bitdefender

ANTIVIRUS 2008

Manual do Utilizador

Copyright© 2008 BitDefender

BitDefender Antivirus 2008

Manual do Utilizador

Publicado 2008.03.26

Copyright© 2008 BitDefender

Aviso Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por quaisquer meios, electrónicos ou mecânicos, incluindo fotocópias, gravação, ou qualquer sistema de arquivo de informação, sem a permissão por escrito de um representante autorizado de BitDefender. A inclusão de pequenas frases do texto em comparativas poderão ser feitas desde que seja feita a menção da fonte da frase em questão. O conteúdo não pode ser de forma alguma modificado.

Aviso e Renúncia. Este produto e a sua documentação estão protegidas por direitos de autor. A informação neste documento é apresentada numa base de "tal como é", sem qualquer garantia. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não serão responsabilizados por qualquer pessoa ou entidade com respeito a qualquer perda ou dano causado ou alegadamente causado directa ou indirectamente pela informação contida neste livro.

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

Marcas Registadas. Nomes de Marcas Registadas poderão aparecer neste livro. Todas as marcas registadas ou não registadas neste documento são da exclusiva propriedade dos seus respectivos proprietários.


bitdefender

Índice

Licença e garantia

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.

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

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

SOFTWARE APLICAÇÃO. Pode instalar e usar BitDefender, em tantos computadores quantos os abrangidos pelo número total de licenças de 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.

GERAL. Este acordo será regido pelas leis da Roménia e pela regulamentação e tratados internacionais de direitos de autor. A jurisdição e foro exclusivo em caso de

qualquer disputa que surja devido aos Termos desta Licença serão os tribunais da Roménia.

Preços, custos e taxas de uso do BitDefender estão sujeitas a alteração sem qualquer aviso prévio.

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 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, ou pelo Tel No: 0040-21-2330780 ou Fax:0040-21-2330763, e-mail address: office@bitdefender.com.

Prefácio

Este manual é dirigido a todos os utilizadores que escolheram **BitDefender Antivirus 2008** como a solução de segurança para os seus computadores pessoais. A informação apresentada neste manual não só é útil e acessível para as pessoas que percebam de computadores, como também é útil e acessível para todas as pessoas que sejam capazes de trabalhar com o sistema operativo Windows.

Este manual dá-lhe uma descrição completa do **BitDefender Antivirus 2008**, da Empresa e da equipa que o desenvolveu, e também irá guiá-lo através do processo de instalação, e explicar-lhe como o pode configurar. Irá ficar a saber como usar o **BitDefender Antivirus 2008**, como o actualizar, testar e personalizar. Em resumo, irá ficar a saber como tirar partido do melhor que o BitDefender tem para lhe oferecer.

Desejamos-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 abaixo.

Aparência	Descrição
`sample syntax`	Exemplos de sintaxe são impressos em caracteres `monospace`.
http://www.bitdefender.com	O link URL está a apontar para algum local externo, num servidor http ou ftp.
support@bitdefender.com	Endereços de e-mail são inseridos no texto para contactar a solicitar mais informação.
“Prefácio” (p. xi)	Este é um link interno, que aponta para uma área dentro do documento.
`filename`	Os ficheiros e as directorias são impressos usando a fonte `monospace`.
option	Todas as opções de produto são impressas usando caracteres a**cheio**.

Aparência	Descrição
`sample code listing`	A listagem de código é impressa com caracteres `monospace`.

1.2. Avisos

Os avisos encontram-se em notas de texto, marcadas graficamente, que lhe dão informação adicional respeitante 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, dá-lhe informação bastante importante.

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

2. A 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. Instruções passo a passo para a instalação do BitDefender numa estação de trabalho. Este é um manual bastante completo de instruções sobre como instalar e usar **BitDefender Antivirus 2008**. Começando pelos pré-requisitos necessários para uma instalação bem-sucedida, é guiado através de todo o processo de instalação. No final, o procedimento de desinstalação é-lhe descrito para o caso de necessitar de desinstalar o BitDefender.

Administração Básica. Descripção de administração básica e manutenção do BitDefender.

Administração de Segurança Avançada. Uma apresentação detalhada das capacidades de segurança fornecida pela BitDefender. Os capítulos explicam em detalhe todas as opções da consola de definições avançadas. É-lhe ensinado como

configurar e usar todos os módulos do BitDefender de forma a proteger eficientemente o seu computador contra todo o tipo de ameças de malware (vírus, spyware, rootkits e por aí fora).

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

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

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 verificámos e testámos 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 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

1. Instalação de BitDefender Antivirus 2008

A secção de **Instalação de BitDefender Antivírus 10** deste guia do utilizador contém os seguintes tópicos:

- Requisitos do Sistema
- Passos da instalação
- Assistente Inicial de Instalação
- Actualização
- Reparar ou Remover o BitDefender

1.1. Requisitos do Sistema

Para um funcionamento correcto do produto, antes de instalar verifique que um dos seguintes sistemas operativos estão a ser executados no seu computador e que os correspondentes requisitos do sistema estão presentes:

- Sistema Operativo: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (ou superior)

Windows 2000

- Processador 800 MHz ou superior
- Mínimo 256 MB de Memória RAM (512 MB recomendado)
- Mínimo 60 MB de espaço disponível em disco

Windows XP

- Processador 800 MHz ou superior
- Mínimo 512 MB de Memória RAM (1 GB recomendado)
- Mínimo 60 MB de espaço disponível em disco

Windows Vista

- Processador 800 MHz ou superior
- Mínimo 512 MB de Memória RAM (1 GB recomendado)
- Mínimo 60 MB de espaço disponível em disco

BitDefender Antivirus 2008 pode ser descarregado para avaliação a partir do site da BitDefender em Portugal: http://www.bitdefender.com.

1.2. Passos da Instalação

Localize o ficheiro de instalação (setup) e clique nele duas vezes com o rato. Isto lançará o assistente que o irá guiar através do processo de instalação:

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

Passos da Instalação

Siga estes passos para instalar o BitDefender Antivirus 2008:

1. Clique em **Seguinte** para continuar ou clique em **Cancelar** se pretende desistir da instalação.
2. Clique em **Seguinte**.

BitDefender Antivirus 2008 avisa-o em caso de ter outros produtos antivírus instalados 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.

3. Por favor leia o Acordo de Licença, seleccione **Eu aceito os termos do Acordo de Licença** e clique em **Seguinte**. Se não concordar com estes termos clique em **Cancelar**. O processo de instalação será cancelado e terminará.
4. Por defeito, BitDefender Antivirus 2008 será instalado em `C:\Programas\Softwin\BitDefender 2008`. Se deseja alterar este cominho de instalação, clique em **Explorar** e seleccione a pasta na qual pretende que o BitDefender seja instalado.

   Clique em **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 final da instalação.
   - **Colocar um atalho no ambiente de trabalho** - para colocar um atalho do BitDefender 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.
   - **Desligar o Windows Defender** - para desligar o Windows Defender; esta opção apenas surge no Windows Vista.

   Clique em **Instalar** de forma a iniciar a instalação do produto.

Importante
Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu**BitDefender Antivirus 2008**, a criar uma conta BitDefender e a configurar o BitDefender para executar tarefas de segurança importantes.
Complete o processo guiado pelo assistente de forma a seguir para o próximo passo.

6. 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.

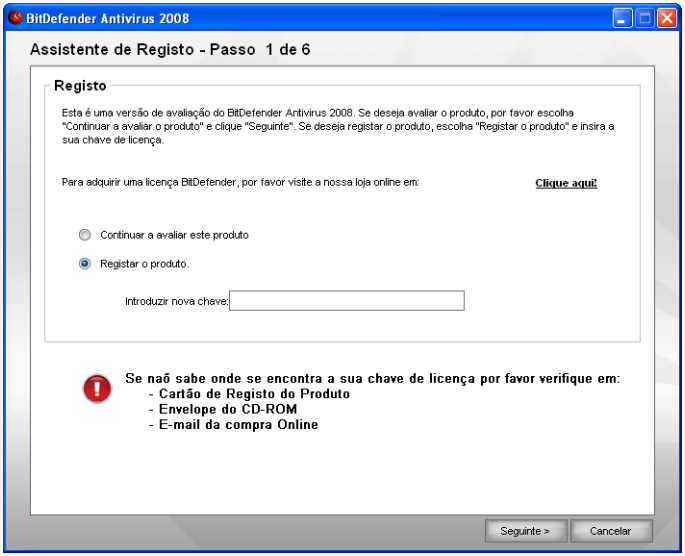
Se aceitou as definições por defeito do caminho da instalação, poderá ver uma pasta com o nome `BitDefender` nos `Programas` que contém a subpasta `BitDefender 2008`.

