advertências encontram-se em notas de texto, marcadas graficamente, que trazem à sua atenção informação adicional que diz respeito ao parágrafo em questão.

Nota
A nota é apenas uma observação curta. Apesar de a poder omitir, a nota providencia-lhe informação valiosa, tal como uma característica específica ou um link para um determinado tópico.

Importante
Este ponto requer a sua atenção e não é recomendável ignorá-lo. Normalmente, providencia-lhe informação bastante importante.

Atenção
Trata-se de informação critica que deve de tratar com cuidados redobrados. Nada de negativo acontecerá se você seguir as indicações. Deve de lê-lo e compreendê-lo, porque descreve algo extremamente arriscado.

2. Estrutura do Manual

O manual é composto da várias partes contendo os tópicos principais. Mais ainda, um glossário é fornecido para ajudar a clarificar alguns termos técnicos.

Instalação e Remoção. Instruções passo-a-passo para instalar o BitDefender num computador. Começando com os pré-requisitos para uma instalação de sucesso, será guiado através de todo o processo de instalação. Finalmente, tem a descrição do processo de desinstalação no caso de necessitar de desinstalar o BitDefender.

Introdução. Contém toda a informação necessária para se iniciar com o BitDefender. É-lhe apresentado o interface do BitDefender e como solucionar as incidências, configurar as definições básicas e registar o seu produto.

Modo Intermédio. Apresenta a Interface do Modo Intermédio do BitDefender.

Modo Avançado. Uma apresentação detalhada da interface do Modo Avançado do 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).

Integração com o Windows e outros programas. Mostra-lhe como utilizar as opções do BitDefender no menu contextual do Windows e as barras de ferramentas do BitDefender integradas em programas compatíveis.

Como. Dá-lhe procedimentos para rapidamente levar a cabo as tarefas mais comuns do BitDefender.

Troubleshooting e Obter Ajuda. Onde procurar e onde pedir ajuda se algo inesperado acontecer.

CD de Emergência BitDefender. Descrição do BitDefender Rescue CD. Ajuda a Compreender e a usar as características existentes neste CD de arranque.

Glossário. O Glossário tenta explicar alguns termos técnicos ou pouco comuns que irá encontrar nas páginas deste documento.

3. Pedido de Comentários

Convidamo-lo a ajudar-nos a melhorar este manual. Nós verificamos e testamos toda a informação com o máximo dos cuidados. Por favor escreva-nos acerca de quaisquer falhas que descubra neste manual ou a forma como acha que o mesmo poderia ser melhorado, de forma a ajudar-nos a dar-lhe a si a melhor documentação possível.

Faça-nos saber enviando um e-mail para documentation@bitdefender.com.

Importante

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

Instalação e Remoção

1. Requisitos do Sistema

Pode instalar o BitDefender Internet Security 2010 apenas nos computadores com os seguintes sistemas operativos:

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

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

Nota

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

1.1. Requisitos Minímos do Sistema

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

1.2. Requisitos de sistema recomendados

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

1.3. Software Suportado

A protecção antiphising está disponível apenas para:

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

Encriptação para Instant Messaging (IM) está disponível para:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

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 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. A preparar a Instalação

Antes de instalar o BitDefender Internet Security 2010, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o computador onde vai instalar o BitDefender contém os requisitos minimos do sistema. Se o seu computador não contém os requisitos mínimos do sistema, o BitDefender não será instalado ou, se instalado, não trabalhará correctamente e provocará lentidão e instabilidade no sistema. Para ver a lista completa dos requisitos mínimos do sistema, por favor consulte o "*Requisitos do Sistema*" (p. 2).
- Ligue-se ao computador utilizando uma conta de Administrador.
- Remova quaisquer outros softwares de segurança do seu computador. Executar dois programas de segurança simultaneamente poderá afectar o seu funcionamento e causar grandes problemas no sistema. Por defeito, o Windows Defender será desactivado antes da instalação começar.
- Desativar ou remover qualquer programa de firewall que possam estar em execução no computer. Executar dois programas de firewall simultaneamente poderá afectar o seu funcionamento e causar grandes problemas no sistema. Por defeito, a Firewall do Windows será desactivada antes da instalação começar.

3. Instalar BitDefender

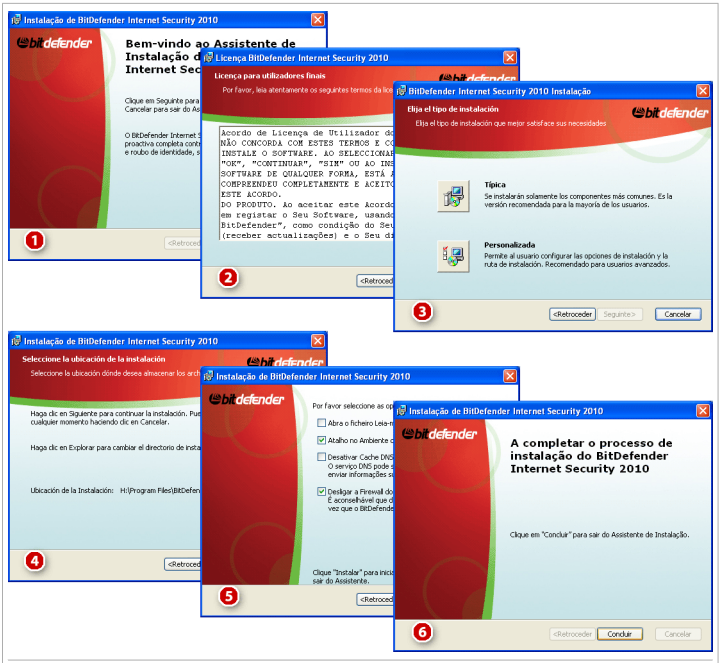
Pode instalar o BitDefender a partir do CD de instalação do BitDefender ou utilizando o ficheiro de instalação descarregado do site da BitDefender ou de outros sites autorizados (por exemplo, de sites de parceiros da BitDefender ou de uma loja on-line). Pode descarregar o ficheiro de instalação do site da BitDefender seguindo este endereço: http://www.bitdefender.com/site/Downloads/.

Para instalar o BitDefender a partir do CD, insira o CD na drive. Uma janela de boas-vindas aparecerá em alguns momentos. Siga as instrucções e começe a instalação.

Se o ecrã de boas vindas não aparecer, siga este caminho `Products\InternetSecurity\install\pt\` da raíz do CD e faça duplo clique `runsetup.exe`.

Para instalar o BitDefender utilizando um ficheiro de instalação descarregado, localize o ficheiro e faça duplo-clique sobre ele.

O instalador irá primeiro verificar o seu sistema para validar a instalação. Se a instalação for validada, o assistente de instalação será exibido. A imagem seguinte mostra os passos do assistente de configuração.



Passos da Instalação

Siga os seguintes passos para instalar o BitDefender Internet Security 2010:

1. Clique **Seguinte**. Pode cancelar a instalação a qualquer altura, clicando em **Cancelar**.

   BitDefender Internet Security 2010 avisa-o no caso de ter outro produto antivírus instalado no seu computador. Clique em **Remover** para desinstalar o respectivo produto. Se deseja continuar sem remover os produtos detectados, clique em **Seguinte**.

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

2. Por favor leia o Acordo de Licença, e clique em **Eu aceito**.

   Importante
   Se não concordar com estes termos clique em **Cancelar**. O processo de instalação será cancelado e terminará.

3. Seleccione o tipo de instalação que deseja executar.
   - **Típica** - para instalar imediatamente o programa, utilizando as opções-padrão de instalação. Se escolher esta opção, salte para o passo 6.
   - **Personalizada** - para configurar as opções de instalação e depois instalar o programa. Esta opção permite-lhe alterar o caminho da instalação.
4. Por defeito, o BitDefender Internet Security 2010 é instalado em`C:\Programas\BitDefender\BitDefender 2010`. Se deseja alterar este caminho de instalação, clique em **Explorar** e seleccione a pasta na qual pretende que o BitDefender seja instalado.

   Clique **Seguinte**.
5. Seleccione as opções que tem a ver com o processo de instalação. Algumas delas serão seleccionadas por defeito:
   - **Abrir o ficheiro leia-me** - para abrir o ficheiro leia-me no fim da instalação.
   - **Colocar um atalho no ambiente de trabalho** - para colocar um atalho do BitDefender Internet Security 2010 no seu ambiente de trabalho, no final da instalação.
   - **Ejectar o CD quando a instalação terminar** - para obter que o CD seja ejectado no final da instalação esta opção aparece quando instala o produto a partir do CD.
   - **Desactive o Cache de DNS** - para desactivar o Cache do DNS (Domain Name System). O serviço Cliente de DNS poderá ser utilizado por aplicações maliciosas para enviar informações para a rede sem o seu concentimento.
   - **Desligar a Firewall do Windows** - para desligar a Firewall do Windows.

     Importante

     Recomendamos que desligue a Firewall do Windows uma vez que o BitDefender Internet Security 2010 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 **Instalar** para que possa iniciar a instalção do produto. Se aina não estiver instalado, o BitDefender instalará em primeiro lugar o .NET Framework 1.1.
6. Espere até que a instalação termine. Clique em **Terminar**. Ser-lhe-á solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação. Recomendamos que o faça assim que seja 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 seu BitDefender Internet Security 2010 e criar uma conta BitDefender.

Se aceitou as definições por defeito do caminho da instalação, poderá ver na pasta `Programas`, uma nova pasta chamada `BitDefender`, que contém a subpasta `BitDefender 2010`.

3.1. Assistente de Registo

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.

TEM de criar uma conta BitDefender de forma a poder receber as actualizações do mesmo. A conta BitDefender também lhe dá acesso a suporte gratuito e a ofertas promocionais especiais. Se perder a sua chave de licença BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Nota

Se não pretender continuar os passos do 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 utilizador.

3.1.1. Passo 1/2 - Registar BitDefender Internet Security 2010

Registo

O BitDefender Internet Security 2010 tem um período de teste de 30 dias. Para continuar a avaliar o produto, seleccione **Quero avaliar o BitDefender** e clique **Seguinte**.

Para registar BitDefender Internet Security 2010:

1. Seleccione **Quero 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.

3. Clique em **Registar Agora**.
4. Clique **Seguinte**.

Se uma chave de licença BitDefender válida for detectada no seu sistema, pode continuar utilizando essa chave, clicando em **Seguinte**.

3.1.2. 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. 10)
- "Já tenho uma conta BitDefender" (p. 11)

Importante

Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias). De outra forma, o BitDefender deixa de ser actualizado.

Não tenho uma conta BitDefender

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

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

- **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender. A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.
- **Re-insira a palavra-passe** - insira novamente a palavra-passe previamente definida.

Nota

Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Seleccione uma das opções disponíveis no menú:
   - **Enviem-me todas as mensagens**
   - **Enviem-me apenas mensagens relativas ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Criar**.
5. Clique em **Terminar** para completar o assistente.
6. **Active a sua conta.** Antes de usar a sua conta, tem de a activar. Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Nesse caso, forneça a palavra-passe da sua conta e clique em **Sign in**. Clique em **Terminar** para completar o assistente.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (conta previamente criada)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota

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

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Seleccione uma das opções disponíveis no menú:
   - **Enviem-me todas as mensagens**
   - **Enviem-me apenas mensagens relativas ao produto**
   - **Não me enviem quaisquer mensagens**

4. Clique em **Sign in**.
5. Clique em **Terminar** para completar o assistente.

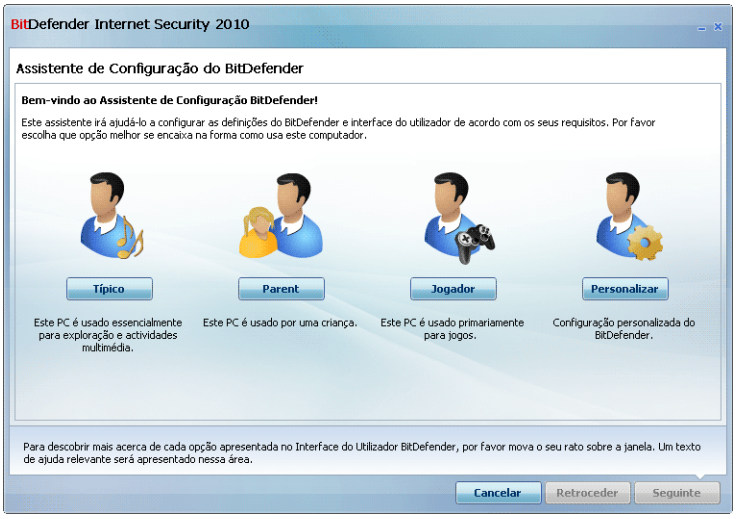
3.2. Assistente de Configuração

Um vez completado o asssitente de registo, aparecerá o assistente de configuração. Este assistente ajuda-o a configurar as principais definições do BitDefender e da interface do utilizador, para que atendam melhor às suas necessidades. No final do assistente, pode fazer o update dos ficheiros do produto e das assinaturas de malware, e analisar os ficheiros do sistema e aplicações para se certificar de que não estão infectados.

O assistente é constituido por alguns passos simples. O número de passos depende das suas escolhas. Aqui estão presentes todos os passos, mas será notificado quando as suas escolhas afectarem o número de passos.

Completar a acção do assistente não é obrigatoria; no entanto, recomendamos que o faça de forma a poupar tempo e assegurar que o seu sistema fica seguro ainda antes de BitDefender Internet Security 2010 estar instalado. Se não pretender continuar os passos do assistente clique em **Cancelar**. BitDefender irá notificá-lo sobre os componentes que necessita de configurar quando abrir o interface do utilizador.

3.2.1. Passo 1 - Seleccione o Perfil de Utilização



Perfil de Utilização

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

Opção	Descrição
Típica	Clique aqui se este PC é usado maioritariamente para exploração e actividades multimédia.
Parent	Clique aqui se este computador é utilizado por crianças e quiser controlar os seus acessos à Internet utilizando o módulo Controlo Parental.
Jogador	Clique aqui se este PC é usado primariamente para jogos.
Personalizada	Clique aqui se quiser configurar todas as definições principais do BitDefender.

Pode apagar mais tarde o perfil de utilização da interface do produto.

3.2.2. Passo 2- Descreva Computador

Descrição do Computador

Seleccione as opções que se aplicam ao seu computador:

- **Este computador está numa rede pessoal.** Seleccione esta opção se deseja gerir remotamente (a partir de outro computador) o produto BitDefender que instalou neste computador. Um passo adicional ao assistente permitir-lhe-á configurar o módulo de Gestor de Rede Pessoal.
- **Este computador é um portátil.** Seleccione esta opção se deseja que o Modo de Portátil esteja ligado por defeito. Enquanto estiver no Modo de Portátil, as tarefas de análise já agendadas não serão efectuadas, pois requerem mais recursos do sistema e, implicitamente, aumentam o consumo energético.

Clique em **Seguinte** para continuar.

3.2.3. Passo 3 - Seleccione o Interface do Utilizador

Modos de Visualização do Interface do Utilizador

Clique no botão que melhor descreve as suas capacidades de computador para seleccionar o modo de visualização do interface apropriado. Pode optar por ver o interface do utilizador em qualquer dos três modos, dependendo do seu computador e sobre a experiência anterior com o BitDefender.

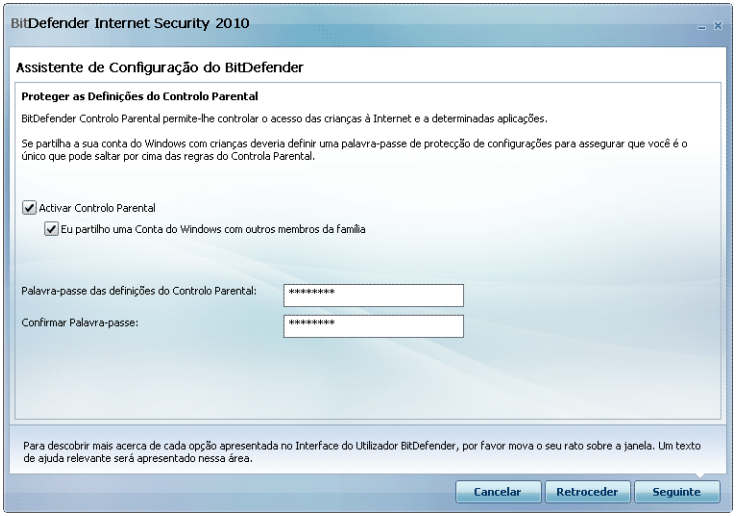
Modo	Descrição
Modo Básico	Indicado para iniciantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incomodos. Este modo é simples de usar e requer a minima interacção da sua parte. Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências. Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.
Modo Intermédio	Destinado a utilizadores com alguns conhecimentos informática, este modo estende o que pode fazer em modo básico.

Modo	Descrição
	Pode corrigir problemas separadamente e escolher quais as questões a serem monitorizadas. Além disso, pode gerir remotamente os produtos BitDefender instalados nos computadores de sua casa.
Modo Avançado	Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender. Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

3.2.4. Passo 4 - Configure o Controlo Parental

Nota

Este passo aparece apenas se tiver seleccionado a opção **Personalizar** no Passo 1.



Configuração do Controlo Parental

O Controlo Parental BitDefender permite-lhe controlar o acesso à Internet e a determinadas aplicações para cada conta de utilizador no sistema.

Se deseja usar o Controlo Parental, siga estes passos:

1. Seleccione **Activar Controlo Parental**.

2. Se está a partilhar a sua conta de utilizador do Windows com os seus filhos, seleccione a opção correspondente e escreva a palavra-passe no campo referente, para proteget as definições do Controlo Parental. Qualquer pessoa que tente alterar as definições do Controlo Parental tem de inserir a palavra-passe que configurou.

Clique em **Seguinte** para continuar.

3.2.5. Passo 5 - Configurar a Rede BitDefender

Nota
Este passo aparece apenas se tem especificado que o computador está ligado a uma rede pessoal no Passo 2.

Configuração da Rede BitDefender

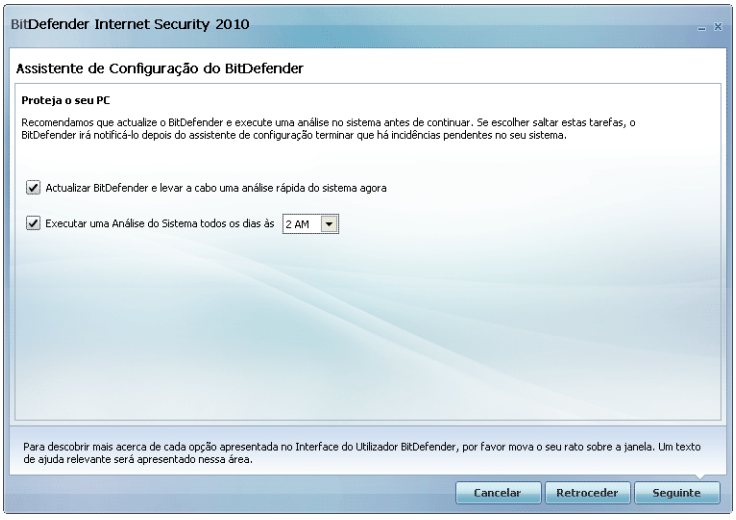
BitDefender permite-lhe criar uma rede virtual com os computadores do seu lar e a administrar os produtos BitDefender instalados nessa rede.

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

1. Seleccione **Activar Rede Pessoal**.
2. Insira a mesma palavra-passe administrativa em cada um dos campos de edição. A palavra-passe permite ao administrador gerir os produtos BitDefender noutro computador.

Clique em **Seguinte** para continuar.

3.2.6. Passo 6 – Seleccionar as Tarefas a Serem Executadas



Selecção das Tarefas

Preparar BitDefender para levar a cabo tarefas importantes para a segurança do seu sistema. Estão disponíveis as seguintes opções:

- **Actualizar o BitDefender e levar a cabo uma análise ao sistema agora** - durante o próximo passo, os ficheiros do produto e as assinaturas do BitDefender serão actualizadas de forma a proteger o seu computador das mais recentes ameaças. Também, assim que a actualização seja comoletada, o Bitdefender irá analisar os ficheiros das pastas `Windows` e `Programas` para assegurar que não estão infectadas. Estas pastas contêm ficheiros do sistema operativo e de aplicações instaladas e são normalmente as primeiras a serem infectadas.
- **Levar a cabo uma Análise ao Sistema todos os dias às 2 AM** - prepara o BitDefender para levar a cabo uma análise standard ao seu computador todos os dias às 2 AM. Para altera a hora em que a análise é feita, clique no menu e escolha a hora de início desejada. Se o computador estiver desligado durante o momento do agendamento, a análise será levada a cabo da próxima vez que iniciar o seu computador.

Nota

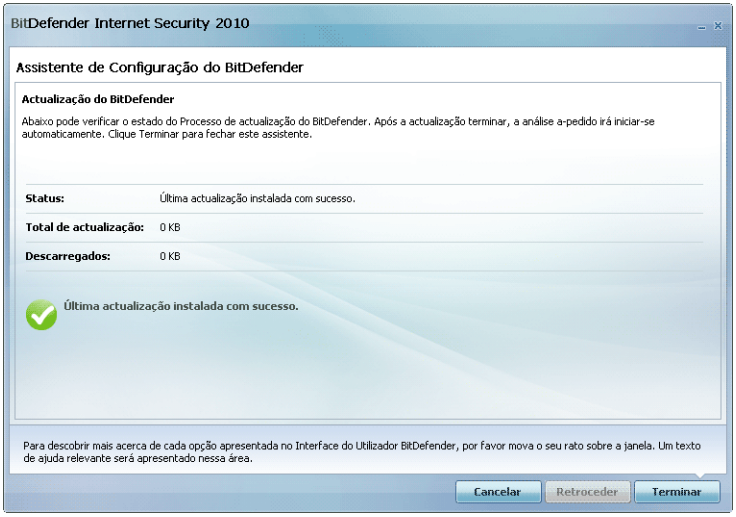
Se mais tarde desejar mudar a hora do agendamento da análise, siga estes passos:
1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.

2. Clique em **Antivirus** do lado esquerdo do menu.
3. Clique na barra **Analisar**
4. Clique botão-direito do rato na tarefa **Análise Completa do Sistema** e seleccione **Agendar**. Uma nova janela irá aparecer.
5. Altere a frequência e a hora de início de acordo com a necessidade.
6. Clique em **Aplicar** para guardar as alterações.

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

Se limpar a primeira caixa de selecção, não haverá tarefas a serem executadas no último passo do assistente. Clique em **Terminar** para completar o assistente.

3.2.7. Passo 7 - Terminar



Estado das Tarefas

Espere que o BitDefender actualize as suas assinaturas de malware e os seus motores de análise. Assim que a actualização esteja completada, uma análise rápida do sistema será iniciada. A análise será levada a cabo silenciosamente, em segundo plano. Pode ver o ícone do progresso da análise na área de notificação. Pode clicar nesse icone para abrir a janela da análise e ver o seu progresso.

Clique em **Terminar** para completar o assistente. Não tem de esperar que a análise termine.

Nota

A análise demorará um pouco. Quando terminar, abra a janela da análise e verifique os resultados da mesma para ver se o seu sistema está limpo. Se foram detectados vírus durante a análise, deve de abrir imediatamente o BitDefender e levar a cabo uma análise completa do sistema.

4. Actualização

Pode fazer upgrade para o BitDefender Internet Security 2010 se estiver a usar a versão beta do BitDefender Internet Security 2010 ou a versão 2008 ou 2009.

Há duas formas de fazer o upgrade:

- Instalar o BitDefender Internet Security 2010 directamente sobre a antiga versão. Se instalar directamente sobre a versão 2009, as listas de Amigos e Spammers e a Quarentena são automaticamente importadas.
- Remova a anterior versão, reinicie o computador e instale a nova versão tal como descrito na secção "*Instalar BitDefender*" (p. 5). Não serão guardadas as definições do produto. Use este método de upgrade se outros falharem.

5. Remover ou Reparar o BitDefender

Se pretende reparar ou remover o BitDefender Internet Security 2010, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar** → **Programas** → **BitDefender 2010** → **Reparar ou Desinstalar**.

Irá se-lhe pedido para confirmar a sua opção ao clicar **Seguinte**. Irá aparecer uma nova janela, na qual pode seleccionar:

- **Reparar** - para reinstalar todos os componentes já instalados no passo anterior;

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

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

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

- **Remover** - para remover todos os componetes 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 Internet Security 2010 do seu computador.

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

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

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

Introdução

6. Vista Geral

Uma vez instalado o BitDefender o seu computador fica protegido. Se não completou o assistente de configuração, deve de abrir o BitDefender assim que possível e reparar as incidências existentes. Poderá ter que configurar componentes específicos do BitDefender ou levar a cabo acções preventivas para proteger o seu computador e os seus dados. Se desejar, pode configurar o BitDefender para não o alertar acerca de determinadas incidências.

Se não registou o produto (e não criou uma conta BitDefender), lembre-se de fazer isso antes que o período de testes termine. Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias). De outra forma, o BitDefender deixa de ser actualizado. Para mais informaçãoon sobre o processo de registo, por favor consulte o "*Registo e a Minha Conta*" (p. 51).

6.1. A abrir o BitDefender

Para aceder ao interface principal do BitDefender Internet Security 2010, utilize o menu do Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2010** → **BitDefender Internet Security 20010** ou mais rapidamente, duplo-clique no ícone do BitDefender que está na área de notificação.

6.2. Modos de Visualização do Interface do Utilizador

O BitDefender Internet Security 2010 vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.

Pode optar por ver o interface do utilizador em qualquer dos três modos, dependendo do seu computador e sobre a experiência anterior com o BitDefender.

Modo	Descrição
Modo Básico	Indicado para iniciantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incomodos. Este modo é simples de usar e requer a minima interacção da sua parte. Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências. Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.

Modo	Descrição
Modo Intermédio	Destinado a utilizadores com alguns conhecimentos informática, este modo estende o que pode fazer em modo básico. Pode corrigir problemas separadamente e escolher quais as questões a serem monitorizadas. Além disso, pode gerir remotamente os produtos BitDefender instalados nos computadores de sua casa.
Modo Avançado	Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender. Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

O interface do utilizador é seleccionavel no assistente de configuração. Este assistente aparece após o assistente registo, na primeira vez que abrir o computador após a instalação do produto. Se cancelar o assistente de registo ou o assistente de configuração, o modo do interface do usuário passará, por defeito, para o Modo Intermédio.

Para alterar o modo de interface de usuário, siga os seguintes passos:

1. Abrir o BitDefender.
2. Clique em **Definições** que se encontra no canto superior direito da janela.
3. Nas Configurações do interface do usuário, clique na seta e seleccione a opção desejada.
4. Clique em **OK** para salvar e aplicar as alterações.

6.2.1. Modo Iniciação

Se é um iniciante em computador, o interface do Modo Básico pode ser a escolha mais adequada para si. Este modo é simples de usar e requer a mínima interacção da sua parte.

Modo Iniciação

A janela está organizada por três secções principais:

- **Estado** - Alerta-o se incidências afectarem o seu computador e ajuda-o a repará-las. Ao clicar em **Reparar todas**, o assistente irá ajuda-lo a remover facilmente quaisquer ameaça do seu computador e segurança de dados. Para mais informações, por favor consulte "*Reparar Incidência*" (p. 40).
- **Protege o seu PC** é onde pode encontrar as tarefas necessárias para proteger o seu computador e os seus dados. As tarefas disponíveis que pode levar a cabo são diferentes dependendo do seu perfil de uso seleccionado.
  - O botão **Analisar Agora** inicia uma análise standard ao seu sistema em busca de vírus, spyware e outro malware. O assistente do Scan de Antivirus irá aparecer e guiá-lo durante o processo. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).
  - O botão **Actualizar Agora**ajuda-o a actualizar as assinaturas de vírus e os ficheiros do produto BitDefender. Surge uma nova janela, onde pode ver o estado da actualização. Se as actualizações são detectadas, são automaticamente descarregadas e instaladas no seu computador.
  - Quando o **Typical** perfil é seleccionado, o botão da **Análise de Vulnerabilidades** inicia um assistente que o ajuda a descobrir reparar as vulnerabilidades do seu sistema, tais como software desactualizado ou actualizações do Windows que estão em falta. Para mais informação, por favor consulte o "*Assistente de verificação de vulnerabilidade*" (p. 68).

- Quando o perfil **Parent** é seleccionado, o botão **Controlo Parental** permite-lhe configurar as definições do Controlo Parental. O Controlo Parental restringe o computador e as actividades online das crianças, baseado nas regras que você definiu. As restrições podem incluir o bloqueio de sites de web inadequados, bem como limitar o acesso à Internet e a jogos a um determinado horário. Para mais informações sobre como configurar o Controlo Parental, por favor consulte o "*Parental Control*" (p. 189).
- Quando o perfil seleccionado é **Jogador**, o botão **Ligar/Desligar Modo Jogo** permite-lhe activar/desactivar Modo Jogo. O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema.

- **Mantenha o seu PC** é onde pode encontrar as tarefas necessárias para proteger o seu computador e os seus dados.
  - **Adicionar ao Cofre** - inicia o assistente que lhe permite armazenar de forma privada os seus ficheiros / documentos importantes ao encriptá-los em drives de cofre especiais.
  - **Análise Minuciosa do Sistema** inicia uma análise muito completa ao seu sistema em busca de todo o tipo de malware.
  - **Análise Os Meus Documentos** analisa em busca de vírus e outro malware as suas pastas normalmente mais usadas: `Meus Documentos` e `Ambiente de Trabalho`. Isto assegurará a segurança dos seus documentos, um espaço de trabalho seguro e aplicações limpas que se executam no iniciar do seu PC.

No canto superior direito da janela encontra-se o botão **Definições**. Ao clicar, abrir-se-á uma janela onde pode mudar o modo do interface do utilizador e activar ou desactivar as definições principais do BitDefender. Para mais informações, por favor consulte "*Configurar Definições Básicas*" (p. 43).

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

Link	Descrição
Comprar/Renovar	Abre uma página web onde poderá adquirir uma chave de licença do produto BitDefender Internet Security 2010.
Registo	Permite-lhe inserir uma nova chave de licença ou ver a actual e o estado do seu registo.
Ajuda & Suporte	Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender.

6.2.2. Modo Intermédio

Destinado a utilizadores com conhecimentos médios de informática, o Modo Intermédio é um interface simples que lhe dá acesso a todos os módulos num nível

básico. Terá que acompanhar as advertências e alertas críticos e corrigir problemas indesejáveis.

Modo Intermédio

A janela Modo Intermédio é composto por cinco páginas. A tabela a seguir descreve brevemente cada guia. Para mais informações, por favor consulte "Modo Intermédio" (p. 94).

Barra	Descrição
Painel	Exibe o estado da segurança do seu sistema e permite-lhe restabelecer o perfil de utilização.
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.
Parental	Mostra o estado do módulo do Controlo Parental. O Controlo Parental permite-lhe restringir o acesso das suas crianças à Internet e a determinadas aplicações.
Cofre de Ficheiros	Mostra o estado do cofre de ficheiros juntamente com os links para o mesmo.

Barra	Descrição
Rede	Mosta a estrutura da rede pessoal BitDefender. Aqui é onde pode levar a cabo diversas acção para configurar os produtos BitDefender instalados na sua rede pessoal. Desta forma, pode gerir a segurança da sua rede pessoal, a partir de um só computador.

No canto superior direito da janela encontra-se o botão **Definições**. Ao clicar, abrir-se-á uma janela onde pode mudar o modo do interface do utilizador e activar ou desactivar as definições principais do BitDefender. Para mais informações, por favor consulte "*Configurar Definições Básicas*" (p. 43).

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

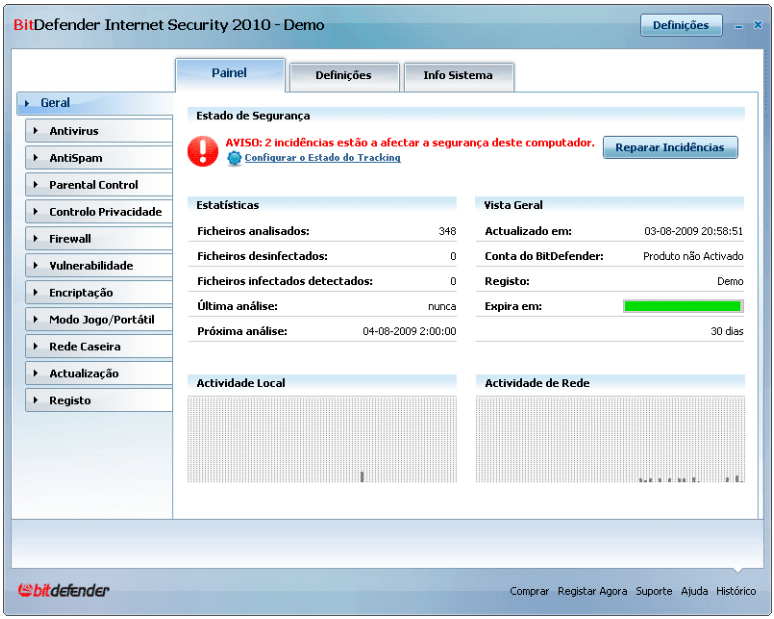
Link	Descrição
Comprar/Renovar	Abre uma página web onde poderá adquirir uma chave de licença do produto BitDefender Internet Security 2010.
Registar	Permite-lhe inserir uma nova chave de licença ou ver a actual e o estado do seu registo.
Suporte	Permite o contacto com a equipa de suporte BitDefender.
Ajuda	Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender.
Ver Relatórios	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

6.2.3. Modo Avançado

O Modo Avançado dá-lhe acesso a cada componente específico do BitDefender. Aqui é onde pode configurar o BitDefender em detalhe.

Nota

O Modo Avançado é adequado para os utilizadores que têm conhecimentos informáticos acima da média, que conhecem o tipo de ameaças a que um computador está exposto e como funcionam os programas de segurança.



Modo Avançado

Do lado esquerdo da janela existe um menu que contém todos os módulos de segurança. Cada módulo possui um ou mais separadores onde pode configurar as respectivas definições de segurança ou executar tarefas de segurança e de administração. A tabela seguinte descreve resumidamente cada módulo. Para mais informações, por favr consulte “Modo Avançado” (p. 119).

Módulo	Descrição
Geral	Permite-lhe aceder às definições gerais ou ver o painel e a info detalhada do sistema.
Antivirus	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.
Controlo Parental	Permite-lhe proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.

Módulo	Descrição
Controlo de Privacidade	Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.
Firewall	Permite-lhe proteger 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.
Vulnerabilidade	Permite-lhe manter o software crucial para o seu PC sempre actualizado.
Encriptação	Permite-lhe encriptar as comunicações do Yahoo e Windows Live (MSN) Messenger e também encriptar localmente os seus ficheiros critícos, as suas pastas ou partições.
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.
Registo	Permite-lhe registar o BitDefender Internet Security 2010, para alterar a chave de licença ou criar uma conta BitDefender.

No canto superior direito da janela encontra-se o botão **Definições**. Ao clicar, abrir-se-á uma janela onde pode mudar o modo do interface do utilizador e activar ou desactivar as definições principais do BitDefender. Para mais informações, por favor consulte "*Configurar Definições Básicas*" (p. 43).

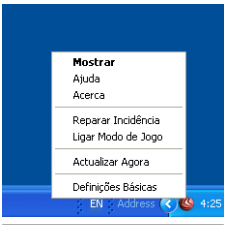
No canto inferior direito da janela, pode encontrar vários links úteis.

Link	Descrição
Comprar/Renovar	Abre uma página web onde poderá adquirir uma chave de licença do produto BitDefender Internet Security 2010.
Registar	Permite-lhe inserir uma nova chave de licença ou ver a actual e o estado do seu registo.
Suporte	Permite o contacto com a equipa de suporte BitDefender.

Link	Descrição
Ajuda	Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender.
Ver Relatórios	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

6.3. Icon da Barra de Tarefas

Para gerir todo o produto mais rapidamente, pode usar o ícone da BitDefender que se encontra na barra de tarefas. Se fizer duplo-clique neste ícone, o BitDefender irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do BitDefender.



Ícone Tray

- **Mostrar** - abre o interface principal do BitDefender.
- **Ajuda** - abre o ficheiro de Ajuda, que explica em detalhe como configurar e usar o BitDefender Internet Security 2010.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Reparar todos incidências** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, é porque não há incidências a reparar. Para mais informações, por favor consulte "*Reparar Incidência*" (p. 40).
- **Ligar/Desligar Modo de Jogo** - activa / desactiva Modo de Jogo.
- **Actualizar agora** - executa uma actualização imediata. Surge uma nova janela, onde pode ver o estado da actualização.
- **Definições Basica** - abre uma janela onde pode mudar o modo de interface do utilizador e activar ou desactivar as principais definições de produto. Para mais informações, por favor consulte "*Configurar Definições Básicas*" (p. 43).

O ícone do BitDefender na area de notificação do sistema, informa quando ha incidências a afectar o seu computador ou a forma como o produto funciona, exibindo um símbolo especial, como o que se segue:

Triângulo vermelho com um ponto de exclamação: Questões críticas afectam a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.

Triângulo amarelo com um ponto de exclamação: Não existem questões críticas que afectem a segurança do seu sistema. Você deve verificar e corrigi-las quando tiver tempo.

Letter G: The product operates in Game Mode.

Se o BitDefender não estiver a funcionar, o ícone da area de notificação do sistema fica com a cor cinzenta . Isto normalmente acontece quando a licença de chave expira. Também pode ocorrer quando os serviços da BitDefender não estão a responder ou quando outros erros afectam a actuação normal da BitDefender.

6.4. Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade de verificação no seu sistema. Esta pequena janela, por defeito, é apenas disponível no Modo Avançado.

As barras cinzentas (a **zona PC**) mostram o número de ficheiros 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 da Análise

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**).

6.4.1. Analisar Ficheiros e Pastas

Pode usar a barra de actividade da análise para analisar rapidamente ficheiros e pastas. Arraste o ficheiro ou a pasta que pretende analisar e deixe-a cair em cima da **Barra de Actividade da Análise**, como apresentado abaixo.

Arraste o ficheiro

Deixe cair o ficheiro

O assistente do Scan de Antivirus irá aparecer e guiá-lo durante o processo. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).

Opções de Análise. As opções de análise estão pré-configuradas para obter os melhores resultados de detecção. Se forem detectados ficheiros infectados, o BitDefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados. As opções de análise são padronizadas e não as pode alterar.

6.4.2. Desactivar/Restaurar Barra de Actividade da Análise

Quando não quiser ver o gráfico de visualização,clique apenas no botão direito e escolha **Esconder**. Para restaurar a barra de actividade da análise, siga os seguintes passos:

1. Abrir o BitDefender.
2. Clique em **Definições** que se encontra no canto superior direito da janela.
3. Na categoria Definição Geral, seleccione a caixa correspondente a **Barra de Actividade da Análise**.
4. Clique em **OK** para salvar e aplicar as alterações.

6.5. Análise Manual BitDefender

A análise manual BitDefender deixa-o analisar uma determinada pasta ou partição do disco sem ter de criar uma tarefa de análise. Esta ferramenta foi desenhada para ser usada quando o Windows está a correr em Modo de Segurança. Se o seu sistema está infectado com um vírus resiliente, pode tentar remover o vírus iniciando o Widnows em Modo de Segurança e analisando cada partição do disco duro usando a Análise Manual BitDefender.

Para aceder à Análise Manual BitDefender, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar → Programas → BitDefender 2010 → Análise Manual BitDefender**. A seguinte análise irá aparecer:

Análise Manual BitDefender

Clique em **Adicionar Pasta**, seleccione a localização que quer analisar e clique **OK**. Se quer analisar várias pastas, repita esta acção para cada localização adicional.

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

Quando não tiver mais locais para adicionar, clique em **Continuar**. O assistente do Scan de Antivirus irá aparecer e guiá-lo durante o processo. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).

Opções de Análise. As opções de análise estão pré-configuradas para obter os melhores resultados de detecção. Se forem detectados ficheiros infectados, o BitDefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados. As opções de análise são padronizadas e não as pode alterar.

O que é o Modo de Segurança?
O Modo de Segurança é uma forma especial de iniciar o Windows, usada apenas para resolver problemas que afectam a operação normal do Windows. Tais problemas vão desde drivers conflituosos até vírus que impedem que o Windows inicie normalmente. No Modo de Segurança, o Windows carrega apenas um minímo de componentes do sistema operativo e drivers básicos. Apenas algumas aplicações funcionam em Modo de Segurança. Essa é a razão pela qual a maioria dos vírus

ficam inactivos quando usa o Windows em Modo de Segurança e então podem ser facilmente removidos.
Para iniciar o Windows em Modo de Segurança, reinicie o seu computador e prima a tecla F8 até que o menu das opções Avançadas do Windows surja. Pode escolher estre várias opções, a opção de iniciar o Windows em Modo de Segurança. Poderá querer seleccionar **Modo de Segurança com Rede>** de forma a poder ter acesso à Internet.

Nota

Para mais informação dobre o Modo de Segurança, vá ao Centro de Ajuda e Suporte do Windows (no menu Iniciar, clique em **ajuda e suporte**). Pode também encontrar informação útil pesquisando a Internet.

6.6. Modo de Jogo e Modo Portátil

Algumas aplicações de computadores, como jogos ou apresentações, exigem um sistema maior de resposta e desempenho, e sem interrupções. Quando o seu computador portátil está ligado apenas com a bateria, é melhor que operações desnecessárias, que consomem mais energia, sejam adiadas até que o portátil esteja ligado á corrente.

Para se adaptar a estas situações especiais, o BitDefender Internet Security 2010 inclui dois modos de funcionamento especial:

- Modo de Jogo
- Modo de Portátil

6.6.1. 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:

- 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 ficheiros mais importantes

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

Usar o Modo de Jogo

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. O BitDefender regressa automaticamente ao modo

normal de operação quando fechar o jogo ou quando a janela da aplicação for minimizada.

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

- Clique com o botão-direito do rato no ícone do BitDefender que está na área de notificação e seleccione **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.

Mudar a Hotkey do Modo de Jogo

Se deseja mudar a hotkey, siga estes passos:

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

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

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

6. Clique em **Aplicar** para guardar as alterações.

6.6.2. Modo Portátil

O Modo de Portátil foi especialmente desenhado para os utilizadores de portáteis. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o portátil estiver a funcionar a bateria. Enquanto estiver no Modo de Portátil, as tarefas de análise já agendadas não serão efectuadas, pois requerem mais recursos do sistema e, implicitamente, aumentam o consumo energético.

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

automaticamente do Modo de Portátil quando detecta que o seu portátil já não está a funcionar a bateria.

Para usar o Modo de Portátil, deve de especificar no assistente de configuração que está a usar um portátil. Se não selecionar a opção adequada ao executar o assistente, pode mais tarde activar o Modo de Portatil da seguinte forma:

1. Abrir o BitDefender.
2. Clique em **Definições** que se encontra no canto superior direito da janela.
3. Na categoria Definição Geral, seleccione a caixa correspondente a **Modo de Detecção de Portátil**.
4. Clique em **OK** para salvar e aplicar as alterações.

6.7. Detecção Automática de Dispositivos

O BitDefender detecta automaticamente quando um dispositivo de armazenamento amovível se liga ao computador, e oferece-se para fazer um scan antes de você aceder aos arquivos. Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detectados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Quando dispositivos como estes são detectados, aparece uma janela de alerta.

Para analizar o dispositivo de armazenamento, clique em **Analizar**. O assistente do Scan de Antivirus irá aparecer e guiá-lo durante o processo. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).

Alerta Detecta Dispositivo

Se não quiser fazer o scan ao dispositivo, deve clicar **Não**. Nesse caso, uma destas opções podem ser úteis:

- **Não me perguntem novamente acerca deste tipo de dispositivo** - BitDefender não irá mais sugerir que analise dispositivos de armazenagem deste tipo quando eles estiverem ligados ao seu computador.
- **Desactivar detecção automática de dispositivos** - Não será mais solicitado para analisar novos dispositivos de armazenagem quando eles estiverem ligados ao computador.

Se acidentalmente desactivar a detecção automática de dispositivos e pretender activar, ou se deseja configurar as suas definições, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Vá a **Antivirus>Análise Virus**.
3. Na lista das taréfas de análise, localize a tarefa **Detecção de Dispositivos**.
4. Clique com o botão direito do rato na tabela e seleccione **Abrir**. Uma nova janela irá aparecer.
5. Na barra **Visão Geral** e configure as opções de análise como desejar. For more information, please refer to "*Configurar Definições da Análise*" (p. 144).
6. No separador **Detecção**, escolha quais os tipos de dispositivos de armanesamento a ser detectados.
7. Clique em **OK** para salvar e aplicar as alterações.

7. Reparar Incidência

O BitDefender utiliza um sistema de emissão de monitoramento para detectar e informá-lo sobre os problemas que podem afectar a segurança do seu computador e dos seus dados. Por defeito, ele irá acompanhar apenas algumas questões que são consideradas muito importantes. No entanto, pode sempre configurá-lo conforme necessário, escolhendo as questões específicas sobre que deseja ser notificado.

É assim que as questões pendentes são notificadas:

- É exibido um símbolo especial sobre o ícone BitDefender system tray para indicar incidências pendentes.

  Triângulo vermelho com um ponto de exclamação: Questões críticas afectam a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
  Triângulo amarelo com um ponto de exclamação: Não existem questões críticas que afectem a segurança do seu sistema. Você deve verificar e corrigi-las quando tiver tempo.

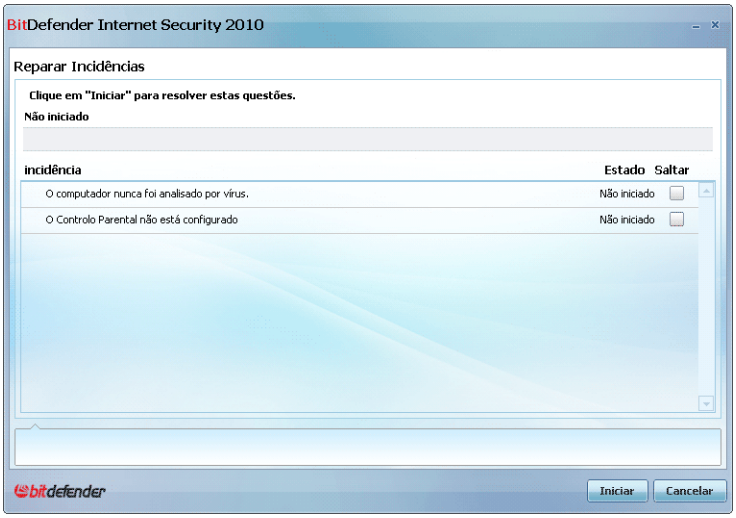
  Além disso, se mover o cursor do rato sobre o ícone, uma janela pop-up irá confirmar a existência de questões pendentes.

- Quando abre o BitDefender, a área de Estado da Segurança vai indicar o número de incidências que afectam o seu sistema.
  - No Modo Intermédio, o estado de segurança aparece no separador **Painel**.
  - No Modo Avançado, vá a **Geral>Painel** Para verificar o estado da segurança.

7.1. Assistente Reparar Todas as Incidências

A forma mais fácil de corrigir as incidências existentes é seguir o passo-a-passo o assistente **Reparar Todas** . O assistente ajuda-o a remover facilmente qualquer ameaça de segurança do seu computador e dados. Para abrir o assistente, faça uma das seguintes coisas:

- Clique com o botão direito do rato no ícone do BitDefender na area de notificação e seleccione **Reparar Todas as Incidências**.
- Abrir o BitDefender. Dependendo do modo de interface do utilizador, proceda da seguinte forma:
  - No Modo Básico, clique em **Reparar Todas as Incidências**.
  - Em Modo Intermédio, vá ao separador **Painel** e clique em **Reparar Todas as Incidências**.
  - Em Modo Avançado, vá a **Geral>Painel** e clique em**Reparar Todas as Incidências**.



Assistente Reparar Todas as Incidências

O assistente apresenta a lista de vulnerabilidades de segurança no seu computador.

Todas as incidências são seleccionadas para serem solucionadas. No caso de existir uma incidência que não quer resolver, escolha a caixa de selecção correspondente. Se o fizer, o estado mudará para **Saltar**.

Nota
Se não deseja ser avisado acerca de determinadas incidências, pode configurar o sistema de tracking de acordo, tal como descrito na próxima secção.

Para resolver a incidência seleccionada, clique em **Iniciar**. Algumas incidências são tratadas imediatamente. Para outras, o assistente ajuda-o a resolvê-las.

A incidência que este assistente o ajuda a tratar pode ser agrupada numa destas categorias:

- **Desactivar definições de segurança.** Tais incidências são reparadas imediatamente, ao activar as respectivas definições de segurança.
- **Ferramentas preventivas de segurança que deve realizar.** Um exemplo dessa tarefa é a análise ao seu computador. É recomendado que faça uma análise ao seu computador pelo menos uma vez por semana. O BitDefender irá automaticamente fazê-lo por si na maioria dos casos. Contudo, se alterou o agendamento das análises ou se o agendamento não se completou, será notificado sobre essa incidência.

Quando reparar a incidência, o assistente ajuda-o a completar com sucesso a tarefa.

- **Vulnerabilidades dos Sistema.** O BitDefender verifica automaticamente o seu sistema por vulnerabilidades e alerta-o sobre eles. As vulnerabilidades do sistema incluem:
  - Senhas fracas para as contas de utilizador do Windows.
  - Software desactualizado no seu computador
  - actualizações do Windows em falta.
  - As actualizações automáticas do Windows estão desativadas.

  Quando essas incidências estão a ser reparadas, o assistente de análise de vulnerabilidades é iniciado. Este assistente ajuda-o a reparar as vulnerabilidades de sistema detectadas. Para mais informação, por favor consulte o "*Assistente de verificação de vulnerabilidade*" (p. 68).

7.2. Configurar a Monotorização de Incidências

O sistema de monotorização de incidências está pré-configgurado para monotorizar e alertá-lo sobre as mais importantes incidências que possam afectar a segurança dos seus dados e computador. Incidências adicionais poderão ser monotorizadas tendo como base as duas escolhas feitas no assistente de configuração (quando configura o perfil de utilização). Para além das incidências monitoradas por defeito, existem outras incidências de que pode vir a ser informado.

Pode configurar o sistema de monotorização para se adaptar às suas necessidades de segurança, escolhendo sobre que incidências específicas quer ser informado. Pode fazê-lo tanto no Modo Intermédio como no Modo Avançado.

- No Modo Intermédio, a monotorizaçao do sistema pode ser configurada a partir de menus diferentes. Siga estes passos:
  1. Vá ao separador **Segurança**, **Parental** ou **Cofre de Ficheiros**.
  2. Click **Configurar Estado Tracking**.
  3. Selecione as opções correspondentes aos itens que pretende monitorizar.

  Para mais informações, por favor consulte "Modo Intermédio" (p. 94).

- Em Modo Avançado, o sistema de monitorização pode ser configurada a partir da zona central. Siga estes passos:
  1. Vá a **Geral>Painél**.
  2. Click **Configurar Estado Tracking**.
  3. Selecione as opções correspondentes aos itens que pretende monitorizar.