1.3. Assistente Inicial de Instalação

Durante o processo de instalação um assistente irá aparecer. esse assistente irá ajudá-lo a registar o seu**BitDefender Antivirus 2008**, a criar uma conta BitDefender e a configurar o BitDefender para executar tarefas de segurança importantes.

Completar a acção do assistente não é obrigatória; no entanto, recomendamos que o faça de forma a poupar tempo e a assegurar que o seu sistema fica seguro ainda antes de BitDefender Antivirus 2008 estar instalado.

1.3.1. Passo 1/6 - Registar BitDefender Antivirus 2008.



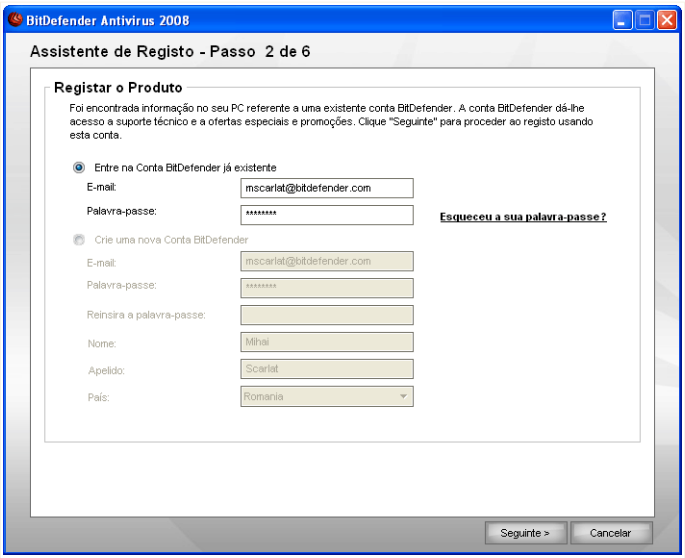
Registo

Escolha **Registar o produto** para registar **BitDefender Antivirus 2008**. Insira a chave de licença no campo**Introduzir nova chave**.

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

Clique em **Seguinte**.

1.3.2. Passo 2/6 - Criar uma conta BitDefender



Criar uma Conta

Não tenho uma conta BitDefender

De forma a beneficiar do suporte técnico gratuíto BitDefender e outros serviços gratuítos necessita de criar uma conta.

Nota
Se deseja criar uma conta mais tarde, selecciona a devida opção.

Para criar uma conta BitDefender seleccione**Criar uma nova conta BitDefender** e forneça a devida informação. Os dados que nos fornecer serão mantidos confidenciais.

- **E-mail** - insira o seu endereço de e-mail.

- **Palavra-passe** - introduza uma palavra-passe para a sua conta BitDefender.

  Nota
  A palavra-passe deve ter pelo menos quatro caracteres em tamanho.

- **Reinsira a palavra-passe** - introduza novamente a palavra-passe que previamente definiu.
- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - seleccione o país em que reside.

Nota
Use o endereço de e-mail e a palavra-passe que forneceu para fazer log à sua conta em http://myaccount.bitdefender.com.

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

Clique em **Seguinte** para continuar.

Já tenho uma conta BitDefender

BitDefender detectará automaticamente se já possui uma conta BitDefender previamente registada no seu computador. Nesse caso, tudo o que tem de fazer é clicar em **Seguinte**.

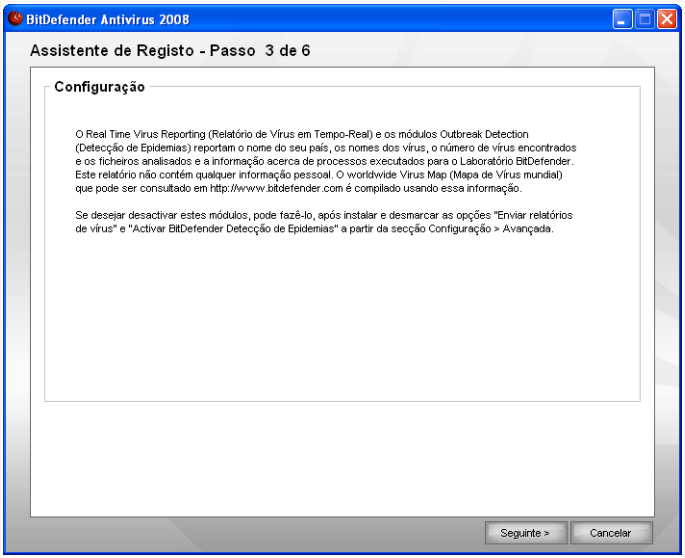
Se já possui uma conta activa, mas o BitDefender não a detecta, seleccione**Entrar numa conta BitDefender existente** e forneça o endereço de e-mail e a palavra-passe da sua conta.

Nota
Se forneceu a palavra-passe incorrecta, será notificado para a re-inserir quando clicar em **Seguinte**. Clique em **OK** para inserir a apalavra-passe novamente ou **Cancelar** para sair do assistente.

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

Clique em **Seguinte** para continuar.

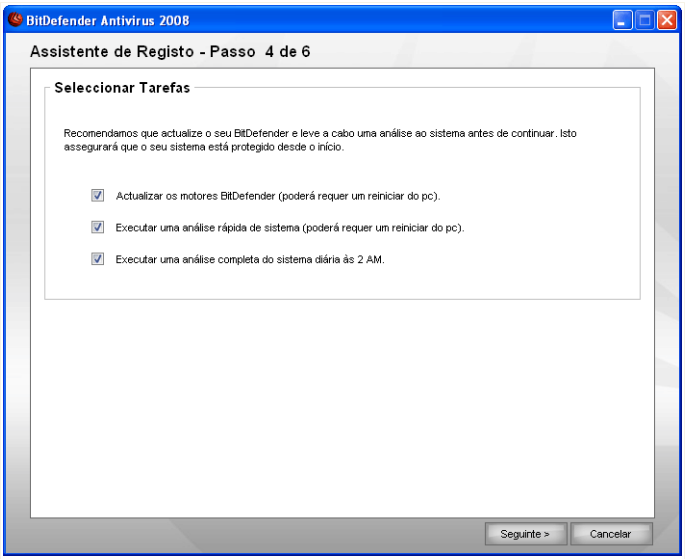
1.3.3. Passo 3/6 - Saber mais acerca de RVTR (Relatório de Vírus em Tempo Real)



Informação de RVTR

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

1.3.4. Passo 4/6 - Seleccionar as Tarefas a Serem Executadas



Selecção das Tarefas

Preparar BitDefender Antivirus 2008 para levar a cabo tarefas importantes para a segurança do seu sistema.

Estão disponíveis as seguintes opções:

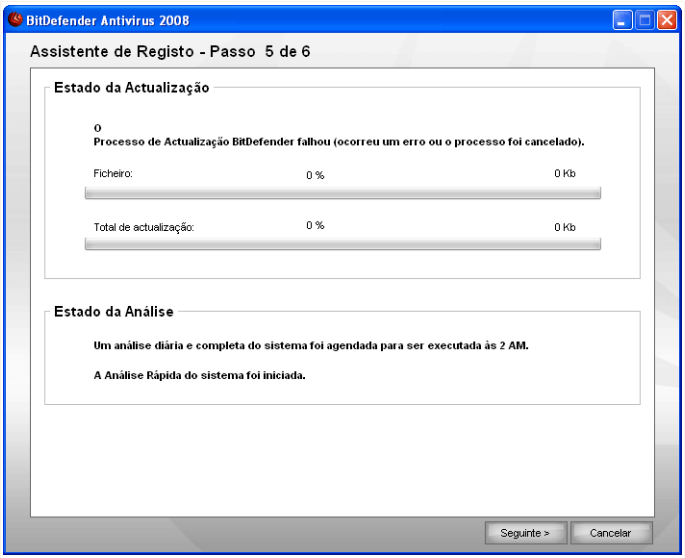
- **Actualizar os motores BitDefender (poderá ser necessário reiniciar)** - durante o próximo passo, será efectuada a actualização dos motores BitDefender de forma a proteger o seu computador contra as ameaças mais recentes.
- **Executar uma análise rápida do sistema (poderá ser necessário reiniciar)**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

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

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

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

1.3.5. Passo 5/6 - Esperar que as Tarefas Terminem

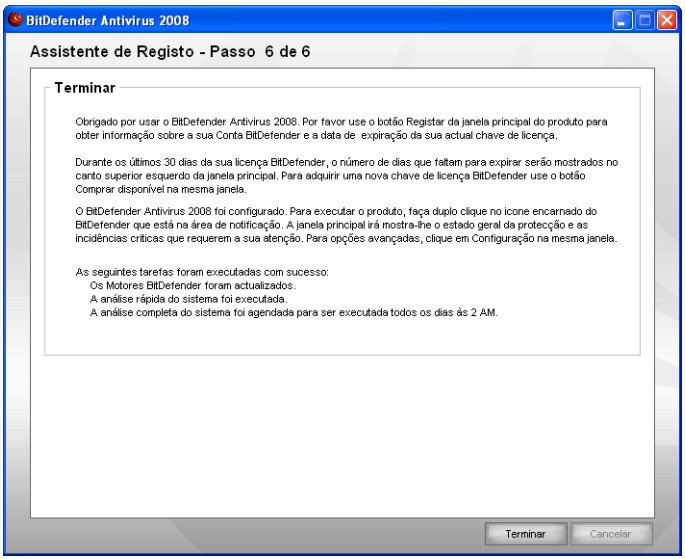


Estado das Tarefas

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

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

1.3.6. Passo 6/6 - Ver Resumo



Terminar

Este é o passo final do assistente de configuração.