  Para mais informações, por favor consulte o capitulo "*Painel*" (p. 120).

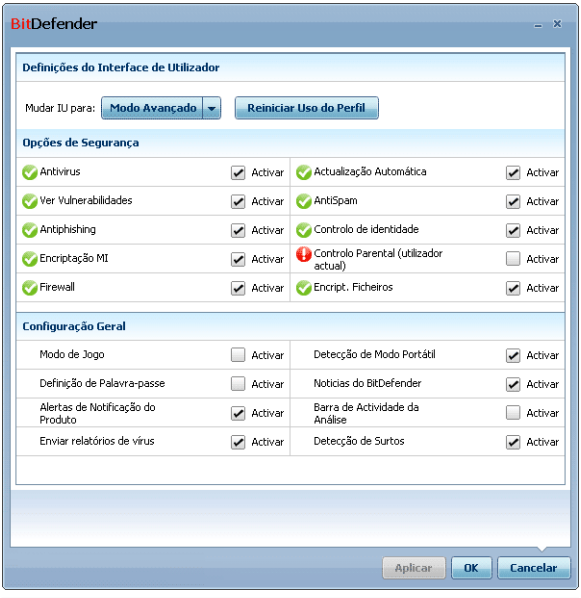
8. Configurar Definições Básicas

Pode configurar as definições do produto (incluindo mudar o modo de vizualização do interface do utilizador) a partir da janela de configurações básicas. Para abri-la, siga um dos seguintes paço:

- Abra o BitDefender e clique em **Definições** que se encontra no canto superior direito da janela.
- Clique com o botão direito do rato no ícone do BitDefender na barra de tarefas e seleccione **Definições Básicas**.

Nota

Para configurar as definições do programa em detalhe, use o Modo Avançado de interface do utilizador. Para mais informações, por favr consulte "Modo Avançado" (p. 119).



Definições Básicas

As definições estão organizadas por três categorias:

- Definições Interface
- Definições Segurança
- Definições

Para aplicar e salvar as alterações, clique em **OK**. Para fechar a janela e não salvar as alterações, clique em **Cancelar**.

8.1. Definições do Interface de Utilizador

Nesta área, pode alternar o modo de vizualização do interface do Utilizador e repor o perfil usuado.

Mudando o modo de visualização do interface de utilizador. Conforme está descrito na secção "*Modos de Visualização do Interface do Utilizador*" (p. 24), há três modos de exibição do interface do utilizador. Cada modo de interface do utilizador é projectado para uma determinada categoria de utilizadores, com base nas suas capacidades informáticas. Desta forma, o interface do utilizador acolhe todo o tipo de utilizadores, desde iniciantes a técnicos em computadores.

O primeiro botão mostra o actual modo de visualização do interface do utilizador. Para alterar o modo do interface do utilizador, clique na seta e seleccione a opção desejada.

Modo	Descrição
Modo Básico	Indicado para iniciantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incomodos. Este modo é simples de usar e requer a minima interacção da sua parte. Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências. Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.
Modo Intermédio	Destinado a utilizadores com alguns conhecimentos informática, este modo estende o que pode fazer em modo básico. Pode corrigir problemas separadamente e escolher quais as questões a serem monitorizadas. Além disso, pode gerir remotamente os produtos BitDefender instalados nos computadores de sua casa.
Modo Avançado	Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender. Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

Redefinir o perfil de utilização. O perfil de utilização reflecte as principais actividades desenvolvidas no computador. Dependendo do perfil de utilização, a interface do produto é organizada para permitir o acesso fácil às suas ferramentas preferidas.

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

8.2. Opções de Segurança

Aqui, pode activar ou desactivar configurações do produto que abrangem diversos aspectos da segurança do computador e dos dados. O actual estado de uma definição é indicado usando um destes ícones:

Círculo verde com uma marca de verificação: A opção está activada.
Circulo vermelho com um ponto de exclamação: A opção não está activada.

Para activar / desactivar uma definição, seleccione a opção**Activar**.

Atenção

Tenha cuidado ao desactivar a protecção em tempo-real do antivírus, a firewall ou a actualização automática. Desactivar estas opções pode comprometer a segurança do seu computador. Se realmente necessita de as desactivar, não se esqueça de as activar novamente o mais rapidamente possível.

A lista de configurações e a respectiva descrição é apresentada no quadro seguinte:

Definições	Descrição
Antivírus	A protecção em tempo-real assegura que todos os ficheiros acedidos por si ou por uma aplicação são analisados.
Actualização Automática	A actualização automática assegura que os produtos e as assinaturas mais recentes da BitDefender são descarregados da Internet e instalados automaticamente numa base regular.
Análise de Vulnerabilidade	A Verificação Automática de Vulnerabilidades assegura que o software crucial no seu PC está actualizado.
Antispam	O Antispam filtra as mensagens de E-mail recebidas, marcando a publicidade não solicidada e o lixo electronico como SPAM.
Antiphishing	A protecção Antiphishing web em tempo-real detecta e alerta-o em tempo-real se uma página web está feita para roubar informação pessoal.

Definições	Descrição
Controlo de Identidade	O Controlo de Identidade ajuda a impedir que os seus dados pessoais sejam expostos na Internet sem o seu consentimento. Bloqueia todas as mensagens instantâneas, mensagens de e-mail ou outras formas de transmissão de dados pela web que tenha definido como sendo privado para destinatários não autorizados (endereços).
Encriptação IM	A encriptação das mensagens instantâneas (MI) através do Yahoo! Messenger e Windows Live Messenger só é possivel se a pessoa de contacto utilizar um producto BitDefender compativel.
Controlo Parental	O Controlo Parental restringe o computador e as actividades online das crianças, baseado nas regras que você definiu. As restrições podem incluir o bloqueio de sites de web inadequados, bem como limitar o acesso à Internet e a jogos a um determinado horário.
Firewall	A Firewall protege o seu computador contra os hackers e os ataques maliciosos externos.
Encriptação de Ficheiros	O Cofre de ficheiros mantém os seus documentos privados ao encriptá-los em drives de cofre especiais. Se desactivar o Cofre de Ficheiros, todos os cofres de ficheiros serão fechados e não será mais capaz de aceder aos ficheiros que eles contêm.

O estado de algumas destas definições podem ser monitorizadas pelo sistema de monitorização do BitDefender. Se desactivar a definição de monitorização, o BitDefender irá identicar como incidencia que necessita de der reparada.

Se nao desejar que uma definição de monitorização que desactivou, seja detectada como Incidência, tem de configurar o sistema de monotorização para tal. Pode faze-lo no Modo Intermédio ou no Modo Avançado.

- Em Modo Intermédio, o sistema de monitorização pode ser configurado a partir de menus diferentes. Para mais informações, por favor consulte “Modo Intermédio” (p. 94).
- Em Modo Avançado, o sistema de monitorização pode ser configurada a partir da zona central. Siga estes passos:
  1. Vá a **Geral>Painél**.
  2. Click **Configurar Estado Tracking**.
  3. Limpe a caixa correspondente ao item que você não quer que seja monotorizado.

Para mais informações, por favor consulte o capitulo "*Painel*" (p. 120).

8.3. Configuração Geral

Aqui, pode activar ou desactivar as definições referentes ao produto e à experiencia do utilizador. O actual estado de uma definição é indicado usando um destes ícones:

Círculo verde com uma marca de verificação: A opção está activada.

Circulo vermelho com um ponto de exclamação: A opção não está activada.

Para activar / desactivar uma definição, seleccione a opção**Activar**.

A lista de configurações e a respectiva descrição é apresentada no quadro seguinte:

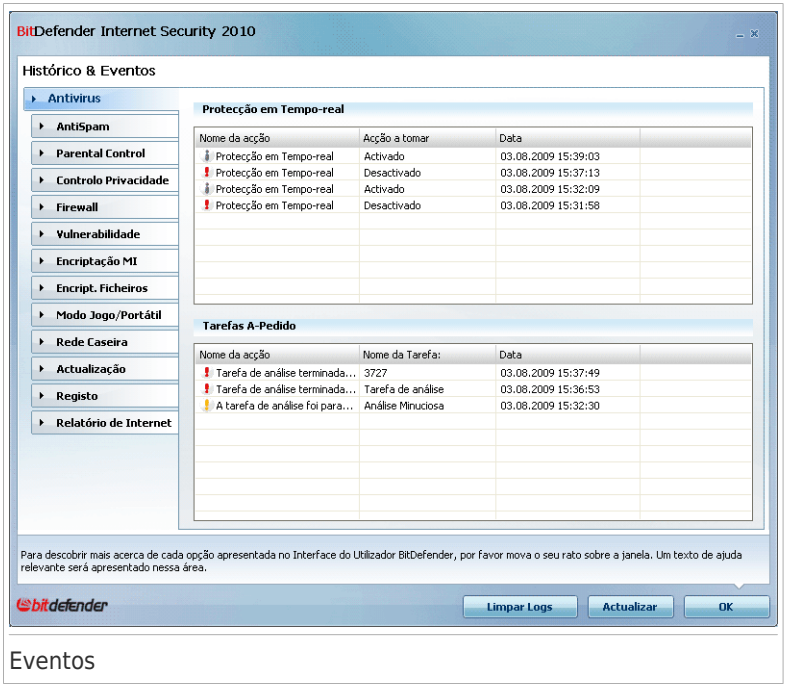
Definições	Descrição
Modo de Jogo	O Modo de Jogo modifica temporariamente as definições de segurança de forma a minimizar o seu impacto no desempenho do seu sistema durante o jogo.
Detecção Modo de Portátil	O Modo Portátil modifica temporariamente as definições de segurança de forma a minimizar o seu impacto sobre o tempo de vida da bateria do seu portátil.
Palavra-passe de Configuração	Isto assegura que as definições do BitDefender só podem ser modificadas pela pessoa que conhece esta palavra-passe. Quando activar esta opção, será solicitado a configurar as definições de palavra-passe. Insira a palavra-passe desejada nos dois campos e clique em **OK** para definir a palavra-passe.
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 da análise é uma janela pequena, transparente, que indica o progresso da actividade da análise do BitDefender. Para mais informação, por favor consulte o "*Barra de Actividade da Análise*" (p. 33).
Enviar Relatórios de Vírus	Ao activar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise.

Definições	Descrição
	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.

9. Histórico e Eventos

O link **Histórico** no fundo da janela principal do 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 facilmente verificar se a actualização foi executada com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc.

Nota
O Link é apenas acessível a partir Modo Intermédio ou no Modo Avançado.



Eventos

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

- **Antivírus**
- **Antispam**
- **Controlo Parental**
- **Controlo Privacidade**
- **Firewall**

- **Vulnerabilidade**
- **Encriptação IM**
- **Encriptação de Ficheiros**
- **Modo de Portátil/Jogo**
- **Rede de Casa**
- **Actualização**
- **Registo**
- **Registo de Internet**

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.

10. Registo e a Minha Conta

O BitDefender Internet Security 2010 tem um período de teste de 30 dias. Durante o período de testes, o produto é 100% funcional e pode testá-lo de forma a ver se está de acordo com as suas expectativas. Por favor repare que, após 15 dias de avaliação, o produto deixará de actualizar, a não ser que crie uma conta BitDefender. Criar uma conta BitDefender é uma parte obrigatória do processo de registo.

Antes de o período de testes terminar, deve de registar o produto de forma a manter o seu computador protegido. O Registo é um processo de dois passos:

1. **Activação do produto (registo de uma conta BitDefender).** Deve de criar uma conta BitDefender de forma a receber actualizações e a ter acesso a suporte técnico gratuito. Se já tem uma conta BitDefender, registe o seu produto BitDefender nessa conta. O BitDefender irá avisá-lo que necessita de activar o seu produto e ajudá-lo-á a reparar essa incidência.

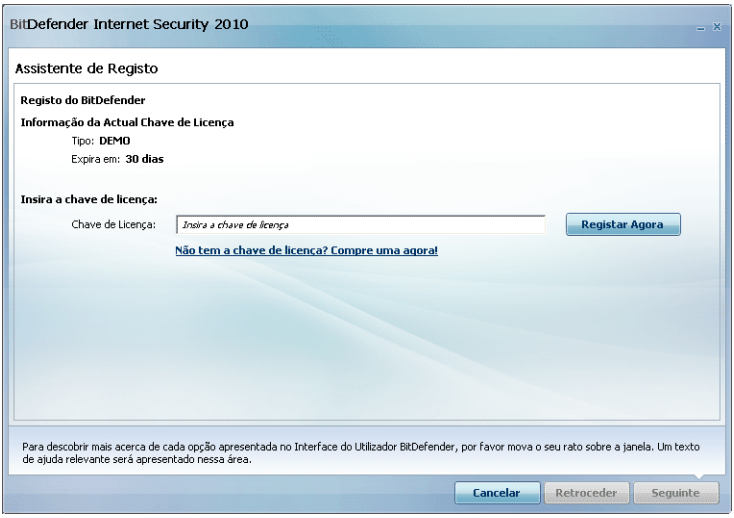
   Importante

   Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias). De outra forma, o BitDefender deixa de ser actualizado.

2. **Registo com uma chave de licença.** A chave de licença especifica durante quanto tempo está autorizado a usar o produto. Assim que a chave de licença expira, o BitDefender pára de executar as suas funções e de proteger o seu computador. Deve de registar o seu produto com uma chave de licença antes que o período de testes termine. Deve de adquirir uma chave de licença ou renovar a sua licença uns dias antes da actual licença expirar.

10.1. Registar BitDefender Internet Security 2010

Se quer registar o produto com uma chave de licença ou se quer alterar a sua chave de licença actual, clique no link **Registar Agora**, localizado no fundo da janela do BitDefender. Irá aparecer a janela de registo de produto .



Registo

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

Para registar BitDefender Internet Security 2010:

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

Nota

Pode encontrar a sua chave de licença:

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

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

2. Clique em **Registar Agora**.
3. Clique em **Terminar**.

10.2. A activar o BitDefender

Para activar o BitDefender, necessita de criar, ou entrar numa conta BitDefender. Se não registar uma conta BitDefender durante o assistente inicial de registo, pode faze-lo da seguinte forma:

- No Modo Básico, clique em **Reparar Todas as Incidências**. O assistente irá ajudá-lo a corrigir todas as incidências pendentes, incluindo a activação do produto.
- Em Modo Intermédio, vá ao separador **Segurança** e clique no botão **Reparar** correspondendo à incidência de activação do produto.
- No Modo Avançado, vá a **Registo** e clique no botão **Activar Produto**.

Irá abrir a janela de registo de conta. Aqui pode criar ou entrar em uma conta Bitdefender para activar o 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. 54)
- “Já tenho uma conta BitDefender” (p. 54)

Importante

Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias). De outra forma, o BitDefender deixa de ser actualizado.

Não tenho uma conta BitDefender

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

1. Clique em **Criar uma nova conta**.
2. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   - **E-mai** - insira o seu endereço de e-mail.
   - **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender. A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.
   - **Re-insira a palavra-passe** - insira novamente a palavra-passe previamente definida.

   Nota
   Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Seleccione uma das opções disponíveis no menú:
   - **Enviem-me todas as mensagens**
   - **Enviem-me apenas mensagens relativas ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Criar**.
5. Clique em **Terminar** para completar o assistente.
6. **Active a sua conta.** Antes de usar a sua conta, tem de a activar. Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Nesse caso, forneça a palavra-passe da sua conta e clique em **Sign in**. Clique em **Terminar** para completar o assistente.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (conta previamente criada)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota

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

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Seleccione uma das opções disponíveis no menú:
   - **Enviem-me todas as mensagens**
   - **Enviem-me apenas mensagens relativas ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Sign in**.
5. Clique em **Terminar** para completar o assistente.

10.3. Comprar Chave de Licença

Se o período de testes vai terminar em breve, deve de adquirir uma chave de licença e registar o seu produto. Abra o BitDefender e clique no link **Comprar/Renovar**, localizado na parte de baixo da janela. O link leva-o para a página web onde poderá adquirir a chave de licença do seu produto BitDefender.

10.4. Renovar a sua Licença

Como cliente BitDefender, você beneficia de um desconto quando renovar a sua licença BittDefender. Pode também mudar de versão do seu produto com um desconto especial ou mesmo inteiramente grátis.

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

11. Assistentes

Para tornar o BitDefender fácil de usar, vários assistentes ajudá-lo-ão a realizar tarefas específicas de segurança ou a configurar definições mais complexas do produto. Este capítulo descreve os assistentes que podem aparecer quando corrigir problemas ou realizar tarefas específicas com o BitDefender. Outros assistentes de configuração são descritos separadamente na parte “Modo Avançado” (p. 119).

11.1. Assistente de Análise Antivírus

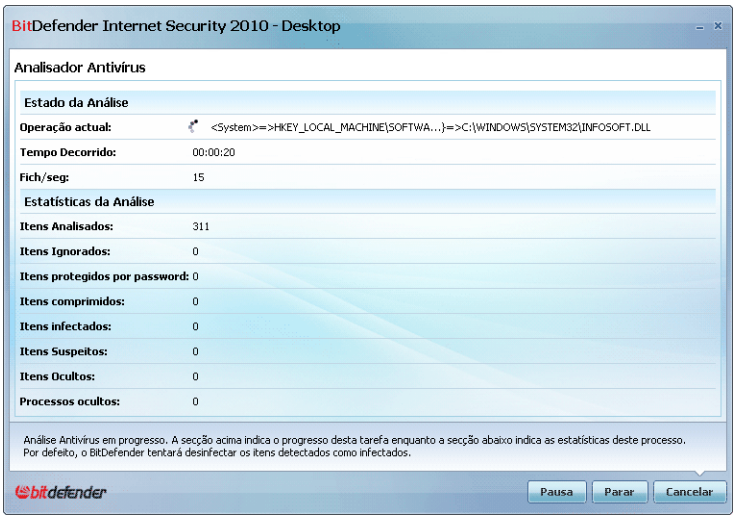
Sempre que inicie uma análise a-pedido (por exemplo, clicar botão direito sobre a pasta e selecionar **Analisar com BitDefender**), o assistente de análise antivírus BitDefender irá aparecer. Siga o processo guiado de três passos para completar o processo de análise.

Nota

Se o assistente de análise não surgir, a análise poderá estar configurada para correr silenciosamente, em segundo plano. Procure pelo ícone do progresso da análise na área de notificação. Pode clicar nesse icone para abrir a janela da análise e ver o seu progresso.

11.1.1. Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

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

Espere que o BitDefender termine a análise.

Nota

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

Arquivos protegidos com palavra-passe. Se o BitDefender detectar um arquivo protegido por palavra-passe durante a análise e a acção por defeito for **Solicitar palavra-passe**, ser-lhe-á solicitado que insera a palavra-passe. Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe. Estão disponíveis as seguintes opções:

- **Quero inserir a palavra-passe para este objecto.** Se quer que o BitDefender analise o arquivo, seleccione esta opção e insira a palavra-passe. Se não sabe a palavra-passe, escolha uma das outras opções.
- **Não quero inserir a palavra-passe para este objecto.** Seleccione esta opção para saltar a análise deste arquivo.
- **Não quero inserir a palavra-passe para nenhum objecto (saltar todos os objectos protegidos por palavra-passe).** Seleccione esta opção se não deseja ser incomodado acerca de arquivos protegidos por palavra-passe. O BitDefender não será capaz de os analisar, mas um registo dos mesmos será mantido no relatório da análise.

Clique em **OK** para continuar a analisar.

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

11.1.2. Passo 2/3 - Seleccionar as acções

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

Acções

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

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

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

Uma ou várias das seguintes opções poderão aparecer no menu:

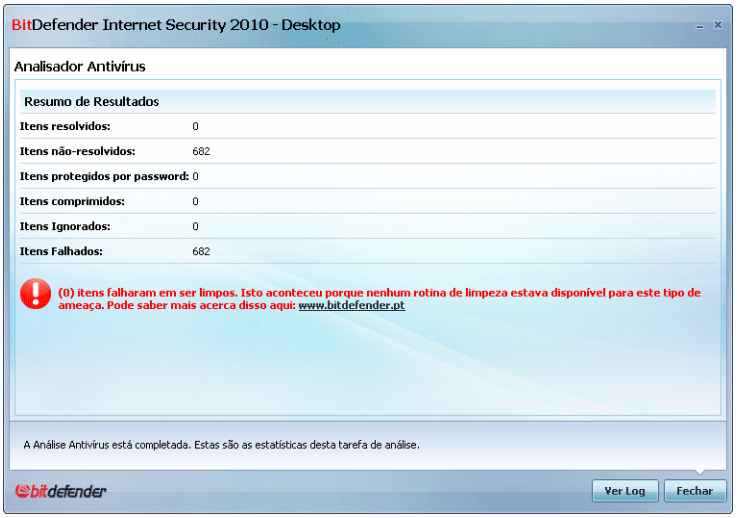
Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.
Desinfectar	Remove o código de malware dos ficheiros infectados.
Apagar	Apaga os ficheiros detectados.
Mover para a quarentena	Move os ficheiros infectados para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

Acção	Descrição
Renomear ficheiros	Altera o nome dos ficheiros ocultos ao acrescentar `.bd.ren` ao seu nome. Como resultado, será capaz de procurar e encontrar tais ficheiros no seu computador, se existirem. Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits. Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

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

11.1.3. Passo 3/3 - Ver Resultados

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



Sumário

Pode ver o resumo dos resultados. Se deseja uma informação completa sobre o processo de análise, clique em **Mostrar ficheiro de log** 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 ficheiro 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 Ficheiros Suspeitos

Ficheiros suspeitos são ficheiros detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura de detecção ainda não foi disponibilizada.

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

11.2. Assistente de Análise Personalizada

O Assistente de Análise Personalizada permite-lhe criar e executar uma tarefa de análise personalizado e, opcionalmente, salvá-la como uma tarefa rápida quando utilizar o BitDefender no Modo Intermédio.

Para correr uma ferramenta de análise personalizada utilizando o Assistente de Análise Personalizada, terá de seguir os seguintes passos:

1. No Modo Intermédio, vá ao separador **Segurança**.
2. Na área de **Tarefas Rápidas** , clique na seta do botão **Análide do Sistema** e seleccione **Análise Personalizada**.
3. Siga o processo guiado de seis passos para completar o processo de análise.

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

Esta é uma janela de boas-vindas

Janela de boas-vindas

Se deseja saltar por cima desta janela quando executar este assistente no futuro, seleccione a caixa de selecção **Não me mostrem este passo da próxima vez que este assistente for executado**.

Clique **Seguinte**.

11.2.2. Passo 2/6 - Seleccionar Alvo

Aqui pode especificar os ficheiros e pastas que quer que sejam analisados bem como as opções de análise.

Seleccionar Alvo

Clique em **Adicionar Alvo**, seleccione o ficheiro ou pasta que deseja adicionar e clique em **OK**. Os caminhos para os locais selecionados serão exibidos na coluna **Analisar Alvos**. Se mudar de ideias quanto à localização, apenas clique no botão **Remover** junto a ela. Clique no botão **Remover Tudo** para remover todas as localizações que foram adicionadas à lista.

Quando terminar de seleccionar as localizações, defina as **Opções de Análise**. Está disponível o seguinte:

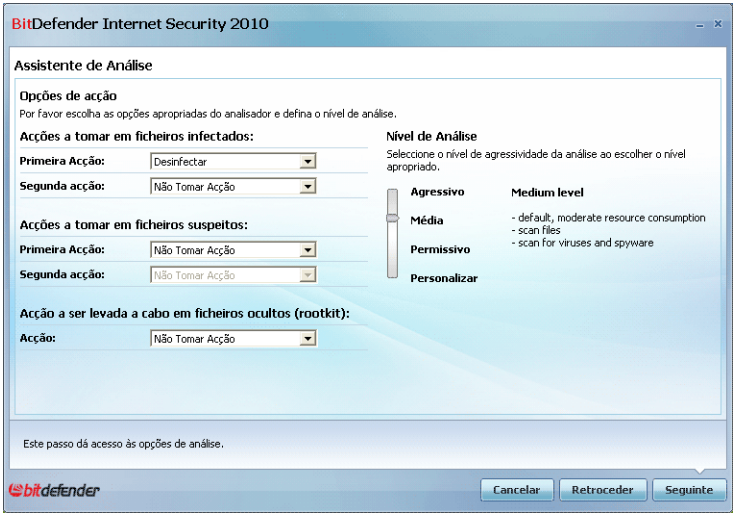
Opção	Descrição
Analisar todos os ficheiros	Seleccione esta opção para analisar todos os ficheiros das pastas seleccionadas.
Analisar apenas os programas	Apenas serão examinados os ficheiros de programa. Isto significa, apenas os ficheiros com as seguintes extensões: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.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`.

Opção	Descrição
Analisar apenas extensões definidas pelo utilizador	Apenas serão examinadas as extensões especificadas pelo utilizador. Estas extensões têm de estar separadas por ";".

Clique **Seguinte**.

11.2.3. Passo 3/6 - Seleccionar as acções

Aqui pode especificar as definições e o nível de análise.



Seleccionar Acções

- Seleccione as acções a ser tomada sobre o ficheiro infectado. Estão disponíveis as seguintes opções:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros infectados. Estes ficheiros aparecerão no ficheiro de relatório.
Desinfectar ficheiros	Remover o código de malware dos ficheiros infectados detectados.

Acção	Descrição
Apagar ficheiros	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
Mover ficheiros para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

- Seleccionar as acções a serem levadas a cabo em ficheiros ocultos (rootkit). Estão disponíveis as seguintes opções:

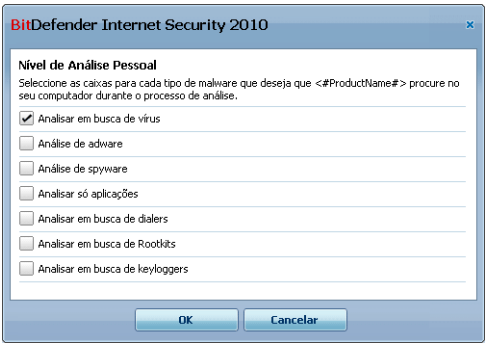
Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros ocultos. Estes ficheiros aparecerão no ficheiro de relatório.
Alterar Nome	Altera o nome dos ficheiros ocultos ao acrescentar `.bd.ren` ao seu nome. Como resultado, será capaz de procurar e encontrar tais ficheiros no seu computador, se existirem.

- Configurar a intensidade da análise. Pode escolher de entre 3 níveis. Arraste o cursor ao longo da barra para definir o nível de protecção adequado:

Nível de Análise	Descrição
Permissivo	Apenas os ficheiros de aplicação são analisádos e apenas em busca de vírus. O nível consumo dos recursos é baixa.
Por Defeito	O nível de consumo dos recursos é moderada. Todos os ficheiros são analisados em busca de vírus e spyware.
Agressivo	Todos os ficheiros (incluindo arquivos)são analisados em busca de vírus e spyware. Ficheiros e processos ocultos são incluidos na análise. O nível de consumo dos recursos é elevado.

Utiilizadores avançados poderão querer tirar vantagem que as definições de anaálise do BitDefender oferecem. O antivirus pode ser configurado para procurar um malware específico. Isto pode reduzir em muito a duração da análise e melhorar a capacidade de resposta do seu computador durante a análise.

Arraste o marcado para seleccionar **Pessoal** e depois clique no botão **Nível Pessoal**. A seguinte análise irá aparecer:



Nível de Análise Pessoal

Especifique que tipo de malware quer que o BitDefender analise seleccionando as opções apropriadas:

Opção	Descrição
Analisar em busca de vírus	Analisa em busca de vírus. O BitDefender também detecta corpos incompletos de vírus, removendo assim qualquer possível ameaça de segurança que possa vir a afectar o seu sistema.
Analisar em busca de adware	Analisa em busca de ameaças de adware. Estes ficheiros serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa.
Análisar spyware	Analisa em busca de ameaças de spyware. Estes ficheiros serão tratados como ficheiros 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 liga~ção para números de valor acrescentado. Estes ficheiros serão tratados como ficheiros 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 (ficheiros e processos), conhecidos por rootkits.

Opção	Descrição
Analisar em busca de Keyloggers	Analisa em busca de aplicações maliciosas que gravam teclas premidas..

Clique **OK** para fechar a janela.

Clique **Seguinte**.

11.2.4. Passo 4/6 - Definições Adicionais

Antes da análise começar, estão disponíveis opções adicionais:

Opções Adicionais

- Para guardar a tarefa pessoal que está a criar para uso futuro seleccione a caixa de selecção **Mostrar esta Tarefa em IU Intermédio** e insira um nome para a tarefa no campo de edição apresentado.

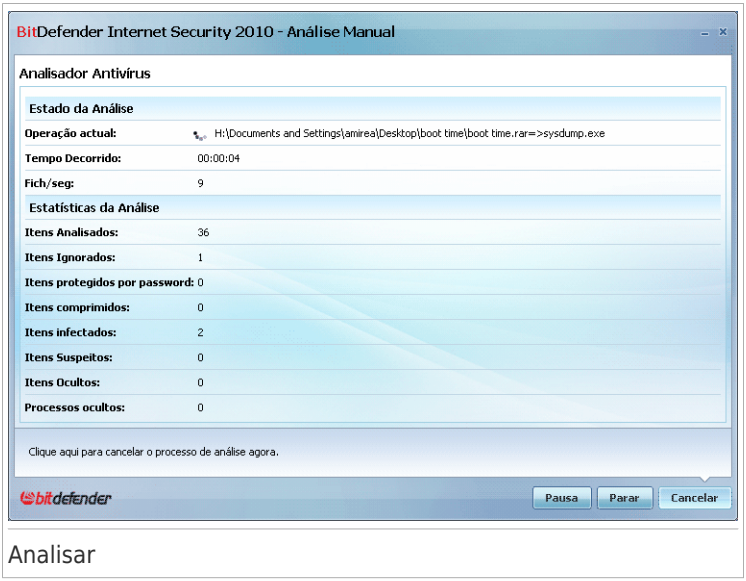
  A tarefa será adicionada à lista de tarefas Rápidas já disponíveis na barra Segurança e também aparecerá no **Modo Avançado > Antivirus > Análisar**.

- Para desligar o computador após a análise terminar, seleccione a caixa de selecção **Desligar PC após a análise terminar, se não forem encontradas ameaças**.

Clique **Seguinte**.

11.2.5. Passo 5/6 - Analisar

BitDefender iniciará a análise dos objectos seleccionados:



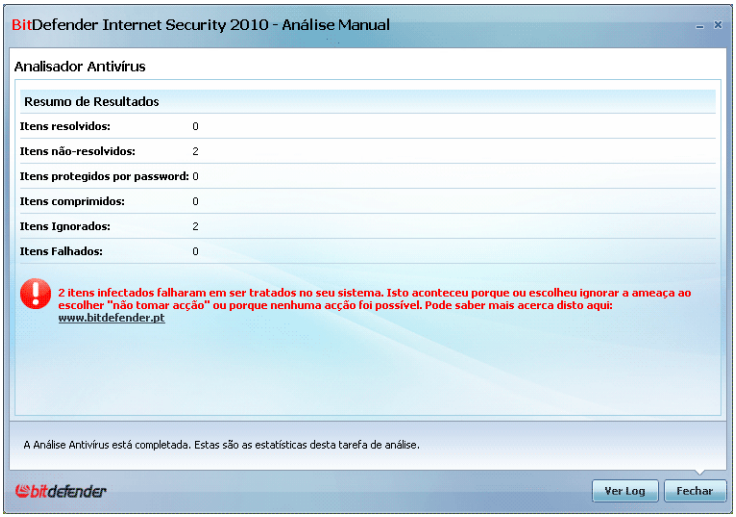
Analisar

Nota

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

11.2.6. Passo 6/6 - Ver Resultados

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



Sumário

Pode ver o sumário dos resultados. Se deseja uma informação completa sobre o processo de análise, clique em **Ver ficheiro de log** 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.

11.3. Assistente de verificação de vulnerabilidade

Este assistente verifica o sistema a procura de vulnerabilidades e ajuda-o a corrigi-los.

11.3.1. Passo 1/6 - Seleccionar Vulnerabilidades a Verificar

Vulnerabilidades

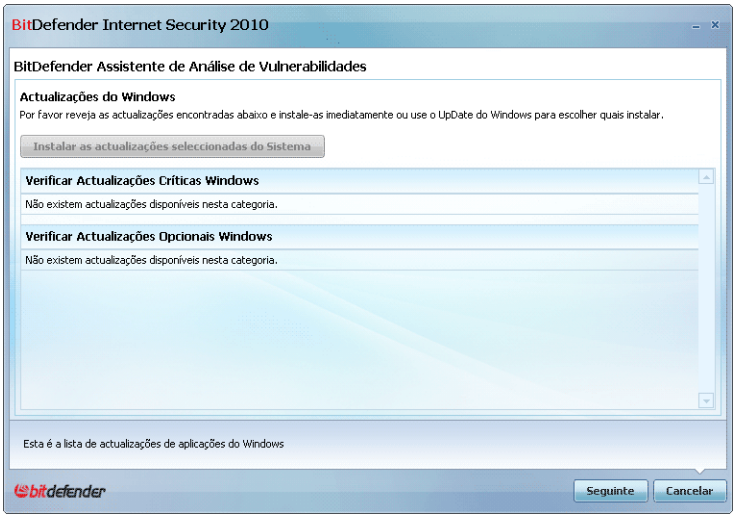
Clique em **Seguinte** para analisar o sistema em busca das vulnerabilidades seleccionadas.

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

Analisar Vulnerabilidades

Espere que o BitDefender termine a análise de vulnerabilidades.

11.3.3. Passo 3/6 - Actualizar Windows



Actualizações do 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 **Seguinte**.

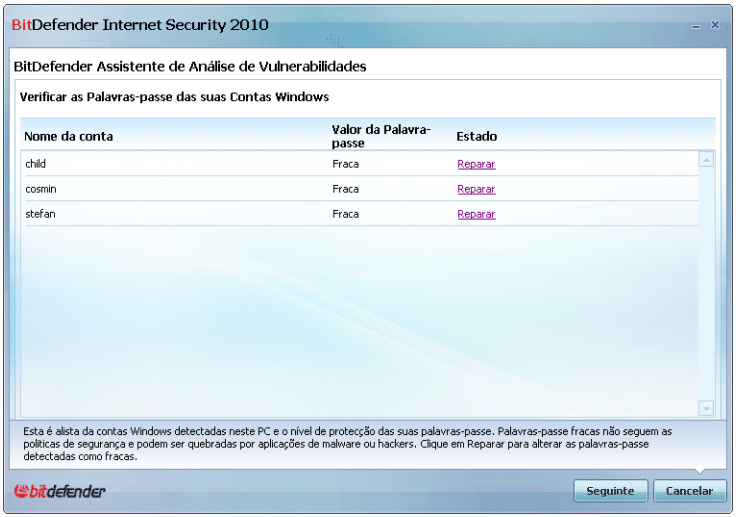
11.3.4. Passo 4/6 - Actualizar Aplicações

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 **Seguinte**.

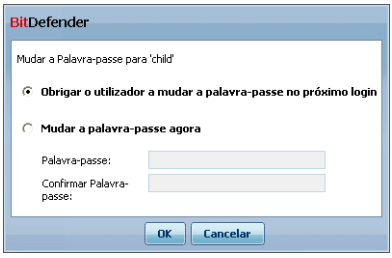
11.3.5. Passo 5/6 - Alterar Palvaras-passe Fracas



Palavras-passe do Utilizador

Pode ver a lista dos utilizadores de contas Windows configurados no seu computador e o nível de protecção que as suas palavras-passe garantem. Uma palavra-passe pode ser **forte** (difícil de adivinhar) ou **fraca** (fácil de quebrar por gente maliciosa usando software para tal).

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



Mudar Palavra-passe

Seleccionar o método para reparar esta incidência:

- **Obrigar o utilizador a mudar a palavra-passe no próximo login.** O BitDefender avisará o utilizador que tem de alterar a palavra-passe da próxima vez que ele entrar no Windows.
- **Mudar a palavra-passe do utilizador.** Deve inserir a nova palavra-passe nos campos editáveis. Certifique-se de avisar o utilizador sobre a alteração de palavra-passe.

Nota

Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @). Pode pesquisar a Internet para mais informação acerca de como criar palavras-passe fortes.

Clique em **OK** para alterar a palavra-passe.

Clique **Seguinte**.

11.3.6. Passo 6/6 - Ver Resultados

Resultados

Clique em **Fechar**.

11.4. Assistentes de Cofre de Ficheiros

O assistente de Cofre de Ficheiros ajuda-o a criar e gerir os cofres de ficheiros do BitDefender. a cofre de ficheiros é um armazenamento encriptado no seu computador onde pode guardar com segurança os seus ficheiros, documentos e até pastas inteiras.

Este assistente não aparece quando trata das incidências, devido ao facto de o cofre de ficheiros ser um método opcional de protecção dos seus dados. Só pode criar um cofre de ficheiros a partir da interface do Modo Intermédio do BitDefender, separador **Gerir Ficheiros**, como se segue:

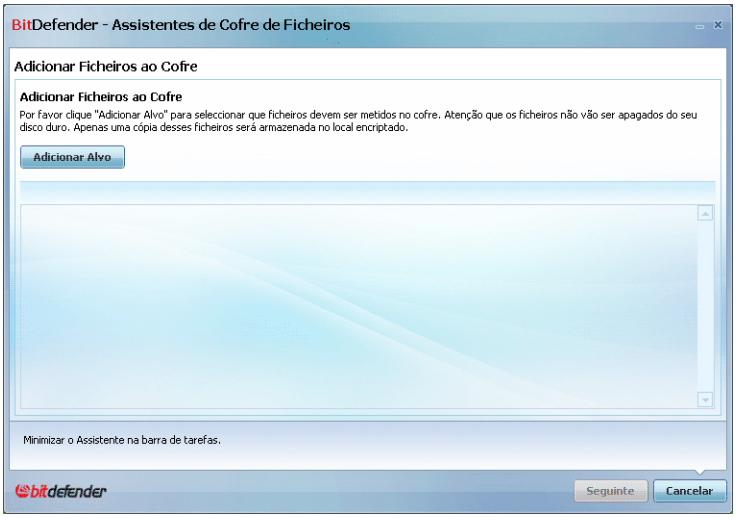
- **Adicionar ao Cofre** - inicia o assistente que lhe permite armazenar de forma privada os seus ficheiros / documentos importantes ao encriptá-los em drives de cofre especiais.
- **Remover do Cofre** - inicia o assistente que lhe permite apagar dados do cofre de ficheiros.
- **Ver cofre** - inicia o assistente que lhe permite ver o conteúdo do cofre de ficheiros.
- **Fechar cofre** - inicia o assistente que lhe permite fechar o cofre de forma a dar início à protecção do seu conteúdo.

11.4.1. Adicionar Ficheiros ao Cofre

Este assistente ajuda-o a criar cofres de ficheiros e a adicionar-lhes ficheiros de forma a armazená-los em segurança no seu computador.

Passo 1/6 - Seleccionar Alvo

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



Alvo

Clique em **Adicionar Alvo**, seleccione o ficheiro 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 **Seguinte**.

Passo 2/6 - Seleccionar cofre

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

Seleccionar Cofre

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

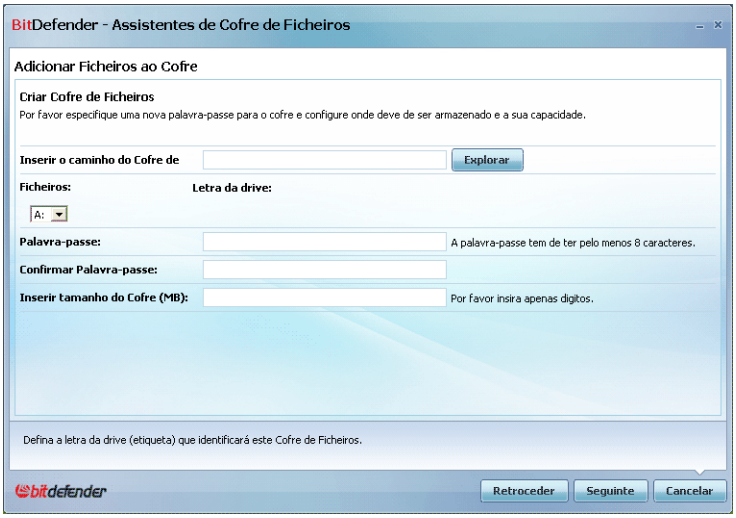
Se clicar em **selecionar um Cofre existente**, deve de clicar no nome do cofre que deseja. Irá de seguida para o passo 5 se o cofre seleccionado estiver aberto (montado) ou para o passo 4 se estiver fechado (desmontado).

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

Clique **Seguinte**.

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 ficheiros, siga estes passos:

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

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

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

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

3. Insira a palavra-passe do cofre de ficheiros no campo correspondente.

   Nota
   A palavra-passe tem de ter pelo menos 8 caracteres.

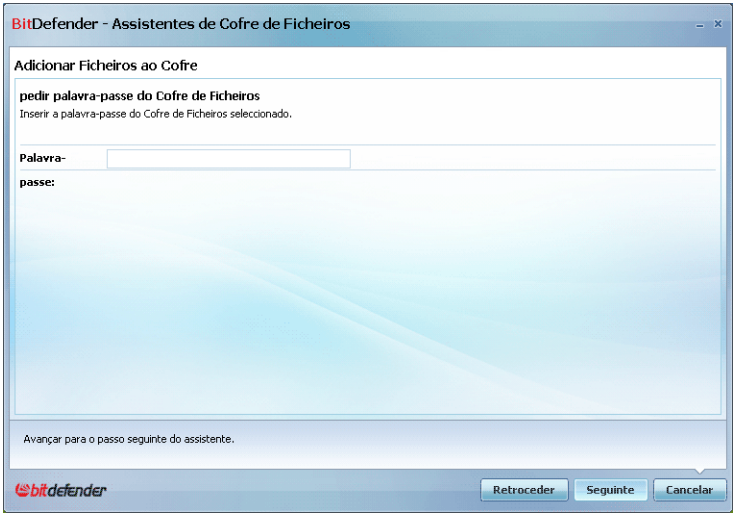
4. Re-inserir a palavra-passe.
5. Defina o tamanho do cofre de ficheiros (em MB) ao inserir o número no campo correspondente.

Clique **Seguinte**.

Irá para o passo 5.

Passo 4/6 - Palavra-passe

Aqui é onde lhe será solicitada a palavra-passe para o cofre seleccionado.

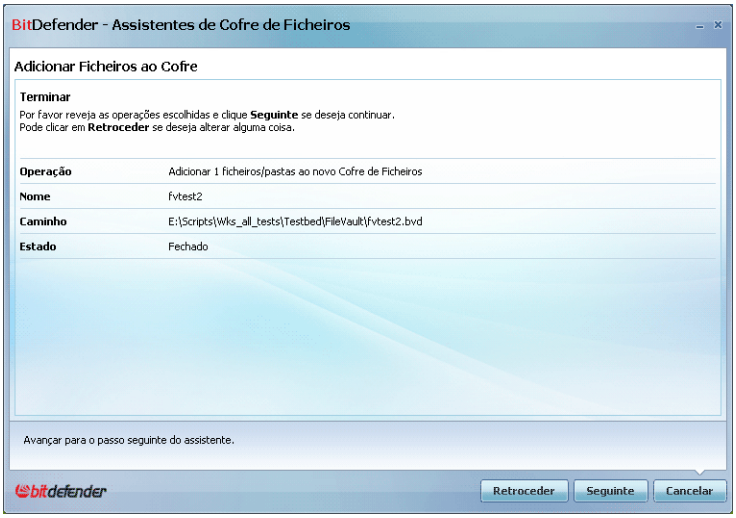


Confirmação da palavra passe

Insira a palavra-passe no campo correspondente e depois clique em **Seguinte**.

Passo 5/6 - Resumo

Aqui é onde pode rever as operações escolhidas.

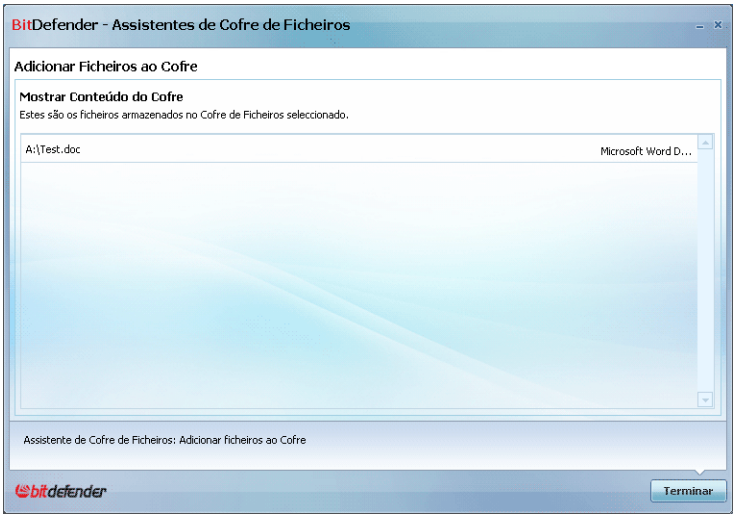


Sumário

Clique **Seguinte**.

Passo 6/6 - Resultados

Aqui é onde pode ver o conteudo do cofre.



Resultados

Clique em **Terminar**.

11.4.2. Remover do Cofre

Este assistente ajuda-o a remover ficheiros de um cofre de ficheiros.

Passo 1/5 - Seleccionar Cofre

Aqui é onde pode seleccionar o cofre de onde deseja remover ficheiros.

Seleccionar Cofre

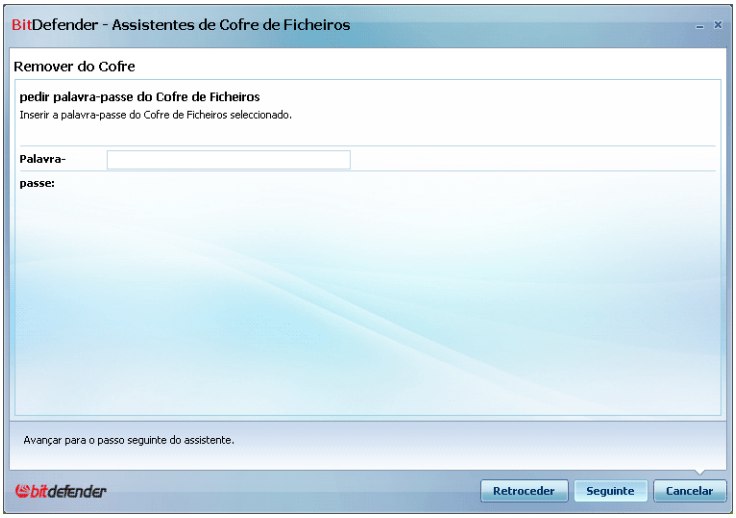
Se seleccionar **Explorar um Cofre de Ficheiros**, deve de clicar em **Explorar** e seleccionar o cofre de ficheiros. Irá de seguida para o passo 3 se o cofre seleccionado estiver aberto (montado) ou para o passo 2 se estiver fechado (desmontado).

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

Clique **Seguinte**.

Passo 2/5 - Palavra-passe

Aqui é onde lhe será solicitada a palavra-passe para o cofre seleccionado.

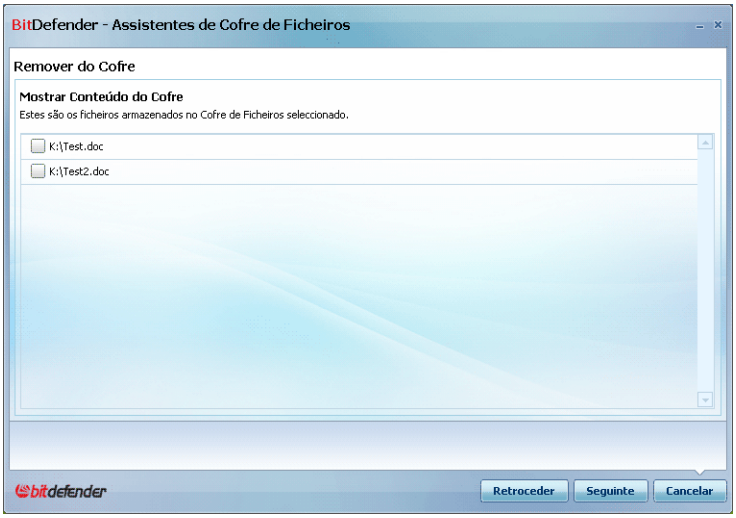


Confirmação da palavra passe

Insira a palavra-passe no campo correspondente e depois clique em **Seguinte**.

Passo 3/5 - Seleccionar ficheiros

Aqui é onde lhe será fornecida a lista dos ficheiros do cofre previamente seleccionado.

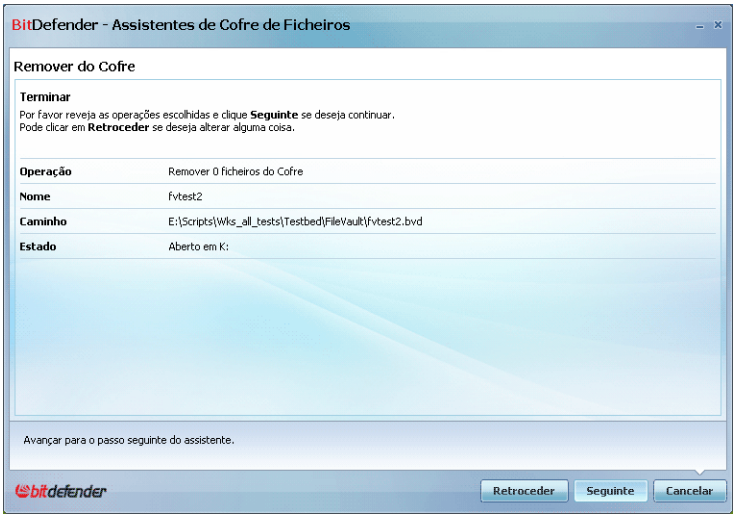


Seleccionar ficheiros

Seleccione os ficheiros a serem removidos e clique **Seguinte**.

Passo 4/5 - Sumário

Aqui é onde pode rever as operações escolhidas.

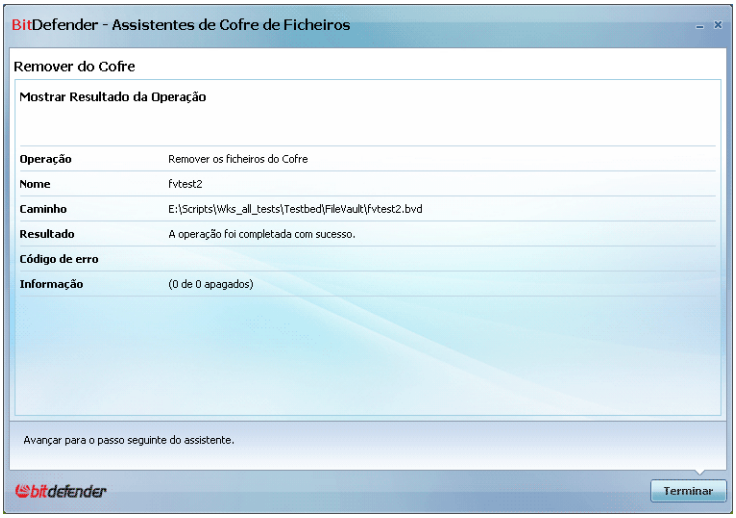


Sumário

Clique **Seguinte**.