Clique em **Terminar** para completar a acção do assistente e continuar com o processo de instalação.

1.4. Upgrade (Mudança de versão)

O procedimento de upgrade (mudança de versão) pode ser feito de uma das seguintes formas:

- **Instalar sem remover a versão anterior – para a v8 ou superior, excepto o Internet Security**

  Faça duplo-clique no ficheiro de instalação e siga o assistente descrito na secção "*Passos da Instalação*" (p. 3).

Importante
Durante o processo de instalação uma mensagem de erro causada pelo `serviço Filespy`, irá aparecer. Clique em **OK** para continuar com a instalação.

- **Desinstale a sua anterior versão e instale a nova – para todas as versões BitDefender**

  Em primeiro, lugar tem de remover a anterior versão, reiniciar o computador e instalar a nova versão tal como descrito na secção "*Passos da Instalação*" (p. 3).

Importante
Se está a mudar de versão a partir de BitDefender v8 ou superior, recomendamos que guarde a configuração BitDefender, a lista de Amigos e a lista de Spammers. Após o processo de mudança de versão estar concluído, poderá carregá-las.

1.5. Remover ou Reparar o BitDefender

Se pretende reparar ou remover o **BitDefender Antivirus 2008**, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar** → **Programas** → **BitDefender 2008** → **Reparar ou Desinstalar**.

Irá ser-lhe pedido para confirmar a sua opção ao clicar em **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 avisado para tal e, depois, clique em **Instalar** para reinstalar o BitDefender Antivirus 2008.

  Uma vez terminado o processo de intalação, surgirá uma nova janela. Clique em **Terminar**.
- **Remover** - para remover todos os componentes instalados.

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

Se escolher desinstalar BitDefender, surgirá uma nova janela.

Importante

Ao remover BitDefender, deixará de estar protegido contra as ameaças de malware, tais como vírus e spyware. Se deseja que o WIndows Defender seja activado após a desinstalação do BitDefender, seleccione a respectiva caixa de selecção. Esta opção só está disponível no Windows Vista.

Clique em **Desinstalar** para dar início à desinstalação do BitDefender Antivirus 2008 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`.

Ocorreu um erro ao desinstalar o BitDefender

Se ocorrer um erro ao desinstalar o BitDefender, o processo de desinstalção será cancelado e surgirá uma nova janela. Clique **Desinstalar** para se certificar que o BitDefender foi removido completamente. A Ferramenta de Desinstalação removerá todos os ficheiros e chaves de registo que não tenham sido removidos durante o processo de desinstalação automática.

Administração Básica

2. Introdução

Uma vez que tenha instalado BitDefender o seu computador fica protegido. Pode abrir o Centro de Segurança BitDefender e verificar o estado de segurança do sistema, tomar medidas preventivas ou configurar o produto na sua totalidade em qualquer altura.

Para aceder ao Centro de Segurança BitDefender, utilize o menu do Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2008** → **BitDefender Antivirus 2008** ou mais rapidamente, fazendo duplo-clique no **ícone BitDefender** na Área de notificação.

Centro de Segurança BitDefender

O Centro de Segurança BitDefender contém duas áreas:

- O **Estado** da área: contém informaçãoe ajuda-o a reparar as vulnerabilidades de segurança do seu computador. Pode facilmente ver quantas incidências poderão estar a afectar o seu computador. Ao clicar no botão vermelho correspondente a **Reparar Todas Incidências** as vulnerabilidades do seu computador serão resolvidas

na hora ou será orientado no sentido de as resolver facilmente. Ao mesmo tempo, quatro botões de estado correspondentes a quatro categorias de segurança estão disponíveis. Botões de estado verdes indicam que não há risco. Botões amarelos ou vermelhos indicam risco de segurança médios ou elevados. Para os reparar, clique no botão amarelo/vermelho, e depois nos botões **Reparar**, uma a um ou no botão **Reparar tudo agora**. Cinzento indica um componente não configurado.

- A área de **Tarefas Rápidas**: ajuda-o a manter o seu sistema seguro e os seus dados protegidos.

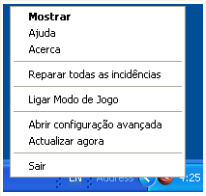
E mais ainda, o Centro de Segurança BitDefender contém diversos atalhos úteis.

Link	*Descrição*
Comprar	Abre uma página web de onde pode comprar o produto.
Minha Conta	Abrir a página da sua conta BitDefender.
Registar	Abrir o assistente de registo.
Ajuda	Abre o ficheiro de ajuda.
Suporte	Abre a página web do suporte BitDefender.
Configuração	Abre a consola de configuração avançada.
Histórico	Abre uma janela com o histórico BitDefender & eventos.

2.1. Ícone BitDefender na Área de Notificação

Para gerir todo o produto mais rapidamente, pode também usar o icone BitDefender na Área de Notificação.

Se fizer duplo-clique neste ícone, o Centro de Segurança 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:



Icone BitDefender

- **Mostrar** - abre o o Centro de Segurança BitDefender.
- **Ajuda**- abre o ficheiro de ajuda.
- **Acerca** - abre a página web do BitDefender.
- **Reparar todos incidências** - ajuda-o a removeras vulnerabilidades de segurança.
- **Ligar / desligar Modo de Jogo** - Liga/desliga Modo de Jogo .
- **Abrir Configuração Avançada** dá-lhe acesso à consola de configuração avançada.

- **Actualizar agora** - executa uma actualização imediata. Surge uma nova janela, onde pode ver o estado da actualização.
- **Sair** - desliga a aplicação.

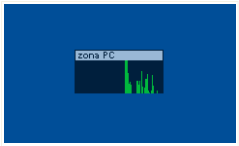
Sempre que o Modo de Jogo está ligado, pode ver a letra G sobre o ícone BitDefender.

Se existem incidências criticas que afectam a segurança do seu sistema, um ponto de exclamação é mostrado por cima do ícone do BitDefender. Pode passar com o rato por cima do icone para ver o número de incidências que estão a afectar a segurança do seu sistema.

2.2. Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade da análise no seu sistema.

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



Barra de Actividade

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

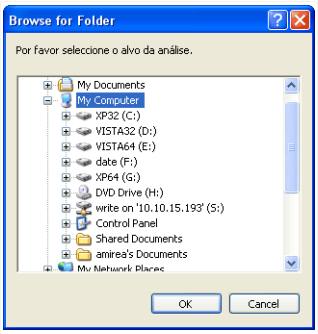
Pode usar a **Barra de Actividade da Análise** para analisar objectos. Apenas arraste os objectos que deseja analisar para cima dela. Para mais informação, por favor consulte o "*Análise por Drag&Drop*" (p. 67).

Quando quiser deixar de ver o gráfico de visualização, faça clique com o botão direito do rato sobre ele e seleccione **Esconder**.

2.3. Análise Manual BitDefender

Se deseja analisar rapidamente uma determinada pasta, pode usar a Análise Manual BitDefender.

Para aceder à Análise Manual BitDefender, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar → Programas → BitDefender 2008 → Análise Manual BitDefender**. A seguinte análise irá aparecer:



Análise Manual BitDefender

Tudo o que tem de fazer é explorar as pastas, seleccionar a que deseja analisar e clicar **OK**. O Analisador BitDefender irá surgir e guiá-lo através do processo de análise.

2.4. Modo de Jogo

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

- Todos os alertas e pop-ups do BitDefender são desactivados.
- O nível da protecção em tempo-real do BitDefender é definida como **Permissivo**.

Sempre que o Modo de Jogo está ligado, pode ver a letra `G` sobre o ícone BitDefender.

2.4.1. Usar o Modo de Jogo

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

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

2.4.2. Mudar a Hotkey do Modo de Jogo

Se deseja mudar a hotkey, siga estes passos:

1. Clique em **Configuração** - no Centro de Segurança BitDefender para abrir a consola de configuração.

   Nota
   Pode clicar com o botão direito do rato no ícone do BitDefender que está na área de notificação e seleccione **Configuração Avançadas**.

2. Clique em **Avançada**.
3. Por baixo da opção **Activar HotKey do Modo de Jogo** , 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 para o Modo de Jogo** irá desactivar a hotkey.

3. Estado de Segurança

O estado de segurança mostra uma lista sistematicamente organizada e facilmente gerida de vulnerabilidades de segurança no seu computador. BitDefender Antivirus 2008 informa-lo-á sempre que surja um problema que possa afectar a segurança do seu computador.

Existem quatro botões de estados de segurança:

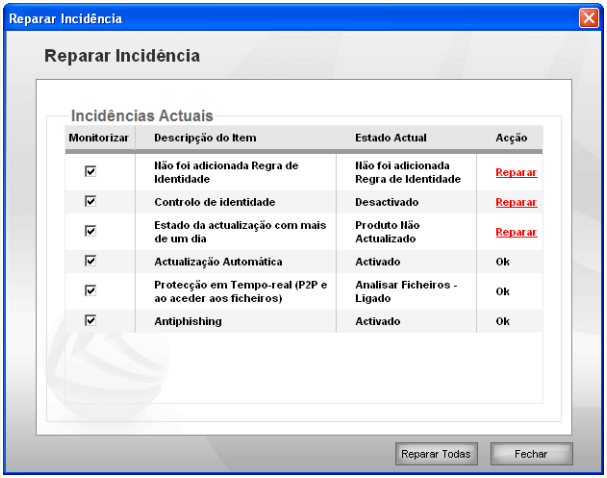
- **ANTIVIRUS**
- **ANTIPHISHING**
- **CONTROLO DE IDENTIDADE**
- **ACTUALIZAÇÃO**

Ao mesmo tempo, à esquerda pode ver o número de incidências que estão a afectar a segurança do seu sistema e um botão vermelho para**Reparar Todas Incidências**.

Os quatro botões de estado, podem estar a verde, amarelo, vermelho ou cinzento, dependendo do actual nível de protecção.

- **Verde** indica um baixo risco de segurança para o seu computador.
- **Amarelo** indica um médio risco de segurança para o seu computador.
- **Vermelho** indica um elevado risco de segurança para o seu computador.
- **Cinzento** indica um componente não-configurado.

Reparar os problemas de segurança não requer qualquer esforço e pode ser feito com um simples click em **Reparar Todas Incidências**. Uma nova janela irá aparecer.



Incidências de Segurança

Verá uma lista das incidências de segurança e uma pequena descripção do seu estado.

Para reparar apena uma incidência em particular clique no botão correspondente **Reparar**. Será resolvida logo aí ou seguindo os passos de um assistente. Se decidir repará-los a todos, clique no botão **Reparar Todas Agora** e siga o assistente correspondente.

Se necessita de ajuda adicional, clique no botão **Mais Ajuda**, localizado no fundo da janela. Uma página de ajuda contextual é mostrada dando-lhe mais informação detalhada sobre as incidências e a forma de as reparar.

Importante

Para cada incidência, existe uma caixa de selecção, activada por defeito. Se não deseja que uma determinada incidência seja tomada em consideração quando é calculado o risco de segurança, limpe a correspondente caixa de selecção. Por favor use esta opção com cuidado, porque é muito fácil aumentar o risco de segurança a que o seu computador está exposto.

Para reparar as incidências mais tarde, clique **Fechar**.

3.1. Botão de Estado Antivírus

Se o botão de estado antivírus estiver verde, não há nada com que se preocupar. Por outro lado, se o botão estiver amarelo, vermelho ou cinzento, existe um risco médio ou elevado de segurança ao qual o seu computador está exposto.

A cor dos botões de estado podem mudar não só quando você configura as definições que poderão afectar a segurança do seu computador, mas também quando se esquece de fazer tarefas importantes. Por exemplo, se a última análise ao sistema for antiga, o botão de estado de segurança ficará amarelo. Se for muita antiga, ficará vermelho.

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	*Cor*
A última análise ao sistema é antiga	Amarelo
A última análise ao sistema é muito antiga	Vermelho
A protecção em tempo-real está desactivada	Vermelho
O nível da protecção antivírus foi definido como permissivo	Amarelo

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado do antivírus.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

3.2. Botão de Estado Antiphising

Se o botão de estado do antiphising estiver verde, não há razão de preocupação. Por outro lado, se o botão estiver vermelho, existe um risco elevado de segurança a que o seu computador está exposto

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	Cor
A protecção antiphising está activada	Verde
A protecção antiphising está desactivada	Vermelho

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado do antiphising.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

3.3. Botão de Estado do Controlo de Identidade

Se o botão de estado do controlo de identidade estiver verde, não há razão de preocupação. Por outro lado, se o botão estiver vermelho ou cinzento, existe um risco elevado de segurança a que o seu computador está exposto.

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	Cor
A protecção de privacidade está definida e LIGADA	Verde
A protecção de privacidade está definida e DESLIGADA	Vermelho
A protecção de privacidade não está definida	Cinzento

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado do Controlo de Identidade.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

3.4. Botão de Estado da Actualização

Se o botão de estado da actualização estiver verde, não há razão de preocupação. Por outro lado, se o botão estiver vermelho, existe um risco elevado de segurança a que o seu computador está exposto

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	*Cor*
A actualização automática está activada	Verde
A actualização automática está desactivada	Vermelho
A última actualização tem um dia	Vermelho

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado da actualização.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

4. Tarefas Rápidas

Por debaixo dos quatro botões de estado está a área de **Tarefas Rápidas**.

4.1. 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**.

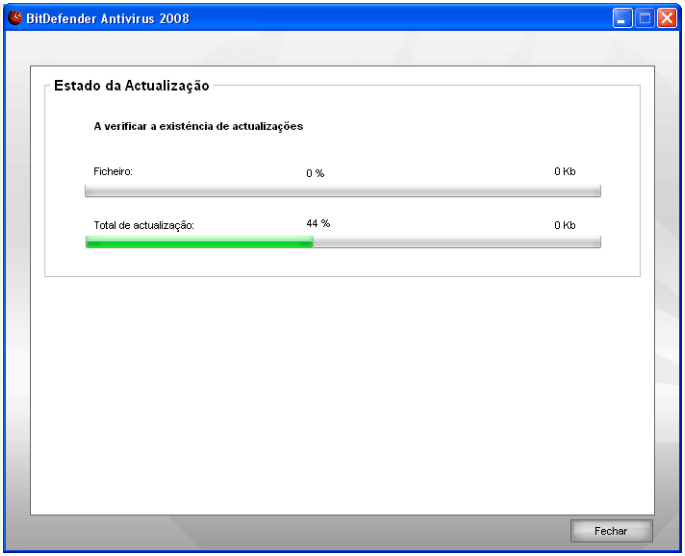
Estão disponíveis os seguintes botões:

- **Actualizar agora** - executa uma actualização imediata.
- **Analisar os Meus Documentos** - inicia uma análise rápida à sua pasta Documents and Settings.
- **Análise Minuciosa do Sistema** - inicia uma análise minuciosa ao seu computador.
- **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.

4.1.1. 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 **Fechar**. 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 requerido. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador: Se não deseja ser mais notificado novamente quando uma actualização necessitar de reiniciar o seu pc, seleccione **Esperar pelo reiniciar, em vez de me avisarem**. Desta forma, da próxima vez que uma actualização necessitar de reiniciar o pc, o produto continuará a funcionar com os ficheiros antigos até que reinicie o seu sistema.

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.

4.1.2. A analisar com BitDefender

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

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

Nota

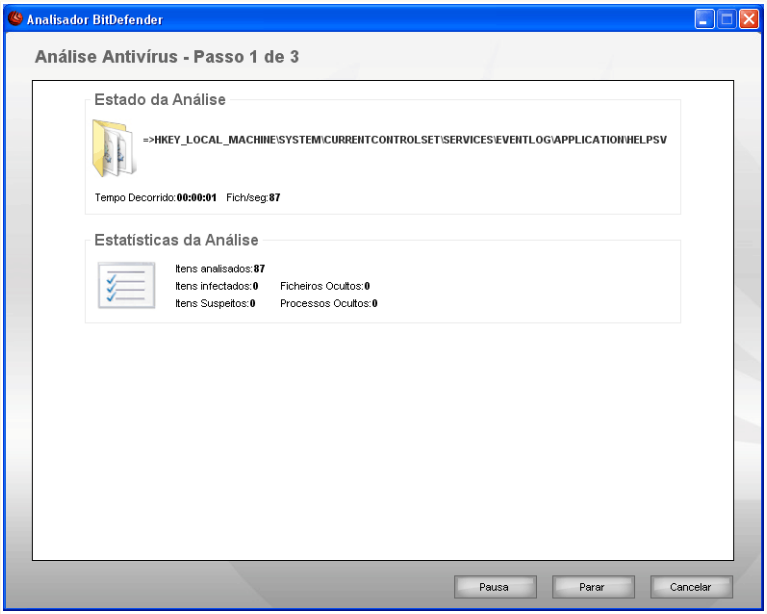
Um vez que as atrefas **Análise Minuciosa do Sistema** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inactivo.