Passo 5/5 - Resultados

Aqui é onde poder ver o resultado da operação.



Resultados

Clique em **Terminar**.

11.4.3. Ver Cofre de Ficheiros

Este assistente ajuda-o a abrir e a ver o conteúdo de um cofre de ficheiros específico.

Passo 1/4 - Seleccionar Cofre

Aqui é onde pode seleccionar o cofre de onde deseja ver os ficheiros.

Seleccionar Cofre

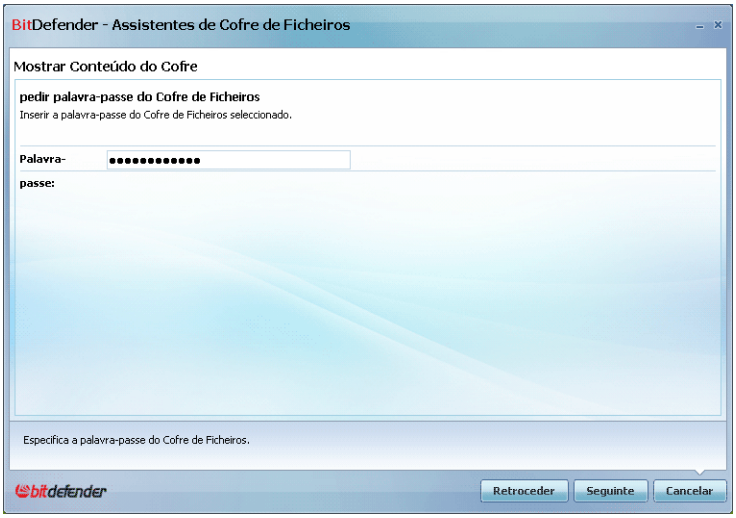
Se seleccionar **Explorar um Cofre de Ficheiros**, deve de clicar em **Explorar** e seleccionar o cofre de ficheiros. Irá de seguida para o passo 3 se o cofre seleccionado estiver aberto (montado) ou para o passo 2 se estiver fechado (desmontado).

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

Clique **Seguinte**.

Passo 2/4 - Palavra-passe

Aqui é onde lhe será solicitada a palavra-passe para o cofre seleccionado.

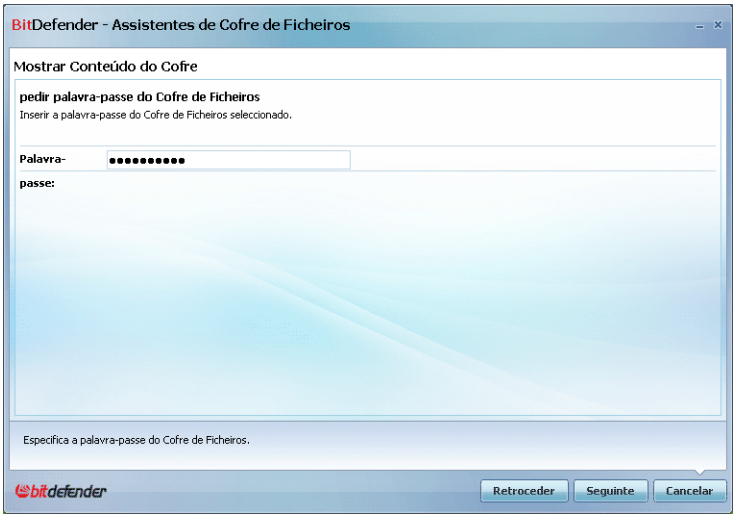


Confirmação da palavra passe

Insira a palavra-passe no campo correspondente e depois clique em **Seguinte**.

Passo 3/4 - Sumário

Aqui é onde pode rever as operações escolhidas.

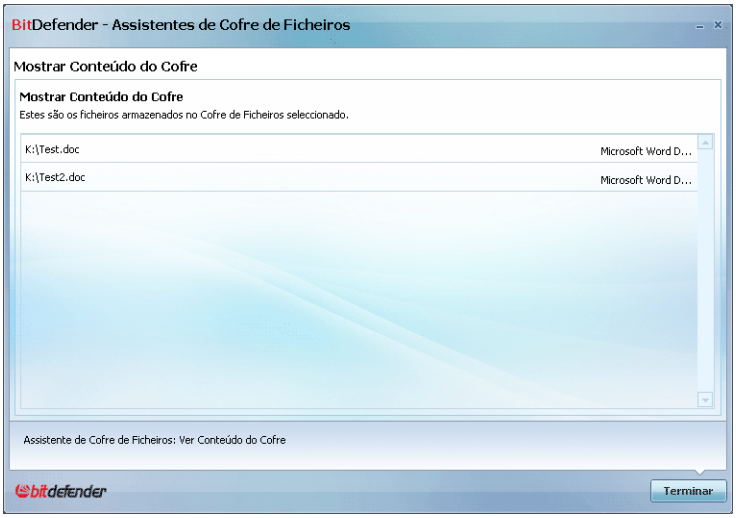


Sumário

Clique **Seguinte**.

Passo 4/4 - Resultados

Aqui é onde pode ver os ficheiros do cofre.



Resultados

Clique em **Terminar**.

11.4.4. Fechar Cofre

Este assistente ajuda-o a fechar um cofre de ficheiros de forma a proteger o seu conteúdo.

Passo 1/3 - Seleccionar Cofre

Aqui é onde pode especificar o cofre a fechar.

Seleccionar Cofre

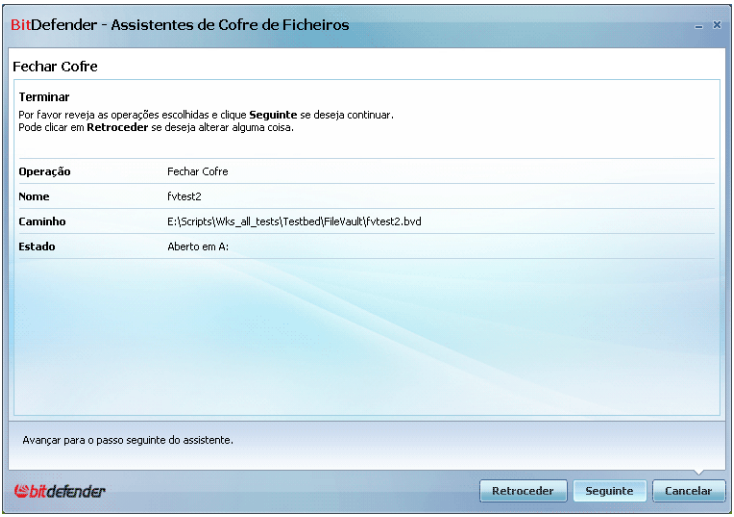
Se seleccionar **Explorar Cofre de Ficheiros**, deve de clicar em **Explorar** e seleccionar o cofre de ficheiros.

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

Clique **Seguinte**.

Passo 2/3 - Sumário

Aqui é onde pode rever as operações escolhidas.

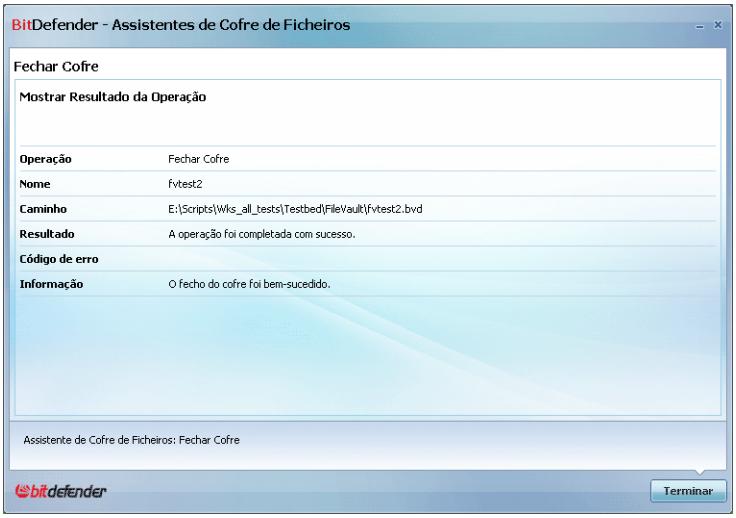


Sumário

Clique **Seguinte**.

Passo 3/3 - Resultados

Aqui é onde poder ver o resultado da operação.



Resultados

Clique em **Terminar**.

Modo Intermédio

12. Painel

O separador do painel fornece informações relativais ao estado de segurança do seu computador e permite-lhe corrigir questões pendentes.

Painel

O painel é composto de várias secções:

- **Estado Geral** - Indica o número de incidências que afectam o seu computador e ajuda-o a repará-las. Se houver incidências pendentes, irá ver um **circulo vermelho com um ponto de esclamação** e o botão **Reparar Todas**. clique no botão para o assistente Reparar Todas as Incidências.
- **Detalhes do Estado** - Indica o estado de cada módulo principal usando frases explícitas e um dos seguintes ícones:

  Círculo verde com uma marca de verificação: Nenhuma incidências a afectar o estado de segurança. O seu computador e os seus dados estão protegidos.

  Círculo cinzento com um ponto de exclamação: A actividade dos componentes deste módulo não estão a ser monotorizados. Assim, não há informação disponível sobre o estado de segurança. Não há incidências específicas relativamente a este módulo.

  Circulo vermelho com um ponto de exclamação: Há incidências a afectarem a segurança do seu sistema. Incidências criticas requerem a sua

atenção imediata. Incidências que não sejam críticas também deverão ser abordadas com a maior brevidade possível

Clique no nome de um módulo para ver mais detalhes acerca do seu estado e para configurar o estado da monitorização dos seus componentes.

- **Perfil de Uso** - Indica o perfil de uso que está actualmente seleccionado e oferece um link para para uma tarefa relevante para esse perfil:
  - Quando o perfil **Tipico** é seleccionado, o botão **Analisar Agora** permite-lhe levar a cabo uma Análise de Sistema usando o Assistente de Análise Antivírus. Todo os sistema será analisado, excepto os arquivos comprimidos. Na configuração por defeito, analisa todo o tipo de malware excepto rootkits.
  - Quando o perfil **Parent** é seleccionado, o botão **Controlo Parental** permite-lhe configurar as definições do Controlo Parental. Para mais informações sobre como configurar o Controlo Parental, por favor consulte o *"Parental Control"* (p. 189).
  - Quando o perfil seleccionado é **Jogador**, o botão **Ligar/Desligar Modo Jogo** permite-lhe activar/desactivar Modo Jogo. O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema.
  - Quando o perfil **Pessoal** é seleccionado, o botão **Actualizar Agora** inicia de imediato uma actualização. Surge uma nova janela, onde pode ver o estado da actualização.

  Se quiser mudar para um perfil diferente ou editar o perfil que estiver a utilizar, clique no perfil e em seguida no configuration">Assistente de Configuração.

13. 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:

- **Área de Estado** - Apresenta o estado actual de todas as componentes de segurança monotorizadas e permite-lhe escolher quais delas devem ser monitorizadas.
- **Tarefas** - Aqui é onde pode encontrar os links para as mais importantes tarefas de segurança: actualizar agora, análise completa ao sistema, análise aos meus documentos, análise minunciosa do sistema, análise personalizada, análise de vulnerabilidades.

13.1. Estado da Área

A área de estado é onde pode ver a lista completa de componentes de segurança monotorizados e o seu estado actual. Ao monotorizar cada módulo de segurança, o BitDefender irá informá-lo não só quando configurar definições que possam afectar a segurança do seu computador, mas também quando se esqueceu de realizar tarefas importantes.

O estado actual de um componente é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

Círculo verde com uma marca de verificação: Não há incidências a infectarem o componente.

Circulo vermelho com um ponto de exclamação: Há incidências a infectarem o componente.

As frases que descrevem as incidências estão escritas a vermelho. Apenas clique no botão **Corrigir** correspondendo à frase para corrigir a incidência reportada. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

13.1.1. Configurar o Estado de Monitorização

Para seleccionar os componentes que o BitDefender deve de monitorizar, clique em **Configurar Estado de Monitorização** e seleccionar a caixa de selecção **Activar alertas** correspondente às opções que deseja monitorizar.

Importante

Tem de activar a monotorização de estado para esta componente se desejar ser notificado quando as incidências afectarem a segurança dessa componente. Para se certificar de que o seu sistema está completamente protegido, por favor permita a análise a todos os componentes e resolva todas as incidências reportadas.

O estado de seguranças das seguintes componentes pode ser monitorizado pelo BitDefender:

- **Antivirus** - O BitDefender monitoriza o estado das duas componentes da funcionalidade Antivírus: proteção em tempo real e uma análise a pedido.

  As incidências comunicadas mais comuns desta componente estão listadas na tabela seguinte.

incidência	Descrição
Protecção de ficheiros em Tempo-real está desactivada	Os ficheiros não são analisados à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.
Nunca analisou o seu computador em busca de malware	Uma análise a-pedido nunca foi levada a cabo para verificar se os ficheiros armazenados no seu computador estão livres de malware.
A última análise ao sistema que iniciou foi abortada antes de ter terminado	Uma análise minunciosa de sistema já começou mas ainda não está completa.

incidência	Descrição
Antivírus está num estado crítico	A protecção em Tempo-real está desactivada e o sistema de análise está lento.

- **Actualização** - O BitDefender monitoriza se as assinaturas do malware estão actualizadas.

  As incidências comunicadas mais comuns desta componente estão listadas na tabela seguinte.

incidência	Descrição
Actualização Automática está desactivada	As assinaturas de malware do seu produto BitDefender não estão a ser automaticamente actualizadas regularmente.
A actualização já não é feita há x dias	As assinaturas de malware do seu produto BitDefender estão desactulizadas.

- **Firewall** - o BitDefender monotoriza o estado do Firewall. Se está desactivado, a incidência **Firewall está desactivado** será reportada.
- **Antispam** - o BitDefender monotoriza o estado do Antispam. Se está desactivado, a incidência **Antispam está desactivado** será reportada.
- **Antiphishing** - O BitDefender monitoriza o estado do Antiphishing. Se não está activado para todas as aplicações suportadas, a incidência **Antiphishing está desactivado** será reportada.
- **Análise de Vulnerabilidade** - O BitDefender monitoriza a opção Análise de Vulnerabilidade. A Análise de Vulnerabilidade permite-lhe saber se necessita de instalar actualizações do Windows, actualizações de aplicações ou se necessita de fortalecer quaisquer palavras-passe.

  As incidências comunicadas mais comuns desta componente estão listadas na tabela seguinte.

Estado	Descrição
A verificação de Vulnerabilidade está desactivada	O BitDefender não verifica vulnerabilidades potenciais com respeito a actualizações do Windows em falta, actualizações de aplicações ou palavras-passe fracas.
Múltiplas vulnerabilidades foram detectadas	O BitDefender descobriu actualizações do Windows/aplicação em falta e/ou palavras-passe fracas.

Estado	Descrição
Actualizações Criticas da Microsoft	Actualizações críticas da Microsoft estão disponíveis mas não instaladas.
Outras Actualizações da Microsoft	Actualizações não-críticas da Microsoft estão disponíveis mas não instaladas.
As Actualizações Automáticas do Windows estão desactivadas	As actualizações de segurança do Windows não estão a ser automaticamente instaladas tão rápido quanto se tornam disponíveis.
Aplicação (desactualizado)	Uma nova versão da Aplicação está disponível mas não está instalada.
Utilizador (Palavra-passe Fraca)	Uma palavra-passe de um utilizador é fácil de quebrar por gente maliciosa com software especializado.

13.2. Tarefas Rápidas

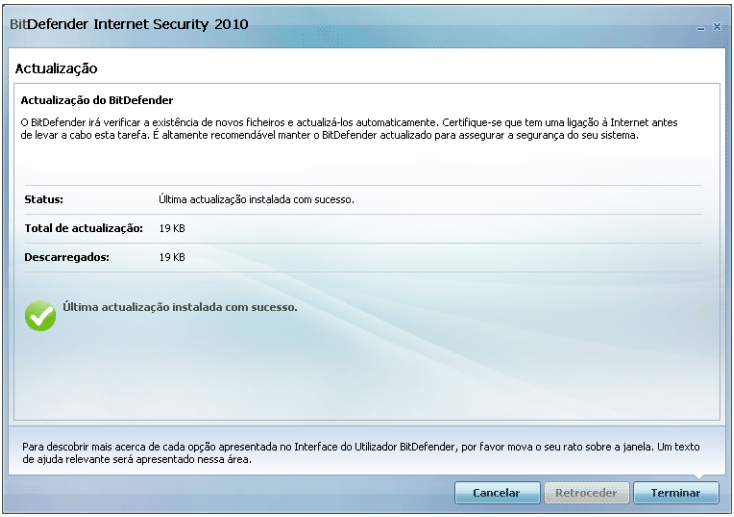
Aqui pode encontrar links para as mais importantes tarefas de segurança:

- **Actualizar agora** - executa uma actualização imediata.
- **Análise do Sistema** - inicia uma análise completa do seu computador (excepto arquivos). Para tarefas de análise adicionais clique na seta neste botão e seleccione uma tarefa de análise diferente: Análise Os Meus Documentos ou Análise Minuciosa do Sistema.
- **Análise Personalizada** - abre um assistente que lhe permite criar e utilizar uma tarefa de análise personalizada.
- **Análise de Vulnerabilidade** - inicia um assistente que verifica o seu sistema em busca de vulnerabilidades e ajuda-o a repará-las.

13.2.1. Actualizar o BitDefender

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado 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 ficheiros 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 está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.

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**. Recomendamos que reinicie o seu sistema o mais rápido possível.

13.2.2. A analisar com BitDefender

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

drop-down. A seguinte tabela aprsenta todas as tarefas disponíveis, com uma descrição de cada uma delas:

Tarefa	Descrição
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
Analisar Os Meus Documentos	Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto assegurará a segurança dos seus documentos, um espaço de trabalho seguro e aplicações limpas que se executam durante o iniciar do windows.
Análise Minuciosa 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 Personalizada	Use esta tarefa para escolher ficheiros ou pastas específicos a serem analisados.

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 nao estiver a ser utilizado.

Quando executa uma Análise ao Sistema, Análise Pormenorizada ao Sistema ou uma Análise aos meus Documentos, o assistente de Análise do Antivírus irá aparecer. Siga o processo guiado de três passos para completar o processo de análise. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).

Quando executa uma Análise Personalizada, o assistente de Análise Personalizada irá guiá-lo através do processo de análise. Siga o guia de seis passos para a análise de pastas e ficheiros específicos. Para mais informações sobre este assistente, por favor consulte o "*Assistente de Análise Personalizada*" (p. 60).

13.2.3. Procurar Vulnerabilidades

Verificação de Vulnerabilidade monitoriza as actualizações do Microsoft Windows, do Microsoft Windows Office e das palavras-passe das suas contas no Microsoft Windows para assegurar que o seu SO se encontra actualizado e não está vulnerável a quebras de palavra-passe.

Para verificar as vulnerabilidades do seu computador, clique em **Analisar Vulnerabilidades** e siga o procedimento do guia de seis-passos. Para mais informações, por favor consulte o "*Reparar Vulnerabilidades*" (p. 247).

14. Parental

O BitDefender Internet Security 2010 inclui um módulo de Controlo Parental. O Controlo Parental permite-lhe restringir o acesso das suas crianças à Internet e a determinadas aplicações. Para verificar o estado do Controlo Parental, clique na barra **Parental**.

Parental

O módulo Parental é composto de duas secções:

- **Área de Estado** - Permite-lhe ver se o Controlo Parental está configurado e permite-lhe activar/desactivar a monotorização da actividade deste módulo.
- **Tarefas** - Aqui é onde pode encontrar os links para as mais importantes tarefas de segurança: análise completa do sistema, análise minuciosa, actualizar agora.

14.1. Estado da Área

O estado actual do módulo de Controlo Parental é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

Círculo verde com uma marca de verificação: Não há incidências a infectarem o componente.

Circulo vermelho com um ponto de exclamação: Há incidências a infectarem o componente.

As frases que descrevem as incidências estão escritas a vermelho. Apenas clique no botão **Corrigir** correspondendo à frase para corrigir a incidência reportada. A incidência mais comum reportada para este módulo é **Controlo Parental não está configurado**.

Se deseja que o BitDefender monitorize o módulo de Controlo Prental, clique em **Configurar Estado de Monitorização** e seleccione a caixa de selecção **Activar alertas** para este módulo.

14.2. Tarefas Rápidas

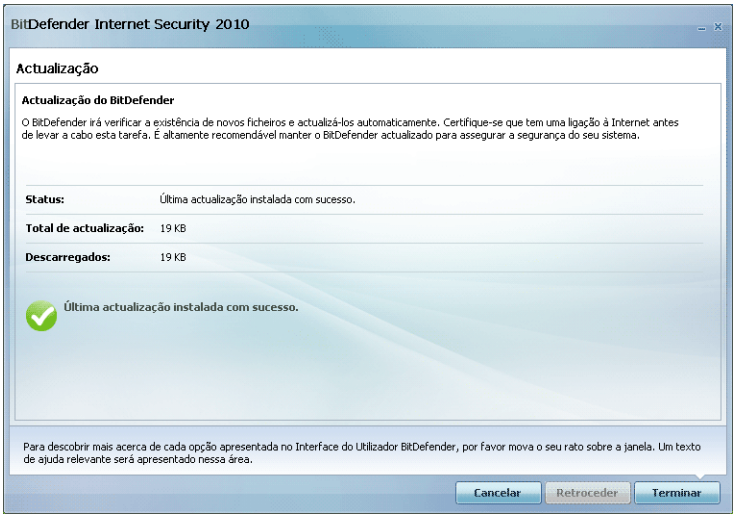
Aqui pode encontrar links para as mais importantes tarefas de segurança:

- **Actualizar agora** - executa uma actualização imediata.
- **Análise Completa do Sistema** - inicia uma análise completa ao seu computador (excluindo arquivos^).
- **Análise Minuciosa do Sistema** - inicia uma análise minuciosa ao seu computador.

14.2.1. Actualizar o BitDefender

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado 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 ficheiros 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 está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.

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**. Recomendamos que reinicie o seu sistema o mais rápido possível.

14.2.2. A analisar com BitDefender

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

Tarefa	Descrição
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
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 leva a cabo uma análise, o assistente de análise antivírus aparece. Siga o processo guiado de três passos para completar o processo de análise. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).

15. Cofre

BitDefender traz consigo um módulo de Cofre de Ficheiros que o ajuda a manter os seus dados não somente seguros, mas também confidenciais. Para atingir esse objectivo use a encriptação de ficheiros.

Com este recurso pode proteger ficheiros ao colocá-los no cofre de ficheiros.

- O cofre de ficheiros é um espaço de armazenamento seguro de informação pessoal ou de ficheiros considerados sensíveis.
- O cofre de ficheiros é um ficheiro 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 ficheiro 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 ficheiros. Será capaz de fazer operações com ficheiros nele (copiar, apagar, alterar, etc.). Os ficheiros estão protegidos na medida em que estejam residentes nesta drive (porque é necessária uma palavra-passe 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 Cofre de Ficheiros, clique na barra **Cofre de Ficheiros**.

Cofre

O módulo de Cofre de Ficheiros é composto de duas secções:

- **Área de Estado** - Permite-lhe ver toda a lista de componentes monotorizados. Pode escolher que componentes deseja monitorizar. É recomendável activar a opção de monitorização para todos eles.
- **Tarefas** - Aqui é onde pode encontrar os links para as tarefas de segurança mais importantes: adicionar, ver, fechar e apagar cofres de ficheiros.

15.1. Estado da Área

O estado actual de um componente é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

Círculo verde com uma marca de verificação: Não há incidências a infectarem o componente.

Circulo vermelho com um ponto de exclamação: Há incidências a infectarem o componente.

As frases que descrevem as incidências estão escritas a vermelho. Apenas clique no botão **Corrigir** correspondendo à frase para corrigir a incidência reportada. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

a área de estado na tabela de Cofre de Ficheiros fornece informação sobre o estado do módulo **Encriptação de Ficheiros**

Se deseja que o BitDefender monitorize o módulo de Encriptação de Ficheiros, clique em **Configurar Estado de Monitorização** e seleccione a caixa de selecção **Activar alertas**.

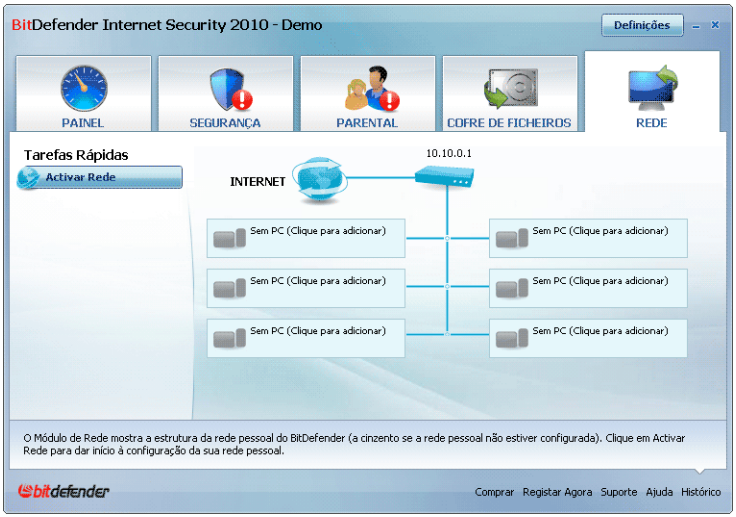
15.2. Tarefas Rápidas

Estão disponíveis os seguintes botões:

- **Adicionar ao Cofre** - inicia o assistente que lhe permite armazenar de forma privada os seus ficheiros / documentos importantes ao encriptá-los em drives de cofre especiais. Para mais informações, por favor consulte o "*Adicionar Ficheiros ao Cofre*" (p. 75).
- **Remover do Cofre** - inicia o assistente que lhe permite apagar dados do cofre de ficheiros. Para mais informações, por favor consulte o "*Remover do Cofre*" (p. 81).
- **Ver cofre** - inicia o assistente que lhe permite ver o conteúdo do cofre de ficheiros. Para mais informações, por favor consulte o "*Ver Cofre de Ficheiros*" (p. 86).
- **Fechar cofre** - inicia o assistente que lhe permite fechar o cofre de forma a dar início à protecção do seu conteúdo. Para mais informações, por favor consulte o "*Fechar Cofre*" (p. 90).

16. Rede

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



Rede

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

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

16.1. Tarefas Rápidas

Inicialmente só um botão está disponível.

- **Activa a Rede** permite-lhe definir a palavra-passe de rede, e assim criar e aderir a uma rede.

Após aderir à rede, mais botões irão surgir.

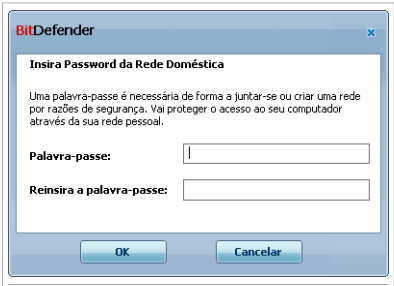
- **Desactiva a Rede** - permite-lhe sair da rede.
- **Adicionar PC** - permite-lhe adicionar computadores à sua rede.

- **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.

16.1.1. Aderir à Rede BitDefender

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

1. Clique em **Activar Rede**. Será notificado para configurar a palavra-passe de gestão de rede pessoal.



Configurar Palavra-passe

2. Insira a mesma palavra-passe em cada um dos campos editáveis.
3. Clique em **OK**.

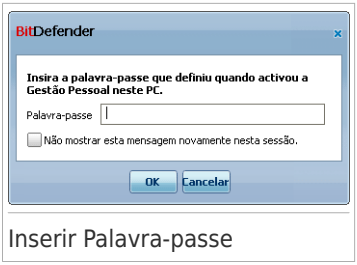
Pode ver o nome do computador a aparecer no mapa de rede.

16.1.2. Adicionar Computadores à Rede BitDefender

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

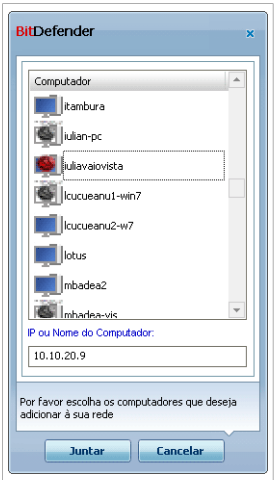
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

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



Inserir Palavra-passe

2. Insira a palavra-passe 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:

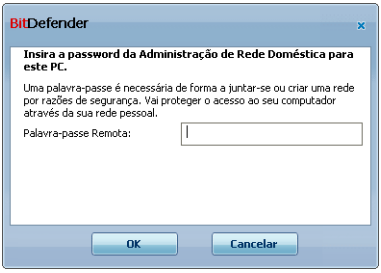
Indica um computador on-line sem produtos BitDefender instalados.

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. Prima **Adicionar**. Será notificado para inserir a sua palavra-passe de gestão de rede pessoal do respectivo computador.



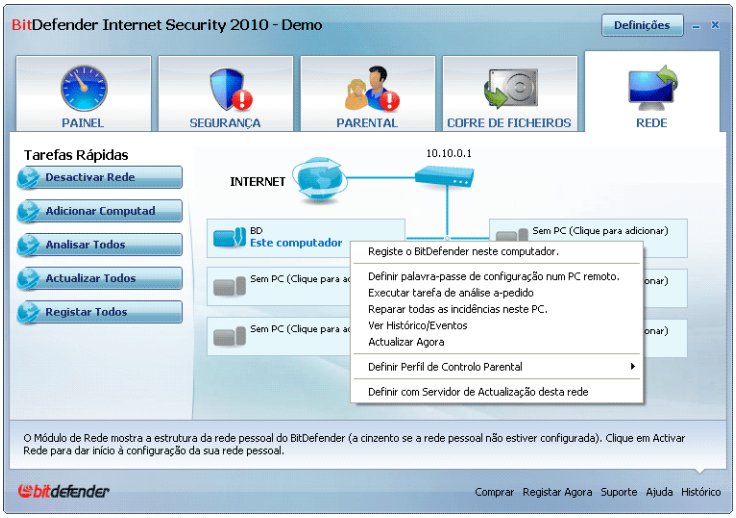
Autenticar

5. Insira a palavra-passe de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**. Se forneceu a palavra-passe correcta, a nome do computador seleccionado aparecerá no mapa de rede.

Nota
Pode adicionar até cinco computadores neste mapa de rede.

16.1.3. Gerir a Rede BitDefender

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



Mapa de Rede

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

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

- **Remover o PC da rede local de casa**

  Permite-lhe remover um PC da Rede.

- **Registar o BitDefender neste computador**

  Permite-lhe registar o BitDefender neste computador introduzindo a chave de licença.

- **Definir palavra-passe para acesso às definições num computador remoto**

  Permite-lhe criar uma password para restringir o acesso às definições do BitDefender nestes PC.

- **Executar uma tarefa de análise a-pedido**

  Permite-lhe executar uma análise a-pedido remota a partir de outro computador. Pode efectuar uma das seguintes tarefas: Análise Os Meus Documentos, Análise Completa do Sistema e Análise Minunciosa do Sistema.

- **Reparar incidências neste computador**

Permite-lhe reparar as incidências que estão a afectar a segurança deste computador seguindo o assistente Reparar Todas as Incidências.

- **Histórico**

  Permite-lhe aceder ao módulo **Histórico&Eventos** do produto BitDefender instalado neste computador.

- **Actualizar Agora**

  Inicia o processo de Actualização para o produto BitDefender installado neste computador.

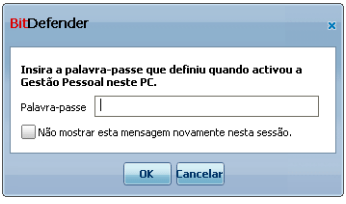
- **Palavra-passe do Controlo Parental**

  Permite-lhe definir as categorias de faixas etárias a serem utilizadas pelo filtro de Web do Controlo Parental: crianças, adolescentes ou adultos.

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

  Permite-lhe definir este computador como servidor de actualizações para todos os produtos BitDefender instalados nos computadores desta rede. A utilização desta opção reduz o trafego de internet, porque apenas um computador vai necessitar de aceder a internet para descarregar as actualizações.

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



Inserir Palavra-passe

Insira a palavra-passe de gestão rede pessoal e clique em **OK**.

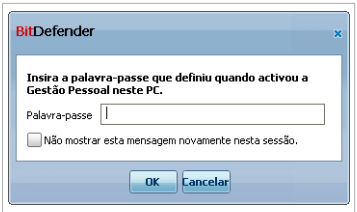
Nota

Se planeia levar a cabo várias tarefas, talvez queira seleccionar **Não me mostrem mais esta mensagem durante esta sessão**. Ao seleccionar esta opção, não será notificado novamente pela palavra-passe durante esta sessão.

16.1.4. Analisar Todos os Computadores

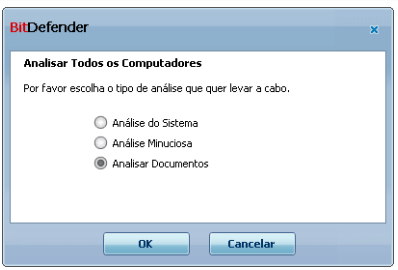
Para analisar todos os computadores geridos, siga estes passos:

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



Inserir Palavra-passe

2. Seleccione o tipo de análise.
   - **Análise Completa do Sistema** - inicia uma análise completa ao seu computador (excluindo arquivos^).
   - **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.



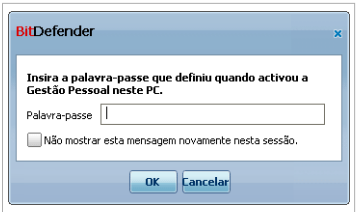
Seleccionar o Tipo de Análise

3. Clique em **OK**.

16.1.5. Actualizar Todos os Computadores

Para actualizar todos os computadores, siga estes passos:

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



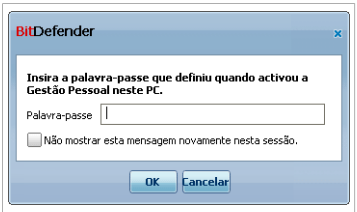
Inserir Palavra-passe

2. Clique em **OK**.

16.1.6. Registar Todos os Computadores

Para registar todos os computadores geridos, siga estes passos:

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



Inserir Palavra-passe

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

Registar Todos

3. Clique em **OK**.

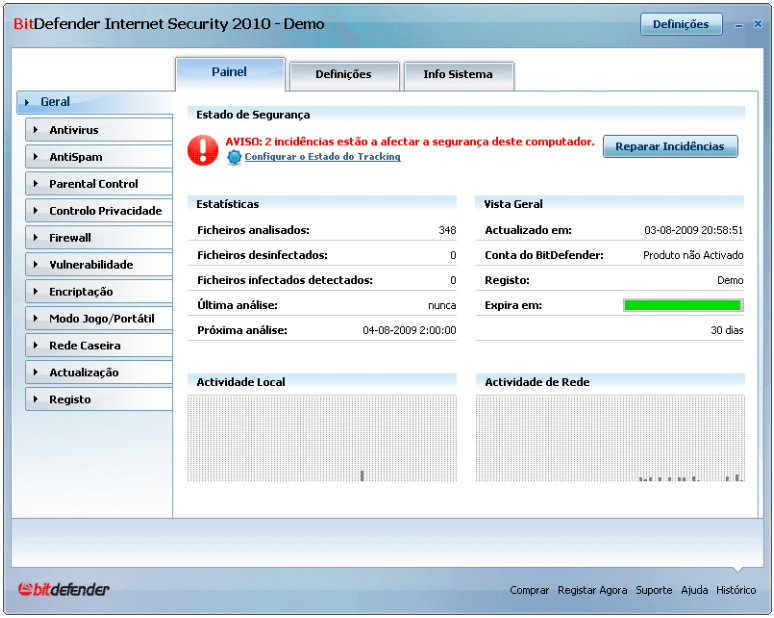
Modo Avançado

17. Geral

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

17.1. Painel

Para ver se alguma incidência está a afectar o seu computador, assim como as estatísticas de actividade do produto e o seu estado de registo, vá em no Modo Avançado a **Geral>Painel**.



Painel

O painel é composto de várias secções:

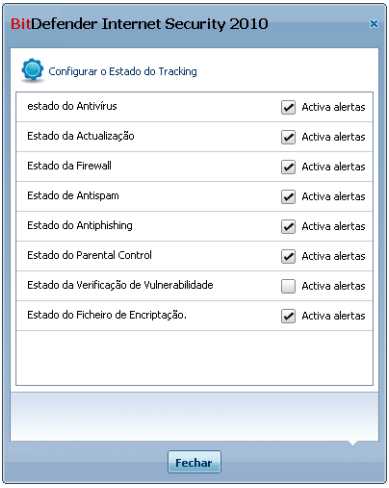
- **Estado Geral** - Informa-lhe de qualquer incidência que esteja a afectar a segurança do seu computador.
- **Estaísticas** - Mostra informação importante com respeitoà actividade do BitDefender.
- **Visão Geral** - Mostra o estado da actualização, o estado da sua conta, e informação do seu registo e licença.

- **Actividade de Ficheiro** - 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.

17.1.1. Estado Geral

Aqui pode verificar a quantidade de incidências que afectam a segurança do seu PC Para remover todas as ameaças, clique em **Reparar Todas as Incidências**. Isto iniciará o assistente Reparar Todas as Incidências.

Para configurar os módulos que serão monotorizados pelo BitDefender Internet Security 2010, clique em **Configurar o Estado da Monitorização**. Uma nova janela irá aparecer.



Configurar o Estado do Tracking

Se deseja que o BitDefender monitoriza um componente, seleccione a caixa de selecção **Activar alertas** para o componente. O estado de seguranças das seguintes componentes pode ser monitorizado pelo BitDefender:

- **Antivirus** - O BitDefender monitoriza o estado das duas componentes da funcionalidade Antivírus: proteção em tempo real e uma análise a pedido.

  As incidências comunicadas mais comuns desta componente estão listadas na tabela seguinte.

incidência	Descrição
Protecção de ficheiros em Tempo-real está desactivada	Os ficheiros não são analisados à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.
Nunca analisou o seu computador em busca de malware	Uma análise a-pedido nunca foi levada a cabo para verificar se os ficheiros armazenados no seu computador estão livres de malware.
A última análise ao sistema que iniciou foi abortada antes de ter terminado	Uma análise minunciosa de sistema já começou mas ainda não está completa.
Antivírus está num estado crítico	A protecção em Tempo-real está desactivada e o sistema de análise está lento.

- **Actualização** - O BitDefender monitoriza se as assinaturas do malware estão actualizadas.

  As incidências comunicadas mais comuns desta componente estão listadas na tabela seguinte.

incidência	Descrição
Actualização Automática está desactivada	As assinaturas de malware do seu produto BitDefender não estão a ser automaticamente actualizadas regularmente.
A actualização já não é feita há x dias	As assinaturas de malware do seu produto BitDefender estão desactulizadas.

- **Firewall** - o BitDefender monotoriza o estado do Firewall. Se está desactivado, a incidência **Firewall está desactivado** será reportada.
- **Antispam** - o BitDefender monotoriza o estado do Antispam. Se está desactivado, a incidência **Antispam está desactivado** será reportada.
- **Antiphishing** - O BitDefender monitoriza o estado do Antiphishing. Se não está activado para todas as aplicações suportadas, a incidência **Antiphishing está desactivado** será reportada.
- **Controlo Parental** - O BitDefender monotoriza o estado do desempenho do Controlo Parental. Se não está activado, a incidência **Controlo Parental não está configurado** será reportada.
- **Análise de Vulnerabilidade** - O BitDefender monitoriza a opção Análise de Vulnerabilidade. A Análise de Vulnerabilidade permite-lhe saber se necessita de

instalar actualizações do Windows, actualizações de aplicações ou se necessita de fortalecer quaisquer palavras-passe.

As incidências comunicadas mais comuns desta componente estão listadas na tabela seguinte.

Estado	Descrição
A verificação de Vulnerabilidade está desactivada	O BitDefender não verifica vulnerabilidades potenciais com respeito a actualizações do Windows em falta, actualizações de aplicações ou palavras-passe fracas.
Múltiplas vulnerabilidades foram detectadas	O BitDefender descobriu actualizações do Windows/aplicação em falta e/ou palavras-passe fracas.
Actualizações Criticas da Microsoft	Actualizações críticas da Microsoft estão disponíveis mas não instaladas.
Outras Actualizações da Microsoft	Actualizações não-críticas da Microsoft estão disponíveis mas não instaladas.
As Actualizações Automáticas do Windows estão desactivadas	As actualizações de segurança do Windows não estão a ser automaticamente instaladas tão rápido quanto se tornam disponíveis.
Aplicação (desactualizado)	Uma nova versão da Aplicação está disponível mas não está instalada.
Utilizador (Palavra-passe Fraca)	Uma palavra-passe de um utilizador é fácil de quebrar por gente maliciosa com software especializado.

- A **Encriptação de Ficheiros** monotoriza o estado do Cofre de Ficheiros. Se não está activada, a incidência **Encriptação de Ficheiros está desactivada** será reportada.

Importante

Para se certificar de que o seu sistema está completamente protegido, por favor permita a análise a todos os componentes e resolva todas as incidências reportadas.

17.1.2. 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
Ficheiros analisados	Indica o número de ficheiros que foram analisados até ao momento da sua última análise.
Ficheiros desinfectados	Indica o número de ficheiros que foram desinfectados até ao momento da sua última análise.
Foram detectados ficheiros infectados	Indica o número de vírus detectados no seu sistema até ao momento da sua última análise.
Última análise do sistema	Indica quando o seu computador foi analisado pela última vez. Se a última análise foi feita há mais de uma semana, faça uma análise ao seu computador o mais rápido possível. Para analisar todo o computador, vá para a barra**Antivirus**, Virus Scan, e execute a Análise Completa do Sistema ou a Análise Minuciosa do Sistema.
Próxima análise	Indica a próxima altura em que o seu computador vai ser analisado.

17.1.3. Vista Geral

Aqui é onde pode ver o estado da actualização, da sua conta e do registo e a informação da sua licença.

Item	Descrição
Última actualização	Indica quando o seu BitDefender foi actualizado da última vez. Leve a cabo actualizações regulares de forma a manter o seu sistema completamente protegido.
Conta BitDefender	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. Tem de criar uma conta BitDefender de forma a activar o produto. Para saber mais informação acerca da conta BitDefender, por favor consulten o “*Registo e a Minha Conta*” (p. 51).
Registo	Indica o seu tipo de licença e o seu estado. Para manter o seu sistema seguro tem de renovar ou efectuar o upgrade do BitDefender se a sua chave de licença tiver expirado.
Expira em	Indica o número de dias que faltam até que a sua chave de licença expire. Se a sua chave de licença expirar nos próximos dias, por favor registe o produto com uma nova chave de licença. Para adquirir a chave de licença ou para

Item	Descrição
	renovar a sua licença, clique no link **Comprar/Renovar**, localizado no fundo da janela.

17.2. Definições

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

Configuração Geral

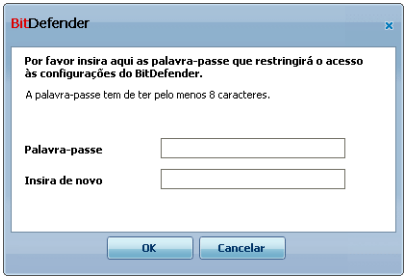
Aqui, pode visualizar o comportamento geral do BitDefender. Por defeito, o BitDefender é carregado ao iniciar o Windows e decorre minimizado da barra do sistema.

17.2.1. Configuração Geral

- **Activar protecção das configurações por palavra-passe** - activa a definição de uma palavra-passe de forma a proteger a configuração do BitDefender.

Nota
Se não for a única pessoa a utilizar este computador, recomendamos que protega as suas configurações do BitDefender com uma palavra-passe.

Se seleccionar esta opção, a seguinte janela aparecerá:



Confirmação da palavra passe

Introduza a palavra-passe no campo **Palavra-role="passe**, insira-a novamente no campo **Inserir de novo** e clique em **OK**.

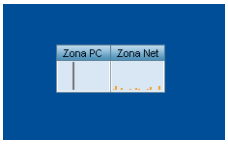
Uma vez que tenha definido a palavra-passe, será solicitado que a insira sempre que deseje alterar as configurações do BitDefender. Os outros administradores de sistema (se existirem) também terão de inserir a palavra-passe se desejarem alterar as configurações do BitDefender.

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

Importante
Se se esqueceu da palavra-passe, terá de reparar o produto para que possa modificar a configuração do BitDefender.

- **Solicitar palavra-passe quando activar o Controlo Parental** - se esta opção estiver activada e nenhuma palavra-passe estiver definida, ser-lhe-á solicitado que a defina quando activar o Controlo Parental. Ao definir uma palavra-passe, irá prevenir que outros utilizadores com direitos administrativos possam mudar as suas definições do Controlo Parental que configurou para um determinado utilizador.
- **Mostrar Notícias BitDefender (notificações de segurança)** - mostra de tempos em tempos, notificações de segurança relacionadas com epidemias de vírus, enviadas pelo servidor do BitDefender.
- **Mostrar pop-ups (notas no ecrã)** - apresenta uma janela de pop-up no windows que mostra o estado do produto. Pode configurar o BitDefender para exibir pop-ups apenas quando a interface está no Modo Básico / Intermédio or no Modo Avançado.

- **Mostra a barra de Actividade da Análise (gráfico no ecrã da actividade do produto)** - Exibe a barra de Actividade da Análisesempre que entrar no Windows. Limpe esta caixa se deseja que a barra de Actividade da Análise não seja mostrada daí em diante.



Barra de Actividade da Análise

Nota

Esta opção pode ser configurada apenas para a actual conta de utilizador Windows. a barra de actividade da análise só está disponível quando o interface está no Modo Avançado.

17.2.2. Configuração do Relatório de Vírus

- **Enviar relatórios de vírus** - envia relatórios que contêm vírus identificados no seu computador para os Laboratórios do BitDefender. Ajuda-nos a seguir o rasto das quebras dos vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados com fins comerciais. A informação fornecida irá conter apenas o nome do vírus e será usada, somente para criar relatórios estatísticos.

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

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o potencial vírus e será usada somente para ajudar a detectar novos vírus.

17.3. Informação do Sistema

BitDefender permite-lhe visualizar, a partir de uma única localização, todas as configurações do sistema e as aplicações registadas para se executarem durante o iniciar do Windows. Desta forma, pode gerir a 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 inicia o sistema assim como os itens carregados pelas diferentes aplicações.

Estão disponíveis três botões:

- **Restaurar** - muda a actual associação de ficheiros para o modo por defeito. Disponível apenas para as definições das **Associações de Ficheiros**!
- **Ir para** - abre uma janela onde o item seleccionado é colocado (o **Registo** por exemplo).

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

- **Actualizar** - reabre a secção de **Info Sistema**.

18. Antivirus

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

- Protecção em Tempo-real - previne que novas ameaças de malware entrem no seu sistema. Poe 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 protecção em Tempo-real, também referida como análise no-acesso - os ficheiros são analisados à medida que os utilizadores lhes acedem.

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

18.1. 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 ficheiros 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**.

Pra dar início a uma análise do sistema, clique **Analisar Agora**.

18.1.1. 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:

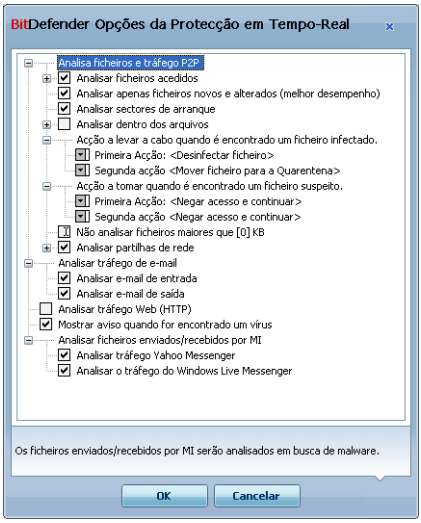
Nível de Protecção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Apenas ficheiros e mensagens de e-mail de entrada são analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/mover para a quarentena.
Por Defeito	Oferece segurança standard. O nível de consumo de recursos é baixo. Todos os ficheiros e mensagens de e-mail de entrada&saida 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 ficheiros infectados são as seguintes: limpar/mover para a quarentena.
Agressivo	Oferece uma segurança elevada. O nível de consumo de recursos é moderado. Todos os ficheiros, mensagens de e-mais de entrada&saida 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 ficheiros infectados são as seguintes: limpar ficheiro/mover para a quarentena.

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

18.1.2. Personalizando Nível de Protecção

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias 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 o "+" para abrir uma opção, ou na caixa com o "-" para fechar uma opção.

Nota
Pode observar que algumas opções de verificação, apesar de terem o sinal "+", não podem ser abertas. Isto acontece porque estas opções ainda não foram seleccionadas. Irá observar que se as seleccionar, elas poderão ser abertas.

- **Analise ficheiros acedidos e opçoes de transferências P2P** - examina os ficheiros acedidos e as comunicações feitas através de aplicações de software de Mensagens Instântaneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Mais adiante, seleccione o tipo de ficheiros que pretender examinar.

Opção		Descrição
Analisar ficheiros acedidos	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Apenas serão examinados os ficheiros de programa. Isto significa, apenas os ficheiros com as seguintes extensões: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`;

Opção		Descrição
		.ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Analisar as extensões definidas pelo utilizador	Apenas serão examinadas as extensões especificadas pelo utilizador. Estas extensões têm de estar separadas por ";".
	Analisar em busca de riskware	Analisar em busca de riskware. Os ficheiros detectados serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa. Seleccione **Saltar aplicaçõess dialers durante a análise** e/ou **Saltar keyloggers durante a análise** se deseja excluir este tipo de ficheiros durante a análise.
Analisar só ficheiros alterados		Analisar ficheiros que não foram anteriormente analisados ou que foram alterados desde a última vez que foram analisados. Ao seleccionar esta opção, pode melhorar grandemente a performance do seu sistema sem comprometer a sua segurança.
Analisar os sectores de saída		Verifica o sector de saída do sistema.
Analisar dentro dos arquivos		Também serão examinados os arquivos acedidos. Com esta opção, o computador irá abrandar. Pode definir o tamanho máximo dos arquivos a serem analisados (em kilobytes, escreva 0 se quiser que todos os arquivos a sejam analisados) e a compressão máxima do arquivo a analisar.
Primeira Acção		Seleccionar do menu drop-down a primeira acção a levar a cabo sobre um ficheiro infectado ou suspeito.
	Negar acesso e continuar	Será negado o acesso de um ficheiro que se encontre infectado.