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

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

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

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

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

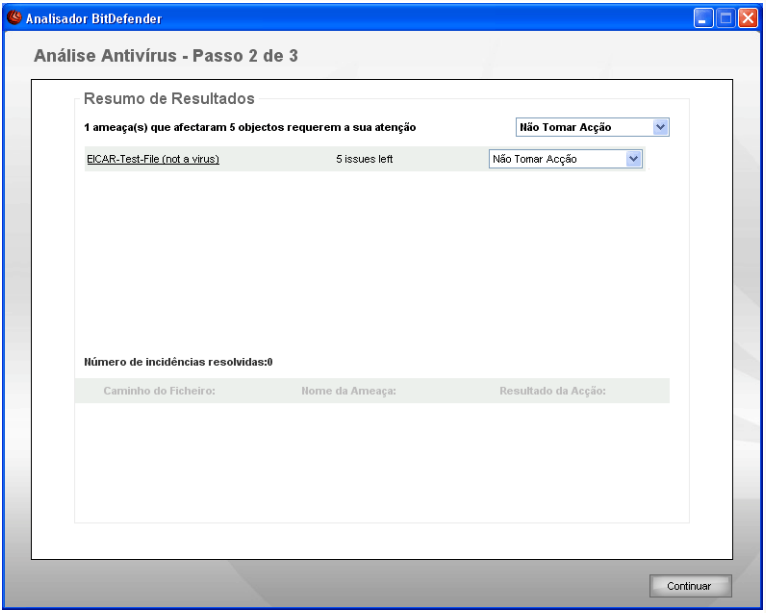
Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

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

Espere que o BitDefender termine a análise.

Passo 2/3 - Seleccionar as acções

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



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 tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.

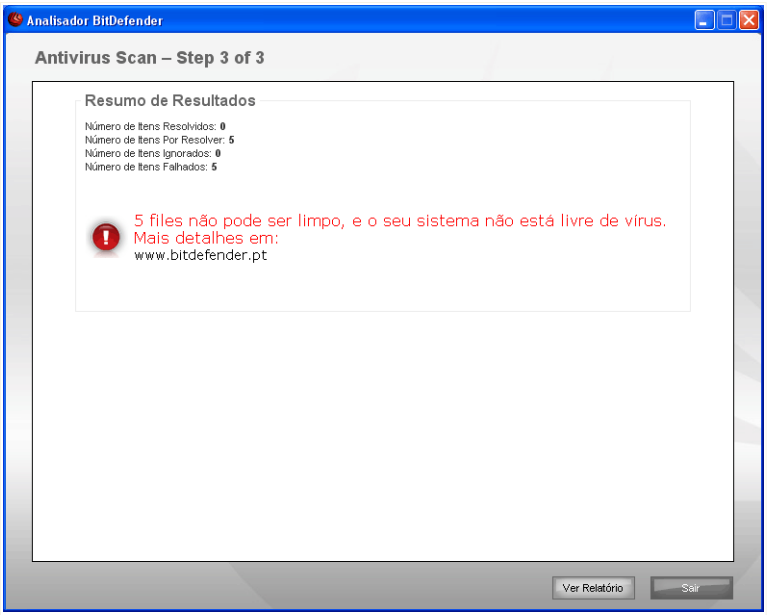
As seguintes opções podem aparecer no menu:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros detectados.
Desinfectar	Desinfecta os ficheiros infectados.
Apagar	Apaga os ficheiros detectados.
Desocultar	Torna visíveis objectos ocultos.

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

Passo 3/3 - Ver Resultados

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



Resumo

Pode ver o resumo dos resultados. O ficheiro do relatório é guardado automaticamente na secção de Logs a partir da janela **Propriedades** da respectiva tarefa.

Importante
Ser-lhe-á solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação.

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

BitDefender Não pode Resolver Algumas Incidências

Na maioria dos casos BitDefender desinfecta com sucesso os ficheiros infectados ou isola a infecção. No entanto, há incidências que não podem ser resolvidas.

Se existirem incidências não resolvidas, recomendamos que contacte o Suporte Técnico BitDefender em www.bitdefender.pt. O nosso suporte técnico ajuda-lo-á a resover as incidências que está a experimentar.

BitDefender Detectou Itens protegidos por Palavra-passe

A categoria de protegidos por palavra-passe inclui dois tipos de itens: arquivos e instaladores. Eles não representam uma verdadeira ameça à segurança do sistema a não ser que contenham ficheiros infectados e apenas quando são executados.

Para ter a certeza de que estes itens estão limpos:

- Se o item protegido por palavra-passe for um arquivo que protegeu com uma palavra-passe, extraia os ficheiros do mesmo e analise-os separadamente. A forma mais fácil de os analisar é clique botão-direito do rato sobre eles e seleccionar **BitDefender Antivirus 2008** a partir do menu.
- Se o item protegido por palavra-passe for um instalador, certifique-se que a protecção em tempo-real está activa antes de executar esse mesmo instalador. Se o instalador estiver infectado, o BitDefender detectará a situação e isolará a infecção.

Se não deseja que estes objectos sejam detectados novamente pelo BitDefender tem de os adiconar como excepções ao processo de análise. Para adicionar excepções à análise, clique em, **Definições** para abrir a consola das configurações e depois vá para **Antivírus > Excepções** . Para mais informação, consulteObjectos Excluídos da Análise

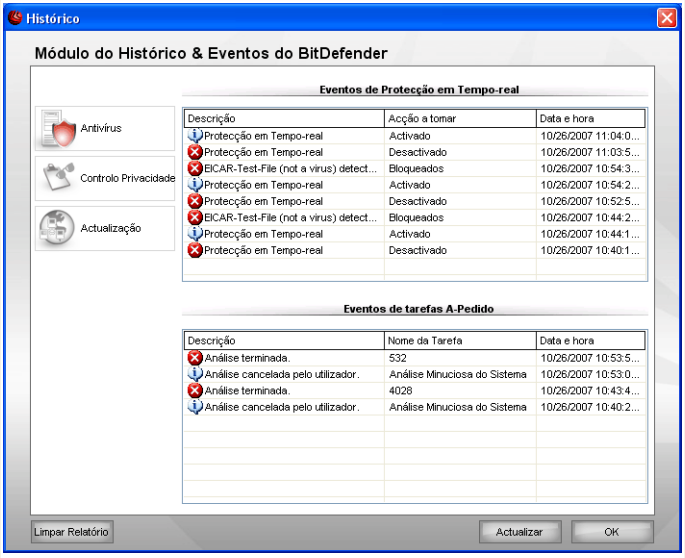
BitDefender Detectou Ficheiros Suspeitos

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 uma análise mais avançada no laboratório do BitDefender.

5. Histórico

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



Eventos

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

- **Antivírus**
- **Controlo Privacidade**
- **Actualização**

Uma lista de eventos está disponível para cada categoria. Cada evento vem com a seguinte informação: uma breve descripção, a acção que o BitDefender tomou e

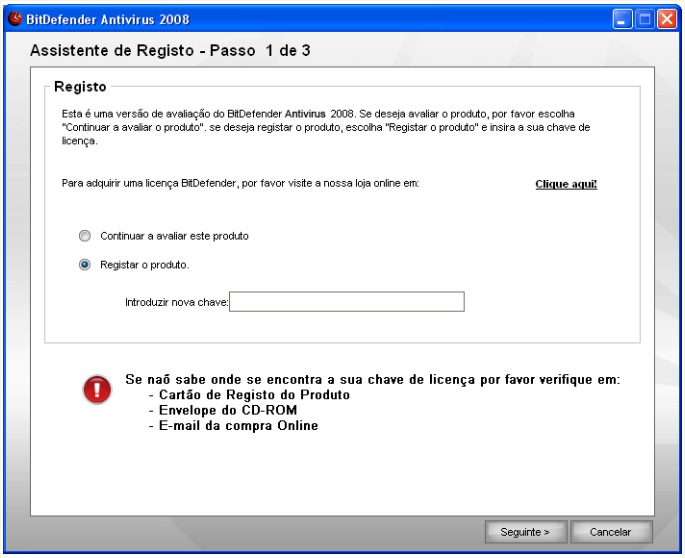
quando aconteceu, e a data e hora em que ocorreu. Se deseja saber mais informação acerca de um evento em particular da lista, faça duplo clique sobre esse evento.