Opção		Descrição
	Desinfectar ficheiro	Remove o código de malware dos ficheiros infectados.
	Apagar ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
	Mover ficheiro para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Segunda Acção		Seleccionar do menu drop-down a segunda acção a levar a cabo sobre um ficheiro infectado, caso a primeira acção falhe.
	Negar acesso e continuar	Será negado o acesso de um ficheiro que se encontre infectado.
	Apagar ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
	Mover ficheiro para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Não analisar ficheiros maiores do que [x] Kb		Insira o tamanho máximo dos ficheiros a serem analisados. Se o tamanho for 0 Kb, todos os ficheiros serão examinados, independentemente do seu tamanho.
Analisar partilhas de rede	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Apenas serão examinados os ficheiros de programa. Isto significa, apenas os ficheiros 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`.

Opção		Descrição
	Analisar as extensões definidas pelo utilizador	Apenas serão examinadas as extensões especificadas pelo utilizador. Estas extensões têm de estar separadas por ";".

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

  Estão disponíveis as seguintes opções:

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.
- **Mostrar aviso quando for encontrado um vírus** - quando um vírus é encontrado num ficheiro ou numa mensagem de e-mail, irá aparecer uma janela de alerta.

  Para um ficheiro infectado, ajanela de alerta contém o nome e o caminho para o vírus, no caso de um e-mail infectado, a janela irá conter informação acerca do emissor, do receptor e o nome do vírus.

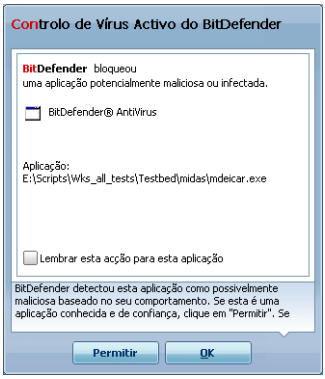
  Em caso de um ficheiro suspeito ser detectado pode executar um wizard a partir da janela de alerta que o ajudará a enviar esse ficheiro para o Laboratório BitDefender para uma análise posterior. Pode inserir o seu endereço de e-mail para receber informação relativa a este relatório.
- **Analisar ficheiros recebidos/enviados por IM.** Para analisar todos os ficheiros enviados ou recebidos via Yahoo Messenger ou Windows Live Messenger, seleccione a correspondente caixa.

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

18.1.3. Configurar as Definições do Controlo Activo de Vírus

O Controlo Activo de Vírus BitDefender (AVC) 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 AVC pode ser configurado para o alertar e pedir-lhe para agir sempre que uma aplicação tentar executar umas acção possivelmente maliciosa.



Alerta do AVC BitDefender

Se conhece e confia na aplicação detectada, clicque em **Permitir**.

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

Seleccione a caixa de selecção **Lembrar esta acção para esta aplicação** antes de fazer a sua escolha e o BitDefender tomará a mesma acção no futuro para a aplicação detectada. A regra criada será listada na tabela abaixo sob **Exclusões**.

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

Definições de AVC do BitDefender

Seleccione a marca da caixa correspondente para activar o Controlo Activo de Vírus.

Importante

Mantenha o Controlo Activo de Vírus activado de forma a estar protegido contra vírus desconhecidos.

Se quiser ser alertado e solicitado a agir pelo Controlo Activo de Vírus sempre que uma aplicação tentar executar uma acção maliciosa, seleccione a caixa de selecção **Pergunte-me antes de tomar uma acção**.

Configurar Nível de Protecção

O nível de protecção do AVC 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. Se definir o nível da protecção em tempo-real como **Permissivo**, o Analisador Comportamental é automaticamente desligado e não o pode configurar.

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	Uma monitorização rigorosa de todas as aplicações, para possíveis acções maliciosas.
Por Defeito	Os niveis de detecção são elevados e há a possibilidade de falsos positivos.
Médio	A monitorização de aplicação é moderada, é possivel de haver falsos positivos.
Permissivo	Os niveis de detecção são baixos e não existem falsos positivos.

Gerir a Lista de Aplicações Confiáveis/Não Confiáveis

Pode adicionar aplicações, que sabe que são fiáveis, à ista de aplicações fiáveis. Essas aplicação não serão mais analisadas pelo Controlo Activo de Vírus do BitDefender e será automaticamente permitido o acesso. Do mesmo modo, as aplicações a que pretende negar o acesso podem ser adicionadas á lista de aplicações não confiáveis e o Controlo Activo de Vírus do BitDefender irá automaticamente bloqueá-las.

As aplicações para as quais criou regras estão listadas na tabela abaixo sob **Exclusões**. O caminho para a aplicação e a acção que definiu para ela (Permitido ou Bloqueado) é exibido para cada regra.

Para gerir a lista, utiize os botões que se encontram por cima da tabela:

- **Adicionar** - para adicionar a nova entrada na lista.
- **Remover** - remove a aplicação da lista.
- **Editar** - Edita uma regra de aplicação.

18.1.4. Desactivando a Protecção em Tempo-real

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

18.1.5. 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 mais informações, por favor consulte *"Integração com Exploradores web"* (p. 291).

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

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

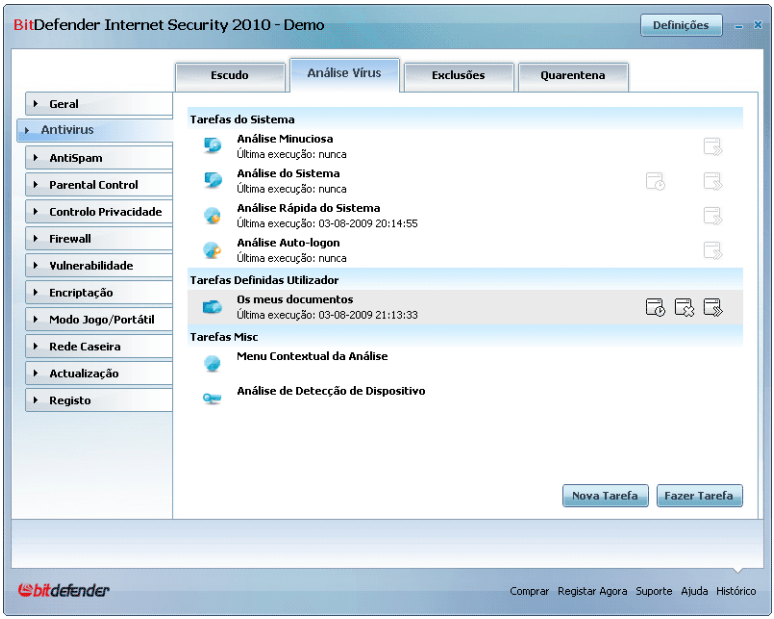
18.2. Análise a-pedido

O objectivo principal do BitDefender é manter o seu computador livre de vírus. Isto é inicialmente e essencialmente feito, mantendo novos vírus fora do seu computador

e ao examinar as suas mensagens de e-mail e novos ficheiros descarregados ou copiados para o seu sistema.

Há o risco de o vírus já ter acedido ao seu sistema, antes mesmo de ter instalado o BitDefender. Este é o motivo, pelo qual é uma excelente ideia verificar vírus residentes no seu computador depois de instalar o BitDefender. E é defenitivamente uma boa ideia, a verificação frequente de vírus no seu computador.

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 utilizador). 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

18.2.1. 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. 143)*.

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 por Defeito	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 do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
Análise Rápida do Sistema	Analisa as pastas do `Windows` e dos `Programas`. Na configuração por defeito, 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 utilizador entra no Windows. Por defeito, a análise ao logon está desactivada. Se deseja usar esta tarefa, faça clique botão direito nela, selecione **Agendar** e defina a tarefa para ser executada no**arranque do sistema**. Pode definir quanto tempo após o iniciar do sistema a tarefa deve de ser iniciada.

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 nao estiver a ser utilizado.

- **Tarefas do Utilizador** - contém as tarefas definidas pelo utilizador.

Uma tarefa chamada `Os Meus Documentos` é fornecida. Use esta tarefa para analisar pastas de utilizadores actuais: `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.

Estão disponíveis três botões à direita de cada tarefa:

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

Nota

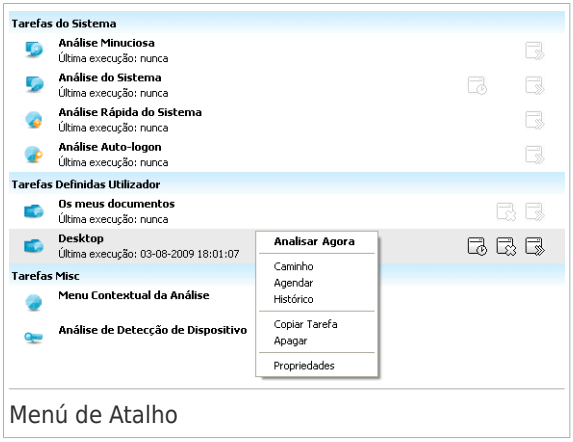
Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

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

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

18.2.2. Usando o Menú de Atalho

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



Menú de Atalho

Os seguintes comandos estão disponíveis no menu de atalho:

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.
- **Caminho** - Abre a janela das **Propriedades**, botão Caminho onde pode modificar o alvo da análise para a tarefa seleccionada.

Nota
No caso de tarefas do sistema, esta opção é substituida por **Mostrar Caminhos de Análise**, onde apenas poderá ver o alvo da sua análise.

- **Agendar** - abre a janela das **Propriedades** e o botão Agendar, onde pode agendar a tarefa seleccionada.
- **Relatórios** - abre a janela das **Propriedades** e o botão Relatórios onde pode ver os relatórios gerados após as tarefas seleccionadas terem sido executadas.
- **Duplicar Tarefa** - duplica a tarefa seleccionada. Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
- **Apagar** - elimina a tarefa seleccionada.

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

- **Propriedades** - abra a janela **Propriedades**, e o botão Geral , onde pode modificar as configurações para a tarefa seleccionada.

Nota
Devido à sua natureza em particular, das **Tarefas Misc** categoria, apenas **Ver Relatório** e **Propriedades** estão disponíveis neste caso.

18.2.3. Criando Tarefas de Análise

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

- Duplique uma tarefa existente, altere o nome e faça as modificaçoes necessárias na janela Propriedades.
- Clique em **Nova Tarefa** para criar uma nova tarefa e configurá-la.

18.2.4. Configurar Tarefas de Análise

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

Nota
Para mais informação sobre ver os logs e a barra de **Logs** tab, por favor consulte "*Ver os Relatórios da Análise*" (p. 163).

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:

Vista Geral

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
Permissivo	Oferece uma eficiência razoável de detecção. O consumo de recursos é baixo.

Nível de Protecção	Descrição
	Os programas são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.
Por Defeito	Oferece uma boa eficiência de detecção. O nível de consumo de recursos é moderado. Todos os ficheiros 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 ficheiros 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:

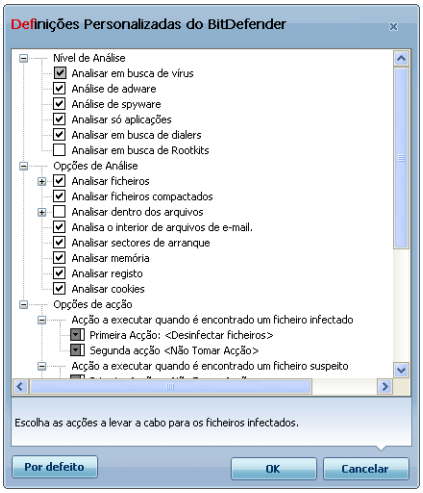
- **Execute a tarefa de análise com prioridade baixa.** Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
- **Minimizar a janela da análise para a área de notificação.** Minimiza a janela da análise no Windows para a área de notificação. Faça duplo-clique sobre o ícone BitDefender para o abrir.
- **Desligar o PC quando a análise terminar 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 utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

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



Configurações da Análise

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

As opções de análise estão 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 ficheiros serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa.
Análisar spyware	Analisa em busca de ameaças de spyware. Estes ficheiros serão tratados como ficheiros infectados.

Opção	Descrição
Analisar aplicações	Analisar aplicações legítimas que podem ser usadas como ferramenta de espionagem, para ocultar aplicações maliciosas ou outras intenções maliciosas.
Analisa em busca de dialers	Procura aplicações de liga~ção para números de valor acrescentado. Estes ficheiros serão tratados como ficheiros 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 (ficheiros e processos), conhecidos por rootkits.

- **Opções de análise de vírus.** Especifique que tipo de objectos devem ser analisados (ficheiros, arquivos e por aí fora) ao seleccionar as opções apropriadas da categoria **Opções de análise de vírus**.

Opção		Descrição
Análise de ficheiros	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros, independentemente do seu tipo.
	Analisar apenas os programas	Verifica apenas ficheiros de programa. Isto significa apenas ficheiros 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`.
	Analisar as extensões definidas pelo utilizador	Apenas serão examinadas as extensões especificadas pelo utilizador. Estas extensões têm de estar separadas por ";".
Analisar ficheiros compactados		Verifica todos os ficheiros compactados.
Analisar dentro dos arquivos		Analisa o interior de arquivos vulgares, tais como `.zip`, `.rar`, `.ace`, `.iso` e outros. Seleccione a **Analisar instaladores e arquivos chm** active a opção se pretender que esses tipos de arquivos sejam analisados.

Opção	Descrição
	Analisar ficheiros arquivados aumento o tempo da análise e requer mais recursos do sistema. Pode definir o tamanho máximo dos arquivos a analisar em kilobytes (KB) ao inserir o tamanho neste campo **Limitar tamanho do arquivo a analisar em**.
Analisar arquivos de e-mail	Verifica arquivos de e-mail internos.
Analisar os sectores de saída	Verifica o sector de saída do sistema.
Analisar Memória	Analisa a memória em busca de vírus e outro malware.
Analisa registo	Analisa entradas de registo.
Analisa cookies	Analisa os ficheiros cookie.

- **Opções de acção.** Especifique as ações a serem tomadas em cada categoria de ficheiros detectados usando as opções nesta categoria.

Nota

Para definir uma nova acção, clique na actual **Primeira acção** e seleccione a opção desejada a partir do menu. Especifique uma **Acção secundária** caso haja falha na principal.

▶ Seleccione a acção a ser tomada sobre o ficheiro infectado. Estão disponíveis as seguintes opções:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros infectados. Estes ficheiros aparecerão no ficheiro de relatório.
Desinfectar ficheiros	Remover o código de malware dos ficheiros infectados detectados.
Apagar ficheiros	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
Mover ficheiros para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

▶ Seleccionar a acção a tomar sobre um ficheiro suspeito. Estão disponíveis as seguintes opções:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros suspeitos. Estes ficheiros aparecerão no ficheiro de relatório.
Apagar ficheiros	Apaga imediatamente e sem qualquer aviso, os ficheiros suspeitos.
Mover ficheiros para a quarentena	Move os ficheiros suspeitos para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

Nota

Há ficheiros 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). Estão disponíveis as seguintes opções:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros ocultos. Estes ficheiros aparecerão no ficheiro de relatório.
Renomear ficheiros	Altera o nome dos ficheiros ocultos ao acrescentar `.bd.ren` ao seu nome. Como resultado, será capaz de procurar e encontrar tais ficheiros no seu computador, se existirem.
Mover ficheiros para a quarentena	Move os ficheiros ocultos para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

Nota

Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits. Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

▶ **Opções de acção para ficheiros protegido por palavra-passe e para ficheiros encriptados.** Os ficheiros encriptados a usar o Windows poderão ser importantes para si. É por isso que pode configurar diferentes acções a serem levadas a cabo em ficheiros infectados ou suspeitos que estejam encriptados a usar o Windows. Outra categoria de ficheiros que requerem atenção especial são aqueles protegidos por palavra-passe. Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe. Use estas opções para configurar as acções a serem levadas a cabo sobre os ficheiros protegidos por palavra-passe ou encriptados em Windows.

– **Acção a levar a cabo quando é encontrado um ficheiro encriptado.** Escolha a acção a ser levada a cabo em ficheiros infectados que estão encriptados em Windows. Estão disponíveis as seguintes opções:

Acção	Descrição
Não Tomar Acção	Apenas registe os ficheiros infectados que estão encriptados em Windows. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.
Desinfectar ficheiros	Remover o código de malware dos ficheiros infectados detectados. A desinfecção pode falhar nalguns casos, tais como quando o ficheiro infectado se encontra dentro de um ficheiro de correio específico.
Apagar ficheiros	Remover imediatamente do disco e sem qualquer aviso, os ficheiros infectados.
Mover ficheiros para a quarentena	Mover os ficheiros infectados da sua localização original para a Quarentena O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

– **Acção a levar a cabo quando é encontrado um ficheiro encriptado suspeito.** Escolha a acção a ser levada a cabo em ficheiros suspeitos que estão encriptados em Windows. Estão disponíveis as seguintes opções:

Acção	Descrição
Não Tomar Acção	Apenas registe os ficheiros suspeitos que estão encriptados em Windows. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

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

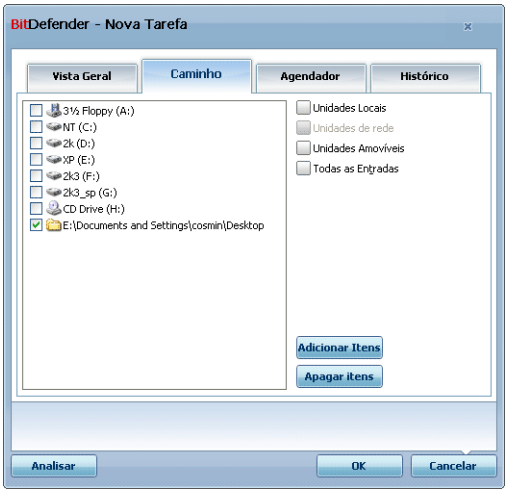
- **Acção a levar a cabo quando é encontrado um ficheiro protegido por palavra-passe.** Seleccione a acção a ser tomada sobre os ficheiros detectados protegidos por palavra-passe. Estão disponíveis as seguintes opções:

Acção	Descrição
Apenas relatório	Apenas manter registo dos ficheiros arquivados protegidos por palavra-passe no relatório da análise. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.
Solicitar palavra-passe	Quando é detectado um ficheiro protegido por palavra-passe, pedir ao utilizador para inserir a palavra-passe de forma a analisar o ficheiro.

Se premir **Defeito** carregará as definições por defeito. Clique em **OK** para guardar as alterações e fechar a janela.

Definir Alvo da Análise

Para definir o alvo da análise de uma determinada tarefa de análise, clique botão direito na tarefa e seleccione **Caminhos**. Alternativamente, se já se encontra na janela das Propriedades da tarefa, seleccione a barra **Caminhos**. A seguinte análise irá aparecer:



Analisar Alvo

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

A secção contém os seguintes botões:

- **Adicionar Pasta (s)** - abre uma janela de exploração onde pode seleccionar o(s) ficheiro(s) que pretende examinar.

  Nota
  Use carregar & descarregar para adicionar à lista ficheiros/pastas.

- **Apagar item** - remove o(s) ficheiro (s) / pasta(s) que foram previamente seleccionados da lista dos objectos a serem analisados.

  Nota
  Apenas podem ser eliminados o(s) ficheiro(s) / pasta(s) que foram adicionados posteriormente, mas não aqueles que foram automaticamente "enviados" pelo BitDefender.

Para além dos botões explicados acima existem também algumas opções que permitem uma selecção rápida das áreas a analisar.

- **Unidades Locais** - para analisar as drives locais.
- **Unidades de Rede** - para analisar todas as drives de rede.

- **Unidades Amovíveis** - para analisar todas as drives amovíveis (CD-ROM, unidade de disquetes).
- **Todas as Entradas** - para analisar todos as drives, independentemente de serem locais, de rede ou amovíveis.

Nota

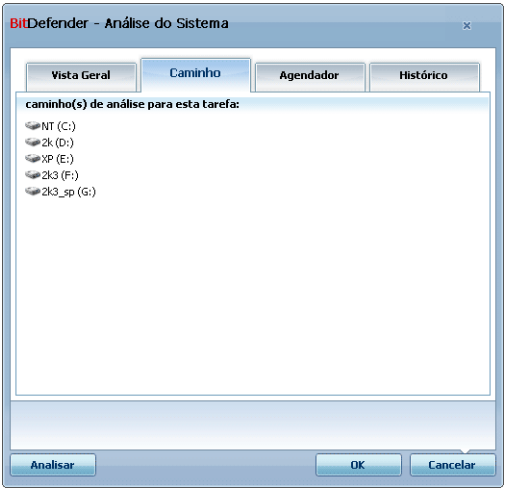
Se pretende analisar em busca de vírus todo o seu computador, seleccione a caixa de selecção correspondente a **Todas as entradas**.

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 rato sobre a tarefa seleccione **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 **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-lo, clique botão direito do rato e seleccione **Agendar**. Se já se encontra na janela das Propriedades, seleccione a barra **Agendador**. 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 utilizador a solicita.
- **Uma vez** - Executa a análise uma só vez, num determinado momento. Definir a data de início e a hora nos campos**Iniciar Data/Hora**
- **Periodicamente** - Executa a análise periodicamente, num determinado intervalo de tempo (horas, dias, semanas, meses, anos) começando a uma determinada data e hora.

Se pretende que a análise seja repetida a um certo intervalo, seleccione a a opção **Periodicamente** e insira na caixa de edição **A cada**, o número de minutos/horas/dias/semanas/meses/anos para indicar a frequência deste 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 utilizador entrar no Windows.

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

18.2.5. Analisar Ficheiros e Pastas

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** em Modo Avançado.

Nota

Para que o BitDefender possa efectuar uma verificação completa, tem de encerrar todos os programas abertos. É, especialmente, importante que encerre a sua conta de e-mail (por ex. Outlook, Outlook Express ou Eudora).

Dicas de Análise

Eis aqui mais algumas dicas sobre a análise que lhe poderão ser úteis:

- Dependendo do tamanho do disco rígido, levar a cabo uma análise completa do seu computador (tal como uma Análise Minuciosa ou uma Análise Completa) pode levar algum tempo (uma hora ou mais). Logo, deve de levar a cabo essas análises em momentos em que não necessita do seu computador (por exemplo, durante a noite).

  Pode agendar a análise para começar quando for mais conveniente. Certifique-se de que deixa o seu computador ligado. Com o Windows Vista, certifique-se que o seu computador não está em Modo de Suspensão na altura para a qual a tarefa está agendada.

- Se descarrega frequentemente ficheiros da Internet para uma determinada pasta, crie uma nova tarefa de análise e defina essa pasta como alvo da análise. Agenda a tarefa para correr diariamente ou até com mais frequência.

- Existe um determinado tipo de malware que se prepara para ser executado durante o arranque do sistema ao alterar as definições do Windows. Para proteger o seu computador contra tal tipo de malware, pode agendar a tarefa de **Análise Autologon** para correr durante o iniciar do sistema. Tenha em atenção que a Análise Autologon pode afectar a performance do sistema durante um curto período de tempo após o iniciar do computador.

Métodos de Análise

O BitDefender permite quatro tipos de análise a-pedido:

- Análise imediata - executa uma tarefa de análise das tarefas do sistema/utilizador.
- Análise contextual - clique com o botão direito do rato sobre um ficheiro ou pasta e seleccione **Analisar com BitDefender**.
- Análise Drag & Drop - Arraste e largue um ficheiro ou pasta em cima da Barra de Actividade da Análise.
- Análise manual - Use a Análise Manual do BitDefender para seleccionar directamente os ficheiros ou pastas a serem analisados.

Análise 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 análise imediata.

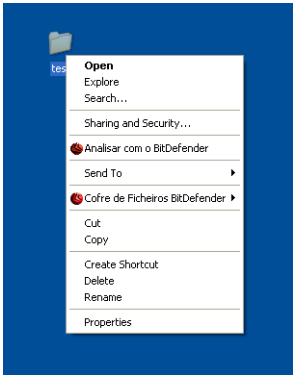
Para executar uma tarefa de análise, use um dos seguintes métodos:

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

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Análise contextual

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



Menu Contextual da Análise

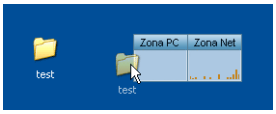
Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar e seleccione **Analisar com o BitDefender**. O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

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

Análise por Drag&Drop

Arraste o ficheiro ou a pasta que pretende analisar e deixe-a cair em cima da **Barra de Actividade da Análise**, como apresentado abaixo.

Arraste o ficheiro



Deixe cair o ficheiro

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Análise Manual

A análise manual consiste em sleccionar 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 pelo BitDefender, no menu Iniciar do Windows, siga o seguinte caminho **Iniciar → Programas → BitDefender 2010 → Análise Manual BitDefender**. A seguinte análise irá aparecer:

Análise Manual

Clique em **Adicionar Pasta**, seleccione a localização que quer analisar e clique **OK**. Se quer analisar várias pastas, repita esta acção para cada localização adicional.

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

Quando não tiver mais locais para adicionar, clique em **Continuar**. O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Assistente de Análise Antivírus

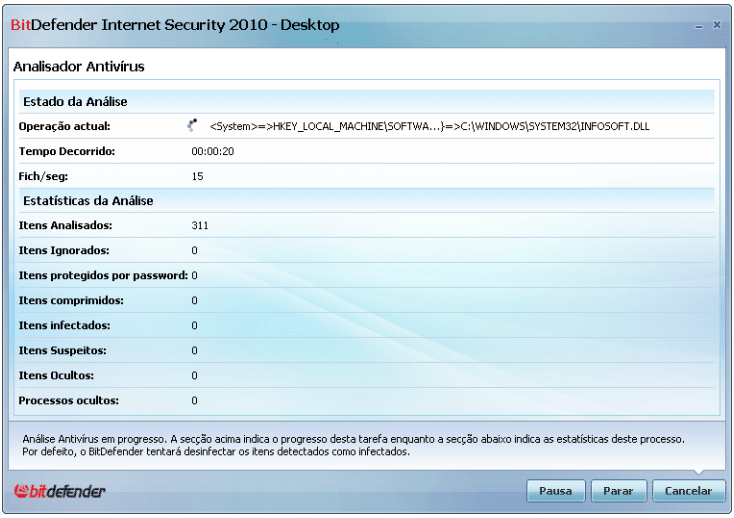
Quando leva a cabo uma análise a-pedido, o assistente de análise antivírus aparece. Siga o processo guiado de três passos para completar o processo de análise.

Nota

Se o assistente de análise não surgir, a análise poderá estar configurada para correr silenciosamente, em segundo plano. Procure pelo ícone do progresso da análise na área de notificação. Pode clicar nesse icone para abrir a janela da análise e ver o seu progresso.

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

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

Espere que o BitDefender termine a análise.

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

Arquivos protegidos com palavra-passe. Se o BitDefender detectar um arquivo protegido por palavra-passe durante a análise e a acção por defeito for **Solicitar palavra-passe**, ser-lhe-á solicitado que insera a palavra-passe. Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe. Estão disponíveis as seguintes opções:

- **Palavra-passe.** Se quer que o BitDefender analise o arquivo, seleccione esta opção e insira a palavra-passe. Se não sabe a palavra-passe, escolha uma das outras opções.
- **Não pergunte pela password e não analise este objecto.** Seleccione esta opção para saltar a análise deste arquivo.
- **Passar todos os itens protegidos por password sem os analisar.** Seleccione esta opção se não deseja ser incomodado acerca de arquivos protegidos por palavra-passe. O BitDefender não será capaz de os analisar, mas um registo dos mesmos será mantido no relatório da análise.

Clique em **OK** para continuar a analisar.

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

Passo 2/3 - Seleccionar as acções

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

Acções

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

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

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

Uma ou várias das seguintes opções poderão aparecer no menu:

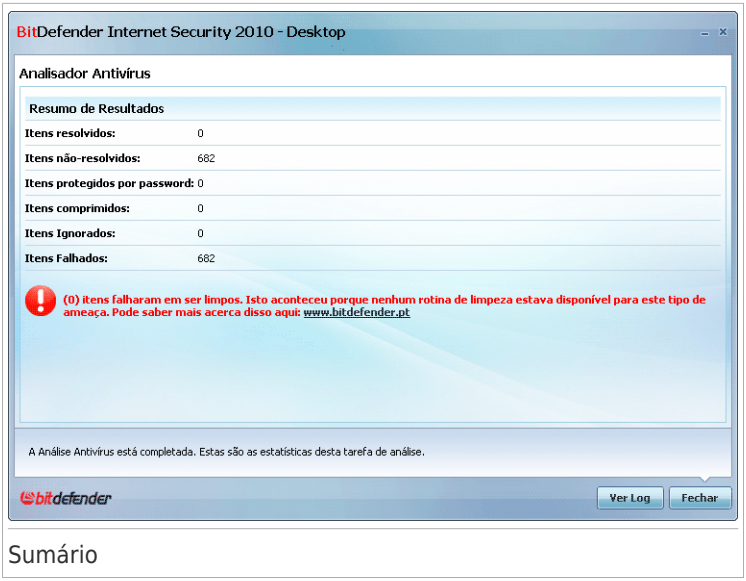
Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros detectados. Após a analisar terminar, pode abrir o

Acção	Descrição
	relatório da análise para ver informação sobres esses ficheiros.
Desinfectar	Remove o código de malware dos ficheiros infectados.
Apagar	Apaga os ficheiros detectados.
Mover para a quarentena	Move os ficheiros infectados para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.
Renomear ficheiros	Altera o nome dos ficheiros ocultos ao acrescentar `.bd.ren` ao seu nome. Como resultado, será capaz de procurar e encontrar tais ficheiros no seu computador, se existirem. Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits. Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

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

Passo 3/3 - Ver Resultados

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



Sumário

Pode ver o resumo dos resultados. Se deseja uma informação completa sobre o processo de análise, clique em **Mostrar ficheiro de log** 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 ficheiro 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 Ficheiros Suspeitos

Ficheiros suspeitos são ficheiros detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura de detecção ainda não foi disponibilizada.

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

18.2.6. Ver os Relatórios da Análise

Para ver os resultados da análise após a tarefa ter sido executada, faça clique com o botão direito do rato sobre a mesma seleccione **Relatório**. A seguinte análise irá aparecer:

Relatórios

Aqui pode ver os relatórios gerados cada vez que uma tarefa foi executada. Cada ficheiro 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.

Estão disponíveis dois botões:

- **Apagar** - para apagar o relatório seleccionado.
- **Mostrar** - para ver o relatório seleccionado. O relatório da análise será aberto no seu explorador da internet.

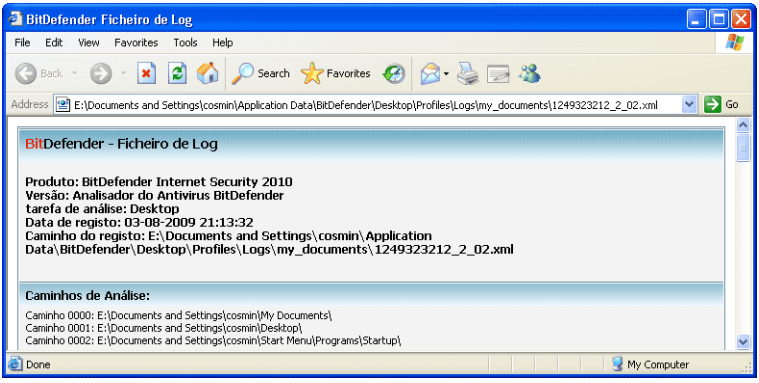
Nota

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

18.3. Objectos Excluídos da Análise

Há casos em que tem de excluir certos ficheiros de serem analisados. Por exemplo, poderá querer excluir um ficheiro de teste EICAR da análise no acesso ou os ficheiros `.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.

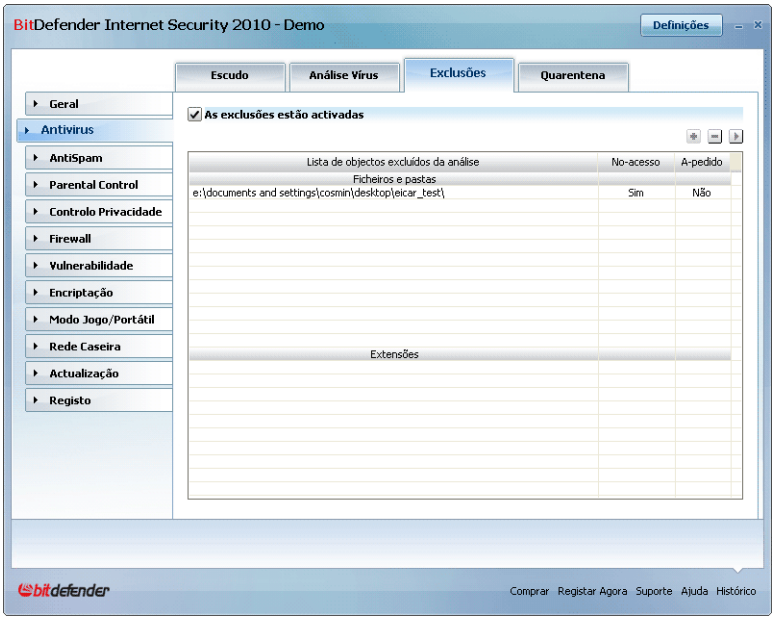
Dois tipos de objectos podem ser excluidos da análise:

- **Caminhos** - o ficheiro ou pasta (incluindo os objectos que contém) indicados por um determinado caminho serão excluídos da análise.
- **Extensões** - todos os ficheiros 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 e gerir os objectos excluídos da análise, vá para **Antivírus>Excepções** no Modo Avançado.



Excepções

Pode ver os objectos (ficheiros, 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 execepções definidas aqui NÃO serão aplicada à análise contextual. Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e selecciona **Analisar com BitDefender**.

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

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 rato e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

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

18.3.1. Excluir Caminhos da Análise

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

Passo 1/4 - Seleccionar o Tipo de Objecto

Tipo de Objecto

Seleccione a opção de excluir um caminho da análise.

Clique **Seguinte**.

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**, seleccione o ficheiro 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 eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Clique **Seguinte**.

Passo 3/4 - Seleccionar o Tipo de Análise

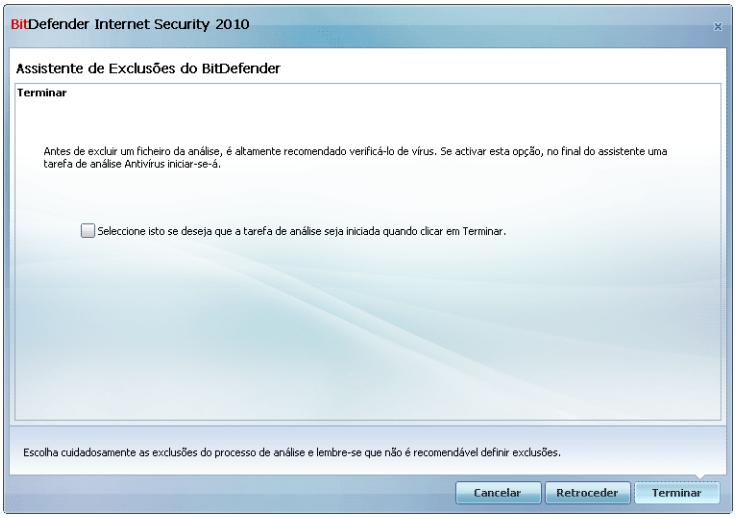
Tipo de Análise

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 **Seguinte**.

Passo 4/4 - Analisar Ficheiros Excluidos



Analisar Ficheiros Excluidos

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

Clique em **Terminar**.

18.3.2. Excluir Extensões da Análise

Para exluir 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.

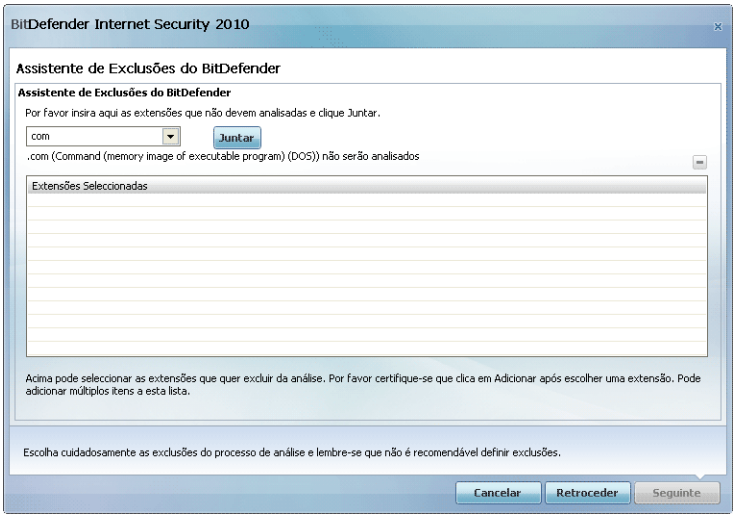
Passo 1/4 - Seleccionar o Tipo de Objecto

Tipo de Objecto

Seleccione a opção de excluir extensões da analise

Clique **Seguinte**.

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.

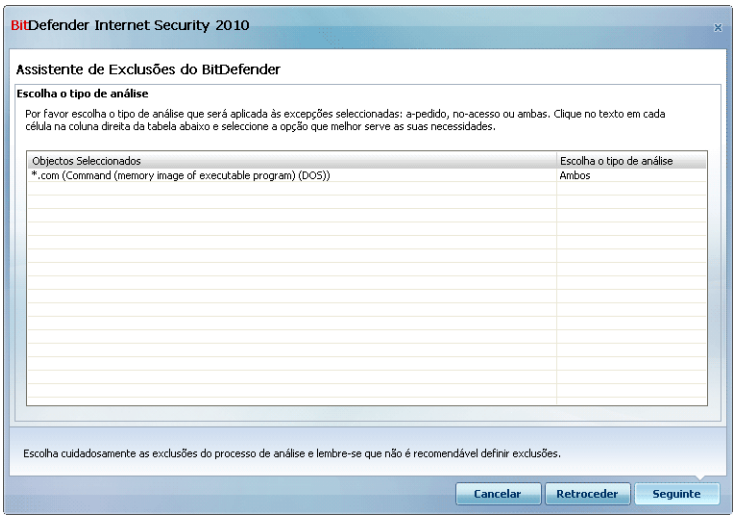
- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

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

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Clique **Seguinte**.

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 **Seguinte**.

Passo 4/4 - Seleccionar o Tipo de Análise

Tipo de Análise

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

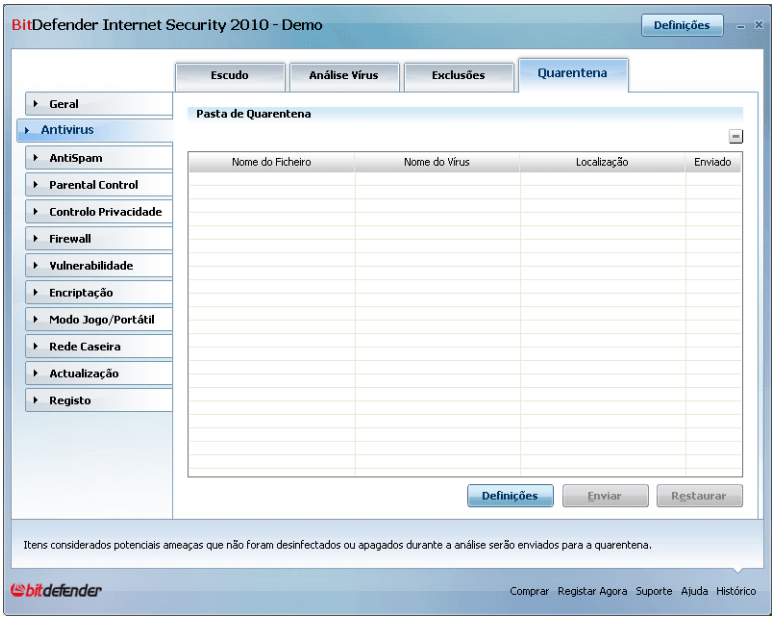
Clique em **Terminar**.

18.4. Àrea de Quarentena

O BitDefender permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Ao isolar estes ficheiros na quarentena, desaparece o risco de infecção,e ao mesmo tempo, terá a possibilidade de enviar estes ficheiros para análise no laboratório do BitDefender.

Em adição, o BitDefender analisa os ficheiros em quarentena após cada actualização das assinaturas de malware. Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para ver e gerir os ficheiros em quarentena e configurar as definições da quarentena, vá para **Antivírus>Quarentena** no Modo Avançado.



Quarentena

A secção de Quarentena mostra todos os ficheiros actualmente isolados na pasta da Quarentena. Para cada ficheiro em qaurentena 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 se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lido nem executado.

18.4.1. Gerir Ficheiros em Quarentena

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

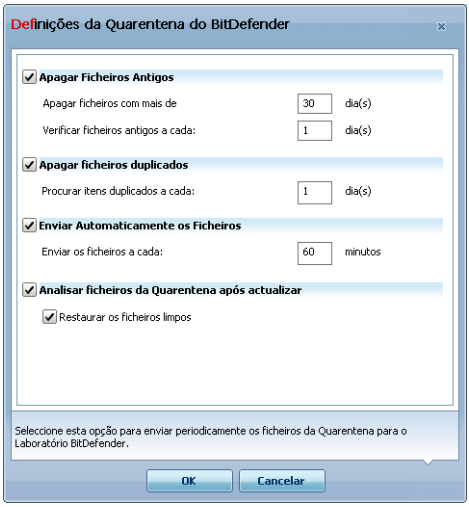
Para apagar um ficheiro seleccionado da lista de quarentena clique no botão **Remover**. Se deseja restaurar o ficheiro seleccionado para a sua localização original clique em **Restaurar**.

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

estão disponíveis. Pode também seleccionar **Actualizar** para actualizar a secção de Quarentena.

18.4.2. Configuração da Quarantena

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



Definições de quarantena

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

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

Nota
Por defeito o BitDefender verificará a antiguidade dos ficheiros a cada dia e apagará os que tenham mais de 30 dias de existência.

Apagar ficheiros duplicados. Para apagar automaticamente ficheiros duplicados na quarentena, seleccione a opção correspondente. Deve especificar o número de dias entre duas verificações consecutivas de duplicados.

Nota
Por defeito, o BitDefender irá verificar ficheiros duplicados na quarentena a cada dia.

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

Nota
Por defeito o BitDefender envia automaticamente os ficheiros em quarentena a cada 60 minutos.

Analisar os ficheiros em quarentena após a actualização. Para analisar automaticamente ficheiros em quarentena após a actualização, seleccione a opção correspondente. Pode escolher mover automaticamente os ficheiros limpos para a sua localização original seleccionado a opção **Restaurar Ficheiros Limpos**.

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

19. AntiSpam

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

19.1. Compreender o Antispam

O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam num largo domínio de formas e tamanhos, e é muito existente.

19.1.1. Filtros Antispam

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 comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

Pode gerir a lista de Amigos / Spammers através do Modo Avançado ou através da barra de ferramentas Antispam integrada em alguns dos clientes de e-mail mais utilizados.

Nota
Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Filtro de caracteres

A maioria das mensagens de spam estão escritas em caracteres Cirílicos ou Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-os como SPAM.

Filtro de Imagem

Uma vez que evitar o filtro heurístico se tornou um desafio e tanto, hoje em dia as pastas de entrada dos e-mails estão cada vez mais cheias de mensagens contendo apenas uma imagem com conteúdo não-solicitado. Para fazer face a este problema crescente, BitDefender introduziu o **Filtro de Imagem** que compara a assinatura do e-mail com aquelas da base de dados do BitDefender. Em caso de igualdade o e-mail será etiquetado com SPAM.

Filtro 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

Desde 19 de Maio de 2004, o Spam com conteúdo de caracter sexual, tem de incluir o aviso `SEXUALMENTE EXPLÍCITO:` no assunto ou está sujeito a multa por violação da lei.

Filtro Bayesiano

O modulo do **Filtro Bayesian** classifica as mensagens de acordo com as informações estatísticas, tendo em conta a taxa de palavras específicas que aparecem nas mensagens classificadas como Indesejadas, comparadas com aquelas que não são Indesejadas (por si ou pelo filtro heurístico).

Isto significa, por exemplo, se uma certa carta de quatro palavras aparece mais frequentemente como Indesejada, é natural que assuma que existe uma maior

possibilidade de a próxima mensagem que a inclua, seja vista como Indesejada. Todas as palavras relevantes, dentro de uma mensagem, são levadas em conta. Ao sintetizar a informação estatística, é computizada a maior probabilidade de toda a mensagem ser Indesejada.

Este modulo apresenta outra característica interessante: é treinável. Adapta-se rapidamente ao tipo de mensagens recebidas por um dado utilizador, e armazena informação acerca de todos. Para funcionar com eficiência, o filtro tem de ser treinado, o que significa, apresentar-lhe amostras de Spam e de mensagens legítimas, tal como um predador é impelido de caçar uma certa presa. Ás vezes o filtro também tem de ser corrigido – pronto a ajustar-se quando toma uma decisão errada.

Importante

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

19.1.2. Operação Antispam

O Motor BitDefender Antispam usa todos os filtros antispam combinados para determinar se um determinado e-mail deve de chegar à pasta **A Receber** ou não.

Importante

As mensagens de spam detectadas pelo BitDefender são marcadas como [SPAM] no campo do assunto. O BitDefender move automaticamente as mensagens de spam para uma determinada pasta, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**. A pasta **Spam** é criada durante a instalação do BitDefender.
- No Outlook Express e no Windows Mail, as mensagens de spam são movidas directamente para os **Itens Eliminados**.
- No Mozilla Thunderbird, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Lixo**. A pasta **Spam** é criada durante a instalação do BitDefender.

Se usa outros cliente de e-mail, tem de criar uma regra para mover os e-mails marcados como [SPAM] pelo BitDefender para uma pasta de quarentena personalizada.

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.

Ainda, o Filtro caracteres irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado com Indesejado e movido para a pasta de **Spam**.

Se o e-mail não estiver escrito em caracteres Cirílicos ou Asiáticos, irá passar pelo Filtro de Imagem. O **Filtro de Imagem** detecta todas as mensagens de e-mail que contêm imagens anexadas com conteúdo de spam.

O Filtro URL irá procurar ligações e compará-las às ligações da base de dados do BitDefender. Em caso de corresponder, irá adiconar ao e-mail uma marca de Spam score.

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 for marcado com SEXUALLY EXPLICIT na linha do sujeito, o BitDefender irá considerá-lo como SPAM.

O modulo do Filtro Bayesian irá seguidamente analisar a mensagem, de acordo com as informações estatísticas, tendo em conta a taxa de palavras específicas que aparecem nas mensagens classificadas como Indesejadas, comparadas com aquelas que não são Indesejadas (por si ou pelo filtro heurístico). Irá ser adicionada à mensagem uma marca de Spam.

Se a pontuação total (pontuação URL + pontuação heurística + pontuação Bayesiana) excederam a pontuação de SPAM para uma mensagem (definida pelo utilizador na secção Estado como nível de tolerância), a mensagem é considerada SPAM.

19.1.3. Actualização do Antispam

Cada vez que executa uma actualização:

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

Isto ajuda a umentar a eficiência da engenharia Antispam.

Para o proteger contra os spammers, BitDefender pode levar a cabo actualizações automáticas. Mantenha a opção **Actualização Automática** active.

19.2. Estado

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

Estado 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 a entrada de Spam na sua **Caixa de Entrada**, mantenha activo o **Filtro Antispam**.

Na secção das **Estatísticas** pode visualizar as estatísticas que dizem respeito ao módulo de Antispam. Os resultados são apresentados por sessão (desde que iniciou o seu computador) ou pode ver um sumário da actividade de Antispam (desde a instalação do BitDefender).

19.2.1. 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**.

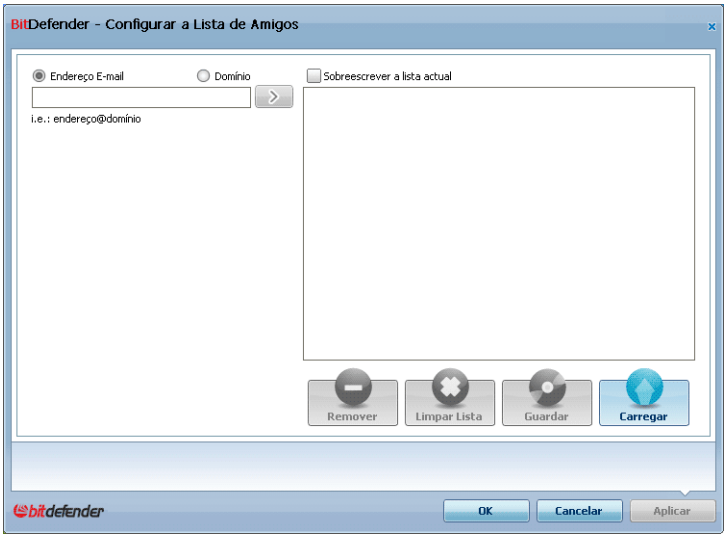
19.2.2. Configurar a Lista de Amigos

A **Lista de amigos** é uma lista de todos os endereços de e-mail, dos quais deseja sempre receber mensagens, independentemente do seu conteúdo. A mensagens dos seus amigos não serão vistas como Indesejadas, mesmo que contenham Spam.

Nota

Qualquer mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada, sem mais demora.

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



Lista de Amigos

Aqui pode adicionar ou remover entrdas da **Lista de amigos**.

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

Importante
Sintaxe: nome@dominio.com.

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

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *dominio* - todos os mails provenientes de dominio (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *com - todos os mails que têm este sufixo de domínio com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

Para remover um ítem da lista, seleccione-o e clique em **Remover**. Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois **Sim** para confirmar a sua escolha.

Pode guardar a lista de Amigos num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto. Para guarda a lista de Amigos, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão `.bwl`

Para carregar uma lista de Amigos previamente guardada, clique no botão **Carregar** e abra o ficheiro `.bwl` correspondente. Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota

Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

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

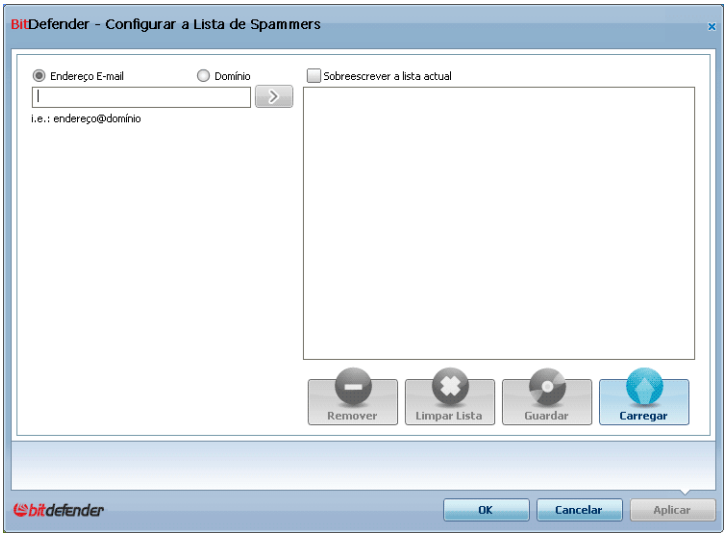
19.2.3. Configurar a lista de Spammers

A **Lista de indesejados** é uma lista de todos os endereços de e-mail, dos quais nunca pretende receber mensagens, independentemente do seu conteúdo.