Clique em **Limpar Log** se deseja remover antigos logs ou **Actualizar** para se certificar que os logs mais recentes são mostrados.

6. Registo

BitDefender Antivirus 2008 funciona durante 30 dias em modo de avaliação. Se deseja registar o BitDefender Antivirus 2008, mudar a chave de licença ou criar uma conta BitDefender, clique no link **Registar**, localizado no topo da janela do Centro de Segurança BitDefender. O assistente de registo irá aparecer.

6.1. Passo 1/3 - Registar BitDefender Antivirus 2008.



Registo

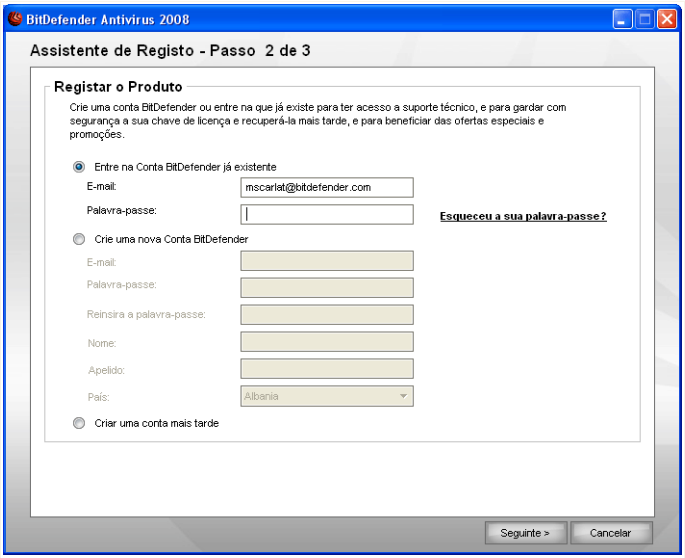
Se não possui uma licença BitDefender, clique no link fornecido para ir para a loja on-line da BitDefender e adquirir uma chave de licença.

Para registar o BitDefender Antivirus 2008, escolha **Registar o produto** e insira a chave de licença no campo**Introduzir nova chave**.

Se o período de avaliação ainda não terminou e deseja continuar a avaliar o produto, seleccione **Continuar a avaliar o produto**.

Clique em **Seguinte** para continuar.

6.2. Passo 2/3 - Criar uma conta BitDefender



Criar uma Conta

Não tenho uma conta BitDefender

De forma a beneficiar do suporte técnico gratuíto BitDefender e outros serviços gratuítos necessita de criar uma conta.

Nota
Se deseja criar uma conta mais tarde, selecciona a devida opção.

Para criar uma conta BitDefender seleccione**Criar uma nova conta BitDefender** e forneça a devida informação. Os dados que nos fornecer serão mantidos confidenciais.

- **E-mail** - insira o seu endereço de e-mail.
- **Palavra-passe** - introduza uma palavra-passe para a sua conta BitDefender.

Nota
A palavra-passe deve ter pelo menos quatro caracteres em tamanho.

- **Reinsira a palavra-passe** - introduza novamente a palavra-passe que previamente definiu.
- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - seleccione o país em que reside.

Nota
Use o endereço de e-mail e a palavra-passe que forneceu para fazer log à sua conta em http://myaccount.bitdefender.com.

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

Clique em **Seguinte** para continuar.

Já tenho uma conta BitDefender

BitDefender detectará automaticamente se já possui uma conta BitDefender previamente registada no seu computador. Nesse caso, tudo o que tem de fazer é clicar em **Seguinte**.

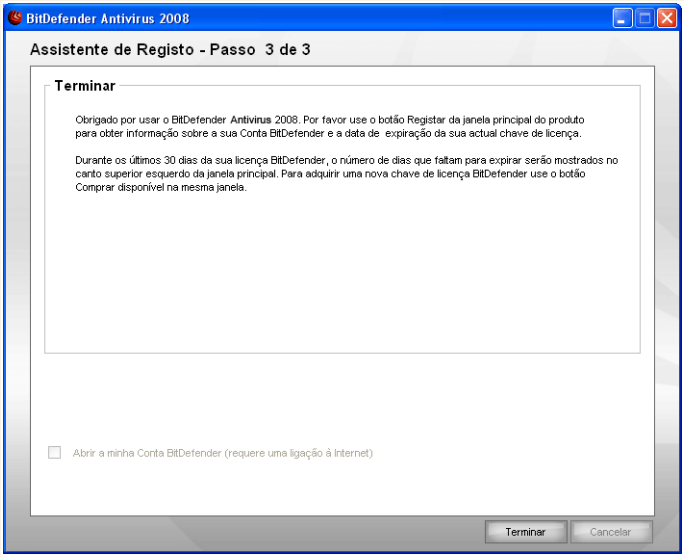
Se já possui uma conta activa, mas o BitDefender não a detecta, seleccione**Entrar numa conta BitDefender existente** e forneça o endereço de e-mail e a palavra-passe da sua conta.

Nota
Se forneceu a palavra-passe incorrecta, será notificado para a re-inserir quando clicar em **Seguinte**. Clique em **OK** para inserir a apalavra-passe novamente ou **Cancelar** para sair do assistente.

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

Clique em **Seguinte** para continuar.

6.3. Passo 3/3 - Registar BitDefender Antivirus 2008.



Resumo

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

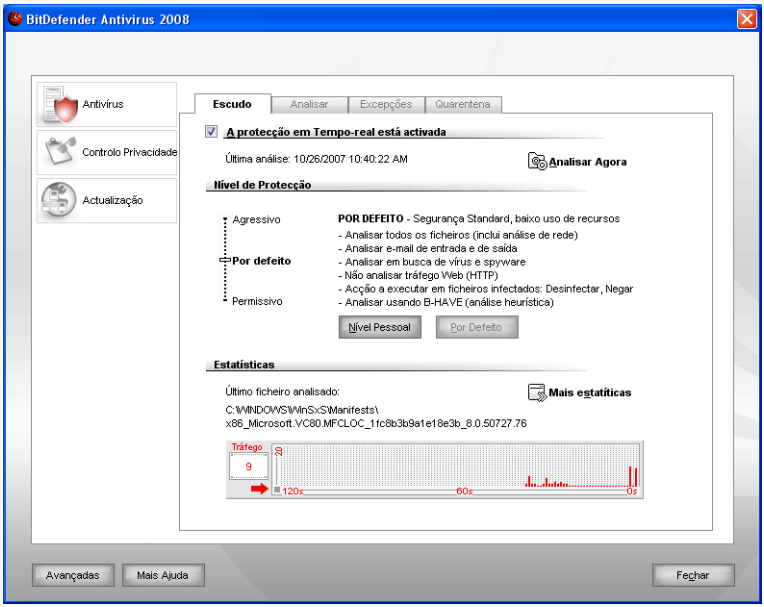
Clique em **Terminar** para fechar a janela.

Administração de Segurança Avançada

7. Consola de Configuração

BitDefender Antivirus 2008 vem com uma consola de configuração centralizada, que permite uma administração e configuração avançada do BitDefender.

Para aceder à consola de configuração, clique no link **Configuração** , localizado no fundo do Centro de Segurança.



Consola de Configuração

A consola de configuração está organizada em dois módulos**Antivírus**, **Controlo Privacidade** e **Actualização**. Isto permite-lhe gerir facilmente o BitDefender baseado no tipo de incidência de segurança abordada.

Do lado esquerdo da consola de configuração, pode ver o seleccionador de módulos:

- Antivírus - nesta secção pode configurar o módulo do **Antivírus**.
- Controlo de Privacidade - nesta secção pode configurar o módulo do **Controlo Privacidadel**.

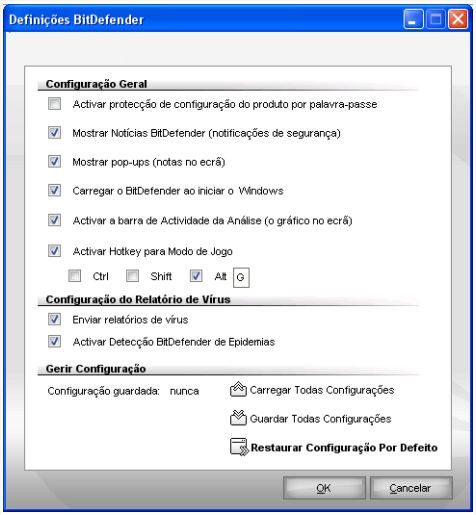
■ Actualização - nesta secção pode configurar o módulo da **Actualização**.

No fundo da consola de configurações, existe um botão de **Mais Ajuda** que abre uma página de ajuda contextual. Clique nesse botão para descobrir mais informação acerca da secção em que se encontra, sempre que necessitar de ajuda adicional.

Se necessita de ajuda adicional, clique no botão **Mais Ajuda**, localizado no fundo da janela. Uma página de ajuda contextual é mostrada e fornece-lhe mais informação detalhada acerca da secção onde se encontra.

7.1. Configurações Gerais

Para efectuar as configurações gerais no BitDefender Antivirus 2008 e gerir as suas definições, clique em **Avançada**. Uma nova janela irá aparecer.



Configurações Gerais

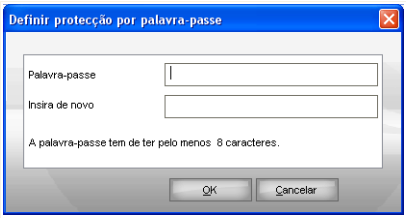
Aqui, pode definir o comportamento geral do BitDefender. Por defeito, o BitDefender é carregado ao iniciar o Windows e é executado minimizado na barra de tarefas.

7.1.1. Configurações Gerais

- **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:



Inserir a palavra-passe

Introduza a palavra-passe no campo **Palavra-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.

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

- **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.
- **Carregar o BitDefender ao iniciar o Windows** - executa automaticamente o BitDefender ao iniciar o sistema. Recomendamos que mantenha esta opção seleccionada.
- **Activar a barra de Actividade da Análise (gráfico no ecrã)** - mostra a Barra de Actividade da Análise sempre que entra no Windows. Limpe esta caixa de selecção se não deseja que a Barra de Actividade de Análise seja mostrada.

Nota
Esta opção só pode ser configurada apenas para o actual utilizador do Windows.

- **Activar Hotkey do Modo de Jogo** - permite usar uma combinação de teclas (hotkey) para activar / desactivar o Modo de Jogo. A hotkey por defeito é `Alt+G`.

  para modificar a hotkey, faça o seguinte:

  1. Seleccione as teclas de modificação que deseja usar apartir das seguintes: tecla Control (`Ctrl`), tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
  2. No campo de edição, insira a letra correspondente à tecla que deseja usar.

7.1.2. Configurações do Relatório de Vírus

- **Enviar relatórios de vírus** - envia relatórios de vírus que foram encontrados no seu computador para os Laboratórios do BitDefender. Ajuda-nos a rastrear as 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 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.

7.1.3. Configurações de Administração

Use os botões **Guardar todas as Configurações** / **Carregar todas as Configurações** para guardar/carregar as configurações que tenha feito ao BitDefender para/de um determinado sítio à sua escolha. Desta forma pode usar as mesmas configurações após reinstalar ou reparar o seu produto BitDefender.

Importante
Apenas os utilizadores com direitos de administrador podem guardar ou carregar configurações.

Para carregar as configurações por defeito, clique em **Restaurar Configurações por Defeito**.

8. Antivírus

BitDefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora).

Para além da análise clássica baseada nas assinaturas do malware, o BitDefender também executa uma análise heurística dos ficheiros. O objectivo da análise heurística é identificar novos vírus, baseado em certos padrões e algoritmos, antes de haver uma nova solução para o vírus. Poderão aparecer falsas mensagens de alarme. Quando é detectado tal programa, este é classificado como suspeito. Nestes casos, recomendamos que envie o ficheiro para análise no laboratório BitDefender.

A protecção que BitDefender oferece está dividida em duas categorias:

- **Análise no-acesso** - previne que novas ameaças de malware entrem no sistema. Isto também é chamado de protecção em tempo-real - os ficheiros são analisados à medida que os usa - no-acesso. 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.
- **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.

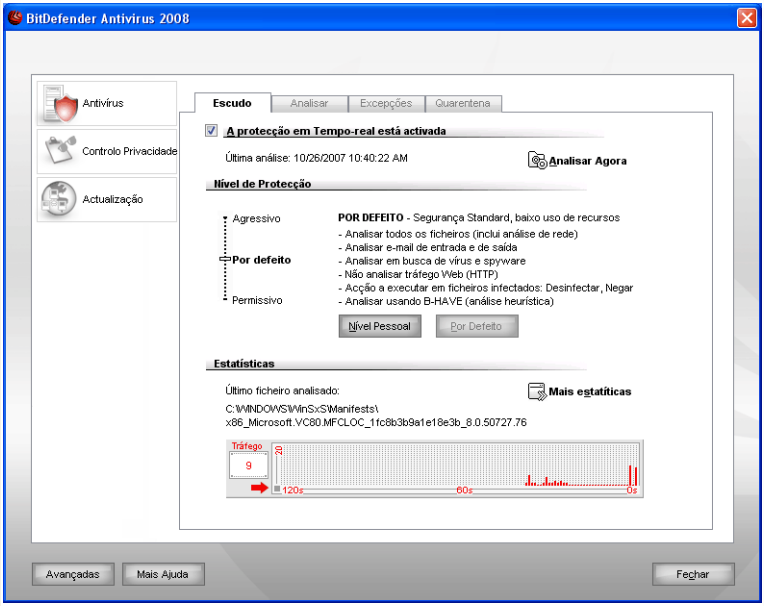
A secção do **Antivírus** deste manual do utilizador contém os seguintes tópicos:

- Análise No-acesso
- Análise A-pedido
- Objectos Excluídos da Análise
- Quarentena

8.1. Análise No-acesso

Analisar ficheiros no -acesso, também conhecida como protecção em tempo-real, mantém o seu computador seguro de 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).

Para configurar e gerir a protecção em tempo-real clique em **Antivírus>Escudo** na consola de configuração. A seguinte análise irá aparecer:



Protecção em Tempo-real

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

Na parte inferior lateral desta secção pode ver as estatísticas da análise de ficheiros e mensagens de e-mail da **Protecção em Tempo-real**. Clique em **Mais estatísticas** se desejar ver uma janela mais detalhada destas estatísticas.

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

8.1.1. Configurar Nível de Protecção

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

Existem 3 níveis de protecção:

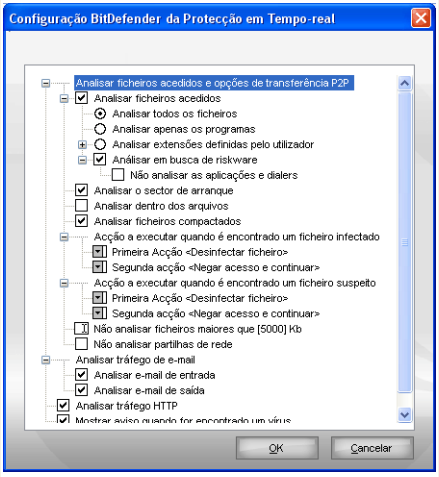
Nível de Protecção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Programas e mensagens de e-mail de entrada são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.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

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

8.1.2. 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 análise, 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.

- **Analisar ficheiros acedidos e opções de transferências P2P** - examina os ficheiros acedidos e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (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 os ficheiros de programas serão analisados. Isto significa, apenas os ficheiros com as seguintes extensões: `.exe`; `.bat`;

Opção		Descrição
		.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 as extensões especificadas pelo utilizador serão analisadas. 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 **Excluir da análise dialers e aplicações** se deseja excluir este tipo de ficheiros da análise.
Analisar o sector de arranque		Analisa o sector de arranque do sistema.
Analisar dentro dos arquivos		Os arquivos acedidos serão analisados. Com esta opção activa, o computador ficará mais lento.
Analisar ficheiros compactados		Todos os ficheiros compactados serão analisados.
Primeira Acção		Seleccionar do menu drop-down a primeira acção a levar a cabo sobre um ficheiro infectado ou suspeito.
	Negar acesso e continuar	Em caso de detecção de um ficheiro infectado, o acesso ao mesmo será negado.
	Limpar Ficheiro	Desinfecta os ficheiros infectados.
	Apagar Ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.

Opção		Descrição
	Mover ficheiro para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial.
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	Em caso de detecção de um ficheiro infectado, o acesso ao mesmo será negado.
	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.
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.
Não analisar partilhas de redes		Se esta opção estiver activada, BitDefender não irá analisar as partilhas de rede, permitindo um acesso de rede mais rápido. Recomendamos que active esta opção aeonas se a rede de que faz parte estiver protegida por uma solução antivírus.

- **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.

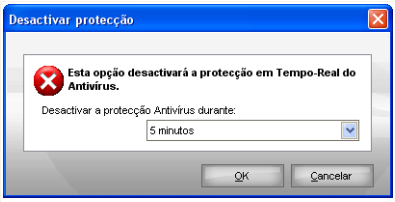
A janela de alerta de um ficheiro infectado, contém o nome e o caminho para o vírus, a acção levada a cabo pelo BitDefender e um link para o site do BitDefender onde poderá encontrar mais informação acerca dele. No caso de um e-mail infectado, a janela de alerta contém também informação acerca do remetente e do destinatário.