Nota

Todo o mail proveniente de um endereço presente na **Lista de indesejados**, será marcado automaticamente com indesejado, sem mais demora.

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



Lista de Spammers

Aqui pode adicionar ou remover entradas da **Lista de indesejados**.

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
Sintaxe: nome@dominio.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
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com serão marcados como INDESEJADOS;
- *dominio* - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- *com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

Atenção

Não adicione domínios de serviços web-mail (tais como o Yahoo, Gmail, Hotmail ou outro) à lista de Spammers. Caso contrário, as mensagens de email recebidas de

algum utilizador registado nesses serviços será detectado como spam. Se, por exemplo, adicionar `yahoo.com` à lista de Spammer, todos as mensagens de e-mais recebidas do endereço `yahoo.com`, serão marcadas como `[spam]`.

Para remover um ítem da lista, seleccione-o e clique em **Remover**. Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois **Sim** para confirmar a sua escolha.

Pode guardar a lista de Spam num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto. Para guarda a lista de Spam, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão `.bwl`

Para carregar uma lista de spammers previamente guardada, clique no botão **Carregar** e abra o ficheiro `.bwl` correspondente. Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique **Aplicar** e **OK** para guardar e fechar a **Lista de indesejados**.

Importante
Se deseja reinstalar o BitDefender será uma boa ideia guardar as listas de **Amigos** / **Indesejados**, antes do processo de reinstalação, depois de o processo ter terminado pode carregá-las.

19.3. Definições

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

Configuração 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 maracada com o sinal "+" para abrir a categoria ou clique na que está marcada com o sinal "-" para fechar a categoria.

Para activar/desactivar uma opção seleccione/limpe a caixa de selecção correspondente a ela.

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

Prima **Aplicar** para guardar as alterações.

19.3.1. Configuração de Antispam

- **Marcar as mensagens indesejadas em questão** - todas as mensagens de e-mail consideradas indesejadas serão marcadas como Indesejadas em assunto.

- **Marcar mensagens phishing no assunto** - todas as mensagens de e-mail consideradas mensagens de phishing serão marcadas como SPAM na linha do assunto.

19.3.2. Filtros Antispam Básicos

- **Listas de amigos / spammers** - filtras as 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.
  - **Adicionar automaticamente à Lista de amigos** - da próxima vez que clicar no botão **Não-Spam** na Barra de ferramentas Antispam, o remetente será automaticamente adicionado à Lista de amigos.
  - **Adicionar automaticamente à Lista de Spammers** - da próxima vez que clicar no botão **É Spam** na Barra de taredas Antispam, o remetente será automaticamente adicionado à 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.

19.3.3. Filtros Antispam Avançados

- **Activar Motor de Aprendizagem (bayesiano)** - activa/desactiva o Motor de Aprendizagem (bayesiano);
  - **Limitar o tamanho do dicionário para 200000 palavras** - com esta opção pode estabelecer o tamanho do dicionário Bayesian – quanto menor mais rápido, maior é mais eficaz.

Nota
O tamanho recomendado é de: 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 URL** - activa/desactiva o Filtro URL;
- **Filtro NeuNet (Heurístico)** - activa/desactiva o Filtro NeuNet (Heurístico);
  - **Bloquear conteúdo explícito** - activa/desactiva a detecção de mensagens com o aviso de conteúdo SEXUALMENTE EXPLÍCITO na linha do assunto.
- **Filtro de Imagem** - activa/desactiva o Filtro de Imagem.

20. Parental Control

O Controlo Parental BitDefender permite-lhe controlar o acesso à Internet e a determinadas aplicações para cada conta de utilizador no sistema.

Pode configurar o Controlo Parental 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 ficheiros e outros.
- mensagens instântaneas enviadas por contacto IM para além dos que estão permitidos.

Importante

Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Controlo Parental. Para ter a certeza de que só você pode modificar as definições do Controlo Parental para qualquer utilizador, pode protegê-las com uma palavra-passe. Ser-lhe-á pedida a palavra-passe cada vez que activar o Controlo Parental para um determinado utilizador.

Para usar com sucesso o Controlo Parental 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 Controlo Parental para as contas de utilizador do Windows que as suas crianças utilizam.

Para configurar o Controlo Parental, clique em **Controlo Parental** no Modo Avançado.

Parental Control

Pode ver informação sobre o estado do Controlo Parental para cada utilizador de contas do Windows. A faixa etária é listada abaixo de cada nome do utilizador se o Controlo Parental estiver ativado. Se o Controlo Parental estiver desactivado, o estado é **não configurado**.

Adicionalmente, poderá ver o estado da funcionalidade de cada Controlo Parental por utilizador:

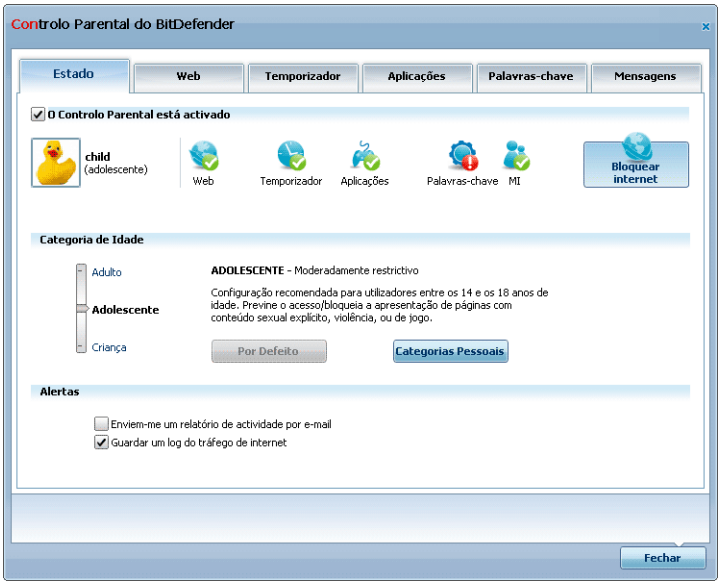
Círculo verde com uma marca de verificação: A opção está activada.
Circulo vermelho com um ponto de exclamação: A opção não está activada.

Clique no botão **Modificar** junto ao nome de utilizador para abrir a janela onde pode configurar as definições do Controlo Parental para as respectivas contas.

As seguintes secções dets capítulo apresentam em detalhe as características do Controlo Parental e a forma de as configurar.

20.1. Configurar o Controlo Parental Para Um Utilizador

Para configurar o Controlo Parental para uma conta de utilizador específica, clique no botão **Modificar** correspondente à conta de utilizador e depois clique na tabela **Estado**.



Estado do Controlo Parental

Para configurar o Controlo Parental para este utilizador, siga estes passos:

1. Para activar o Controlo Parental para esta utilizador marque a caixa de selecção ao pé do **Controlo Parental**.

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

2. Definir palavra-passe para proteger as Definições do Controlo Parental. Para mais informação, por favor consulte o *"Proteger as Definições do Controlo Parental"* (p. 192).
3. Insira a categoria da faixa etária para permitir que a sua criança acesse aos sites apropriados para a sua idade. Para mais informações, consulte o *"Definir Categorias de Idade"* (p. 193).
4. Configure as opções necessárias de monotorização para este utilizador:
   - **Envie-me um relatório de actividade para o e-mail.** Sempre que o Controlo Pearental do BitDefender bloqueia uma actividade no utilizador, é enviada uma notificação de email.

- **Guardar registo de tráfego de internet.** Regista os sites visitados pelo utilizador.

Para mais informações, consulte o "*Monotorizar Actividade das Crianças*" (p. 196).

5. Clique num ícone ou num separador para configurar as características do Controlo Parental:
   - **Controlo Web** - para filtrar a navegação na Internet de acordo com as regras definidas por si na secção Web .
   - **Controlo de Aplicações** - para bloquear o acesso às aplicações no seu computador de acordo com as regras definidas por si na secçãoAplicações.
   - **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 .
   - **Controlo Mensagens Instântaneas** - permitir ou bloquear o chat IM de acordo com as regras definidas por si na secção Tráfego IM.
   - **Temporizador Web** - para permitir o acesso à web de acordo com a tabela de horário definida por si na secçãoTemporizador .

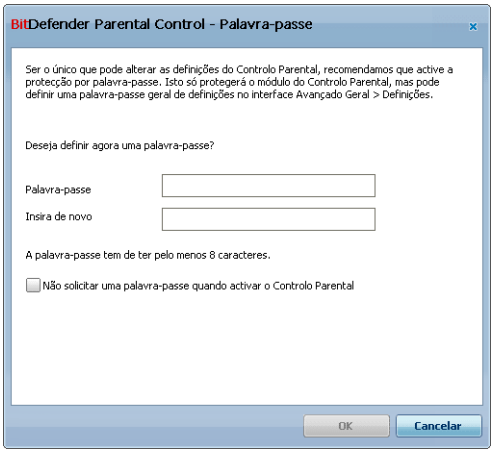
   Nota
   Para aprender como configurá-los, por favor consulte os seguintes tópicos deste capítulo.

Para bloquear completamente o acesso á internet, clique no botão **Bloquear Internet**

20.1.1. Proteger as Definições do Controlo Parental

Se não for a única pessoa com direitos administrativos a utilizar este computador, recomendamos que protega as suas configurações do Controlo Parental com uma palavra-passe. Ao definir uma palavra-passe, irá prevenir que outros utilizadores com direitos administrativos possam mudar as suas definições do Controlo Parental que configurou para um determinado utilizador.

BitDefender irá solicitar-lhe por defeito que defina uma palavra-passe quando activar o Controlo Parental.



Definir protecção por palavra-passe

Para definir protecção por palavra-passe, faça o seguinte:

1. Digite a palavra-passe na campo **Palavra-passe** .
2. Insira de novo a palavra-passe no campo **Reinserir Palavra-passe** para a confirmar.
3. Clique em **OK** para guardar a palavra-passe e fechar a janela.

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

Nota
A palavra-passe não protege quaisquer outras definições do BitDefender.

Caso não defina uma palavra-passe e não queira que a janela para o efeito lhe surja novamente, seleccione **Não solicitar palavra-passe quando activar Controlo Parental**.

20.1.2. Definir Categorias de Idade

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

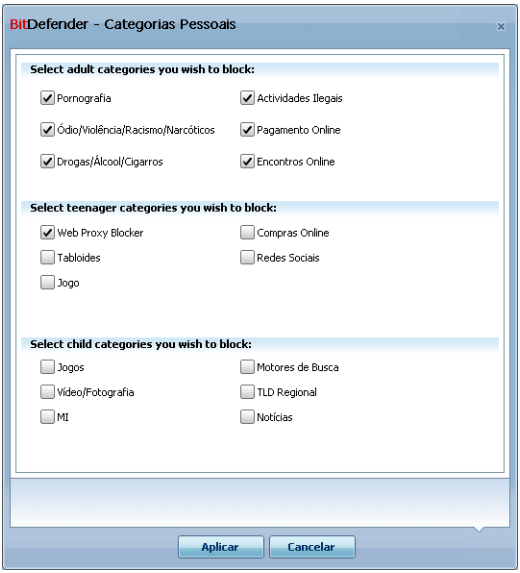
ao longo da escala para definir o nível de tolerância que considera apropriado para o utilizador seleccionado.

Existem 3 níveis de tolerância:

Nível de tolerância	Descrição
Criança	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para utilizadores 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 utilizadores 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.

Se deseja mais controlo sobre o tipo de conteúdo a que o utilizador é exposto na internet, pode definir categorias de conteúdo que serão bloqueadas pelo filtro da web. Para escolher que tipos de contéudo da Web serão bloqueados, clique em **Categorias Personalizadas**. Uma nova janela irá aparecer.



Categorias de Filtros de Web

Seleccione a caixa de seleccão correspondente á categoria que quer bloquear e o utilizador não será mais autorizado a aceder a sites de internet dessa categoria. Para tornar mais fácil a sua selecção, as categorias de conteúdo da web são listados de acordo com a faixa etária para a qual um deles poderia considerar adequado:

- **Categorias de Perfil de Crianças** inclui conteúdo que as crianças acima da idade de 14 podem ter acesso.

Categoria	Descrição
Jogos	Sites onde se oferecem jogos on-line, fóruns de discução sobre jogos, descarregamento de jogos, códigos, tutoriais, etc.
Videos/Fotos	Sites que contêm galerias de vídeos ou fotografia.
Mensagens Instantâneas	Aplicações de Mensagens Instantâneas.
Motores de Busca	Motores de Análise e procurar portais.
TLD Regional	Sites que têm um nome de domínio fora da sua região.
Notícias	Jornais Online

- **Categorias de Perfil de Adolescente** inclui conteúdo que poderá ser considerado seguro para crianças entre os 14 e os 18 anos de idade.

Categoria	Descrição
Bloqueador da Web Proxy	Sites usados para esconder o URL dos sites solicitados.
Tablóides	Revistas Online
Jogar a Dinheiro	Casinos on-line, sites de apostas, sites que oferecem dicas de apostas, fóruns de apostas, etc.
Pagamento On-line	Lojas on-line
Rede Social	Sites de Redes Sociais.

- **Categorias de Perfile de Adulto** inclui conteúdo que não é apropriado para crianças ou adolescentes.

Categoria	Descrição
Pornografia	Sites da web com conteúdo pornográfico.
Ódio / Violência / Racismo / Narcóticos	Sites da web com conteúdo violento ou racista, promovendo o terrorismo ou o uso de narcóticos.
Drogas / Alcool / Cigarros	Sites da web de venda ou publicidade de produtos de droga, alcool ou tabaco.
Actividades Ilegais	Sites da web que promovem ou contém conteúdos pirateados.
Pagamento On-line	Formas de pagamento on-line na web e confira secções de lojas on-line. O utilizador pode navegar em lojas on-line, mas as tentativas de compra são bloqueados.
Encontros On-line	Sites de encontros de adultos, com salas de conversação, videos e compartilhamento de fotos.

Clique em **Aplicar** para guardar as categorias de conteúdo web bloqueadas para este utilizador.

20.2. Monotorizar Actividade das Crianças

BitDefender ajuda-o a acompanhar o que seus filhos estão a fazer no computador, mesmo quando está ausente. Os alertas podem ser-lhe enviados via e-mail, cada vez que o módulo Controlo Parental bloqueia uma actividade. Também pode ser gravado um relatório com o historico de websites visitados.

Seleccione a opção que quer activar:

- **Envie-me um relatório de actividade para o e-mail.** Sempre que o Controlo Pearental do BitDefender bloqueia uma actividade no utilizador, é enviada uma notificação de e-mail.
- **Guardar registo de tráfego de internet.** Regista os sites visitados pelo utilizador para os quais o Controlo Parental está activado.

20.2.1. A Verificar Sites Visitados

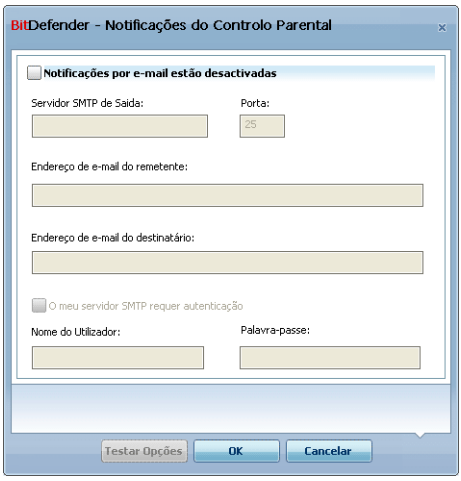
Por defeito, o BitDefender regista os sites visitados pelas suas crianças.

Para ver o registo, clique em **Ver Registo** para abrir Histórico&Eventos e seleccione **Registo de Internet**.

20.2.2. A Configurar Notificações de E-mail

Para receber notificações via e-mail quando o Controlo Parental bloquear uma actividade, seleccione **Envie-me um relatório de actividade por e-mail** na configuração geral da janela do Controlo Parental. Será solicitado a configurar as definições da sua conta de e-mail. Clique em **Sim** para abrir a janela de configuração.

Nota
Pode abrir a janela de configuração mais tarde ao clicar **Definições de Notificação**.



Definições de E-mail

Tem de configurar as definições de conta de e-mail como se segue:

- **Servidor SMTP de Envio** - digite o endereço do servidor de e-mail utilizado para enviar mensagens e-mail.
- Se o servidor usa uma porta diferente do que o padrão porta 25, digite-o no campo correspondente.
- **Endereço de e-mail dos remetentes** - digite o endereço que quer que apareça no campo **De** do e-mail.
- **Endereço de e-mail do destinatário** - digite o endereço de e-mail para onde quer que os relatórios sejam enviados.
- Se o servidor requer autentificação, seleccione a caixa de selecção **O meu servidor SMTP requer autentificação** e digite o nome de utilizador e palavra-passe nos respectivos campos.

Nota

Se não sabe o que são estas definições, abra a sua conta de cliente e verifique as duas definições de conta de e-mail.

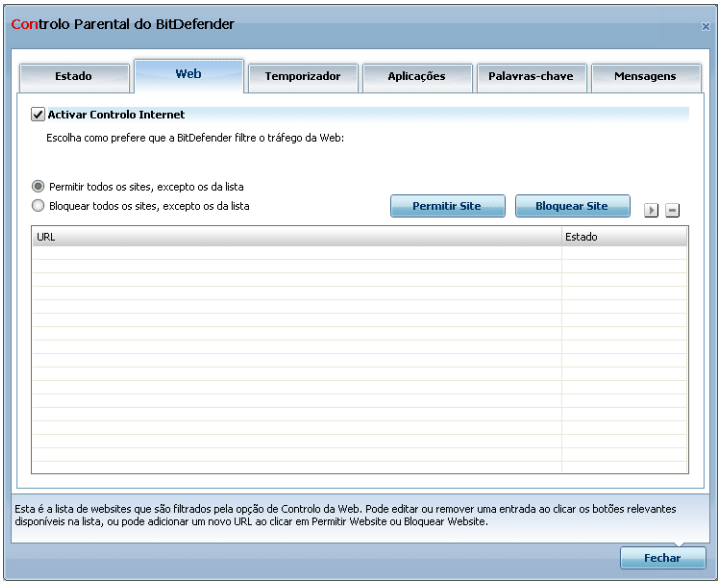
Para validar a configuração, clique no botão **Testar Definições**. Se alguma incidência for encontrada durante a validação, o BitDefender irá informá-lo que áreas requerem a sua atenção.

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

20.3. Controlo Internet

O **Controlo Web** ajuda-o a bloquear o acesso a web sites com conteúdo inapropriado. Uma lista de candidatos a serem bloqueados, quer sites quer partes dos mesmos, é fornecida e actualizada pelo BitDefender, como parte do processo normal de actualização.

Para configurar o Controlo da Web para uma conta de utilizador específica, clique no botão **Modify** correspondendo a essa conta e clique no separador **Web**.



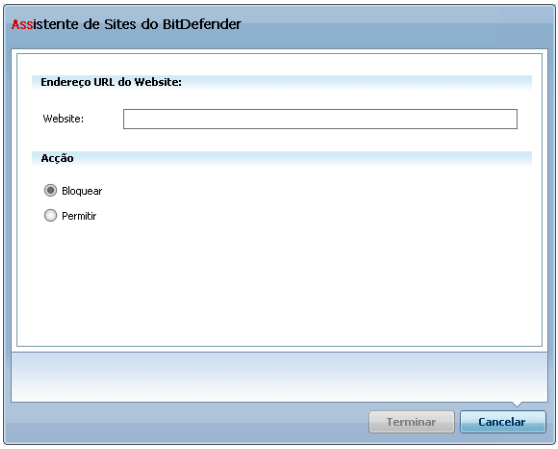
Controlo Internet

Para activar esta protecção seleccione a caixa de selecção correspondente a **Activar Controlo Internet**.

20.3.1. Criar Regras de Controlo de Internet

Para permitir ou bloquear acesso a um website, siga estes passos:

1. Clique em**Permitir Site** ou **Bloquear Site**. Uma nova janela irá aparecer:



Especificar Sites Web

2. Entre no endereço do website no **campo do Website**.

Sintaxe:

- `*.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.

3. Seleccione a acção desejada para esta regra - **Permitir** ou **Bloquear**.
4. Clique em **Terminar** para adicionar a regra.

20.3.2. Gerir Regras de Controlo de Internet

As regras de Controlo do Website que já foram configuradas estão listadas na tabela que se encontra na parte inferior da janela. O endereço do Website e o estado actual estão listados para cada regra de Controlo da Web.

Para editar uma regra, seleccione-a e clique no botão **Editar** e faça as mudanças necessárias na janela de configuração. Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

Também deve escolher qual acção o Controlo Parental do BitDefender deve ter em sites para os quais não existe controlo de regras Web:

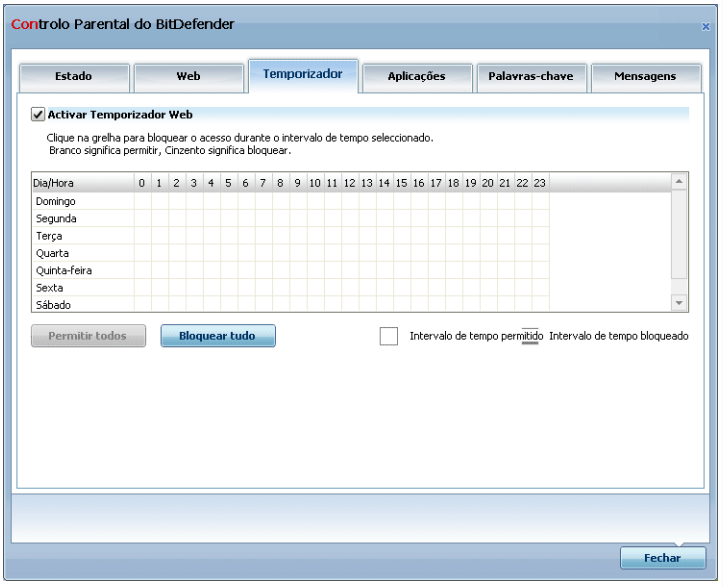
- **Permite todos os sites menos os da lista**. Seleccione esta opção para permitir todos os websites excepto aqueles que definiu a acção de**Bloquear**.
- **Bloqueia todos os sites menos os da lista**. Seleccione esta opção para bloquear todos os websites excepto aqueles que definiu a acção de**Permitir**.

20.4. Limitador de Tempo Web

O **Limitador de tempo de Internet** ajuda-o a permitir ou bloquear acessos à web por parte dos utilizadores ou aplicações durante determinados intervalos de tempo.

Nota
O BitDefender efectuará a actualização a cada hora independentemente das definições do **Limitador de tempo de Internet**.

Para configurar o Limitador de Tempo Web para um utilizador específico, clique no botão **Modificar** correspondente à conta de utilizador e clique no separador **Limitador de Web**.



Limitador de Tempo Web

Limitador de tempo de Internet **Activar limitador de tempo de Internet**.

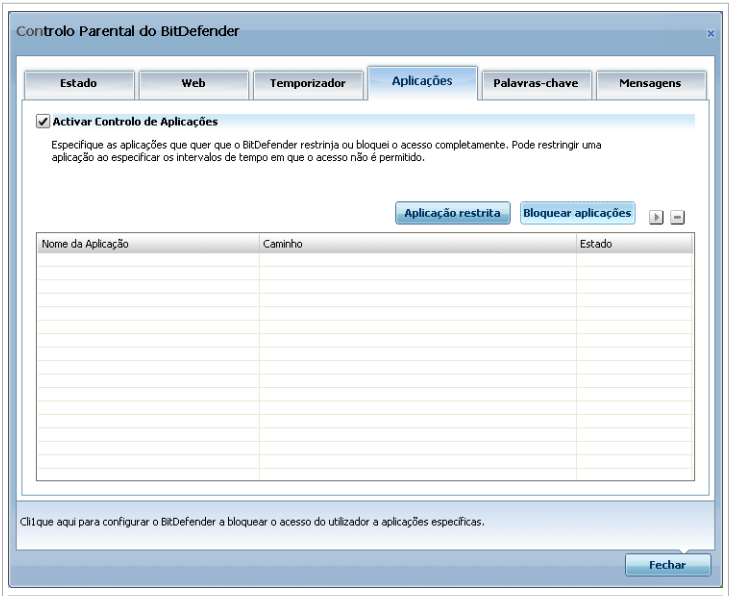
Seleccione os intervalos de tempo em que todas as conexões de internet serão bloquadas. Pode clicar em células individuais, ou pode clicar e arrastar para cobrir periodos mais longos. Além disso, pode clicar em **Bloquear tudo** para seleccionar todas as células e, implicitamente, bloquear totalmente o acesso à web. Se clicou em **Permitir tudo**, o acesso à internet será permitido a qualquer altura.

Importante
As caixas coloridas a cinzento representam intervalos de tempo em que as ligações à Internet estão bloqueadas.

20.5. Controlo de Aplicações

O **Controlo de aplicações** ajuda-o a bloquear qualquer programa impedindo-o de se executar. Jogos, software de multimédia e de mensagens, assim como outras categorias de software e malware podem ser bloqueadas desta forma. As aplicações bloqueadas desta forma ficam também protegidas de modificações, e não podem ser copiadas ou movidas. Pode bloquear permanentemente as aplicações ou apenas durante um intervalo de tempo, tais como os que os seus filhos utilizam para fazer os trabalhos de casa.

Para configurar o Controlo de Aplicações para uma conta de utilizador específica, clique no botão **Modificar** correspondente a essa conta de utilizador e depois clique no separador **Aplicações**.



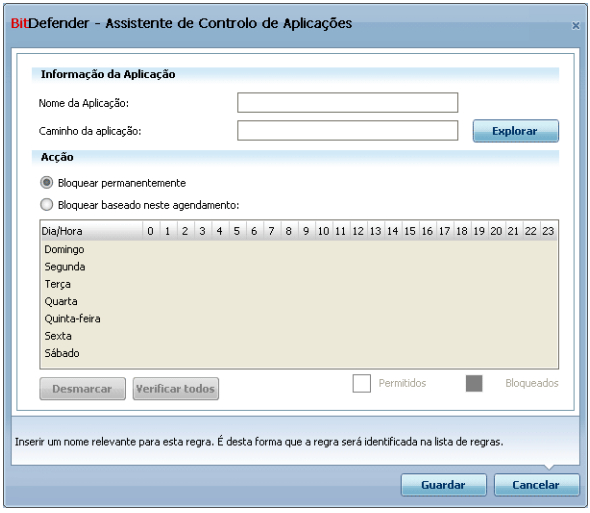
Controlo de Aplicações

Para activar esta protecção seleccione a caixa de selecção correspondente para **Activar Controlo de Aplicações**.

20.5.1. Criar Regras de Controlo de Aplicações

Para bloquear ou restrinjir acesso a uma aplicação, siga estes passos:

1. Clique em **Bloquear Aplicação** ou **Restringir Aplicação**. Irá aparecer uma nova janela:



Especifique aplicação

2. Clique em **Explorar** para localizar a aplicação a que quer bloquear/restringir o acesso.
3. Seleccionar a acção da regra:
   - **Bloquear permanentemente** para bloquear completamente o acesso à aplicação.
   - **Bloqueia baseado nesta agenda** para restrinjir o acesso a determinados intervalos de tempo.

   Se optar por restringir o acesso em vez de bloquear completamente a aplicação, deve também escolher a partir de que dia e intervalos de tempo é que o acesso é bloquado. Pode clicar em células individuais, ou pode clicar e arrastar para cobrir periodos mais longos. Além disso, pode clicar em **Seleccionar tudo** para seleccionar todas as células e, implicitamente, bloquear totalmente a aplicação.

Se clicou em **Desmarcar tudo**, o acesso à aplicação será permitido a qualquer altura.

4. Clique em **Terminar** para adicionar a regra.

20.5.2. Gerir Regras de Controlo de Aplicações

As regras de Controlo de Aplicação que já foram configuradas estão listadas na tabela que se encontra na parte inferior da janela. O nome da aplicação, o caminho e o estado actual estão listados para cada regra de Controlo de Aplicação.

Para editar uma regra, seleccione-a e clique no botão **Editar**e faça as mudanças necessárias na janela de configuração. Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

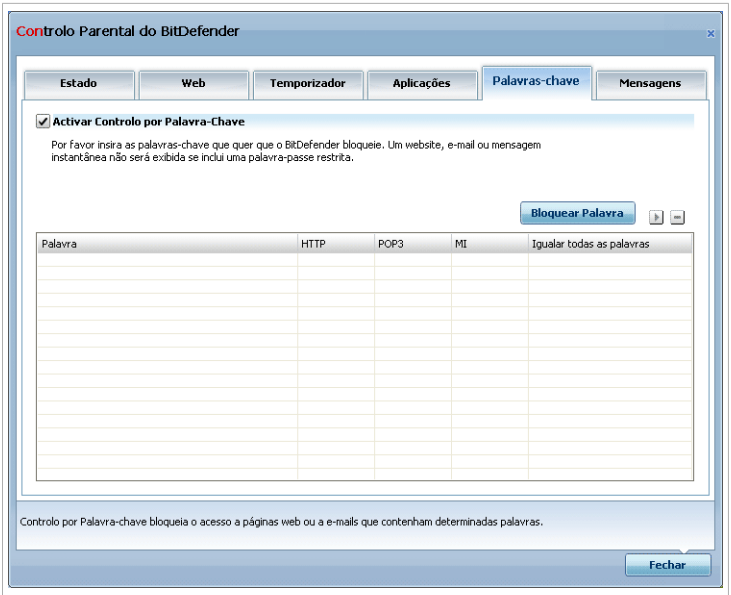
20.6. Controlo de Palavras-Chave

A Filtragem por Palavra-chave ajuda-o a bloquear o acesso dos utilizadores 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 o Controlo de Palavras-chave para uma conta de utilizador específica, clique no botão **Modificar** correspondendo a essa conta de utilizador e clique no separador **Palavras-chave**.



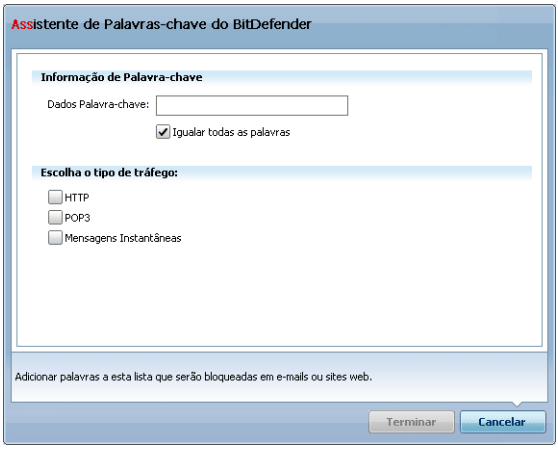
Controlo de Palavras-Chave

Marque a caixa **Activar Filtragem Palavra-chave** se pretende usar esta opção de controlo.

20.6.1. Criar Regras de Controlo de Palavras-chave

Para bloquear uma palavra ou frase, siga estes passos:

1. Clique em **Bloquear palavra-chave**. Uma nova janela irá aparecer:



Específique Palavras-chave

2. Escreva a palavra ou frase que deseja bloquear no campo editar. Se somente quiser que sejam detectadas palavras inteiras, selecione o **Igualar Todas as Palavras** check box.
3. Seleccione o tipo de tráfego que o BitDefender deverá analisar para essa palavra específica.

Opção	Descrição
HTTP	As páginas web que contenham a palavra-chave são bloqueadas.
POP3	As mensagens de e-mail que contenham a palavra-chave são bloqueadas.
Mensagens Instântaneas	As mensagens instântaneas que contenham a palavra-chave são bloqueadas.

4. Clique em **Terminar** para adicionar a regra.

20.6.2. Gerir Regras de Controlo de Palavras-Chave

As regras de Controlo de Palavras-chave que já foram configuradas estão listadas na tabela que se encontra na parte inferior da janela. As palavras e o estado actual de cada diferente tipo de tráfego estão listados para cada regra de Controlo de Palavras-chave.

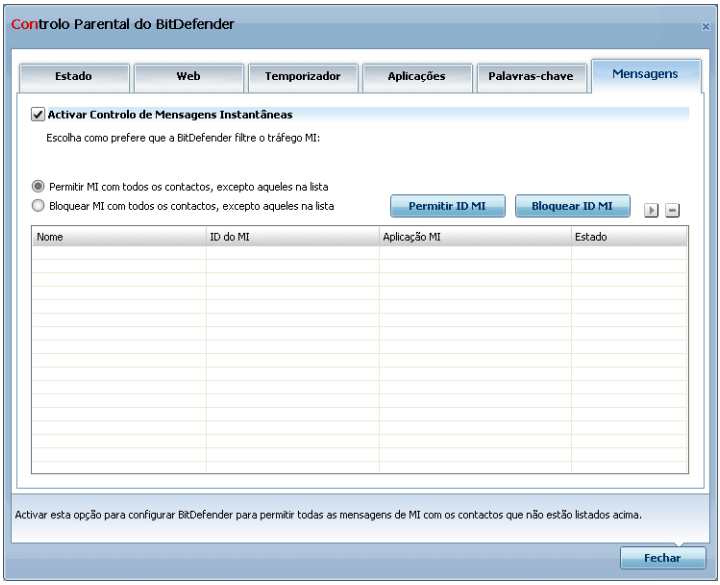
Para editar uma regra, seleccione-a e clique no botão **Editar**e faça as mudanças necessárias na janela de configuração. Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

20.7. Controlo de Mensagens Instântaneas (IM)

O Controlo de Mensagens Instântaneas (IM) permite-lhe especificar os contactos IM com os quais a sua criança pode fazer chat.

Nota
O Controlo de Mensagens Instântaneas (IM) só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.

Para configurar o Controlo de MI para uma conta de utilizador específica, clique no botão **Modificar** correspondendo a essa conta de utilizador e clique no separador de**Mensagem**.



Controlo de Mensagens Instantâneas

Marque a caixa **Activar Controlo de Mensagens Instântaneas** se deseja utilizar esta opção de controlo.

20.7.1. Criando Regras de Controlo de Mensagens Instantâneas (MI)

Para permitir ou bloquear as mensagens instantâneas com um contacto, siga estes passos:

1. Clique em **Bloquear o ID do IM** ou **Permitir o ID de IM**. Aparecerá uma nova janela:

Adicionar um contacto MI

2. Digite o nome do contacto no campo **Nome**.
3. Digite o endereço de e-mail ou o nome de utilizador usado pelo contacto do IM no campo **E-mail ou ID IM** .
4. Escolher o program de IM com o qual o contacto se associa.
5. Seleccione a acção desejada para esta regra - **Bloquear** ou **Permitir**.
6. Clique em **Terminar** para adicionar a regra.

20.7.2. Gerindo Regras de Controlo de Mensagens Instantâneas (MI)

As regras de Controlo de Mensagens Instantâneas que já foram configuradas estão listadas na tabela que se encontra na parte inferior da janela. O nome, o ID do MI, a aplicação MI e o estado actual estão listados para cada regra de Controlo de Mensagens Instantâneas.

Para editar uma regra, seleccione-a e clique no botão **Editar**e faça as mudanças necessárias na janela de configuração. Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

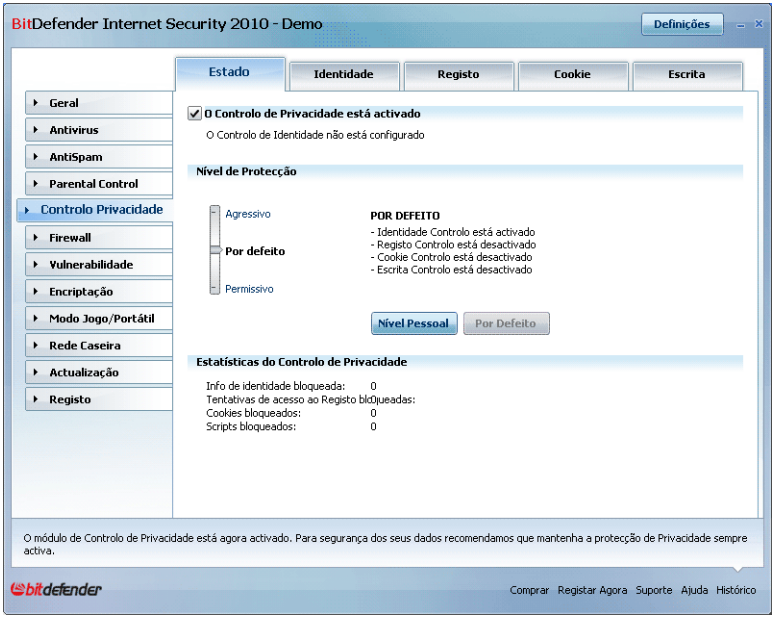
Deve também seleccionar a acção que o Controlo Patental do BitDefender deverá ter em relação a contactos de MI para os quais não tenham sido criadas regras. Seleccione **Bloquear** ou **Permitir MI com todos os contactos, exepto os da lista**.

21. Controlo de Privacidade

BitDefender monitoriza dezenas de potenciais “hotspots” no seu sistema onde o spyware poderá actuar, e também verifica quaisquer mudanças feitas ao seu sistema e ao seu software. É bastante eficaz no bloqueio de cavalos de Tróia e outras ferramentas instaladas por hackers, que tentam comprometer a sua privacidade e enviar a sua informação pessoal, tal como números de cartão de crédito, do seu computador para o do hacker.

21.1. Estado do Controlo de Privacidade

Para configurar o Controlo de Privacidade e ver informação quanto à sua actividade, vá para **Controlo de Privacidade>Estado** no Modo Avançado.



Estado do Controlo de Privacidade

Pode ver se o Controlo de Privacidade está activo ou inactivo. Se deseja mudar o estado do Controlo de Privacidade, limpe ou marque a correspondente caixa de selecção.

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

O Controlo de Privacidade protege o seu computador usando estes controlos de protecção importantes:

- Controlo 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 secção de Identidade.
- O Controlo 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 Controlo de Cookies - irá pedir a sua permissão sempre que um novo site web tentar definir uma cookie.
- O Controlo de script - irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

Ao fundo da secção poderá ver as **Estatísticas do Controlo de Privacidade**.

21.1.1. 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	Todos os controlos de protecção estão desactivados.
Por Defeito	Apenas o **Controlo de Identidade** está activo.
Agressivo	**Controlo de indentidade**, **Controlo de registo**, **Controlo de Cookies** e **Controlo de Script** estão activos.

Pode personalizar o nível de protecção clicando em **Nível Pessoal**. Na janela que lhe irá aparecer, escolha o controlos de protecção que deseja activar e clique em **OK**.

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

21.2. Controlo 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 Controlo de Identidade protege-o contra o roubo de informação sensível quando se encontra on-line. Baseado nas regras que criar, o Controlo 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-utilizador é fornecido de forma a que os utilizadores de diferentes contas do Windows possam configurar e usar as suas próprias regras de identidade. Se a sua conta de Windows é uma conta de administrador, as regras que cria podem ser configuradas para também se aplicarem a utilizadores de outras contas do computador.

Porquê usar o Controlo de Identidade?

- O Controlo 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.

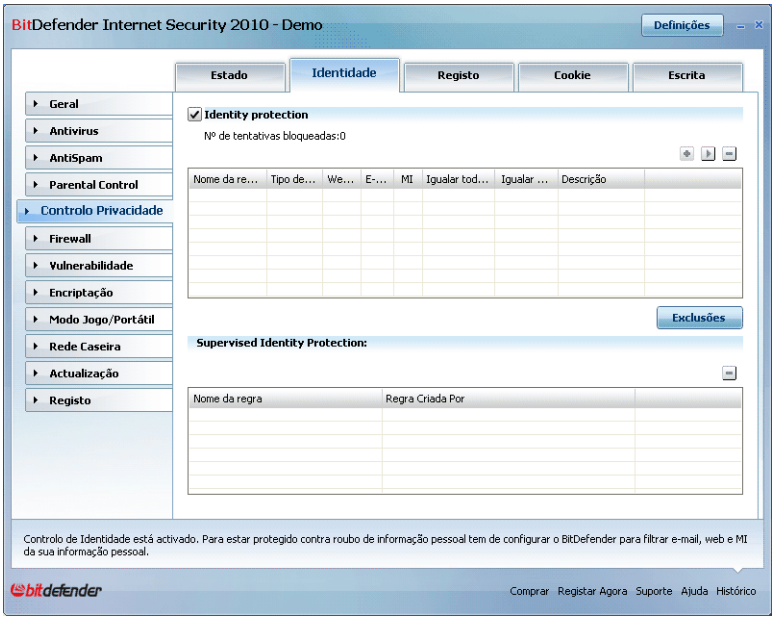
  Supondo que tal aplicação funciona de forma a evitar a detecção antivírus, a mesma não pode enviar os dados roubados por e-mail, web ou mensagens instântaneas se tiver criado as regras de protecção de identidade adequadas.

- O Controlo 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 Controlo de Identidade, vá a **Controlo de Privacidade>Identidade** no Modo Avançado.



Controlo de identidade

Se deseja usar p Controlo de Identidade, siga estes passos:

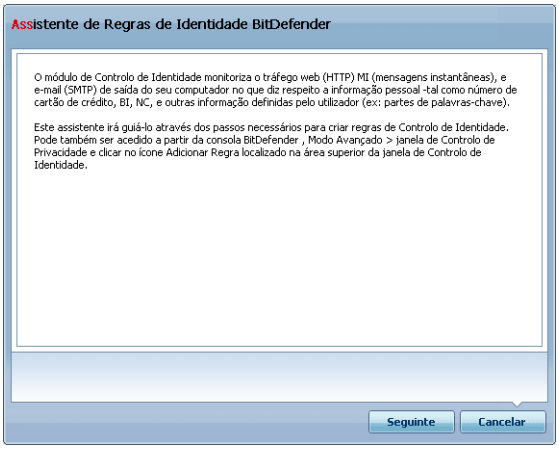
1. Seleccione a opção **Activar Controlo de Identidade**.
2. Criar regras para proteger a sua informação sensível. Para mais informação, por favor consulte o “*Criar Regras de Identidade*” (p. 214).
3. Se necessário, defina excepções específicas para as regras que criou. Para mais informação, por favor consulte o “*Definir Excepções*” (p. 217).
4. Se for um administrador no computador, pode auto excluir-se das regras de identidade criadas por outros administradores.

   Para mais informação, por favor consulte “*Regras definidas por outros Administradores*” (p. 219).

21.2.1. Criar Regras de Identidade

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

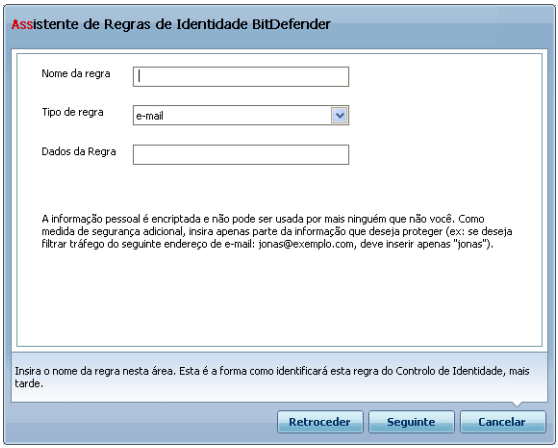
Passo 1/4 - Janela de Boas-vindas



Janela de boas-vindas

Clique **Seguinte**.

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.

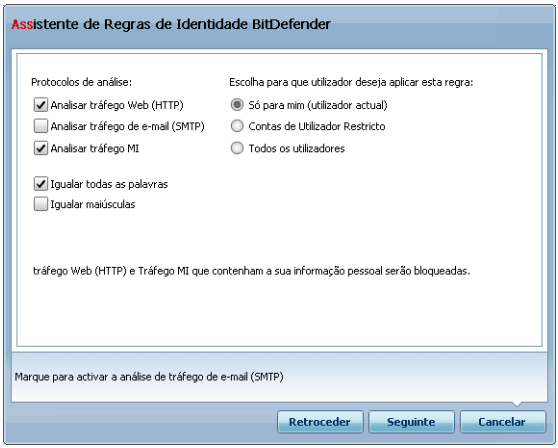
Nota

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 **Seguinte**.

Passo 3/4 - Seleccione o Tipo e Utilizadores de Tráfego.



Seleccione Utilizadores e Tipo de Trafego.

Seleccione o tráfego que quer que o BitDefender analise. Estão disponíveis as seguintes opções:

- **Analisar Web (tráfego HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar e-mail (tráfego 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.

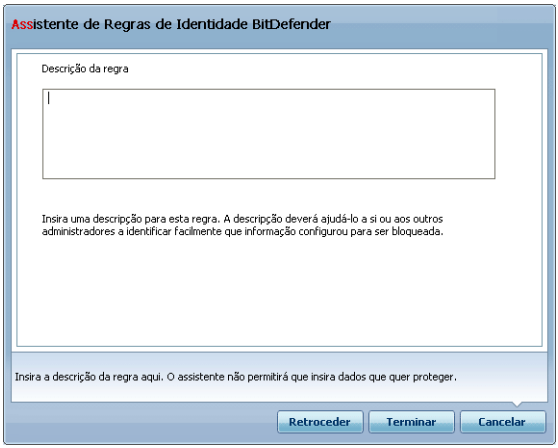
Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

Específique para que utilizadores se aplicam as regras.

- **Apenas para mim (utilizador actual)** - a regra será aplicada à sua conta de utilizador.
- **Utilizadores limitados** - a regra será aplicada a si e a todas as contas de Windows limitadas.
- **Todos os utilizadores** - a regra será aplicada a todas contas do Windows.

Clique **Seguinte**.

Passo 4/4 - Descrever Regra



Descrever Regra

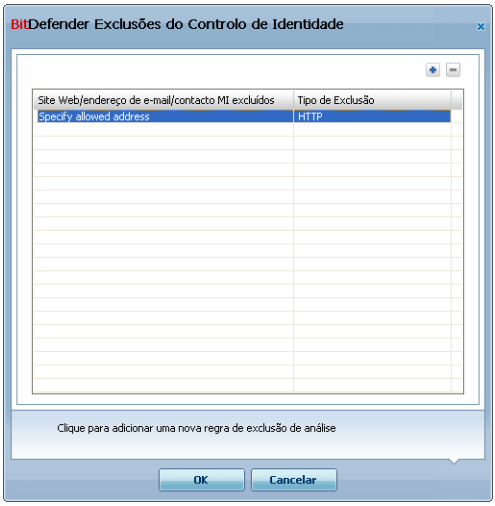
Insira uma breve descrição da regra no campo de edição. Um vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

Clique em **Terminar**. A regra aparecerá na tabela.

21.2.2. 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**.



Exclusões

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 item excluído** e inserir o endereço web, endereço de e-mail ou o contacto IM que deseja adicionar como excepção.
3. Duplo-clique em**Tipo de Tráfego** 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 **Email (SMTP)**.
   - Se especificou um contacto IM, seleccione**IM**.

Para remover uma excepção da lista, seleccione-a e clique em **Remover**.

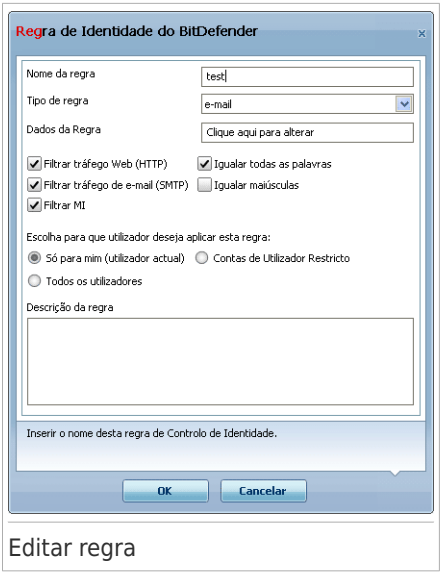
Clique em **Aplicar** para guardar as alterações.

21.2.3. 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.

21.2.4. Regras definidas por outros Administradores

Quando não é o único utilizador com direitos administrativos no seu sistema, os restantes administradores podem criar as suas proprias regras. No caso de desejar que regras criadas por outros uitilizadores nao se apliquem enquando está ligado, o BitDefender permite-lhe excluir-se de qualquer regra que não tenha criado.

Pode ver a lista de regras criadas por outros administradores na tabela em baixo de**Identificar Regras de Controlo**. Para cada regra, está listado na tabeça o nome da regra e o nome do utilizador que a criou.

Para se excluir a si de uma regra, seleccione a regra na tabela e clique no botão **Apagar**.

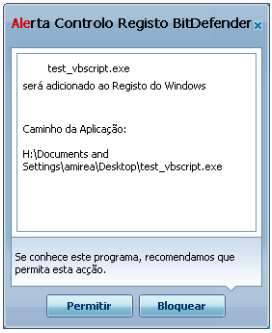
21.3. Controlo de registo

Uma parte muito importante do sistema operativo do Windows é chamada de **Registo**. Aqui é o local onde o guarda as suas definições, programas instalados, informação acerca do utilizador e por aí a diante.

O **Registo** também é utilizado para definir quais os programas que deverão ser lançados automaticamente ao iniciar o Windows. Frequentemente, os vírus usam

isto para se lançarem automaticamente quando o utilizador reiniciar o seu computador.

O **Controlo de registo** vigia o Registo do Windows – mais uma vez, isto é útil para detectar Cavalos de Tróia. Irá alertá-lo sempre que um programa tente modificar uma entrada de registo para poder ser executado ao iniciar o Windows.



Alerta de Registo

Poderá ver o programa que está a tentar alterar o registo do Windows.

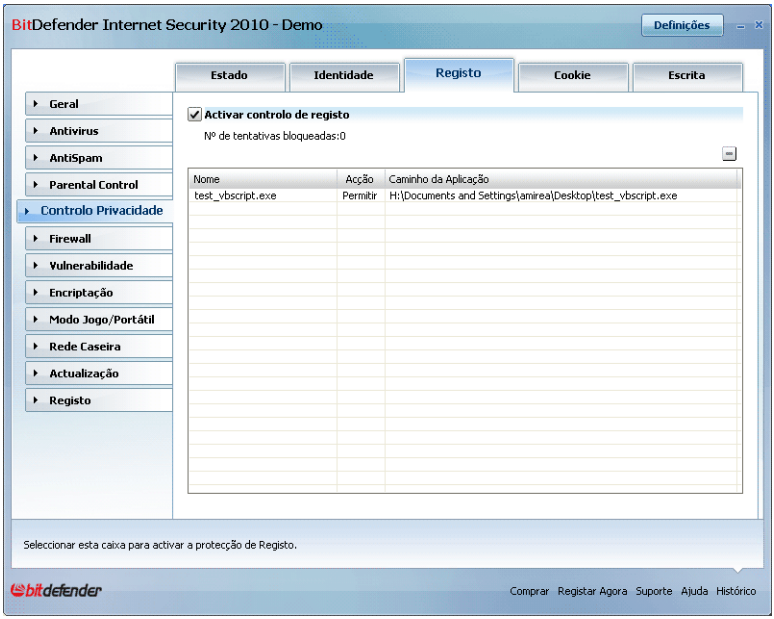
Se não reconhece o programa e lhe parecer suspeito, clique em **Bloquear** para evitar que ele modifique o registo do Windows. De outra forma, clique em **Permitir** para permitir a modificação.

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 irá, normalmente, alertá-lo quando instalar novos programas que necessitem decorrer na próxima inicialização do seu computador. Na maioria dos casos, estes programas são legítimos e podem ser confiáveis.

Para configurar o Controlo de Registo, clique em **Controlo Privacidade>Registo** no Modo Avançado.



Controlo de registo

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

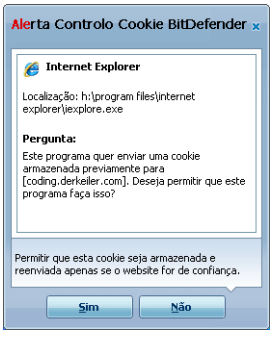
21.4. Controlo de cookies

As Cookies são uma ocurrência muito comum na Internet. Elas são ficheiros peqenos armazenados no seu computador. Os sites da Web criam estas cookies para manter o rasto da informação específica acerca de si.

As Cookies são geralmente criadas para facilitar a sua vida. Por exemplo, elas podem ajudar o site da Web a lembrar-se do seu nome e preferências, para que não tenha de as voltar a introduzir sempre que os visitar.

Mas as cookies também podem ser usadas para comprometer a sua privacidade, ao seguir o rasto das patentes da sua navegação.

É aqui que o **Controlo de Cookies** ajuda. Quando activo, o **Controlo de Cookies** irá pedir a sua permissão sempre que um site da web tentar estabelecer uma cookie:



Alerta de cookie

Pode ver o nome da aplicação que está a tentar enviar um ficheiro de cookie.

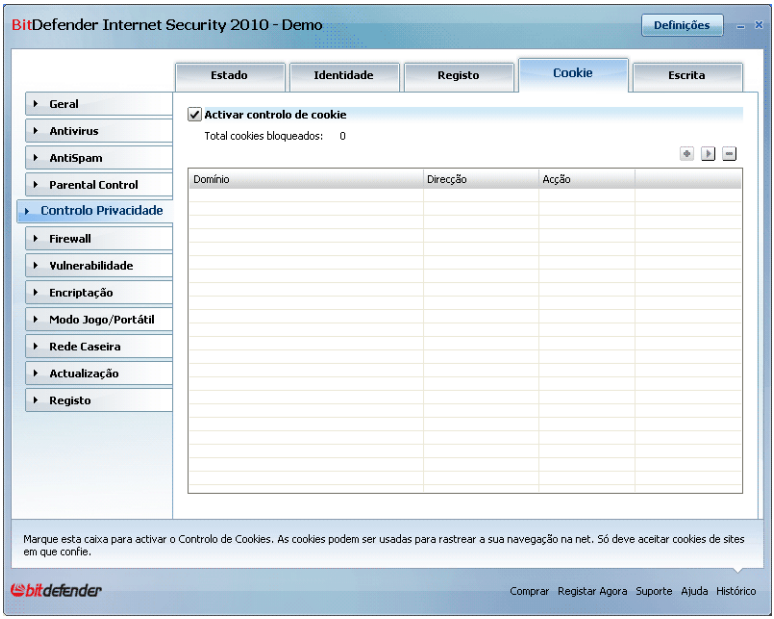
clique em **Sim** ou **Não** e será criada, aplicada e listada uma regra na tabela das regras.

Isto irá ajudá-lo a escolher quais os sites da web em quais confiar ou não.

Nota

Devido ao grande número de cookies usadas hoje na Internet, o **Controlo de Cookie** pode ser um pouco aborrecido ao começo. Inicialmente, irá perguntar uma série de questões acerca de sites que tentam colocar cookies no seu computador. Logo que adicione os seus sites habituais à lista-regra, a navegação tornar-se-á tanto facilitada como anteriormente.

Para configurar o Controlo de Cookies, clique em **Controlo Privacidade>Cookie** no Modo Avançado.



Controlo de cookies

Pode ver as regras criadas até agora listadas na tabela.

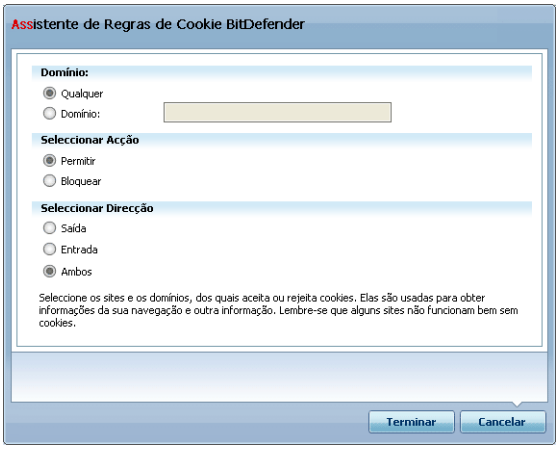
Importante
A prioridade das regras é feita de baixo para cima, o que significa que a última regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para alterar os parametros de uma regra, seleccione a regra no botão **Editar** ou faça duplo clique. Faça as alterações desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

21.4.1. Janela de Configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



Seleccione Endereço, Acção e Direcção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, no qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os cookies desse domínio serão executados.
Bloquear	Os cookies desse domínio não serão executados.

- **Sentido** - selecciona o sentido do tráfego.

Tipo	Descrição
Saída	A regra será aplicada apenas às cookies que são enviadas para fora do site conectado.
Entrada	A regra será aplicada apenas às cookies que são recebidas do site conectado.
Ambos	A regra aplica-se em ambos os sentidos.

Nota
Pode aceitar cookies mas nunca as poderá devolver, ao estabelecer a acção para **Negar** e a direcção para **Saída**.

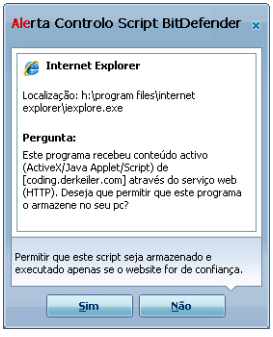
Clique em **Terminar**.

21.5. Controlo de script

Escritas e outros códigos tais como Controlos de ActiveX e Java applets, os quais são usados para criar páginas da web interactivas, podem ser programados para ter efeitos inofensivos. Os elementos do ActiveX, por exemplo, podem ganhar total acesso aos seus dados e podem ler dados do seu computador, informação eliminada, capturar palavras-passe e interceptar mensagens enquanto você está em linha. Apenas deverá aceitar conteúdo activo de sites que conhece e confia totalmente.

BitDefender deixa-o escolher entre permitir ou bloquear a execução destes elementos.

Com o **Controlo de script** terá a seu cargo escolher os sites da web, nos quais confia ou não. O BitDefender irá pedir a sua permissão sempre que um site da web tente activar uma escrita ou outro conteúdo activo:

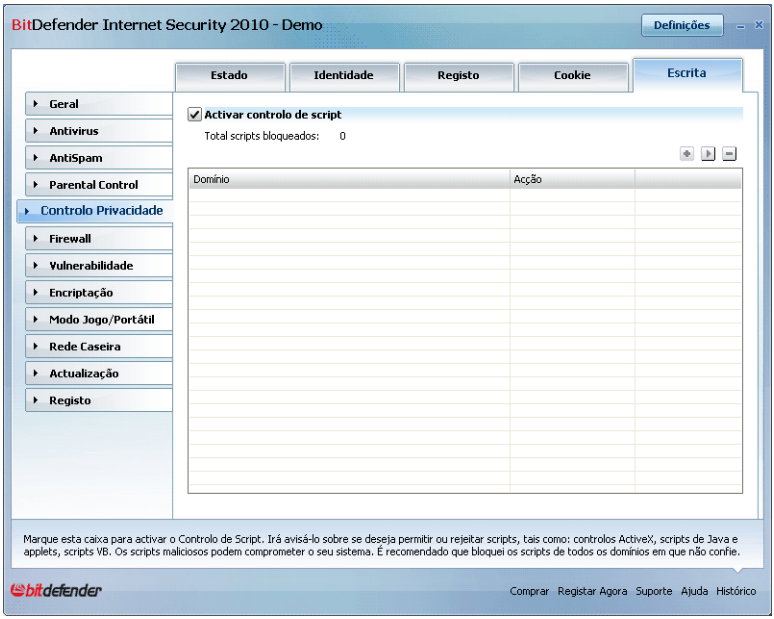


Alerta de script

Pode ver o nome do recurso.

clique em **Sim** ou **Não** e será criada, aplicada e listada uma regra na tabela das regras.

Para configurar o Controlo de Script, clique em **Controlo Privacidade>Script** no Modo Avançado.



Controlo de script

Pode ver as regras criadas até agora listadas na tabela.

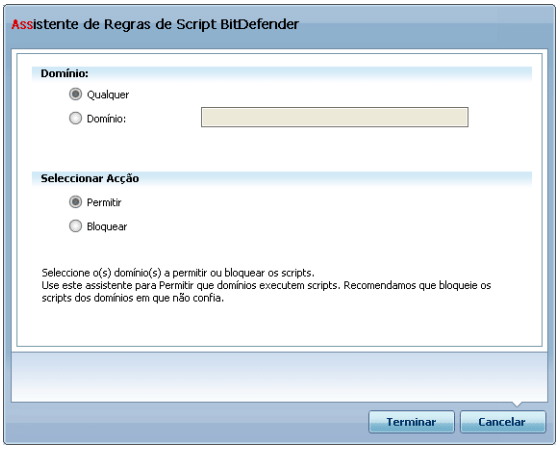
Importante
A prioridade das regras é feita de baixo para cima, o que significa que a última regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para alterar os parametros de uma regra, seleccione a regra no botão **Editar** ou faça duplo clique. Faça as alterações desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

21.5.1. Janela de Configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



Seleccione Endereço e Acção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, no qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os scripts desse domínio serão executados.
Bloquear	Os scripts desse domínio não serão executados.

Clique em **Terminar**.

22. 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
A firewall é essencial se tiver uma ligação de banda larga ou ADSL.

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).

22.1. Definições

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 se manter protegido contra os ataques da Internet, mantenha activa a **Firewall**.

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 a **Firewall** esteja desactivada.

22.1.1. Definir a Acção por Defeito

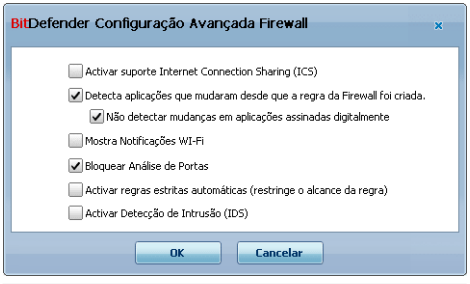
Por defeito o BitDefender permite automaticamente que todos os programas conhecidos da sua lista branca acedam aos serviços da rede e à Internet. Para todos os outros programs o BitDefender consulta-o através de uma janela de alerta para que decida a acção a tomar. A acção que determinar será aplicada 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 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 operativo. Para ver toda a Lista Branca, clique em **Ver Lista Branca**.
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.

22.1.2. Configuração Avançada da Firewall

Clique em **Avançada** para configurar as definições avançadas da firewall.



Opções Avançadas da Firewall

Estão disponíveis as seguintes opções:

- **Activar Suporte de Internet Connection Sharing (ICS)** - activa o suporte para Internet Connection Sharing (ICS).

  Nota
  Esta opção não activa automaticamente o ICS no seu sistema, mas apenas permite este tipo de ligação em caso de a activar no seu sistema operativo.

  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).

- **Detectar aplicações que mudaram desde que a regra da firewall foi criada** - verifica cada aplicação que se tenta ligar à Internet para ver se ela mudou desde que a regra que controla o seu acesso foi adicionada. Se a aplicação foi alterada, uma alerta aparecerá para que permita ou bloqueie o acesso dessa 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).

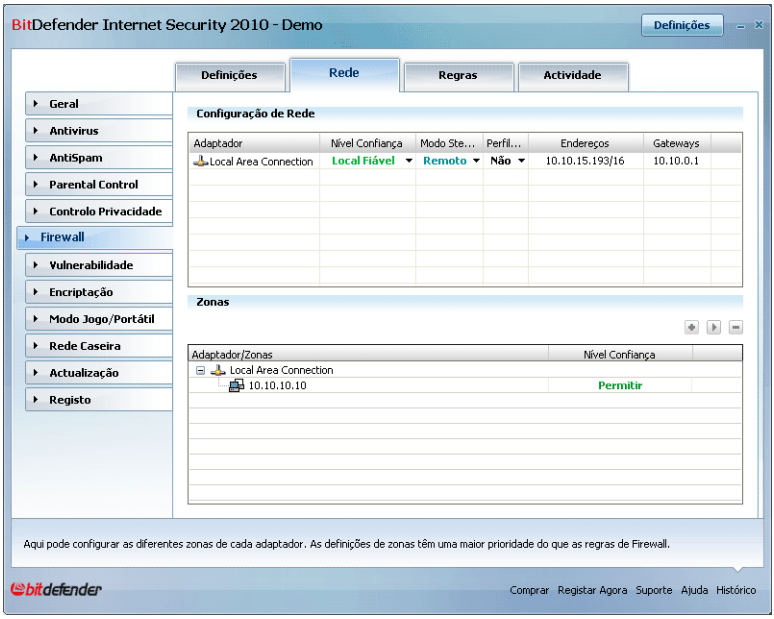
- **Bloquear scans de portas** - detecta e bloqueia todas as tentativas de descobrir que portas se encontram abertas.

  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.

22.2. 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.

- **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.

22.2.1. 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).
Bloqueado	Bloqueia completamente o tráfego de rede e de Internet através do respectivo adaptador.

22.2.2. 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.

22.2.3. 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**.

22.2.4. Zonas de Rede

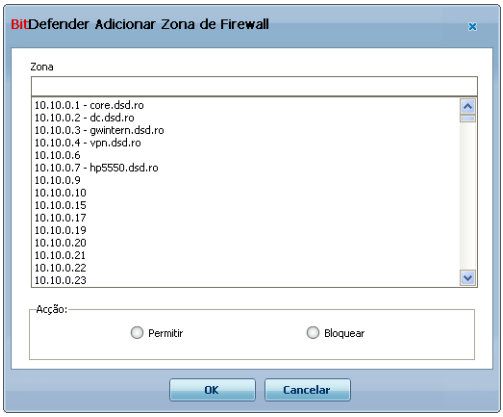
Pode adicionar computadores autorizados ou bloqueados a uma determinado adaptador.

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** .



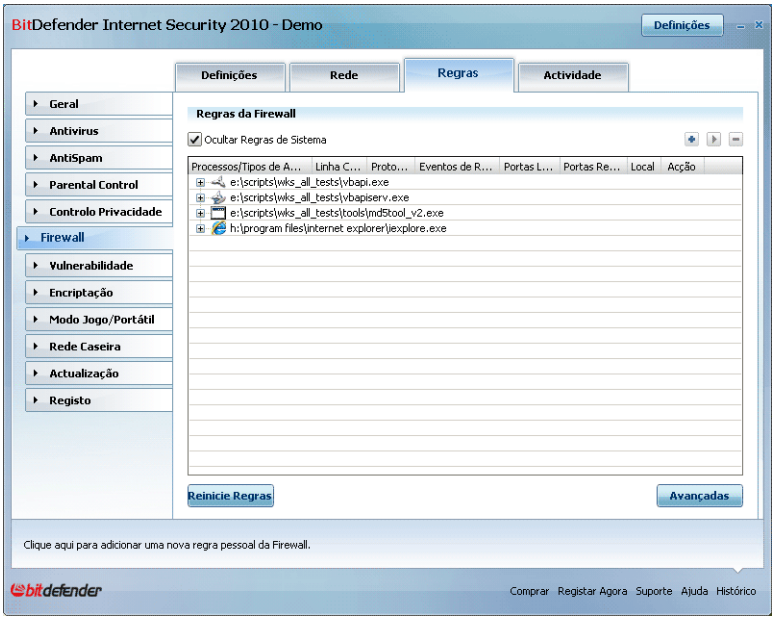
Adicionar Zona

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**.

22.3. 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 permite que dois hosts estabeleçam uma ligação e troquem dados entre si. O TCP garante a entrega dos dados e também garante que os pacotes serão entregues na mesma ordem em que foram enviados.
UDP	User Datagram Protocol - UDP é um meio de transporte baseado em IP desenhado para uma elevada performance. Os jogos e outras aplicações baseadas em vídeo usam com frequência o 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.

22.3.1. 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 ficheiro 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.

22.3.2. Apagar e Redifinir 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**.

Se deseja carregar o conjunto de regras por defeito para o nível de confiança seleccionado, clique **Reiniciar Regras**.

22.3.3. 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.

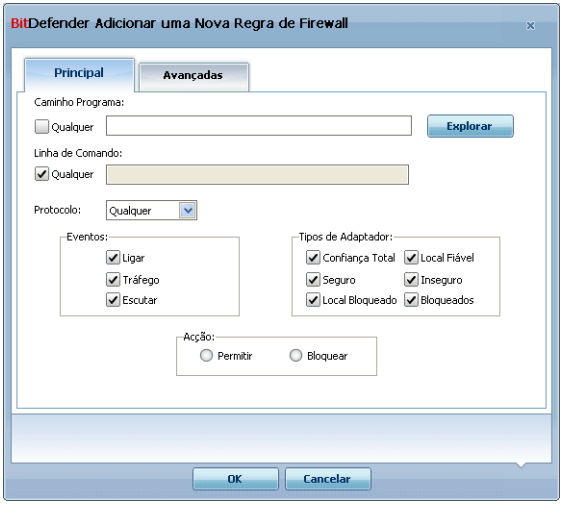
Modificar regras. Para modificar uma regra existente, siga os seguintes passos:

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 **Aplicar** para guardar 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 ao TCP, seleccione **TCP**.
  - Se deseja que a regra se aplique ao UDP, seleccione **UDP**.

▶ 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:

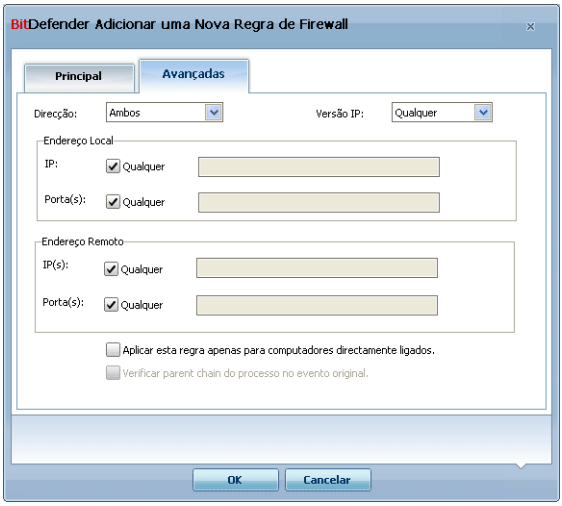
Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma. Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo 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.

- **Tipos de Adaptador.** Seleccione os tipos de adaptador a que as regras se aplicam.
- **Acção.** Seleccione uma das seguintes acções disponíveis:

Acção	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Bloquear	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	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

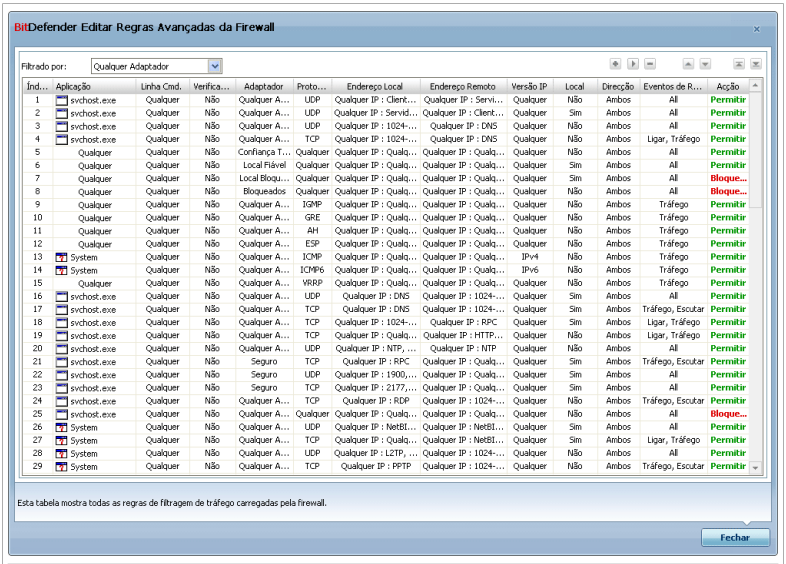
- **versão IP.** Seleccione do menu a versão do IP (IPv4, IPv6 ou qualquer) ao qual a regra se aplica.
- **Endereço Local.** Especifique o endereço IP local e a porta aos quais a regra se aplica da seguinte forma:
  - Se tem mais de um adaptador de rede, pode limpar a caixa **Todos** e inserir um endereço 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.

22.3.4. Gestão Avançada de Regras

Se necessita de controlo 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**.

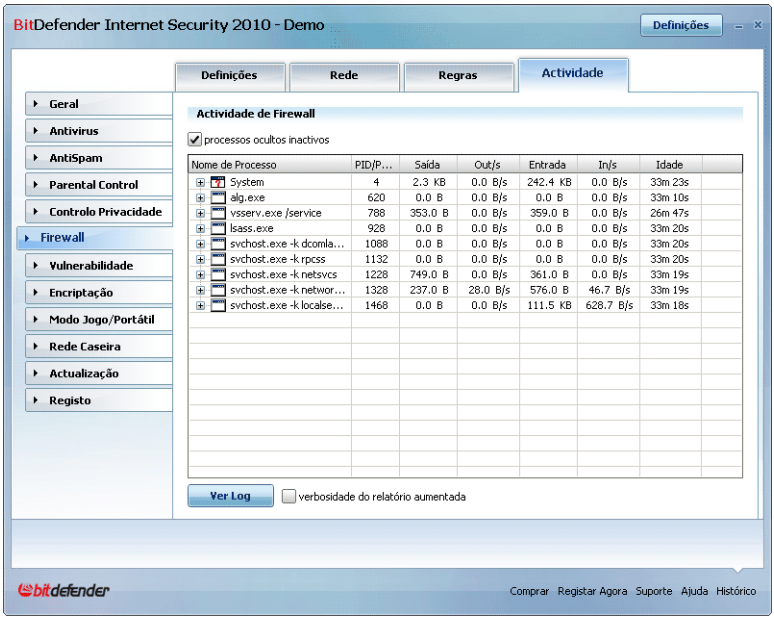
Para editar uma regra, seleccione-a e clique no botão **Editar Regra** ou faça duplo-clique sobre ela.

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.

22.4. Controlo de Ligação

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.



Controlo de Ligação

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 de saída.
- Indica uma ligação de entrada.
- 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 (activar/desactivar 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 ficheiro de relatório da Firewall do BitDefender que pode ser visualizado clicando em **Mostrar Relatório**. O ficheiro está localizado na pasta Ficheiros Comuns do actual utilizador do Windows, no caminho: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Se deseja que o relatório contenha mais informação, seleccione **Aumentar verbosidade do relatório**.

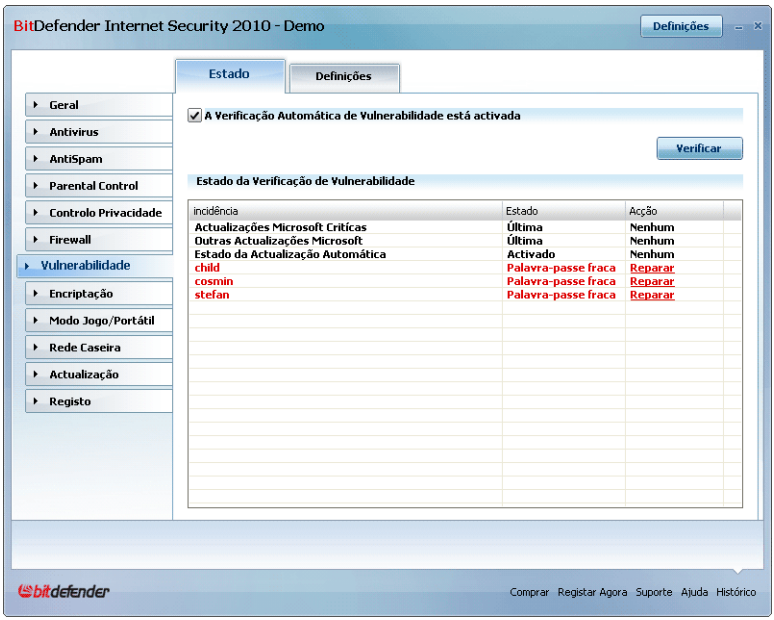
23. Vulnerabilidade

Um passo importante na protecção do seu computador contra as pessoas e aplicações maliciosas é manter actualizado o seu sistema operativo e as aplicações que usa regularmente. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, palavras-passe fortes (palavras-passe que não são fáceis de adivinhar) devem de ser criadas para cada conta de utilizador do Windows.

O BitDefender analisa regularmente o seu sistema em busca de vulnerabilidades e notifica-o das incidências existentes.

23.1. Estado

Para configurar a análise automática de vulnerabilidades, ou levar a cabo uma, clique em **Vulnerabilidade>Estado** no Modo Avançado.



Estado Vulnerabilidade

A tabela mostrará as incidências que foram encontradas na ultima verificação de vulnerabilidade e o seu estado. Pode ver a acção levada a cabo para reparar cada uma das vulnerabilidades, caso tivesse havido alguma. Se a acção for **Nenhuma**, então a respectiva incidência não representa uma vulnerabilidade.

Importante

Para ser automaticamente notificado acerca das vulnerabilidades do seu sistema e aplicações, mantenha a **Análise Automática de Vulnerabilidades** activada.

23.1.1. Reparar Vulnerabilidades

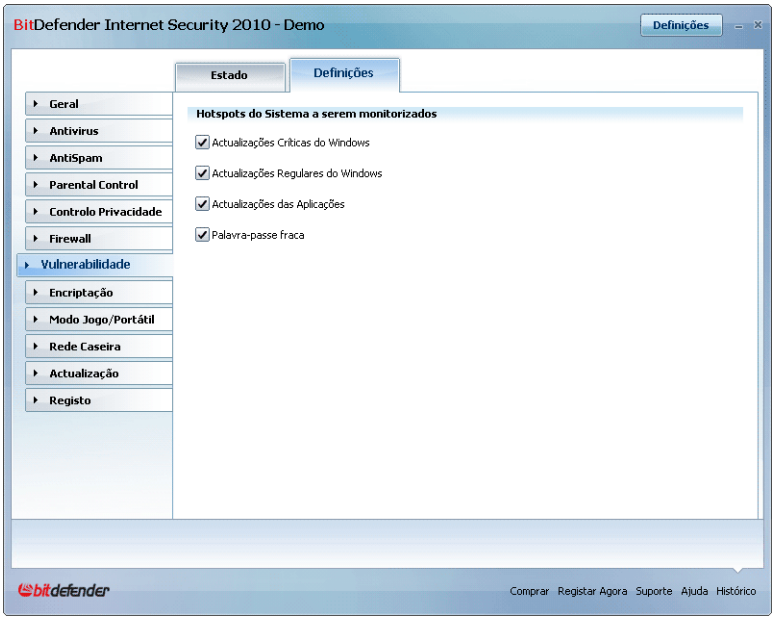
Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:

- Se estiverem disponiveis actualizações do Windows, clique em **Instalar** na coluna **Acções** para as instalar.
- Se a aplicação não estiver actualizada, use o link fornecido da **Página Web** para descarregar e instalar a versão mais recente dessa aplicação.
- Se uma conta de utilizador do Windows tem uma palavra-passe fraca, clique em **Reparar** para forçar o utilizador a mudar a palavra-passe da próxima vez que entrar no windows ou mude você mesmo a palavra-passe. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

Pode clicar em **Analisar Agora** e seguir o assistente para reparar as vulnerabilidades passo a passo. Para mais informação, por favor consulte o "*Assistente de verificação de vulnerabilidade*" (p. 68).

23.2. Definições

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**
- **Actualizações de Aplicações**
- **Palavras-passe Fracas** .

Nota

Se limpar a a caixa correspondente a uma determinada vulnerabilidade, o BitDefender não o irá mais notificar acerca das incidências relacionadas.

24. Encriptação

BitDefender offers encryption capabilities to protect your confidential documents and your instant messaging conversations through Yahoo Messenger and MSN Messenger.

24.1. Encriptação de Mensagens Instantâneas (IM)

By default, BitDefender encrypts all your instant messaging chat sessions provided that:

- Your chat partner has a BitDefender version installed that supports IM Encryption and IM Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use either Yahoo Messenger or Windows Live (MSN) Messenger.

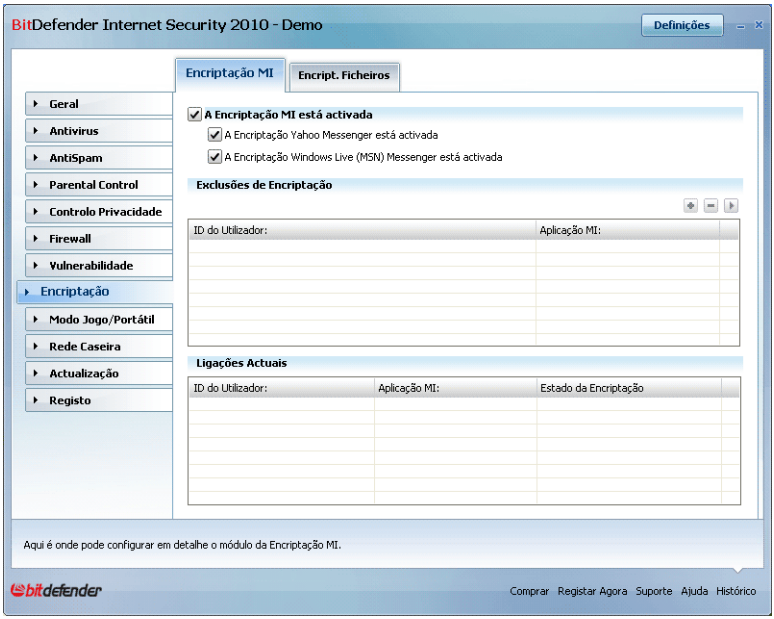
Importante

BitDefender não irá encriptar uma conversação se o parceiro usar uma aplicação de chat web-based, tal como a Meebo, ou se um parceiro de conversação usar o Yahoo Messenger e o outro usar o Windows Leve (MSN).

Para configurar a encriptação de Mensagens Instantâneas, clique em **Encriptação>Encriptação IM** no Modo Avançado.

Nota

You can easily configure instant messaging encryption using the BitDefender toolbar from the chat window. Para mais informações, por favor consulte o *"Integração com os programas de Mensagens Instântaneas"* (p. 294).



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.

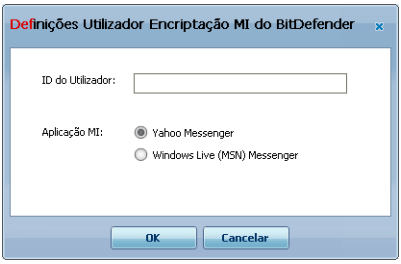
São mostradas duas tabelas:

- **Exclusões da Encriptação** - lista os IDs dos utilizadores e o programa de IM associado para os quais a encriptação está desactivada. Para remover um contacto da lista , seleccione-o e clique no botão **Remover**.
- **Ligações Actuais** - lista as actuais ligações de mensagens (IDs dos utilizadores 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.

24.1.1. Desactivar a Encriptação para Utilizadores Específicos

Para desactivar a encriptação para um determinado utilizador, 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 utilizador do seu contacto.
3. Seleccione a aplicação de mensagens instântaneas associada ao contacto.
4. Clique em **OK**.

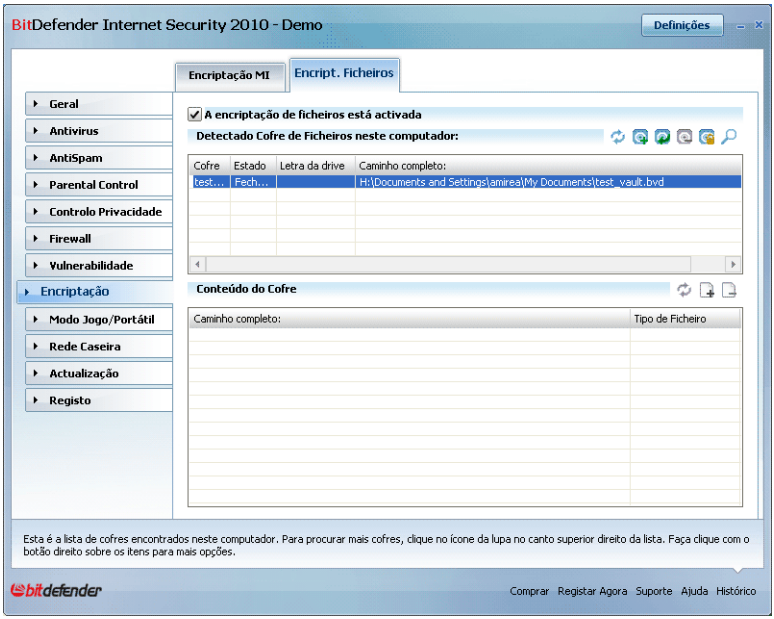
24.2. Encriptação Ficheiros

O Cofre de Ficheiros BitDefender permite-lhe criar drives lógicas encriptadas, e protegidas por palavra-passe (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis. Os dados armazenados nos cofres apenas podem ser acedidos pelos utilizadores que sabem a palavra-passe.

A palavra-passe 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 ficheiros, aceder aos que lá estão ou alterá-los.

Fisicamente, o cofre é um ficheiros armazenado no seu disco duro local com a extensão `.bvd`. Apesar dos ficheiros físicos que representam as drives de cofre poderem ser acedidos a partir de um sistema operativi 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 Ficheiros** no Modo Avançado.



Cofre

Para desactivar o Cofre de Ficheiros, limpe a caixa**Cofre de Ficheiros activado** e clique em **Sim** para confirmar. Se desactivar o Cofre de Ficheiros, todos os cofres de ficheiros serão fechados e não será mais capaz de aceder aos ficheiros que eles contêm.

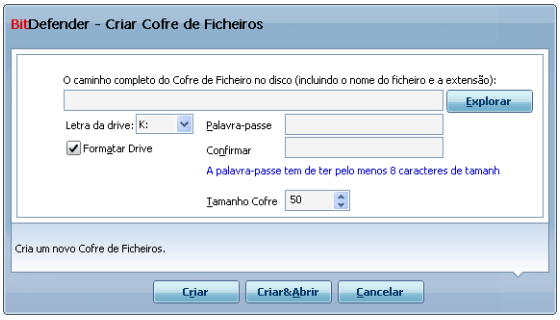
A tabela no topo mostra os cofres de ficheiros no seu computador. Pode ver o nome, o estado (aberto / fechado), a letra da drive e o caminho completo para o cofre. A tabela do fundo mostra o conteúdo dos cofre seleccionado.

24.2.1. Criar um Cofre

Para criar um cofre, use um dos seguintes métodos:

- Clique **Criar cofre**.
- Clique botão direito do rato na tabela dos cofres e seleccionar **Criar**.
- Clique botão direito do rato no seu Ambiente de Trabalho ou numa pasta do seu computador, apontar para **Cofre Ficheiros BitDefender** e seleccionar **Criar**.

Uma nova janela irá aparecer.



Criar Cofre de Ficheiros

Proceder da seguinte forma:

1. Especificar a localização e o nome do cofre de ficheiros.
   - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
   - Apenas insira o nome do cofre no campo correspondente para criá-lo em Os Meus Documentos. Para abrir Os Meus Documentos, clique em start menu Inciar do Windows, e depois **Os Meus Documentos**.
   - Insira o caminho completo do cofre de ficheiros no disco. Por exemplo, `C:\meu_cofre.bvd`.
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 nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe**. Qualquer pessoa que tente abrir o cofre e aceder aos seus ficheiros tem de inserir a palavra-passe.
4. Seleccione **Formatar drive** para formatar a drive virtual atribuida ao cofre. Deve de formatar primeiro a drive antes de adicionar ficheiros 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**.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

Nota
Poderá ser conveniente que guarde todos os cofres de ficheiros no mesmo local. Desta forma poderá localizá-los mais rapidamente.

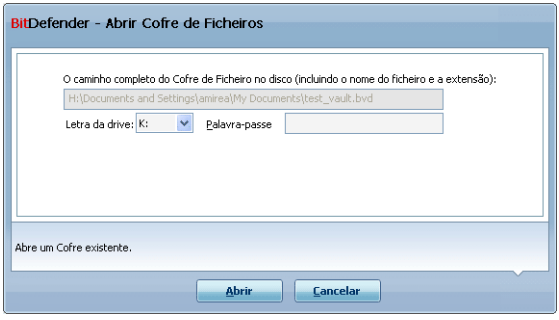
24.2.2. Abrir um Cofre

De forma a poder aceder e trabalhar com os ficheiros 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 ficheiros no seu computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Abrir**.

Uma nova janela irá aparecer.



Abrir Cofre de Ficheiros

Proceder da seguinte forma:

1. Escolha a letra da drive a partir do menu.
2. Insira a palavra-passe do cofre no campo **Palavra-passe** .
3. Clique em **Abrir**.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

24.2.3. Fechar um Cofre

Quando terminou de trabalhar sobre um cofre de ficheiros, deve de o fechar de forma a proteger os seus dados. Ao fechar o cofre, o correspondente disco virtual

desaparecerá de O Meu Computador. Logo, o acesso aos dados armazenados no cofre fica completamente bloqueado.

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 rato no cofre da tabela e seleccione **Fechar**.
- Clique com o botão-direito do rato no correspondente disco virtual em O Meu Computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Fechar**.

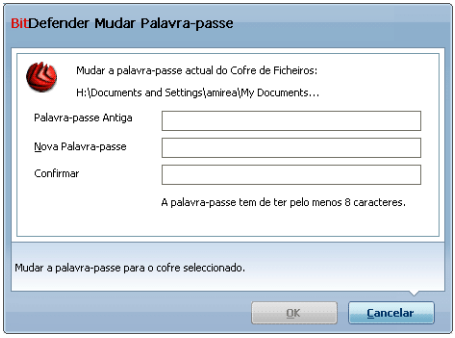
O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

24.2.4. Mudar Palavra-passe do Cofre

O cofre tem de ser fechado antes que possa mudar a sua palavra-passe. Para mudar a palavra-passe do cofre, use um dos seguintes métodos:

- Seleccione o cofre na tabela e clique em **Alterar palavra-passe**.
- Clique com o botão-direito do rato no cofre da tabela e seleccione **Alterar palavra-passe**.
- Clique com o botão-direito do rato no cofre de ficheiros do seu computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Alterar palavra-passe do cofre**.

Uma nova janela irá aparecer.



Alterar Palavra-passe do Cofre

Proceder da seguinte forma:

1. Insira a palavra-passe actual do cofre no campo **Palavra-passe antiga** .

2. Insira a nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe** .

Nota

A palavra-passe tem de ter pelo menos 8 caracteres. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

3. Clique em **OK** para alterar a palavra-passe.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

24.2.5. Adicionar Ficheiros ao Cofre

Para adicionar ficheiros ao cofre, siga os seguintes passos:

1. Seleccione da tabela de cofres o cofre para onde quer adicionar ficheiros.
2. Se o cofre estiver fechado, deve em primeiro lugar abri-lo (clicar botão direiro do rato sobre ele e seleccionar **abrir cofre**).
3. Clique **Adicionar ficheiro**. Uma nova janela irá aparecer.
4. Seleccione os ficheiros / pastas que deseja adicionar ao cofre.
5. Clique em **OK** para copiar os objectos seleccionados para o cofre.

Uma vez que o cofre esteja aberto, pode usar directamente o disco virtual correspondente ao cofre. Siga estes passos:

1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.
2. Insira a drive virtual correspondente ao cofre. Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Copiar-colar ou drag&drop os ficheiros ou pastas directamente para a drive virtual.

24.2.6. Remover Ficheiros do Cofre

Para remover ficheiros do cofre, siga os seguintes passos:

1. Seleccione da tabela de cofres o cofre que contém o ficheiro a ser removido.
2. Se o cofre estiver fechado, deve em primeiro lugar abri-lo (clicar botão direiro do rato sobre ele e seleccionar **abrir cofre**).
3. Seleccione o ficheiro a ser removido a partir da tabela que mostra o conteúdo do cofre.
4. Clique **Remover ficheiros/pastas**.

Se o cofre estiver aberto, pode remover directamente os ficheiros a partir da drive virtual atribuida ao cofre. Siga estes passos:

1. Abra O Meu Computador (clique em 

menu Inciar do Windows, e depois **O Meu Computador**.
2. Insira a drive virtual correspondente ao cofre. Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Remover os ficheiros ou pastas como normalmente faz no Windows (por exemplo, clique botão-direito no ficheiro que quer apagar e seleccione **Apagar**).

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 definição, clique em Actualização >Configuração e limpe a caixa **Não actualizar se o Modo de Jogo estiver ligado**.

- As tarefas de análise 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 letra G sobre o  icone do BitDefender.

Para configurar o Modo de Jogo, clique em **Jogo / Modo Portatil>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

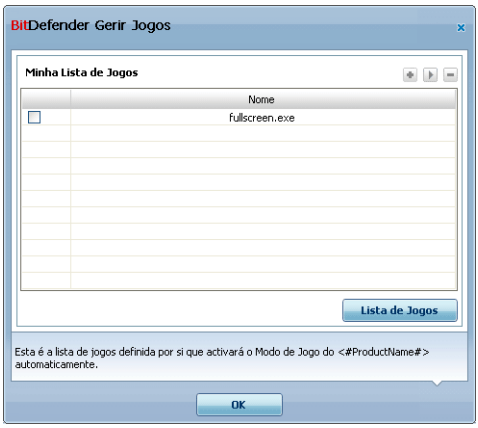
O Modo de Jogo Automático permite que o BitDefender entre automaticamente em Modo de Jogo quando um jogo é detectado. Pode configurar as seguintes opções:

- **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 **Lista de Jogos**.
- **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 gerira a lista de jogos, clique em **Gerir Jogos**. Uma nova janela irá aparecer.



Lista de Jogos

Novas aplicações são adicionadas automaticamente à lista quando:

- Inicia um jogo da lista de jogos conhecidos do BitDefender. Para ver esta lista, clique em **Lista de Jogos**.
- Após siar do modo de ecrã inteiro, pode adicionar a aplicação à lista de jogos a partir da janela de notificação.

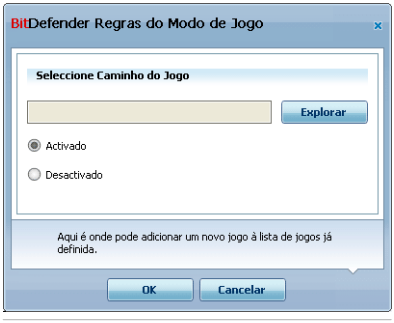
Se deseja descativar o Modo de Jogo Automático para uma determinada aplicação da lista, limpe a correspondente caixa de selecção. Deve de desactivar o Modo de Jogo Automático para as aplicações que regularmente entram em modo de ecrã inteiro, tais como os exploradores da Internet e os leitores de filmes.

Para gerir a lista de jogos, pode usar os botões colocados no topo da tabela:

- **Adicionar** - adiciona uma nova aplicação à lista de jogos.
- **Remover** - remove uma aplicação da lista de jogos.
- **Editar** - edita uma entrada 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:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada se execute enquanto o Modo de Jogo estiver ligado. Pode seleccionar 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.

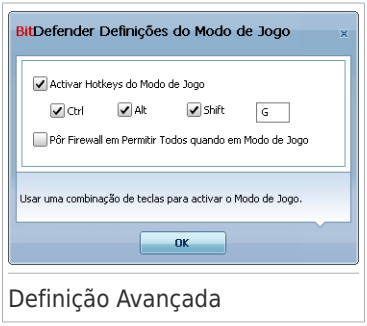
Para desactivar automaticamente a firewall BitDefender enquanto estiver no Modo de Jogo, siga os seguintes passos:

1. Clique em **Configuração Avançada**. Uma nova janela irá aparecer.
2. Seleccione a caixa de selecção **Definir Firewall em Permitir Todas (Modo de Jogo) quando em Modo de Jogo**.
3. Clique em **Aplicar** para guardar 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.



Definição Avançada

2. Por baixo da opção **Usar HotKey** , defina a hotkey desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

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

   Nota
   Remover a selecção ao pé de **Activar HotKey** irá desactivar a hotkey.

3. Clique em **Aplicar** para guardar as alterações.

25.2. Modo Portátil

O Modo de Portátil foi especialmente desenhado para os utilizadores de portáteis. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o portátil 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 de Portátil, clique em **Jogo / Modo Portatal>Modo Portatal** no Modo Avançado.

Modo 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

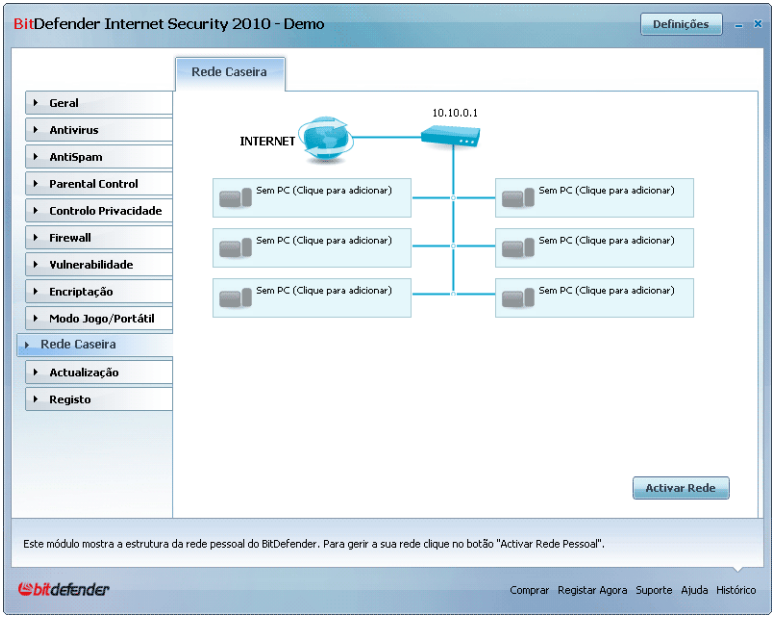
Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada se execute enquanto o Modo de Portátil estiver ligado. Pode seleccionar 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 de Casa

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

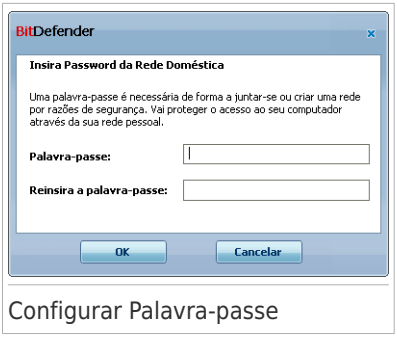
Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

1. Adira à rede pessoal do BitDefender no seu computador. Aderir à rede consiste em configurar uma palavra-passe administrativa para o gestor da rede pessoal.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a palavra-passe).
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 **Activar Rede**. Será notificado para configurar a palavra-passe de gestão de rede pessoal.



Configurar Palavra-passe

2. Insira a mesma palavra-passe em cada um dos campos editáveis.
3. Clique em **OK**.

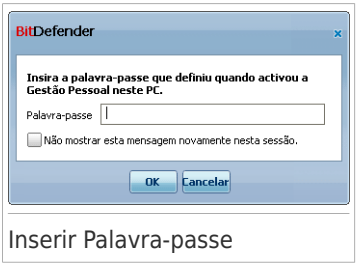
Pode ver o nome do computador a aparecer no mapa de rede.

26.2. Adicionar Computadores à Rede BitDefender

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

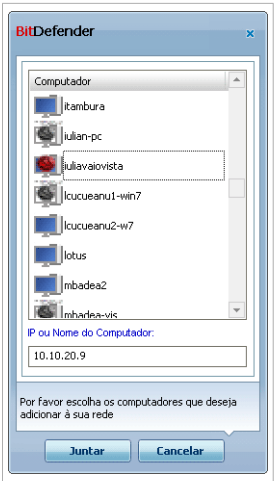
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

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



Inserir Palavra-passe

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

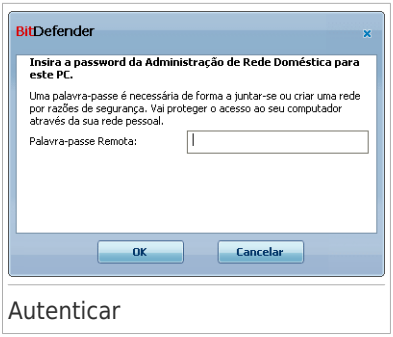


Adicionar Computador

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. Prima **Adicionar**. Será notificado para inserir a sua palavra-passe de gestão de rede pessoal do respectivo computador.



Autenticar

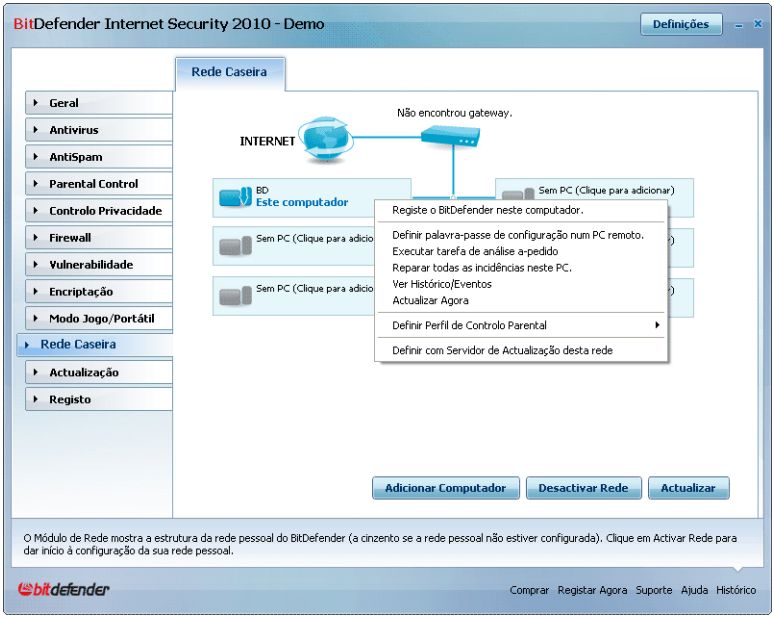
5. Insira a palavra-passe de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**. Se forneceu a palavra-passe correcta, a nome do computador seleccionado aparecerá no mapa de rede.

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 rato sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afectar a segurança do sistema, o estado de registo do BitDefender).

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

- **Remover o PC da rede local de casa**

  Permite-lhe remover um PC da Rede.

- **Registar o BitDefender neste computador**

  Permite-lhe registar o BitDefender neste computador introduzindo a chave de licença.

- **Definir palavra-passe para acesso às definições num computador remoto**

  Permite-lhe criar uma password para restringir o acesso às definições do BitDefender nestes PC.

- **Executar uma tarefa de análise a-pedido**

  Permite-lhe executar uma análise a-pedido remota a partir de outro computador. Pode efectuar uma das seguintes tarefas: Análise Os Meus Documentos, Análise Completa do Sistema e Análise Minunciosa do Sistema.

- **Reparar incidências neste computador**

  Permite-lhe reparar as incidências que estão a afectar a segurança deste computador seguindo o assistente Reparar Todas as Incidências.

- **Histórico**

  Permite-lhe aceder ao módulo **Histórico&Eventos** do produto BitDefender instalado neste computador.

- **Actualizar Agora**

  Inicia o processo de Actualização para o produto BitDefender installado neste computador.

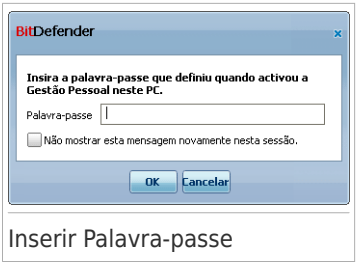
- **Palavra-passe do Controlo Parental**

  Permite-lhe definir as categorias de faixas etárias a serem utilizadas pelo filtro de Web do Controlo Parental: crianças, adolescentes ou adultos.

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

  Permite-lhe definir este computador como servidor de actualizações para todos os produtos BitDefender instalados nos computadores desta rede. A utilização desta opção reduz o trafego de internet, porque apenas um computador vai necessitar de aceder a internet para descarregar as actualizações.

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



Inserir Palavra-passe

Insira a palavra-passe 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 seleccionar esta opção, não será notificado novamente pela palavra-passe durante esta sessão.

27. Actualização

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado com as últimas assinaturas de malware.

Se está ligado à Internet através de banda larga ou ADSL, o BitDefender executa esta operação sozinho. Quando liga o computador o BitDefender verifica se há novas actualizações e depois disso fá-lo a cada **hora** .

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.

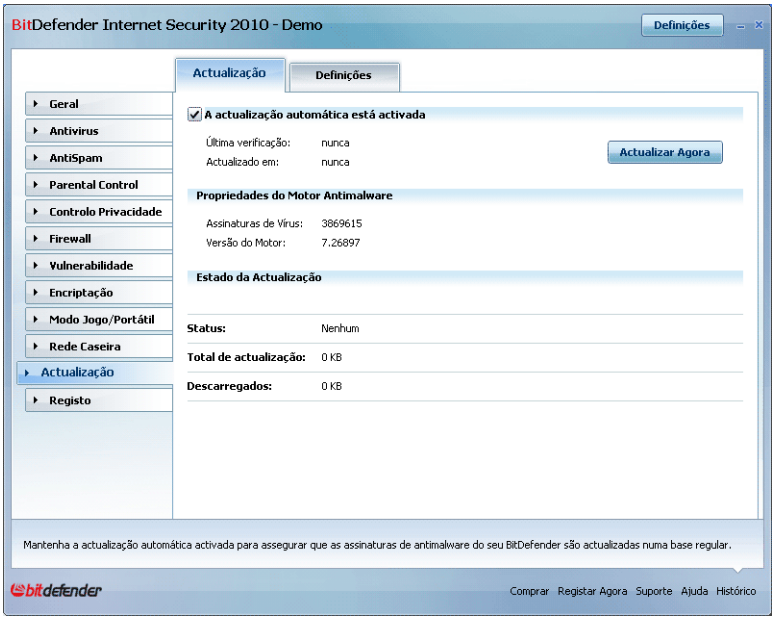
O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituidos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

As actualizações vêm em quatro “sabores”:

- **Actualizações para a engenharia Antivírus** - à medida que vão surgindo novas ameaças, os ficheiros que contêm assinaturas de vírus têm de ser actualizados para assegurar a protecção actualizada permanente contra os vírus. Esta actualização é também conhecida como **Virus Definitions Update**.
- **Actualizações para a engenharia Antispam** - novas regras serão adicionadas ao Filtro Heurístico e ao Filtro URL e filters novas assinaturas de imagens serão adicionadas ao Filtro de Imagem. Isto irá a judar a melhorar a eficiência da sua engenharia Antispam. Esta actualização é também conhecida como **Antispam Update**.
- **Actualizações para o motor de Antispyware** - novas assinaturas de spyware serão adicionadas à base de dados. Esta actualização é também conhecida como **Antispyware Update**.
- **Actualizações do produto** - quando é lançada uma nova versão do produto, são introduzidas novas configurações e técnicas de verificação, com o objectivo de melhorar o desempenho do produto. Esta actualização é também conhecida como **Product Update**.

27.1. Actualização Automática

Para ver informação relacionada com actualizações e executar actualizações automáticas, clique em **Actualização>Actualização** no Modo Avançado.



Actualização 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 ficheiro 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 actualização automática pode também ser feita a qualquer altura que deseje premindo o botão **Actualizar Agora**. Esta actualização é também conhecida como **actualização a pedido do utilizador**.

O módulo de **Actualização** estabelece ligação ao servidor de actualizações do BitDefender e verificará se há actualizações disponíveis. Se detectar uma actualização, dependendo das opções definidas na secção Opções da Actualização Manual, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

Importante
Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça o quanto antes.

Nota
Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.

27.1.2. Desactivar Actualização Automática

Se deseja desactivar a actualização automática, uma janela de aviso aparecerá. 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. Configuração da actualização

As actualizações podem ser executadas através da rede local, da Internet, directamente ou através de 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>Definições** no Modo Avançado.

Configuração da 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. Configuração da Localização da Actualização

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 actualizações mais rápidas e fiáveis, pode configurar dois locais de actualização: um **Local primário de actualização** e um **Local alternativo de actualização**. 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 defini 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. 275)

27.2.2. Configurar Actualização 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 consecutivas de actualizações no campo **Intervalo de 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:

- **Actualização silenciosa** - O BitDefender faz automaticamente o download e a implementação da actualização.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar actualizações** - cada vez que uma actualização for descarregada, será consultado antes da sua instalação ser feita.

27.2.3. Configurar Actualização Manual

Para definir como a actualização manual (actualização a pedido do utilizador) deve ser executada, seleccione uma das seguintes opções na categoria **Configuração Actualização Manual**:

- **Actualização silenciosa** - a actualização manual será feita em segundo plano automaticamente.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.

27.2.4. Configuração Avançada

Para evitar que o processo de actualização do BitDefender interfira com o seu trabalho, configure as opções na categoria **Configuração Avançada**:

- **Esperar pelo reiniciar, em vez se o solicitar** - Se uma actualização requer um reiniciar, o produto continuará a funcionar com os antigos ficheiros até que o sistema reinicie. Ao utilizador não lhe será solicitado que o reinicie, logo o processo de actualização do BitDefender não interferirá com o trabalho do utilizador.

- **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 interrompido.

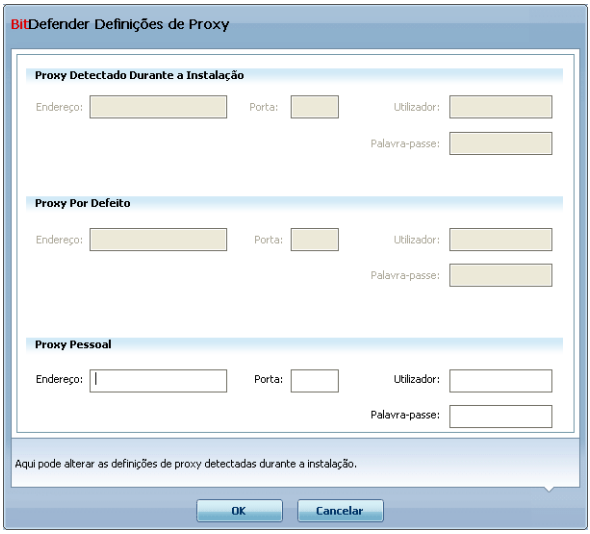
- **Não actualizar se o modo de jogo estiver ligado** - O BitDefender não actualizará se o Modo de Jogo estiver ligado. Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.

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 actualize sozinho. De outra forma, usará as definições do administrador que instalou o produto ou o utilizador actual por defeito do browser, caso haja algum.

Nota
As definições do proxy só podem ser configuradas por utilizadores com direitos administrativos no computador ou por power users (utilizadores que sabem a palavra-passe da configuração do produto).

Para gerir as definições de proxy, clique em **Gerir Proxies**. Aparecerá uma nova janela.



Gestor Proxy

Existem três categorias de definições de proxy:

- **Proxy detectado 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 utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.
- **Browser por Defeito do Proxy** - as definições do proxy do actual utilizador, extraídas do browser por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deve de os inserir 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 actual utilizador.

- **Personalizar 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.
  - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.

- **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.

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 utilizador actual 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 guardar as alterações, ou clique em **Defeito** para retornar às definições por defeito.

28. Registo

Para saber toda a informação sobre o seu produto BitDefender e o estado do registo, clique em**Registo** no Modo Avançado.

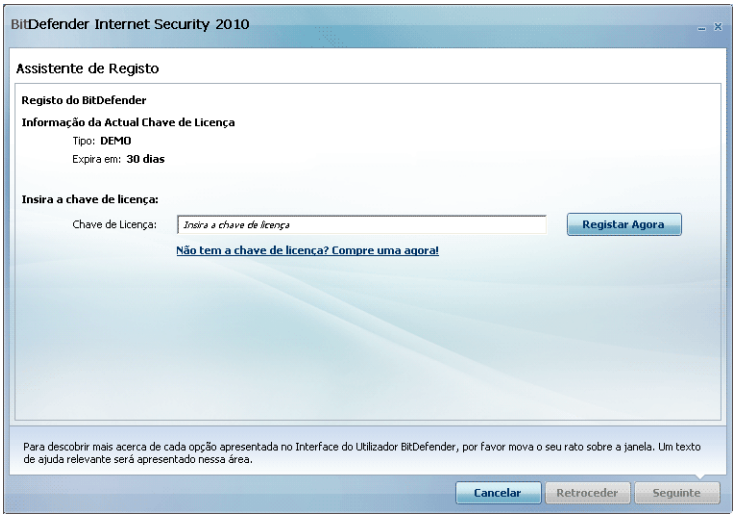
Registo

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 BitDefender Internet Security 2010

Clique em **Registar agora** para abrir a janela de registo do produto.



Registo

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

Para registar BitDefender Internet Security 2010:

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

Nota

Pode encontrar a sua chave de licença:

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

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

2. Clique em **Registar Agora**.
3. Clique em **Terminar**.

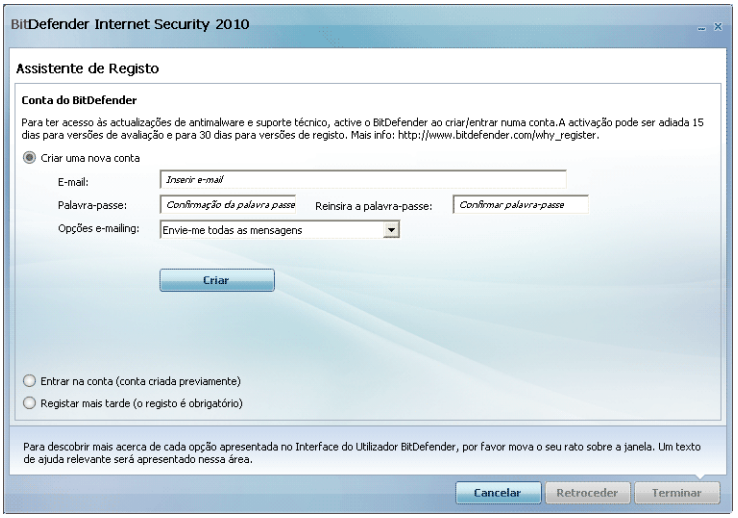
28.2. Criar uma conta BitDefender

Como parte do processo de registo, TEM de criar uma conta BitDefender. A conta BitDefender dá-lhe acesso às actualizações BitDefender, suporte técnico gratuito e a ofertas promocionais especiais. Se perder a sua chave de licença BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Importante

Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias). De outra forma, o BitDefender deixa de ser actualizado.

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. 280)
- “Já tenho uma conta BitDefender” (p. 281)

Não tenho uma conta BitDefender

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

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

- **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender. A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.
- **Re-insira a palavra-passe** - insira novamente a palavra-passe previamente definida.

Nota

Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Seleccione uma das opções disponíveis no menú:
   - **Enviem-me todas as mensagens**
   - **Enviem-me apenas mensagens relativas ao produto**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Criar**.
5. Clique em **Terminar** para completar o assistente.
6. **Active a sua conta.** Antes de usar a sua conta, tem de a activar. Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Nesse caso, forneça a palavra-passe da sua conta e clique em **Sign in**. Clique em **Terminar** para completar o assistente.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (conta previamente criada)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota

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

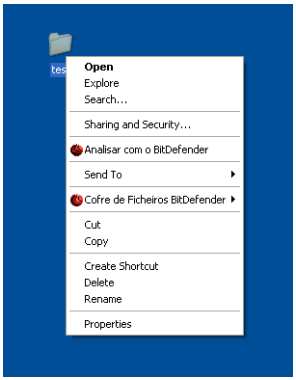
3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Seleccione uma das opções disponíveis no menú:
   - **Enviem-me todas as mensagens**
   - **Enviem-me apenas mensagens relativas ao produto**
   - **Não me enviem quaisquer mensagens**

4. Clique em **Sign in**.
5. Clique em **Terminar** para completar o assistente.

Integração com o Windows e outros programas

29. Integração no Menu Contextual do Windows

O menu contextual do Windows aparece sempre que clica com o botão direito do rato sobre um ficheiro ou pasta do seu computador ou sobre um objecto do seu ambiente de trabalho.



Menu Contextual do Windows

O BitDefender integra-se no menu contextual do Windows para o ajudar a analisar facilmente ficheiros e prevenir que outros utilizadores acedam aos seus ficheiros mais importantes. Pode facilmente localizar as opções BitDefender no menu contextual ao procurar pelo icone BitDefender.

- Analisar com o BitDefender
- Cofre de Ficheiros BitDefender

29.1. Analisar com BitDefender

Pode facilmente analisar ficheiros, pastas e mesmo drives de disco inteiras usando o menu contextual do Windows. Clique com o botão direito do rato sobre o objecto que pretende analisar e seleccione no menu **Analisar com o BitDefender**. O Assistente de Análise BitDefender irá surgir e guiá-lo através do processo de análise.

Opções de Análise. As opções de análise estão pré-configuradas para obter os melhores resultados de detecção. Se forem detectados ficheiros infectados, o BitDefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados.

Se deseja alterar as opções da análise, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.

2. Clique em **Antivirus** do lado esquerdo do menu.
3. Clique na barra **Analisar**
4. Clique botão-direito do rato na tarefa **Analisar** e seleccione **Abrir**. Uma nova janela irá aparecer.
5. Clique em **Personalizar** e configure as opções de análise como desejar. Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
6. Clique em **Aplicar** para guardar as alterações.
7. Clique **OK** para confirmar e aplicar as novas opções da análise.

Importante

Não deve de alterar as opções de análise deste método de análise a não ser que tenha uma razão bastante forte para o fazer.

29.2. Cofre de Ficheiros BitDefender

O Cofre de Ficheiros BitDefender ajuda-o a armazenar em segurança os seus documentos confidenciais através do uso de cofres de ficheiros.

- O cofre de ficheiros é um espaço de armazenamento seguro de informação pessoal ou de ficheiros considerados sensíveis.
- O cofre de ficheiros é um ficheiro 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 ficheiro 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 ficheiros. Será capaz de fazer operações com ficheiros nele (copiar, apagar, alterar, etc.). Os ficheiros estão protegidos na medida em que estejam residentes nesta drive (porque é necessária uma palavra-passe para a operação de montagem).

  Quando terminar, fechar (desmontar) o seu cofre de forma a iniciar a protecção do seu conteúdo.

Pode facilmente identificar os cofres de ficheiros BitDefender no seu computador pelo icone BitDefender e pela extensão `.bvd`.

Nota

Esta secção mostra-lhe como criar e e gerir os cofres de ficheiros BitDefender usando as opções fornecidas no menu contextual do Windows. Pode sempre criar e gerir os cofres de ficheiros a partir do interface do BitDefender.

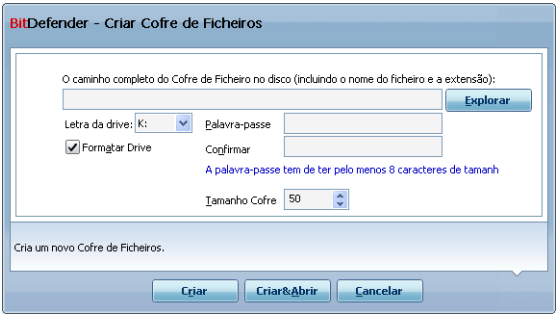
- No Modo Intermédio, vá ao separador Gerir Ficheiros e use as opções a partir da área de **Tarefas**. Um assistente ajudá-lo-á a completar cada uma das tarefas.
- Para uma aproximação mais directa, mude para Modo Avançado e clique em **Encriptação** no menu do lado esquerdo. Na barra de Cofre de Ficheiros, pode ver e gerir os cofres de ficheiros existentes e o seu conteúdo.

29.2.1. Criar Cofre

Mantenha em mente que um cofre é na realidade apenas um ficheiro com a extensão `.bvd`. Só quando abre o ficheiro, é que uma drive de disco virtual aparece em O Meu Computador e pode, de forma segura, armazenar ficheiros no seu interior. Quando cria um cofre, deve de especificar onde e sobre que nome o deve de guardar no seu computador. Deve também de especificar uma palavra-passe para proteger o seu conteúdo. Apenas os utilizadores que sabem a palavra-passe podem abrir o cofre e aceder aos documentos e dados armazenados no seu interior.

Para criar um cofre, siga estes passos:

1. Clique no botão direito do rato no seu Ambiente de Trabalho ou numa pasta do seu computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Criar**. A seguinte análise irá aparecer:



Criar Cofre de Ficheiros

2. Especificar a localização e o nome do cofre de ficheiros.
   - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
   - Apenas insira o nome do cofre no campo correspondente para criá-lo em Os Meus Documentos. Para abrir Os Meus Documentos, clique em start menu Inciar do Windows, e depois **Os Meus Documentos**.
   - Insira o caminho completo do cofre de ficheiros no disco. Por exemplo, `C:\meu_cofre.bvd`.

3. 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.
4. Insira a nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe**. Qualquer pessoa que tente abrir o cofre e aceder aos seus ficheiros tem de inserir a palavra-passe.
5. Seleccione **Formatar drive** para formatar a drive virtual atribuida ao cofre. Deve de formatar primeiro a drive antes de adicionar ficheiros ao cofre.
6. Se deseja mudar o tamanho por defeito (50 MB) do cofre, insira o valor desejado no campo **Tamanho Cofre** .
7. 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**.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

Nota

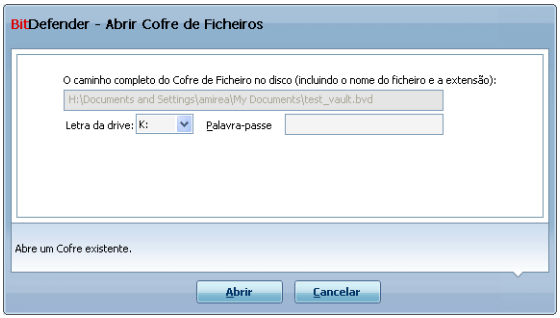
Poderá ser conveniente que guarde todos os cofres de ficheiros no mesmo local. Desta forma poderá localizá-los mais rapidamente.

29.2.2. Abrir Cofre

De forma a poder aceder e trabalhar com os ficheiros 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 um cofre, siga estes passos:

1. Localize no seu computador o ficheiro `.bvd` que representa o cofre que deseja abrir.
2. Clique com o botão-direito no ficheiro, aponte para **Cofre Ficheiros BitDefender** e seleccione **Abrir**. Uma alternativa mais rápida seria fazer duplo clique sobre o ficheiro, ou clicar com o botão-direito do rato sobre ele e seleccionar **Abrir**. A seguinte análise irá aparecer:



Abrir Cofre de Ficheiros

3. Escolha a letra da drive a partir do menu.
4. Insira a palavra-passe do cofre no campo **Palavra-passe** .
5. Clique em **Abrir**.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

29.2.3. Fechar Cofre

Quando terminou de trabalhar sobre um cofre de ficheiros, deve de o fechar de forma a proteger os seus dados. Ao fechar o cofre, o correspondente disco virtual desaparecerá de O Meu Computador. Logo, o acesso aos dados armazenados no cofre fica completamente bloqueado.

Para fechar um cofre, siga estes passos:

1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.
2. Identifique a drive de disco virtual correspondente ao cofre que deseja fechar. Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Clique com o botão-direito do rato no correspondente disco virtual em O Meu Computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Fechar**.

Também pode clicar com o botão direito do rato `.bvd` no ficheiro que representa o cofre, apontar para **Cofre de Ficheiros BitDefender** e clicar em **Fechar**.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

Nota

Se diveros cofres estiverem abertos, deve de usar o interface BitDefender em Modo Avançado. Se for à barra **Encriptação**, Cofre de Ficheiro, poderá visualizar uma tabela que lhe dá informação sobre os cofres existentes. Esta informação inclui sobre se o cofre está aberto e, se sim, qual a letra da drive que lhe está atribuida.

29.2.4. Adicionar ao Cofre de Ficheiros

Antes que possa adicionar ficheiros ou pastas ao cofre, deve de abri-lo. Uma vez que um cofre esteja aberto, pode facilmente armazenar ficheiros ou pastas no seu interior usando o menu contextual. Clique com o botão-direito no ficheiro ou pasta que deseja copiar para o cofre, aponte para **Cofre Ficheiros BitDefender** e seleccione **Adicionar ao Cofre de Ficheiros**.

- Se apenas um cofre estiver aberto, o ficheiro ou pasta é copiado directamente para esse cofre.
- Se vários cofres estiverem abertos, ser-lhe-á solicitado que escolha o cofre para onde deseja copiar o item. Seleccione do menu a letra da drive correspondente ao cofre desejado e clique **OK** para o copiar.

Pode sempre usar a drive virtual correspondente ao cofre. Siga estes passos:

1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.
2. Insira a drive virtual correspondente ao cofre. Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Copiar-colar ou drag&drop os ficheiros ou pastas directamente para a drive virtual.

29.2.5. Remover do Cofre de Ficheiros

De forma a remover os ficheiros ou pastas do cofre, o cofre deve de ser aberto. Para remover os ficheiros ou pastas do cofre, siga os seguintes passos:

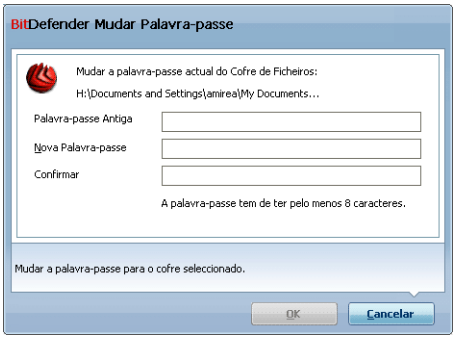
1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.
2. Insira a drive virtual correspondente ao cofre. Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Remover os ficheiros ou pastas como normalmente faz no Windows (por exemplo, clique botão-direito no ficheiro que quer apagar e seleccione **Apagar**).

29.2.6. Alterar Palavra-passe do Cofre

A palavra-passe protege o conteúdo do cofre contra acessos não-autorizados. Apenas os utilizadores que sabem a palavra-passe podem abrir o cofre e aceder aos documentos e dados armazenados no seu interior.

O cofre tem de ser fechado antes que possa mudar a sua palavra-passe. Para mudar a palavra-passe do cofre, siga os seguintes passos:

1. Localize no seu computador o ficheiro `.bvd` que representa o cofre.
2. Clique com o botão-direito do rato no ficheiro, aponte para **Cofre Ficheiros BitDefender** e seleccione **Alterar palavra-passe do cofre**. A seguinte análise irá aparecer:



Alterar Palavra-passe do Cofre

3. Insira a palavra-passe actual do cofre no campo **Palavra-passe antiga** .
4. Insira a nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe** .

> **Nota**
>
> A palavra-passe tem de ter pelo menos 8 caracteres. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

5. Clique em **OK** para alterar a palavra-passe.

O BitDefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo. Clique **OK** para fechar a janela.

30. 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 ícone do BitDefender , encontra-se 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, no presente explorador de internet.
- **Configuração** - abre uma janela onde pode especificar as definições da barra de ferramentas do antiphishing. Estão disponíveis as seguintes opções:
  - **Protecção Antiphishing Wen em Tempo-real** - detecta e alerta-o em tempo-real se um site web é de phishing (preparado para lhe roubar informação pessoal). Esta opção controla a protecção antiphishing BitDefender apenas no actual explorador da internet.
  - **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.

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

Lista Branca do AntiPhishing

Pode ver toda a lista dos sites web que não estão a ser analisados pelos motores de antiphishing do BitDefender. Se deseja remover um site da Lista Branca de

forma a que seja notificado acerca de qualquer possibilidade de ameaça de phishing existente nesse site, clique no botão **Remover** ao pé do mesmo.

Pode adicionar sites à Lista Branca nos quais confia absolutamente, de forma a que eles não sejam mais analisados pelos motores antiphishing. Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

- **Relatar como Phishing** - informa o Laboratório BitDefender que você considera determinado site web como sendo usado para phishing. Ao reportat sites de phishing você ajuda a proteger outros contra o roubo de identidade.
- **Ajuda** - abre a documentação electrónica.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

31. Integração com os programas de Mensagens Instântaneas

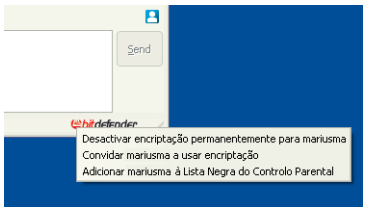
BitDefender offers encryption capabilities to protect your confidential documents and your instant messaging conversations through Yahoo Messenger and MSN Messenger.

By default, BitDefender encrypts all your instant messaging chat sessions provided that:

- Your chat partner has a BitDefender version installed that supports IM Encryption and IM Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use either Yahoo Messenger or Windows Live (MSN) Messenger.

Importante
BitDefender não irá encriptar uma conversação se o parceiro de chart usar uma aplicação de chat web-based, tal como a Meebo, ou outra aplicação de chat que suporta o Yahoo Messenger ou o MSN.

You can easily configure instant messaging encryption using the BitDefender toolbar from the chat window. A toolbar deve de estar no canto inferior direito da janela de chat. Procure aí o logo do BitDefender.



Toolbar BitDefender

Nota
A toolbar indica que a conversação é encriptada ao mostrar um pequena chave ao pé do logo do BitDefender.

Ao clicar na toolbar do BitDefender são-lhe apresentadas as seguintes opções:

- **Desactivar permanentemente a encriptação para o contacto.**
- **Convidar contacto a usar a encriptação.** Para encriptar as suas conversações, o seu contacto deve de instalar o BitDefender e usar um programa de MI compatível.
- **Adicionar contacto à lista negra do Controlo Parental.** Se adicionar um contacto à lista negra do Controlo Parental e o mesmo estiver ligado, não terá mais acesso às mensagens instântaneas enviadas por esse contacto. Para remover o contacto da lista negra, clique na barra de ferramentas e seleccione **Remover contacto da lista negra do Controlo Parental**.

32. Integração com Clientes de Mail

O BitDefender Internet Security 2010 inclui um módulo Antispam. O Antispam verifica as mensagens de e-mail que recebe e identifica aquelas que são spam. As mensagens de spam detectadas pelo BitDefender são marcadas como [SPAM] no campo do assunto.

Nota
A protecção Antispam é fornecida para todos os clientes de e-mail POP3/SMTP.

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

O BitDefender move automaticamente as mensagens de spam para uma determinada pasta, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**. A pasta **Spam** é criada durante a instalação do BitDefender.
- No Outlook Express e no Windows Mail, as mensagens de spam são movidas directamente para os **Itens Eliminados**.
- No Mozilla Thunderbird, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Lixo**. A pasta **Spam** é criada durante a instalação do BitDefender.

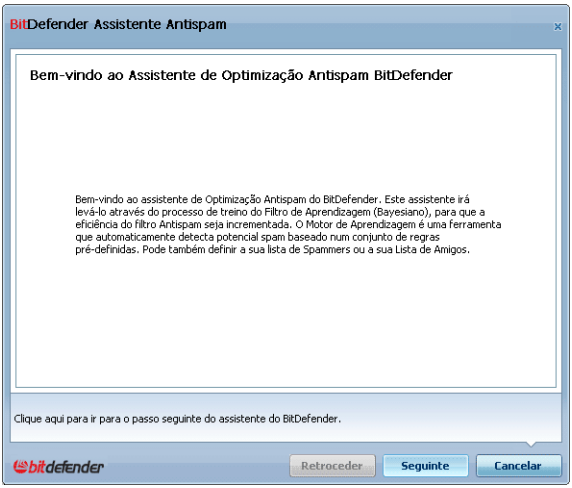
Se usa outros cliente de e-mail, tem de criar uma regra para mover os e-mails marcados como [SPAM] pelo BitDefender para uma pasta de quarentena personalizada.

32.1. Assistente de Configuração Antispam

A primeira vez que executar o seu cliente de e-mail, um assistente irá aparecer para o ajudar a configurar a Lista de Amigos e a Lista de Spammers e a treinar o Filtro Bayesiano, para aumentar a eficiência dos filtros Antispam.

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

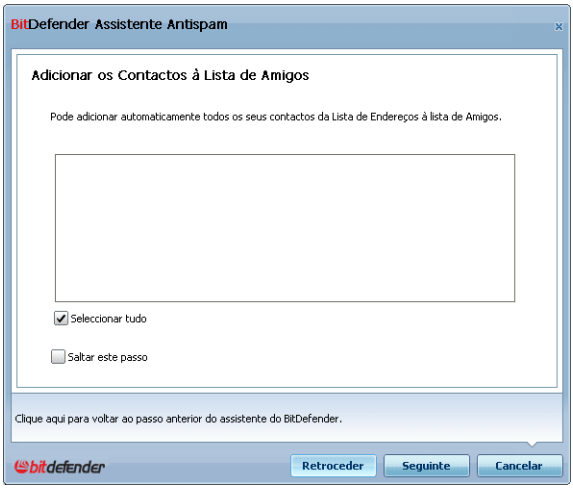
32.1.1. Passo 1/6 - Janela de Boas-vindas



Janela de boas-vindas

Clique **Seguinte**.

32.1.2. Passo 2/6 - Preencher a Lista de Amigos



Preencher a Lista de Amigos

Aqui pode ver todos os endereços do seu **Livro de Endereços**. Por favor seleccione os que pretende adicionar à sua **Lista de Amigos** (recomendamos que seleccione todos). Irá receber todas as mensagens de e-mail desses endereços, independentemente do seu conteúdo.

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

Se quiser passar este passo de configuração, seleccione **Saltar este passo**. Clique em **Seguinte** para continuar.

32.1.3. Passo 3/6 - Apagar a Base de Dados Bayesiana

Apagar a Base de Dados Bayesiana

Poderá achar que o filtro de Antispam começou a perder eficiência. Isto pode estar relacionado com o treino impróprio (por ex. por erro, marcou um número de mensagens legítimas como Indesejadas, ou vice versa). Se o seu filtro for pouco impreciso, poderá necessitar de limpar a base de dados e voltar a treinar o filtro ao seguir os passos do assistente.

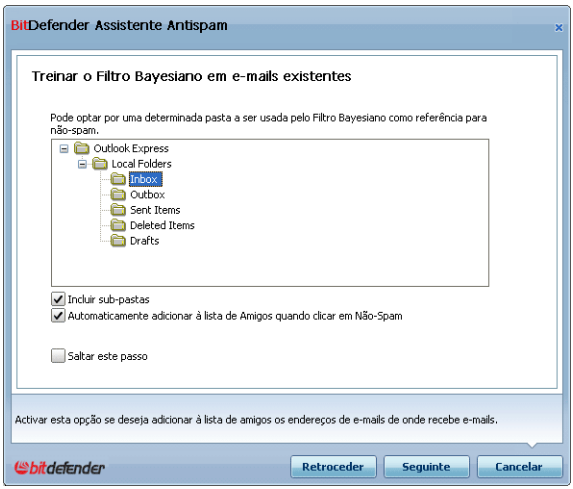
Seleccione **Limpar dados do filtro Antispam** se pretende efectuar uma nova composição da base de dados do filtro Bayesian.

Pode guardar a base de dados Bayesiana num ficheiro para que o possa utilizar com outros produtos BitDefender ou após reinstalar o BitDefender. Para guardar a base de dados Bayesiana, clique no botão **Guardar Bayes** e guarde no local desejado. o ficheiro terá a extensão `.dat`.

Para carregar uma base de dados Bayesiana anterior, clique no botão **Carregar Bayes** e abra o ficheiro correspondente.

Se quiser passar este passo de configuração, seleccione **Saltar este passo**. Clique em **Seguinte** para continuar.

32.1.4. Passo 4/6 - Treinar o filtro Bayesiano com E-mails Legítimos



Treinar o filtro Bayesiano com E-mails Legítimos

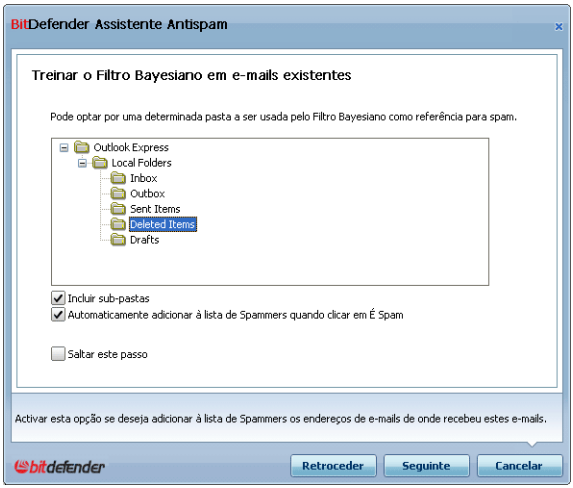
Por favor seleccione a pasta que contém mensagens de e-mail legítimas. Estas mensagens serão usadas para treinar o filtro Bayesian.

existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir sub-pastas** - para adicionar as sub-pastas à sua selecção.
- **Adicionar automaticamente à lista de Amigos** - para adicionar os remetentes à lista de Amigos.

Se quiser passar este passo de configuração, seleccione **Saltar este passo**. Clique em **Seguinte** para continuar.

32.1.5. Passo 5/6 - Treinar o filtro Bayesiano com Spam



Treinar o filtro Bayesiano com Spam

Por favor seleccione a pasta que contém mensagens de e-mail indesejadas. Estas mensagens serão usadas para treinar o filtro Bayesian.

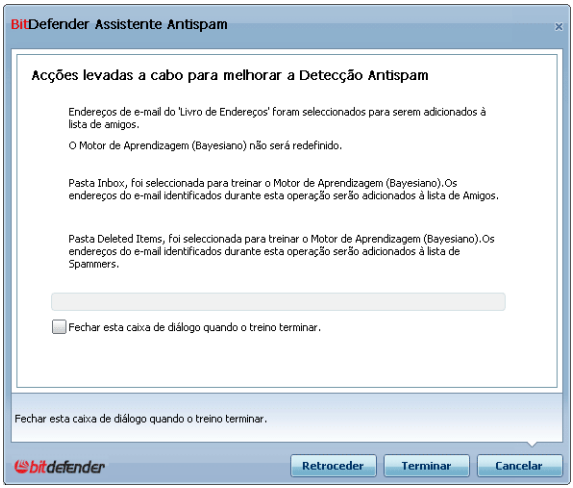
Importante
Por favor certifique-se que a pasta que escolher não contém, de modo, algum, me-mails legítimos; de outro modo, o desempenho do Antispam será consideravelmente reduzido.

existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir sub-pastas** - para adicionar as sub-pastas à sua selecção.
- **Adicionar automaticamente à lista de Spammers** - para adicionar os remetentes à lista de Spammers. As mensagens de E-mail destes remetentes irão aparecer sempre marcados como SPAM e serão processadas como tal.

Se quiser passar este passo de configuração, seleccione **Saltar este passo**. Clique em **Seguinte** para continuar.

32.1.6. Passo 6/6 - Sumário



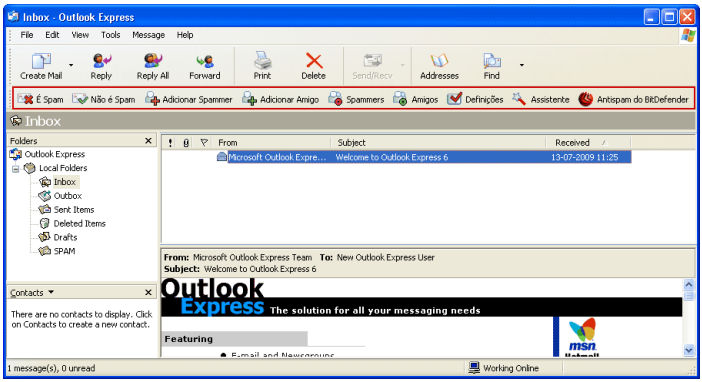
Sumário

Nesta janela pode visualizar todas as definições do assistente de configuração, podendo efectuar alterações, ao retornar aos passos anteriores (clique em **Atrás**).

Se não deseja fazer quaisquer modificações, prima **Terminar** para finalizar o wizard.

32.2. Barra de Ferramentas do Antispam

No lado superior da janela do seu cliente de mail pode ver a barra de ferramentas do Antispam. A barra de ferramentas do Antispam ajuda-o a gerir a protecção antispam directamente do seu cliente de e-mail. Pode facilmente corrigir o BitDefender se ele marcar uma mensagem legítima como SPAM.



Barra de Ferramentas do Antispam

Cada botão é 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**.

  Futuras mensagens que se enquadem nas mesmas patentes serão marcadas como INDESEJADAS.

  Nota
  Pode seleccionar uma mensagem de e-mail ou quantas pretender.

- **Não é Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado não é spam, e que o BitDefender não o deve marcar como tal. Este e-mail será movido da pasta **Spam** para o directório **Caixa de Entrada**.

  Futuras mensagens que se enquadem nas mesmas patentes já não serão marcadas como INDESEJADAS.

  Nota
  Pode seleccionar uma mensagem de e-mail ou quantas pretender.

  Importante
  O botão **Não é Spam** fica activo quando seleccionar uma mensagem marcada como SPAM pelo BitDefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

- **Adicionar Spammer** - adiciona o remetente da mensagem de e-mail à lista de Spammers.

Adicionar Spammer

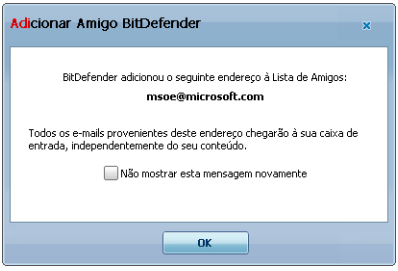
Seleccione **Não mostrar esta mensagem novamente** se não pretender que lhe seja sugerida confirmação, quando adiciona à lista um endereço indesejado.

Clique **OK** para fechar a janela.

As futuras mensagens de e-mail provenientes desses endereços serão marcadas como INDESEJADAS.

Nota
Pode seleccionar um emissor ou quantos pretender.

- **Adicionar Amigo** - adiciona o remetente da mensagem de e-mail à lista de Amigos.



Adicionar Amigo

Seleccione **Não mostrar esta mensagem novamente** se não pretender que lhe seja sugerida confirmação, quando adiciona à lista um endereço amigo.

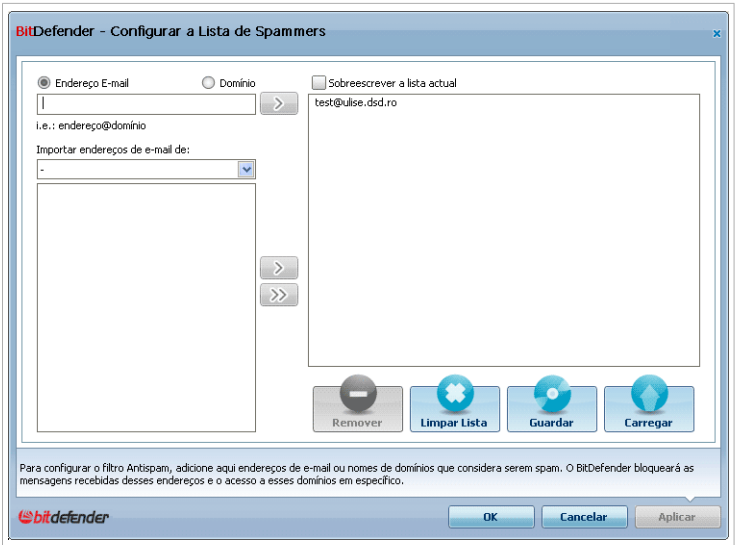
Clique **OK** para fechar a janela.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Nota
Pode seleccionar um emissor ou quantos pretender.

- **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
Todo o mail proveniente de um endereço presente na **Lista de indesejados**, será marcado automaticamente com indesejado, sem mais demora.



Lista de Spammers

Aqui pode adicionar ou remover entradas da **Lista de indesejados**.

Se pretender adicionar um endereço de e-mail seleccione a opção **E-mail**, introduza-o e clique no botão . Os endereços irão aparecer na **Lista de Spammers**.

Importante
Sintaxe: nome@dominio.com.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique em . O domínio irá aparecer na **Lista de Spammers**.

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com serão marcados como INDESEJADOS;
- *dominio* - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- *com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

Atenção

Não adicione domínios de serviços web-mail (tais como o Yahoo, Gmail, Hotmail ou outro) à lista de Spammers. Caso contrário, as mensagens de email recebidas de algum utilizador registado nesses serviços será detectado como spam. Se, por exemplo, adicionar `yahoo.com` à lista de Spammer, todos as mensagens de e-mais recebidas do endereço `yahoo.com`, serão marcadas 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** aparecerá uma nova janela de onde poderá seleccionar a pasta que contém os endereços de e-mail que deseja adicionar à **Lista de spammers**. Escolha-os e clique em **Seleccionar**.

Em ambos os casos, os endereços de e-mail aparecerão na lista de importação. Seleccione os que deseja e clique em para os adicionar à **Lista de Spammers**. Se clicar em todos os endereços de e-mail serão adicionados à lista.

Para remover um ítem da lista, seleccione-o e clique em **Remover**. Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois **Sim** para confirmar a sua escolha.

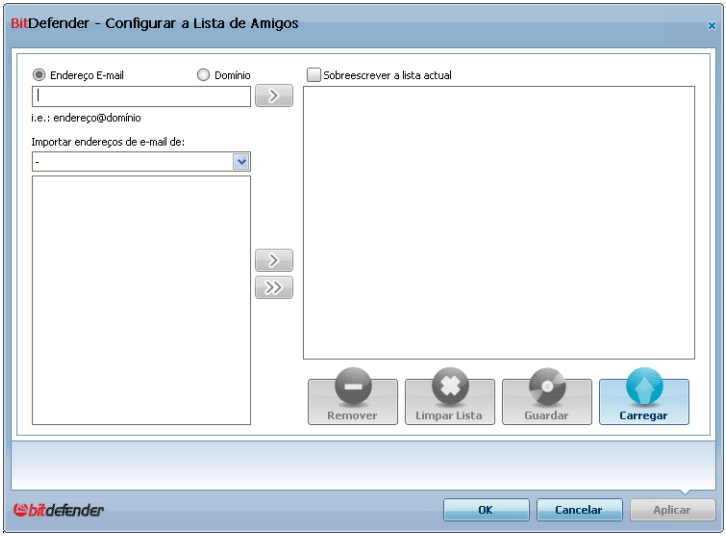
Pode guardar a lista de Spam num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto. Para guarda a lista de Spam, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão `.bwl`

Para carregar uma lista de spammers previamente guardada, clique no botão **Carregar** e abra o ficheiro `.bwl` correspondente. Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique **Aplicar** e **OK** para guardar e fechar a **Lista de indesejados**.

- **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 mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada, sem mais demora.



Lista de Amigos

Aqui pode adicionar ou remover entrdas 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
Sintaxe: nome@dominio.com.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique em . O domínio irá aparecer na **Lista de amigos**.

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *dominio* - todos os mails provenientes de dominio (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;

- *com - todos os mails que têm este sufixo de domínio com chegarão à sua **Caixa de Entrada** independentemente do 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** aparecerá uma nova janela onde poderá seleccionar a pasta que contém os endereços de e-mail que deseja adicionar à **Lista de Amigos**. Escolha-os e clique em **Seleccionar**.

Em ambos os casos, os endereços de e-mail aparecerão na lista de importação. Seleccione os desejados e clique em para os adicionar à **Lista de Amigos**. Se clicar em todos os endereços de e-mail serão adicionados à lista.

Para remover um ítem da lista, seleccione-o e clique em **Remover**. Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois **Sim** para confirmar a sua escolha.

Pode guardar a lista de Amigos num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto. Para guarda a lista de Amigos, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão `.bwl`

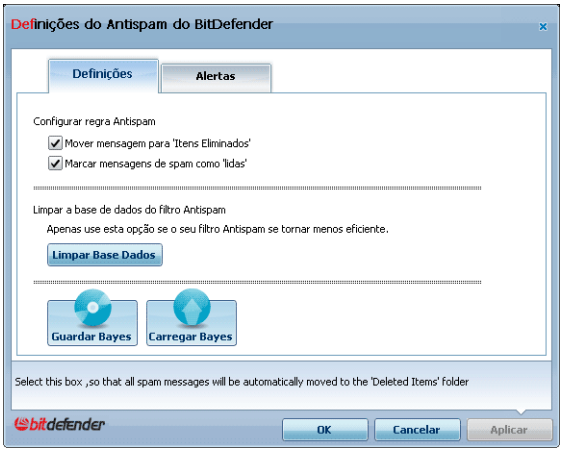
Para carregar uma lista de Amigos previamente guardada, clique no botão **Carregar** e abra o ficheiro `.bwl` correspondente. Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota

Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

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

- **Configuração** - abre a janela das **Configurações** onde pode definir algumas opções para o módulo **Antispam**.



Definições

Estão disponíveis as seguintes opções:

- **Mover mensagens para Itens eliminados** - para mover as mensagens de spam para os **Itens eliminados** (apenas para o Microsoft Outlook Express / Windows Mail);
- **Marcar mensagem como 'Lida'** - para marcar todas as mensagens Indesejadas como lidas, para que, quando chegarem novas mensagens Indesejadas não seja perturbado.

Se o seu filtro Antispam for muito impreciso, pode necessitar de limpar a base de dados do filtro e voltar a treinar o Filtro Bayesian. Clique em **Limpar dados do filtro Antispam** se pretende fazer nova composição da base de dados do filtro Bayesian.

Pode guardar a base de dados Bayesiana num ficheiro para que o possa utilizar com outros produtos BitDefender ou após reinstalar o BitDefender. Para guardar a base de dados Bayesiana, clique no botão **Guardar Bayes** e guarde no local desejado. o ficheiro terá a extensão `.dat`.

Para carregar uma base de dados Bayesiana anterior, clique no botão **Carregar Bayes** e abra o ficheiro correspondente.

Clique na barra **Alertas** se deseja aceder à secção onde poderá desactivar a aparição da janela de confirmação para os botões **Adicionar Spammer** e **Adicionar 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 assistente de configuração antispam, que o ajudará a treinar o filtro Bayesiano de forma a aumentar a eficiência da filtragem Antispam BitDefender. Também pode adicionar endereços do seu Livro de Endereços à sua Lista de Amigos / Lista de Spammers.
- **Antispam BitDefender** - abre o interface do utilizador BitDefender.

Como

33. Como analisar Ficheiros e Pastas

A análise é simples e flexível com o BitDefender. Existem 4 formas de definir o BitDefender para analisar ficheiros e pastas em busca de vírus e outro malware:

- Usar o Menu Contextual do Windows
- Usar Tarefas de Análise
- Usar Análise Manual BitDefender
- Usar Barra de Actividade da Análise

Uma vez que inicie uma análise, o assistente de Análise de Antivírus irá aparecer e guiá-lo através do processo de análise. Para mais informação sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 56).

33.1. Usar o Menu Contextual do Windows

Esta é a forma mais fácil e recomendada para analisar um ficheiro ou pasta no seu computador. Clique com o botão direito do rato sobre o objecto que pretende analisar e seleccione no menu **Analisar com o BitDefender**. Siga o assistente de Análise Antivírus para completar a análise.

Situações tipicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega da Internet ficheiros que julga serem perigosos.
- Quer analisar uma partilha de rede antes de copiar os ficheiros para o seu computador.

33.2. Usar Tarefas de Análise

Se deseja analisar o seu computador ou determinadas pastas regularmente, deve de considerar usar as tarefas de análise. Tarefas de análise indicam ao BitDefender as áreas a analisar, e que opções ou acções de análise devem ser usadas. Mais ainda, pode Agendá-las para serem levadas a cabo numa base regular ou numa determinada altura.

Para analisar o seu computador usando as tarefas de análise, deve de abrir o interface BitDefender e levar a cabo a tarefa de análise desejada. Dependendo do modo do interface do utilizador, são várias as etapas a seguir para executar o scan.

Levar a cabo Tarefas de Análise em Modo Básico

No Modo Básico, apenas pode levar a cabo uma análise standard de todo o computador clicando em **Analisar Agora**. Siga o assistente de Análise Antivírus para completar a análise.

Levar a cabo Tarefas de Análise em Modo Intermédio

Na Modo Intermédio, pode executar várias tarefas pré-configuradas de scan. Também pode configurar e executar tarefas de scan personalizadas especificando a sua localização nas opções de scan. Siga estes passos para levar a cabo uma tarefa de análise em Modo Intermédio:

1. Clique na barra **Segurança** .
2. No lado direito da área das Tarefas Rápidas, clique **Análise de Sistema** para iniciar uma análise standard de todo o computador. Para iniciar uma análise diferente clique na seta no fundo e seleccione a tarefa de análise desejada. Para configurar e executar uma anákise personalizada, clique em **Análise Personalizada**. Estas são as tarefas de análise disponíveis:

Tarefa de Análise	Descrição
Análise do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
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 utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.
Análise Personalizada	Esta opção permite-lhe configurar e executar uma análise personalizada, permitindo-lhe especificar as opções gerais de análise e o que quer analisar. Pode guardar as tarefas personalizadas de análise para que possa, mais tarde, ter acesso a elas no Modo Intermédio e no Modo Avançado.

3. Siga o assistente de Análise Antivírus para completar a análise. Se preferir executar uma análise personalizada, deverá completar o assistente de Análise Personalizada.

Executar uma Tarefa de Análise em Modo Avançado

Em Modo Avançado, pode levar a cabo todas as tarefas de análise pré-configuradas, e também alterar as suas opções. Mais ainda, pode criar as suas próprias tarefas

de análise se deseja analisar locais especificos no seu computador. Siga estes passos para levar a cabo uma tarefa de análise em Modo Avançado:

1. Clique em **Antivirus** do lado esquerdo do menu.
2. Clique na barra **Analisar** Aqui pode encontrar um conjunto de tarefas de análise pré-configuradas e pode criar as suas próprias tarefas de análise. Estas são as análises pré-configuradas que pode utilizar:

Tarefa por Defeito	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 do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
Análise Rápida do Sistema	Analisa as pastas do `Windows` e dos `Programas`. Na configuração por defeito, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.
Os Meus Documentos	Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

3. Duplo clique sobre a tarefa de análise que quer levar a cabo.
4. Siga o assistente de Análise Antivírus para completar a análise.

33.3. Usar a Análise Manual BitDefender

A análise manual BitDefender deixa-o analisar uma determinada pasta ou partição do disco sem ter de criar uma tarefa de análise. Esta ferramenta foi desenhada para ser usada quando o Windows está a correr em Modo de Segurança. Se o seu sistema está infectado com um vírus resiliente, pode tentar remover o vírus iniciando o Widnows em Modo de Segurança e analisando cada partição do disco duro usando a Análise Manual BitDefender.

Para analisar o seu computador usando a Análise Manual BitDefender, siga estes passos:

1. No menu Iniciar do Windows, siga o caminho **Iniciar** → **Programas** → **BitDefender 2010** → **Análise Manual BitDefender**. Uma nova janela irá aparecer.
2. Clique em **Adicionar Pasta** para seleccionar o alvo da análise. Uma nova janela irá aparecer.
3. Seleccione o alvo da análise:
   - Para analisar o seu ambiente de trabalho, seleccione apenas **Ambiente de Trabalho**.
   - Para analisar a partição completa, seleccione-a de O Meu Computador.
   - Para analisar uma determinada pasta, localize-a e seleccione-a.
4. Clique em **OK**.
5. Clique em **Continuar** para iniciar a análise.
6. Siga o assistente de Análise Antivírus para completar a análise.

O que é o Modo de Segurança?
O Modo de Segurança é uma forma especial de iniciar o Windows, usada apenas para resolver problemas que afectam a operação normal do Windows. Tais problemas vão desde drivers conflituosos até vírus que impedem que o Windows inicie normalmente. No Modo de Segurança, o Windows carrega apenas um minímo de componentes do sistema operativo e drivers básicos. Apenas algumas aplicações funcionam em Modo de Segurança. Essa é a razão pela qual a maioria dos vírus ficam inactivos quando usa o Windows em Modo de Segurança e então podem ser facilmente removidos.
Para iniciar o Windows em Modo de Segurança, reinicie o seu computador e prima a tecla F8 até que o menu das opções Avançadas do Windows surja. Pode escolher estre várias opções, a opção de iniciar o Windows em Modo de Segurança. Poderá querer seleccionar **Modo de Segurança com Rede>** de forma a poder ter acesso à Internet.

Nota

Para mais informação dobre o Modo de Segurança, vá ao Centro de Ajuda e Suporte do Windows (no menu Iniciar, clique em **ajuda e suporte**). Pode também encontrar informação útil pesquisando a Internet.

33.4. Usando a Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade de verificação no seu sistema. Esta pequena janela, por defeito, é apenas disponível no Modo Avançado.

Pode usar a barra de actividade da análise para analisar rapidamente ficheiros e pastas. Drag &

Barra de Actividade da Análise

drop o ficheiro ou pasta a ser analisado para a barra de actividade da análise. Siga o assistente de Análise Antivírus para completar a análise.

Nota

Para mais informação, por favor consulte o “*Barra de Actividade da Análise*” (p. 33).

34. Como Agendar a Análise do Computador

Analisar o seu computador periodicamente é a melhor prática para o manter livre de malware. O BitDefender permite-lhe agendar as tarefas de análise de forma a poder analisar automaticamente o seu computador.

Para agendar o BitDefender de forma a analisar o seu computador, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Clique em **Antivirus** do lado esquerdo do menu.
3. Clique na barra **Analisar** Aqui pode encontrar um conjunto de tarefas de análise pré-configuradas e pode criar as suas próprias tarefas de análise.
   - As tarefas de sistema estão disponíveis e podem ser levadas a cabo em qualquer conta de utilizador Windows.
   - Tarefas de utilizador estão apenas disponíveis para o mesmo e só podem ser usadas por quem as criou.

   Estas são as análises pré-configuradas que pode agendar:

Tarefa por Defeito	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 do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
Análise Rápida do Sistema	Analisa as pastas do `Windows` e dos `Programas`. Na configuração por defeito, 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 utilizador entra no Windows. Para usar esta tarefa, deve de agendá-la para ser levada a cabo durante o iniciar do sistema. Por defeito, a análise ao logon está desactivada.
Os Meus Documentos	Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de

Tarefa por Defeito	Descrição
	trabalho segura e aplicações limpas a serem executadas no arranque.

Se nenhuma destas tarefas de análise servir, pode criar uma nova tarefa de análise que pode depois agendar para ser levada a cabo quando quiser.

4. Clique com o botão-direito na tarefa de análise desejada e seleccione **Agendar**. Uma nova janela irá aparecer.
5. Agende a tarefa para ser levada a cabo quando quiser:
   - Para levar a cabo a tarefa de análise uma só vez, seleccione **Uma só vez** e especifique a data e hora de inicio.
   - Para levar a cabo a tarefa de análise após o iniciar do sistema, seleccione **No iniciar do sistema**. Pode definir quanto tempo após o iniciar do sistema a tarefa deve de ser iniciada.
   - Para levar a cabo a tarefa de análise numa base regular, seleccione **Periodicamente** e especifique a frequência e a data e hora de inicio.

   Nota

   Por exemplo, para analisar o seu computador cada Sábado às 2 PM, deve de configurar o agendar da seguinte forma:

   a. Seleccione **Periodicamente**.
   b. No campo **A cada**, insira 1 e depois seleccione **semanas** do menu. Desta forma, a tarefa é levada a cabo a cada semana.
   c. Defina como data de início o primeiro Sábado a aparecer.
   d. Defina como hora de início `2:00:00 AM`.

6. Clique em **OK** para guardar o agendamento. A tarefa de análise irá ser levada a cabo automaticamente de acordo com o agendamento que definiu. Se o computador estiver desligado durante o momento do agendamento, a tarefa será levada a cabo da próxima vez que iniciar o seu computador.

Troubleshooting e Obter Ajuda

35. Solução de problemas

Este capítulo apresenta alguns dos problemas que poderão surgir enquanto utiliza o BitDefender, e providencia possiveis soluções. A maioria destes problemas podem ser resolvidos através da configuração adequada das definições do produto.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contacta os representantes do suporte técnico da BitDefender como está representado no capítulo "*Suporte*" (p. 335).

35.1. Problemas de Instalação

Este artigo vai ajuda-lo a solucionar os problemas de instalação mais comums do BitDefender. Estes problemas podem ser agrupados nas seguintes categorias:

- Erros de validação de Instalação: o assistente de configuração não pode ser executado devido a condições específicas do seu sistema.
- Instalações falhadas: iniciou a instalação do assistente de configuração, mas não foi concluída com êxito.

35.1.1. Erros de Validação da Instalação

Quando você iniciar o assistente de instalação, um número de condições são verificadas para validar se a instalação pode ser iniciada. A seguinte tabela apresenta as validadções e erros das instalações mais comuns, bem como o ajuda a solucioná-las.

Erro	Descrição&Solução
Não possui privilégios suficientes para instalar o programa.	Para poder executar o assistente de instalação e instalar o BitDefender necessita de provilégios de administrador. Faça uma das coisas seguintes: ● Entre com uma conta de administrador do Windows e execute de novo o assistente de instalação. ● Clique com o botão-direito no ficheiro de instalação **Executar como**. Digite no sistema o nome de utilizador e a palavra-passe de uma conta de administrador do Windows.
O instalador detectou uma versão anterior do produto BitDefender que não foi devidamente desinstalada.	O BitDefender foi anteriormente instalado no seu sistema, mas a instalação não foi completamente removida. Esta condição bloqueia uma nova instalação do BitDefender.

Erro	Descrição&Solução
	Para superar este erro e instalar o BitDefender, siga estes passos: 1. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador. 2. Execute a ferramenta de desinstalação com direitos de administrador. 3. Reinicie o seu computador. 4. Volte a iniciar o assistente de instalação para reinstalar o BitDefender.
O produto BitDefender não é compatível com o seu sistema operativo.	Está a tentar instalar o BitDefender num sistema operativo nao suportado. Por favor consulte o "*Requisitos do Sistema*" (p. 2) para saber em que sistemas operativos pode instalar no BitDefender. Se o seu sistema operativo é o Windows XP com o Service Pack 1 ou sem nenhum service pack, pode instalar o Service Pack 2 ou superior e em seguida executar novamente o assistente de instalação.
O ficheiro de instalação foi concebido para um diferente tipo de processador.	Se receber esse erro, significa que está a tentar executar uma versão incorreta do ficheiro de instalação. Existem duas versões do ficheiro de instalação do BitDefender: um para processadores 32-bit e outro para processadores 64-bit. Para se certificar que tem a versão correta para o seu sistema, faça o download do ficheiro de instalação diretamente do site www.bitdefender.com.

35.1.2. Falha na Instalação

Existem várias possibilidades para instalação falhar:

- Durante a instalação, aparece uma imagem de erro. Pode-lhe ser solicitado para cancelar a instalação ou um botão pode ser fornecido para executar a ferramenta de desinstalação que irá limpar o sistema.

Nota
Imediatamente após iniciar a instalação, pode ser informado de que não possui espaço livre suficiente no disco rídigo para instalar o BitDefender. Nesse caso, liberte o espaço necessário em disco na partição onde quer que o BitDefender seja instalado e depois continue ou recomeçe a instalação.

- A instalação trava e possivelmente, o seu sistema bloqueia. Apenas o reiniciar restaura a responsividade do sistema.
- A instalação foi concluída, mas não pode utilizar algumas ou todas as funções BitDefender.

Para detectar o problema de uma falha na instalação e instalar o BitDefender, siga os seguintes passos:

1. **Limpe o sistema depois da falha de instalação.** Se a instalação falhar, algumas chaves de registo e ficheiros do BitDefender poderão manter-se no seu sistema. Podem também afectar o desempenho e a estabilidade do sistema. Por isso deve removê-los antes de tentar instalar o produto novamente.

   Se o ecrã de erro fornece um botão para executar uma ferramenta de desinstalação, clique nesse botão para limpar o sistema. Caso contrário, proceda da seguinte forma:

   a. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador.

   b. Execute a ferramenta de desinstalação com direitos de administrador.

   c. Reinicie o seu computador.

2. **Verificar causas possíveis para a instalação ter falhado.** Antes de avançar para reinstalar o produto, verifique e remova possíveis condições que podem ter causado a falha da instalação:

   a. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.

   b. Também deve verificar se seu sistema está infectado. Faça uma das coisas seguintes:

      - Utilize o BitDefender Rescue CD para analisar seu computador e remover quaisquer ameaças existentes. Para mais informação, por favor consulte o "CD de Emergência BitDefender" (p. 338).
      - Abra a janela do Internet Explorer, vá a www.bitdefender.com e execute a análise online (clique no botão **scan online**).

3. Volte a tentar instalar o BitDefender. É recomendado que descarregue e execute a ultima versão do ficheiro de instalação em www.bitdefender.com.
4. Se a instalação falhar, contacte a BitDefender para suporte, como descrito na secção "*Suporte*" (p. 335).

35.2. Os serviços BitDefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de*Os Serviços BitDefender não estão a responder*. Pode encontrar esse erro da seguinte forma:

- O icon BitDefender na Barra de Notificação está a cinzenta e um pop-up informa que os serviços do BitDefender não estão a responder.
- A janela do BitDefender indica que os serviços do BitDefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes factores:

- Está a ser instalada uma actualização importante.
- problemas temporários de comunicação entre os serviços da BitDefender.
- alguns dos serviços da BitDefender estão parados.
- Outras soluções de segurança em execução no seu computador, ao mesmo tempo que o BitDefender.
- Os vírus no seu sistema afectam o funcionamento normal do BitDefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração. Este erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até o BitDefender iniciar. Abra o BitDefender e veja se o erro se mantém. Reiniciar o computador normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.
4. Se o erro persistir, pode haver um problema mais grave (por exemplo, pode estar infectado com um vírus que interfere com o BitDefender). Por favor contacte a BitDefender para suporte, como descrito na secção “*Suporte*” (p. 335).

35.3. A partilha de ficheiros e impressoras em Wi-Fi (Wireless) A Rede Não Funciona

Este artigo ajuda a solucionar os seguintes problemas com a firwall do BitDefender em redes Wi-Fi:

- Não é possível compartilhar arquivos com computadores na rede Wi-Fi.
- Não é possível aceder a uma impressora de rede ligada à rede Wi-Fi.
- Não é possível aceder a uma impressora partilhada na rede Wi-Fi.

- Não é possivel compartilhar a sua impressora com computadores na rede Wi-Fi.

Antes de iniciar a resolução destes problemas, deverá informar-se primeiro sobre a segurança e a configuração do firewall do BitDefender em redes Wi-Fi. Seguindo um ponto de vista de segurança, as redes Wi-Fi podem ser classificadas numa destas categorias:

- **Redes Wi-Fi seguras.** Este tipo de rede só permite a conexão a dispositivos activados Wi-Fi. O acesso à rede está condicionada por uma palavra-passe. Um exemplo de redes Wi-Fi seguras são as montadas nas redes de escritórios.
- **Abrir rede Wi-Fi (Não-segura).** Qualquer dispositivo Wi-Fi activado dentro da linha de alcançe de uma rede Wi-Fi Não-segura pode livremente conectar-se a ela. Redes Wi-Fi não-seguras são amplamente utilizadas. Elas são compostas por quase todas as redes públicas Wi-Fi (tais como nos estabelecimentos de ensino, cafés, aeroportos e outros). Uma rede que configurou usando um router sem fio também é insegura até que active a segurança no router.

  Redes Wi-Fi Não-seguras representam um grande risco para a segurança porque o seu computador liga-se a um computador desconhecido. Sem a proteção adequada fornecida pelo firewall, alguém ligado à rede pode acessar aos seus ficheiros partilhados e até mesmo entrar no seu computador.

Quando ligado a uma rede não-segura de Wi-Fi, o BitDefender bloqueia automaticamente a comunicação com o computador dessa rede. Apenas pode aceder á Internet, mas não pode partilhar ficheiros ou impressoras com outros utilizadores da rede.

Para activar a comunicação com uma rede Wi-Fi, existem duas soluções:

- A solução "computador fiável" permite a partilhar de impressora e ficheiros apenas com computadores específicos (computadores fiáveis) na rede Wi-Fi. Utilize esta solução quando está ligado a uma rede pública de Wi-Fi (por exemplo, uma rede de um estabelecimento de ensino ou de um café) e quer partilhar ficheiros ou uma impressora com um amigo ou aceder a uma impressora que se encontra na rede Wi-Fi.
- A solução "rede segura" permite a partilha de impressora e ficheiros com toda a rede Wi-Fi (rede segura). Esta solução não é recomendada por motivos de segurança, mas poderá ser útil em situações específicas (por exemplo, pode utilizá-la na rede Wi-Fi de casa ou do escritório).

35.3.1. Solução "Computador Fiável"

Para configurar o firewall do BitDefender para permitir a partilhar de ficheiros e impressoras com um computador da rede Wi-Fi, ou aceder a uma impressora da rede Wi-Fi, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.

2. Clique em **Firewall** do lado esquerdo do menu.
3. Clique na barra **Rede**.
4. Na tabela Zonas, seleccione a rede Wi-Fi e depois clique no botão **Adicionar**.
5. Seleccione o computador ou impressora da rede Wi-Fi desejada, da lista de dispositivos detectados na rede Wi-Fi Se esse computador ou impressora não foi automaticamente detectado, pode digitar o IP no campo **Zona**
6. Seleccione a acção **Permitir**.
7. Clique em **OK**.

Se continua a não conseguir partilhar ficheiros ou uma impressora com o computador escolhido, provavelmente isso não será causado pelo firewall do BitDefender. Procure por outras potenciais causas, tais como as seguintes:

- O firewall que se encontra no outro computador pode bloquear o compartilhamento de ficheiros e impressoras na rede (pública) de Wi-Fi não-segura.
  - Se o firewall for de um produto BitDefender 2009 ou BitDefender 2010, o mesmo procedimento deve ser seguido no outro computador para permitir o compartilhamento de ficheiros e impressora com o seu computador.
  - Se o Firewall do Windows está a ser utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte fomra: abra a janela das definições do Firewall do Windows, separador **Excepções** e seleccione a caixa de selecção **Partilha de Ficheiros e Impressoras**.
  - Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.
- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.
  - As permissões são definidas para a impressora compartilhada para permitir acesso a um computador específico e apenas utilizadores. Se está a compartilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro computador está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora compartilhada, verifique com o utilizador do outro computador se tem permissão para se conectar com a impressora.
  - A impressora ligada ao seu computador ou ao outro computador não está a ser compartilhada.
  - A impressora compartilhada não está adicionada ao computador.

Nota

Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

Se continua a não conseguir aceder à impressora da rede Wi-Fi, provavelmente isso não será causado pelo firewall do BitDefender. O acesso à impressora da rede Wi-Fi pode ser restringido a computadores ou apenas a utilizadores. Deverá verificar com o administrador da rede Wi-Fi se tem ou não permissão para aceder à impressora.

Se suspeita que o problema se encontra no firewall do BitDefender, pode contacta a BitDefender para suporte como descrito na seccção *"Suporte"* (p. 335).

35.3.2. Solução para "Rede Segura"

É recomendado que utilize esta solução apenas para redes Wi-Fi de casa ou escritórios.

Para configurar o firewall do BitDefender para permitir a partilha de ficheiros e impressora com toda a rede Wi-Fi, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Clique em **Firewall** do lado esquerdo do menu.
3. Clique na barra **Rede**.
4. Na coluna da tabela de Configuração de Rede, **Nível de Segurança** column, clique na seta ▾ na linha correspondente à rede de Wi-Fi.
5. Dependendo do nível de segurança que quer obter, escolha uma das seguintes opções:
   - **Insegura** - para aceder aos ficheiros e impressoras partilhadas na red Wi-Fi, sem permitir o acesso aos seus documentos partilhados.
   - **Segura** - para permitir a partilha de ficheiros e impressoras dos dois lados. Isto significa que os utilizadores conectados à rede Wi-Fi também podem aceder aos seus ficheiros e impressora partilhados.

Se continua a não conseguir partilhar ficheiros ou uma impressora com computadores específicos da rede Wi-Fi, provavelmente isso não será causado pelo firewall do BitDefender. Procure por outras potenciais causas, tais como as seguintes:

- O firewall que se encontra no outro computador pode bloquear o compartilhamento de ficheiros e impressoras na rede (pública) de Wi-Fi não-segura.
  - Se o firewall for de um produto BitDefender 2009 ou BitDefender 2010, o mesmo procedimento deve ser seguido no outro computador para permitir o compartilhamento de ficheiros e impressora com o seu computador.

- Se o Firewall do Windows está a ser utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte fomra: abra a janela das definições do Firewall do Windows, separador **Excepções** e seleccione a caixa de selecção **Partilha de Ficheiros e Impressoras**.
- Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.

- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.
  - As permissões são definidas para a impressora compartilhada para permitir acesso a um computador específico e apenas utilizadores. Se está a compartilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro computador está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora compartilhada, verifique com o utilizador do outro computador se tem permissão para se conectar com a impressora.
  - A impressora ligada ao seu computador ou ao outro computador não está a ser compartilhada.
  - A impressora compartilhada não está adicionada ao computador.

Nota

Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

Se continua a não conseguir aceder a uma impressora da rede Wi-Fi, provavelmente isso não será causado pelo firewall do BitDefender. O acesso à impressora da rede Wi-Fi pode ser restringido a computadores ou apenas a utilizadores. Deverá verificar com o administrador da rede Wi-Fi se tem ou não permissão para aceder à impressora.

Se suspeita que o problema se encontra no firewall do BitDefender, pode contacta a BitDefender para suporte como descrito na seccção “*Suporte*” (p. 335).

35.4. O Filtro Antispam Não Está a Funcionar Correctamente

Este artigo ajuda a solucionar os seguintes problemas relacionados com a operação de filtragem do Antispam do BitDefender:

- Um número de mensagens de e-mail legítimas são marcadas como [spam].
- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.

- O filtro antispam não detecta qualquer mensagem de spam.

35.4.1. Mensagens Legítimas são marcadas como [spam]

Mensagens legítimas são marcadas como `[spam]` simplesmente porque elas parecem spam para o filtro antispam do BitDefender. Pode normalmente resolver este problema ao configurar adequadamente o filtro Antispam.

O BitDefender adiciona automaticamente os remetentes das suas mensagens de e-mail à Lista de Amigos. As mensagens de e-mail recebidas dos contactos na lista de Amigos são consideradas legítimas. Elas não são verificadas pelo filtro antispam e, deste modo, elas nunca são marcadas como `[spam]`.

A configuração automática da lista de Amigos não impede a detecção de erros que podem ocorrer nestas situações:

- Recebeu muitos e-mails publicitários solicitados como resultado de se inscrever em vários sites. Neste caso, a solução é adicionar à Lista de Amigos o endereço de e-mail do qual recebeu esses e-mails.
- Uma parte significativa dos seus mails legitimos são de pessoas com quem nunca trocou e-mails antes, tais como clientes, potenciais parceiros empresariais e outros. Outras soluções são requeridas neste caso.

Se estiver a utilizar um cliente de e-mail com o qual o BitDefender é compatível, experimente uma das seguintes soluções:

1. Indica detecção de erros. Isto é utilizado para treinar o Motor de Aprendizagem (Bayesiano) do filtro de antispam e ajuda a prevenir futuros erros de detecção. O Motor de Aprendizagem analisa as mensagens indicadas e aprende os seus padrões. Os próximos e-mails que se encaixem nos mesmos padrões, não serão marcadas como `[spam]`.
2. Diminui o nível de protecção antispam. Ao diminuir o nível de protecção, o filtro de antispam necessitará de mais indicadores de spam para classificar uma mensagem de e-mail como spam. Experimente esta solução apenas se várias mensagens legitimas (incluindo mensagens publicitárias solicitadas) estão a ser incorrectamente detectadas como spam.
3. Retreinar o Motor de Aprendizagem (filtro Bayesiano). Tente esta solução unicamente se as soluções anteriores não oferecem resultados satisfatórios.

Nota

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o “*Software Suportado*” (p. 2).

Se está a utilizar um mail de cliente diferente, não pode indicar detecção de erros e instruir o Motor de Aprendizagem. Para resolver este problema, tente diminuir o nível de protecção antispam.

Adicionar os Contactos à Lista de Amigos

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens legítimas à lista de Amigos. Siga estes passos:

1. No seu cliente de mail, seleccione a mensagem de e-mail do remetente que quer adicionar à lista de Amigos.
2. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do BitDefender.
3. Poderá ser convidado a reconhecer os endereços adicionados à lista de Amigos. Seleccione **Não mostrar esta mensagem outra vez** e clique **OK**.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Se está a utilizar um cliente de mail diferente, poderá adicionar os contactos à lista Amigos a partir do interface do BitDefender. Siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.
4. Clique em **Gerir Amigos**. A janela de configuração irá aparecer.
5. Digite o endereço de e-mail de que quer receber sempre mensagens e cique no botão para adicionar o endereço à Lista de Amigos.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Indique os Erros de Detecção.

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio electrónico que não deveriam ter sido marcadas como`[spam]`). Se o fizer, irá melhorar consideravelmente a eficiência do filtro antispam. Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo electrónico, para onde são movidas as mensagens.
3. Seleccione a mensagem legítima incorrectamente marcada como `[spam]` pela BitDefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do BitDefender para adicionar o remetente à lista de Amigos. Pode necessitar de

clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

5. Clique no botão **Não é Spam** na barra de antispam BitDefender (normalmente localizada na parte superior da janela do cliente de e-mail). Isto indica ao Mecanismo de Aprendizagem que a mensagem seleccionada não é spam. A mensagem de e-mail será movida para a pasta Recebidos. Os próximos e-mails que se encaixem nos mesmos padrões, não serão marcadas como `[spam]`.

Diminuir o Nível de Protecção do Antispam

Para diminuir o nível de protecção do antispam, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.
4. Baixe a seta na barra deslocação.

É recomendado a baixar apenas um nível de protecção e depois espere o tempo suficiente para avaliar os resultados. Se muitas mensagens de e-mail legitimas continuam a ser marcadas como `[spam]`, pode baixar o nível de protecção. Se reparar que muitas mensagens spam nao estão a ser detectadas, não deverá baixar o nível de protecção.

Retreinar o Motor de Aprendizagem (Bayesiano)

Antes de iniciar o treino do Motor de Aprendizagem (Bayesiano), prepare uma pasta que contenha apenas mensagens SPAM e outra que contenha apenas mensagens legitimas. O Motor de Aprendizagem irá analisá-los e aprender as características que o definem como spam ou legitimar mensagens que normalmente recebe. Para que a formação seja eficaz, tem de haver mais de 50 mensagens em cada categoria.

Para redefinir a base de dados Bayesiana e retreinar o Motor de Aprendizagem, siga os seguintes passos:

1. Abra o mail de cliente.
2. Na barra de ferramentas antispam do BitDefender, clique no botão **Assistente** para iniciar o assistente de configuração do antispam. Informação detalhada neste assistente é providenciada na secção *"Assistente de Configuração Antispam" (p. 295)*.
3. Clique **Seguinte**.
4. Seleccione **Saltar este passo** e clique em **Seguinte**.
5. Seleccione **Limpar dados do filtro antispam** e clique **Seguinte**.
6. Seleccione a pasta que contém as mensagens legítimas e clique em **Seguinte**.

7. Seleccione a pasta que contém as mensagens SPAM e clique em **Seguinte**.
8. Clique em **Terminar** para dar início ao processo de treino.
9. Quando o treino está completo, clique em **Fechar**.

Pedir Ajuda

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Suporte*" (p. 335).

35.4.2. Muitas Mensagens de Spam Não São Detectadas

Se está a receber muitas mensagens spam que não estão marcadas como `[spam]`, tem de configurar o filtro antispam BitDefender de modo a melhorar a sua eficiência.

Se estiver a utilizar um cliente de e-mail com o qual o BitDefender é compatível, experimente uma das seguintes soluções:

1. Indica mensagens de spam não detectadas. Isto é utilizado para treinar o Motor de Aprendizagem (Bayesiano) do filtro de antispam e ajuda a melhorar a detecção do antispam. O Motor de Aprendizagem analisa as mensagens indicadas e aprende os seus padrões. Os próximos e-mails que se encaixem nos mesmos padrões, serão marcadas como `[spam]`.
2. Adicione spammers à lista de Spammers. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como `[spam]`.
3. Aumente o nível de protecção antispam. Ao aumentar o nível de protecção, o filtro de antispam necessitará de menos indicadores de spam para classificar uma mensagem de e-mail como spam.
4. Retreinar o Motor de Aprendizagem (filtro Bayesiano). Utilize esta solução quando a detecção antispam for muito insatisfatória e a indicação de mensagens de spam não detectadas, não funcionar mais.

Nota

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Software Suportado*" (p. 2).

Se está a utilizar um mail de cliente diferente, não pode mais indicar mensagens spam e instruir o Motor de Aprendizagem. Para resolver este problema, tente aumentar o nível de protecção e adicionar spams à lista Spammers.

Indica Mensagens de Spam não detectadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Ao fazê-lo melhora, em muito, a eficiência do filtro de antispam. Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Seleccione as mensagens spam não detectadas
4. Clique no botão **É Spam** na barra de tarefas do BitDefender (normalmente localizada na parte superior da janela de cliente de mail). Isto indica ao Motor de Aprendizagem que as mensagens seleccionadas são spam. São imediatamente marcadas como `[spam]` e movidas para a pasta de lixo electrónico. Os próximos e-mails que se encaixem nos mesmos padrões, serão marcadas como `[spam]`.

Adicionar Spammers à lista de Spammers

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens spam à lista Spammers. Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo electrónico, para onde são movidas as mensagens.
3. Seleccione a mensagem marcada como `[spam]` pela BitDefender.
4. Clique no botão **Adicionar Spammer** da barra de tarefas antispam do BitDefender.
5. Poderá ser convidado a reconhecer os endereços como Spammers. Seleccione **Não mostrar esta mensagem outra vez** e clique **OK**.

Se está a ultizar uma conta de mail diferente, pode manualmente adicionar spammers à lista Spammers do interface do BitDefender. É conveniente que o faça apenas quando receber várias mensagens spam do mesmo endereço e-mail. Siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.
4. Clique em **Gerir Spammers**. A janela de configuração irá aparecer.
5. Digite o email do spam e clique no botão para adicionar o endereço à Lista Spammers.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Aumentar o Nível de Protecção do Antispam

Para aumentar o nível de protecção do antispam, siga estes passos:

1. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.

4. Suba a seta na barra deslocação.

Retreinar o Motor de Aprendizagem (Bayesiano)

Antes de iniciar o treino do Motor de Aprendizagem (Bayesiano), prepare uma pasta que contenha apenas mensagens SPAM e outra que contenha apenas mensagens legitimas. O Motor de Aprendizagem irá analisá-los e aprender as características que o definem como spam ou legitimar mensagens que normalmente recebe. Para que a formação seja eficaz, tem de haver mais de 50 mensagens em cada pasta.

Para redefinir a base de dados Bayesiana e retreinar o Motor de Aprendizagem, siga os seguintes passos:

1. Abra o mail de cliente.
2. Na barra de ferramentas antispam do BitDefender, clique no botão **Assistente** para iniciar o assistente de configuração do antispam. Informação detalhada neste assistente é providenciada na secção "*Assistente de Configuração Antispam*" (p. 295).
3. Clique **Seguinte**.
4. Seleccione **Saltar este passo** e clique em **Seguinte**.
5. Seleccione **Limpar dados do filtro antispam** e clique **Seguinte**.
6. Seleccione a pasta que contém as mensagens legítimas e clique em **Seguinte**.
7. Seleccione a pasta que contém as mensagens SPAM e clique em **Seguinte**.
8. Clique em **Terminar** para dar início ao processo de treino.
9. Quando o treino está completo, clique em **Fechar**.

Pedir Ajuda

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Suporte*" (p. 335).

35.4.3. O Filtro Antispam Não Detecta Nenhuma Mensagem Spam

Se nenhuma mensagem spam for marcada como `[spam]`, poderá haver algum problema como o filtro Antispam do BitDefender. Antes de resolver este problema, certifique-se de que não é causado por nenhuma das seguintes condições:

- A protecção de Antispam do BitDefender está disponível apenas para clientes de correio electrónico configurado para receber mensagens de e-mail via protocolo POP3. Isto significa o seguinte:
  - As mensagens de Email obtidas atraves de Webmail (Yahoo, Gmail, Hotmail ou outros) não são filtradas como spam pelo BitDefender.

- Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo que não o POP3 (por exemplo, IMAP4), o filtro Antispam do BitDefender não as analisará à procura de spam.

Nota

POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, solicite à pessoa que o configurou.

- O BitDefender Internet Security 2010 não analisa o tráfego POP3 do Lotus Notes.

Deverá também verificar as possiveis seguintes causas:

1. Certifique-se que o Antispam está activado.
   a. Abrir o BitDefender.
   b. Clique em **Definições** que se encontra no canto superior direito da janela.
   c. Nas Definições de Segurança, verifique o estado do antispam.

   Se o Antispam estava desactivado, era isso que estava a causar o problema. Active o Antispam e acompanhe a operação para ver se o problema é corrigido.
2. Embora seja muito improvável, poderá ver se você (ou alguém) configurou o BitDefender para não marcar as mensagens spam como `[spam]`.
   a. Abra o BitDefender e altere a interface de utilizador para Modo Avançado.
   b. Clique em **Antispam** localizado no lado esquerdo do menu e em seguida clique no separador **Definições**.
   c. Assegure-se de que a opção **Marcar mensagens spam como spam no assunto** está seleccionada.

Uma solução possivel é reparar ou reinstalar o produto. Contudo, poderá contacta a BitDefender para suporte, como descrito na secção “*Suporte*” (p. 335).

35.5. A Desinstalação do BitDefender Falhou

Este artigo ajuda-o a resolver erros que possam ocorrer quando remover o BitDefender. Há duas situações possíveis:

- Durante a remoção, aparece uma imagem de erro. O ecrã apresenta um botão para executar uma ferramenta de desinstalação que irá limpar o sistema.
- A remoção trava e possivelmente, o seu sistema bloqueia. Clique em **Cancelar** para abortar a desinstalação. Se isso não funcionar, reinicie o sistema.

Se a desinstalação falhar, algumas chaves de registo e ficheiros do BitDefender poderão manter-se no seu sistema. Esses resquícios podem impedir uma nova instalação do BitDefender. Podem também afectar o desempenho e a estabilidade do sistema. Para remover completamente o BitDefender do seu sistema, deverá executar a ferramenta de desinstalação.

Se a desinstalação falhar com um erro no ecrã, clique no botão para executar a ferramenta de desinstalação para limpar o sistema. Caso contrário, proceda da seguinte forma:

1. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador.
2. Execute a ferramenta de desinstalação com direitos de administrador. A Ferramenta de Desinstalação removerá todos os ficheiros e chaves de registo que não tenham sido removidos durante o processo de desinstalação automática.
3. Reinicie o seu computador.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Suporte*" (p. 335).

36. Suporte

Como fornecedor qualificado, a BitDefender esforça-se por fornecer aos seus clientes um nível de suporte rápido e eficaz. A BitDefender Knowledge Base dá-lhe artigos que contêm soluções para a maioria dos seus problemas e questões relacionados com o BitDefender. Se não consegue encontrar a solução na Knowledge Base, pode contactar o Suporte Técnico BitDefender. O nosso suporte responderá às suas questões de uma forma atempada e dar-lhe-á toda a asistência que necessite.

36.1. BitDefender Knowledge Base

A BitDefender Knowledge Base é um repositório de informação on-line acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das actividades de reparação de erros por parte da equipe técnica do suporte BitDefender e da equipe de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de vírus, a administração de soluções BitDefender e explicações pormenorizadas, e muitos outros artigos.

A BitDefender Knowledge Base encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na BitDefender Knowledge Base, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

A BitDefender Knowledge Base encontra-se disponível a qualquer altura em http://kb.bitdefender.com.

36.2. Pedir Ajuda

De forma a poder solicitar ajuda, deve de usar o Serviço Web BitDefender. Apenas siga estes passos:

1. Vá para http://www.bitdefender.com/help. Aqui é onde pode encontrar a BitDefender Knowledge Base. A BitDefender Knowledge Base possui inúmeros artigos que contêm soluções para incidências relacionadas com o BitDefender.
2. Procure na BitDefender Knowledge Base os artigos que lhe poderão dar a solução para o seu problema.
3. Por favor leia os artigos relevantes e tente a solução que os mesmos lhe propõem.
4. Se esta solução não resolver o problema, use o link no artigo para contactar o Suporte Técnico BitDefender.
5. Entrar na sua conta BitDefender.
6. Contacte o suporte BitDefender por e-mail, chat ou telefone.

36.3. Contactos

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

36.3.1. Endereços Web

Departmento Comercial: comercial@bitdefender.pt
Suporte Técnico: www.bitdefender.com/help
Documentação: documentation@bitdefender.com
Partner Program: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Contactos Imprensa: pr@bitdefender.com
Oportunidades de Trabalho: jobs@bitdefender.com
Submeter Vírus: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Site internacional do produto: http://www.bitdefender.com
Ficheiros ftp do produto: ftp://ftp.bitdefender.com/pub
Distribuidor Local: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

36.3.2. Escritórios BitDefender

Os escritórios BitDefender estão preparados para responder a quaisquer perguntas respeitantes às suas áreas de operação, quer sejam questões comerciais e de assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

Spain

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

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street

Bucharest
Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
E-mail Vendas: sales@bitdefender.ro
Suporte Técnico: http://kb.bitdefender.ro
Website: http://www.bitdefender.ro

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefone (office&sales): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Germany

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

UK e Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-mail: info@bitdefender.co.uk
Telefone: +44 (0) 8451-305096
Vendas: sales@bitdefender.co.uk
Suporte Técnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

CD de Emergência BitDefender

37. Vista Geral

BitDefender Internet Security 2010 vem com um CD de arranque (CD de Emergência BitDefender) capaz de analisar e desinfectar todos os discos rígidos antes de o seu sistema operativo iniciar.

Deve usar o CD de Emergência BitDefender em qualquer altura que o seu sistema operativo não esteja a funcionar bem devido a infecções com vírus. Isso normalmente acontece quando não tem instalado um produto antivírus.

A actualização das assinaturas dos vírus é feita automaticamente, sem haver necessidade de intervenção por parte do utilizador, cada vez que arranca com o Cd de Emergência do 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/

37.1. Requisitos do Sistema

Antes de arrancar com o CD de Emergência BitDefender, deve em primeiro lugar verificar se o seu sistema possui os seguintes requisitos.

Tipo de Processador

x86 compatível, mínimo 166 MHz, mas não espere uma boa performance neste caso. A geração i686 de processador, a 800MHz, seria uma escolha mais apropriada.

Memória

Mínimo 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.

ligação 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.

37.2. Software incluído

O CD de Emergência BitDefender inclui os seguintes pacotes de software.

Xedit
Este é um ficheiro de um editor de texto.

Vim
Este é um poderoso ficheiro 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 ficheiros gráficos.

Para mais informação, consultar a página internet da RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) um gestor de ficheiros 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 ficheiros de sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 para um ficheiros 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 ficheiro.

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.

38. 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 dadosdo 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 utilizador.

38.1. Iniciar o CD de Emergência BitDefender

Para iniciar o CD, prepare a BIOS do seu computador para arrancar pelo CD, coloque o CD na drive e reinicie o computador. Cerifique-se que o seu computador pode arrancar pelo CD.

Espere até ao próximo ecrã aparecer e siga as instruções no ecrã para iniciar o CD de Emergência BitDefender.

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 de arranque terminar poderá ver o próximo ambiente de trabalho. Pode então começar a usar o CD de Emergência BitDefender.

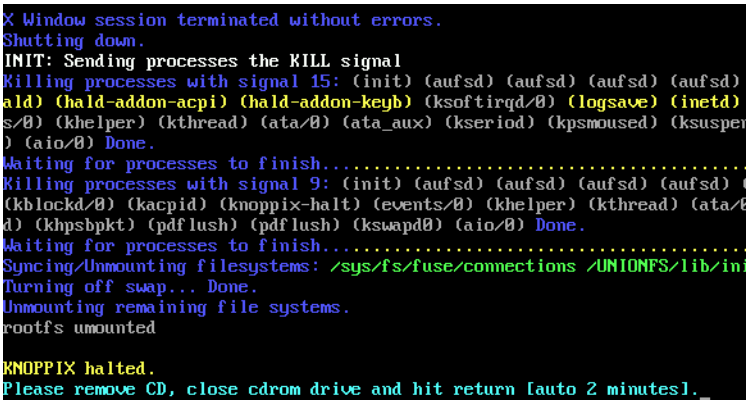
O Ambiente de Trabalho

38.2. Parar o CD de Emergência 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.

Seleccionar "SAIR"

Quando o CD de Emergência BitDefender fechar com sucesso todos os programas mostra-lhe um ecrã como a imagem seguinte. Pode remover o CD de forma a arrancar pelo seu disco duro. Agora é OK desligar o seu computador ou reiniciá-lo.



Aguarde por esta mensagem quando estiver a desligar o seu pc

38.3. Como posso levar a cabo uma análise completa ao sistema?

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 o "+" para abrir um grupo, ou na caixa com o "-" 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 resumo dos resultados.

Se quiser analisar apenas um determinado directório, pode utilizar uma das seguintes opções:

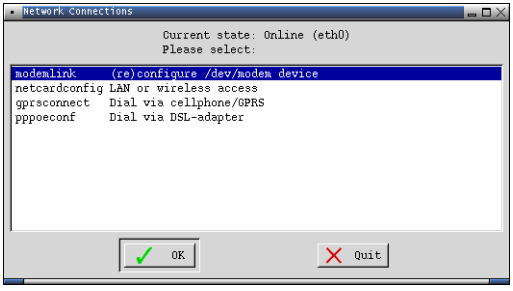
- Use o **BitDefender Scanner for Unices**.
  1. Duplo clique o ícone START SCANNER no Ambiente de Trabalho. Isto irá levar a cabo o **BitDefender Scanner for Unices**.
  2. Clique **Scanner**, e uma nova janela irá aparecer.
  3. Seleccione o directório que deseja analisar e clique **Abrir** para iniciar a análise usando o mesmo assistente que apareceu durante o primeiro boot.
- Utilize o menu contextual - explore as suas pastas, clique com o botão-direito do rato num ficheiro ou directoria e seleccione **Enviar para**. Depois escolha **Analisador BitDefender**.
- Ou pode emitir o próximo comando de raiz, de um terminal. O **Analisador Antivírus BitDefender** começará com o ficheiro ou pasta seleccionado como a localização por defeito a analisar.

```
# bdscan /path/to/scan/
```

38.4. Como posso configurar a Ligação à Internet?

Se está numa rede DHCP e possui uma placa de rede ethernet, a ligação à Internet deve ser detectada e configurada. Para uma configuração manual, siga os seguintes passos.

1. Clique botão direito 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.

Ligação	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 no ecrã. Se não tem a certeza do que escrever, contacte o seu administrador de sistema para mais 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 rato 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
```

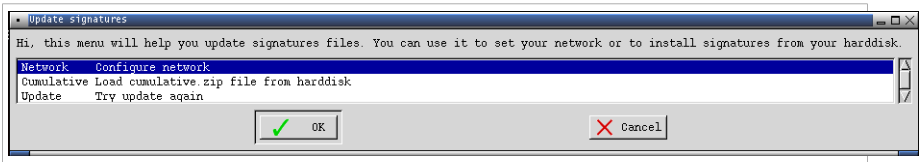
4. Siga as instruções no ecrã. Se não tem a certeza do que escrever, contacte o seu administrador de sistema para mais detalhes.

38.5. Como posso actualizar o BitDefender?

No momento do arranque, a atualização de assinaturas de vírus é feita automaticamente. Contudo, se quiser passar este passo á frente ou desejar fazer a actualização depois do arranque, aqui estão duas formas de actualizar o BitDefender.

- Use o **BitDefender Scanner for Unices**.
  1. Duplo clique o ícone START SCANNER no Ambiente de Trabalho. Isto irá levar a cabo o **BitDefender Scanner for Unices**.
  2. Clique em **Actualizar**.
- Use o atalho **Actualizar Assinaturas** que está no Ambiente de Trabalho.

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:
   - Seleccione **Cumulativa** para instalar as assinaturas guardadas no seu disco duro devido a ter descarregado no seu computador o ficheiro `cumulative.zip` .
   - Seleccione **Actualização** para ligar-se imediatamente à internet e descarregar as últimas assinaturas de vírus.
3. Clique em **OK**.

38.5.1. 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 as assinaturas de vírus.

Para actualizar o BitDefender via um proxy, use uma das seguintes opções:

- Use o **BitDefender Scanner for Unices**.
  1. Duplo clique o ícone START SCANNER no Ambiente de Trabalho. Isto irá levar a cabo o **BitDefender Scanner for Unices**.
  2. Clique **Definições**, e uma nova janela irá aparecer.
  3. Por baixo de **Definições de Actualização**, seleccione a caixa de selecção **Activar Proxy HTTP**. Especifique o Proxy host (a ser definido como se segue: `host[:porta]`), utilizador Proxy (a ser definido como se segue: `[domain\]Utilizador`) e Palavra-passe. Seleccione a caixa de selecção**Saltar servidor proxy quando não disponível** para uma ligação directa a ser usada se o servidor proxy não estiver disponível.
  4. Clique em **Guardar**.
  5. Clique em **Actualizar**.
- Usar Terminal (como raiz).
  1. Clique botão direito do rato 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 ficheiro usando o GNU Midnight Commander (mc).

5. Uncomment a seguinte linha: `#HttpProxy =` (apenas apague o sinal #) e especifique o domínio, nome, palavra-passe 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 ficheiro actual, confirme o guardar, e depois prima **F10** para o fechar.
7. Digite o comando: **bdscan update**.

38.6. 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

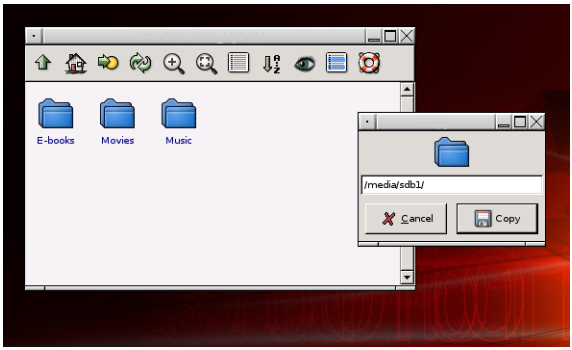
3. Faça duplo clique sobre a partição onde os dados que deseja salvar se encontram (ex. `[sda3]`).

   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 rato sobre a directoria desejada e seleccione **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`.

38.7. Como usar o modo consola?

Se a sua resolução de ecrã não é alta o suficiente para executar a interface gráfica do utilizador, pode executar o CD de Emergência do BitDefender no modo de consola. O modo simples de texto permite-lhe fazer uma análise completa ao seu computador.

Para levar a cabo o CD em modo de consola, defina a BIOS do seu computador para arrancar pelo CD, ponha o CD na drive e reinicie o computador. Espere que o ecran de arranque apareça e seleccione **Inicia knoppix em modo de consola**.

Após iniciar, siga as instruções para executar uma análise completa ao seu computador.

O BitDefender detecta as partições do seu disco rígido e actualiza automaticamente a base de dados das assinaturas de malware antes da análise começar. Se algum ficheiro infectado for detectado, o BitDefender irá desinfectá-lo. Após o processo de análise estar completo, o registo da análise aparecerá.

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

Glossário

ActiveX

O ActiveX é um modelo de escrita de programas, para que outros programas e o sistema operativo o possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e compartam-se como programas de computador, em vez de páginas estácticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da Web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável para um leque completo de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa de as aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Arquivo

Um disco, cassete, ou directório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Porta das traseiras

Um buraco na segurança de um sistema deliberadamente deixado ao acaso pelos desenhadores e protectores. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, saem fora das caixas com contas priveligiadas, intencionadas para o uso no terreno por técnicos de serviço ou pelo vendedor dos programas de manutenção.

Sector de saída

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí a diante). Para discos de inicialização, o sector de saída também contém um progrma que carrega o sistema operativo.

Vírus de saída

Um vírus que infecta o sector de saída de um disco fixo ou de uma unidade de disquetes. A tentativa de retirar uma disquete infectada por um vírus de saída, irá causar a activação do vírus na memória. Sempre que iniciar o seu sistema daquele ponto, terá o vírus activo na memória.

Browser

Diminuitivo para browser de internet, que é um software usado para localizar e mostrar páginas Web. Os dois mais populares browsers são o Netscape Navigator e o Microsoft Internet Explorer. Ambos são browsers gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos browsers modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de necessitarem de plug-ins para alguns formatos.

Linha de comando

Numa interface de linha do comado, o utilizador introduz comandos no espaço providenciado directamente no ecrã, usando a linguagem de comando.

Cookie

Desntro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é encontrar alvos publicitários directamente do que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado aé eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (você sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Enquanto este ponto de vista possa ser extremo, em alguns casos é preciso.

Componente (drive) do disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma componente de disco rígido lê e escreve discos rígidos.

Uma componente de disquetes acede às disquetes.

As componentes do disco tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Descarga (Download)

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. Também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

E-mail

Correio electrónico. É um serviço que envia mensagens em computadores via local ou redes globais.

Eventos

Uma acção ou ocorrência detectada por um programa. Os eventos podem ser acções do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tais como ficar sem memórias.

Falso positivo

Ocorre quando o verificador identifica um ficheiro como infectado, quando na verdade ele não está.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras. Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostEscrito, ".txt" para texto arbitrário.

Heurístico

Um método baseado na regra de identificar novos vírus. Este método de exame não se fia em assinaturas específicas de vírus. A vantagem do exame heurístico, é que não se deixa enganar por uma nova variante de um vírus existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP séquito que é responsável dos endereços de IP, rotas, e a fragmentação e reabertura dos pacotes de IP.

Java applet

Um programa Java, o qual é desenhado para correr apenas numa página da web. Para usar uma applet numa página da web, you deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o motor de busca descarrega a applet de um servidor e corre-a apenas na máquina do utilizador (o cliente). As applets diferem das aplicações, nas quais são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets correrem no cliente, elas não podem escrever nem lêr dados para a máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas lêr e escrever dados provenientes do mesmo domínio, no qual elas são servidas.

Macro vírus

Um tipo de vírus de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Cliente de mail

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassates ou discos. Todo o computador vem com uma certa quantidade de memótia física, normalmente referida como memória pricipal ou RAM.

Não-heurístico

Este método de exame confia em assinaturas de vírus especificas. A vantagem de um exame não-heurístico, é que ele não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente isto iria requerer dez de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a ser substituidos. Neste caso, os dez espaços iriam requeres apenas dois bytes. Esta é apenas uma técnica de compactar, há muitas.

Caminho

As direcções exactas para um ficheiro num computador. Estas direcções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dosi dados pontos, tal como os canais de comunicação entre dois.

Phishing

O acto de enviar um e-mail a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoa, tal como passwords e números de cartões de crédito, segurança social, e

números de contas bancárias, que a legítima organização já possui. O site Web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Vírus polimórfico

Um vírus que altera a sua forma com cada ficheiro que infecta. Dado que eles não têm uma consistência de patente binária, tais vírus são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais tendo vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs, e tecladoss. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Ficheiro de reporte

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados 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, ficheiros, 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 ficheiros 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 ficheiros e relatórios e evitarem ser detectados.

Escrita

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interacção do utilizador.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio não-solicitado.

Spyware

O estabelecimento de ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também reunir informação acerca de endereços de e-mail e até mesmo passwords e números de cartões de crédito.

O spyware é similar a um cavalo-de-troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Itens que começam a funcionar ao ínicio

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã que abra no ínicio, um ficheiro de som a ser tocado quando ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si próprio.

Caixa do sistema

Introduzido com o Windows 95, a área de notificação está localizada na barra de tarefas do Windows (normalmente em baixo junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema tais como, fax, impressora, modem, volume, etc. Faça duplo-clique ou clique botão-direito sobre o ícone para ver e aceder aos detalhes e controlos.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões

de como os computadores comunicam e convenções para conectar redes e rotas de tráfego.

Tróiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais incidente é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Actualização

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O BitDefender tem o seu próprio modulo de actualização que lhe permite verificar actualizações manualmente, ou permitir actualizar o produto automaticamente.

Vírus

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e decorre contra a sua vontade. A maioria dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Ainda um mais perigoso tipo de vírus é aquele capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

Definição de vírus

A patente binária de um vírus, usada pelo programa de anti-vírus para detectar e eliminar os vírus.

Minhoca

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.