Em caso de ser detectado um ficheiro suspeito pode executar um assistente a partir da janela de alerta que o ajudará a enviar esse ficheiro para o Laboratório BitDefender para uma análise mais avançada. Pode inserir o seu endereço de e-mail para receber informação relativa a esse relatório.

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

8.1.3. Desactivando a Protecção em Tempo-real

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



Desactivar Protecção em Tempo-real

Deverá confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a sua protecção em tempo-real fique desactivada. Pode desactivar a sua protecção em tempo-real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças do malware.

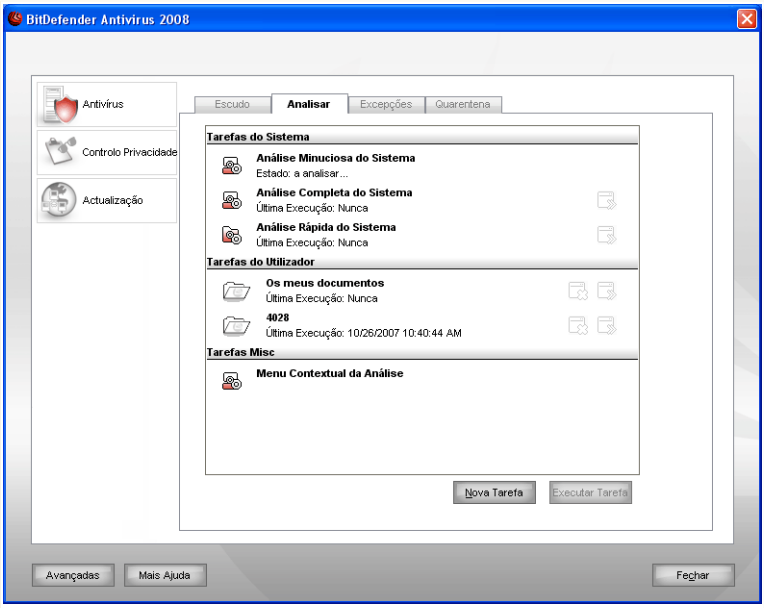
8.2. Análise A-pedido

O objectivo principal do BitDefender é manter o seu computador limpo de vírus. Isto é essencialmente feito ao manter os novos vírus fora do seu computador e ao analisar

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

Há o risco de um vírus já se encontrar alojado no seu sistema, mesmo antes de ter instalado o seu BitDefender. Este é o motivo pelo qual é uma excelente ideia analisar o seu computador em busca de vírus residentes depois de instalar o BitDefender. E é definitivamente uma boa ideia, analisar frequentemente o seu computador em busca de vírus.

Para configurar e iniciar uma análise a-pedido, clique **Antivírus>Análise** na consola de configuração. A seguinte análise irá aparecer:



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

8.2.1. 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. 55).

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 Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Rápida do Sistema	Analisa as pastas `Windows`, `Programas` e `All Users`. Na configuração por defeito, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.

Nota

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

- **Tarefas do 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.

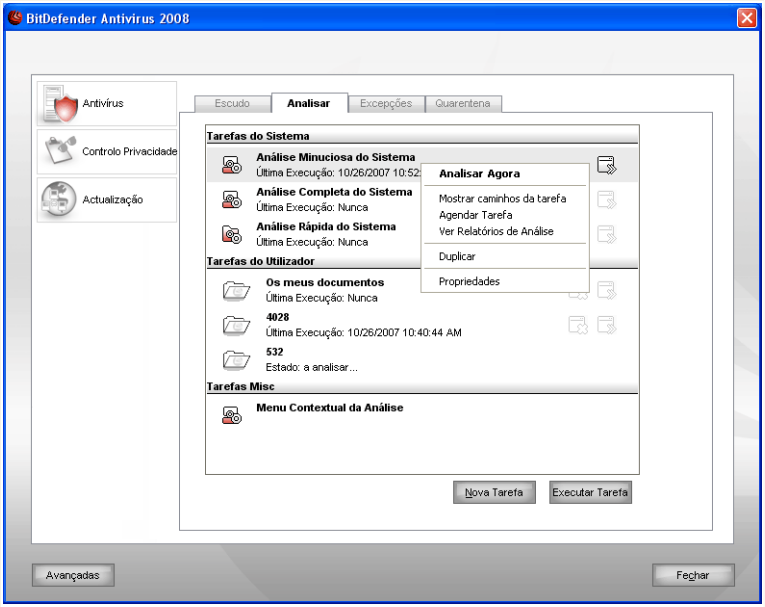
> ***Nota***
> Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **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.

8.2.2. Usando o Menú de Atalho

Um menú de atalho está



Menú de Atalho

disponível para cada tarefa. Clique com o botão direito do rato sobre a tarefa para a abrir.

Os seguintes comandos estão disponíveis no menu de atalho:

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

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

- **Agendar Tarefa** - abre a janela das **Propriedades**e o botão **Agendar**, onde pode agendar a tarefa seleccionada.

- **Ver Relatórios de Análise** - abre a janela das**Propriedades** e a barra**Relatórios de Análise** onde pode ver os relatórios gerados após as tarefas seleccionadas terem sido executadas.
- **Duplicar** - duplica a tarefa seleccionada.

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

Nota
Devido à sua natureza em particular, apenas as opções**Propriedades** e **Ver Relatórios de Análise** estão disponíveis para as tarefas na categoria **Tarefas Misc**.

8.2.3. Criando Tarefas de Análise

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

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

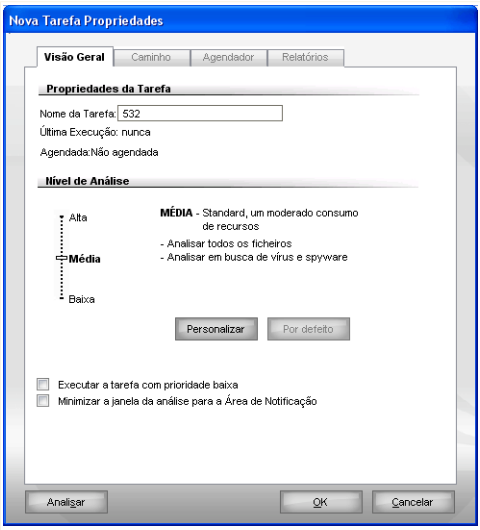
8.2.4. Configurar Tarefas de Análise

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

Nota
Para mais informação sobre ver os logs e a barra de **Logs** tab, por favor consulte "*Ver os Relatórios da Análise*" (p. 73).

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:



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

Nível de Protecção	Descrição
	Programas são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.
Médio	Oferece uma boa eficiência de detecção. O nível de consumo de recursos é moderado. 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:

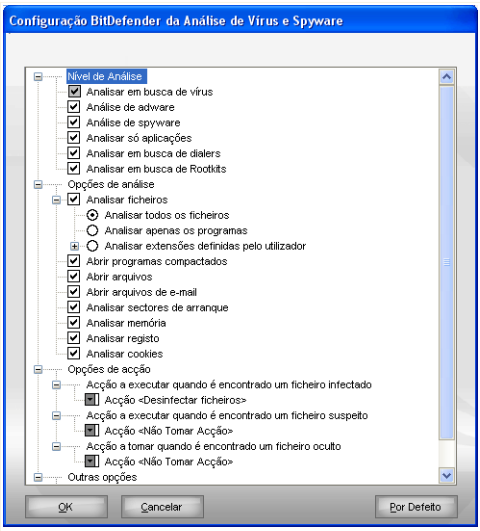
Opção	Descrição
Execute a tarefa de análise com prioridade baixa	Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
Minimizar a janela da análise ao iniciar para a área de notificação	Minimiza a janela da análise no Windows para a área de notificação. Faça duplo-clique sobre o ícone BitDefender para o abrir.

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 verificação estão agrupadas em quatro categorias:

- **Nível de Análise**
- **Opções de análise de vírus**
- **Opções de acção**
- **Outras opções**

- Especifica o tipo de malware que deseja que o BitDefender analise em busca de ao seleccionar determinadas opções da categoria **Nível de Análise**.

  Estão disponíveis as seguintes opções:

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.
Analisar em busca de spyware	Analisa em busca de ameaças de spyware. Estes ficheiros serão tratados como ficheiros infectados.
Analisar aplicações	Analisa ficheiros (`.exe` e `.dll` das aplicações).
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.

- Especifique que tipo de objectos devem ser analisados (ficheiros, mensagens de e-mail e por aí fora) e outras opções. Isto é feito através de seleccionar determinadas opções da categoria **Opções de análise de vírus**.

  Estão disponíveis as seguintes opções:

Opção		Descrição
Análise de ficheiros	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Analisa 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`;

Opção		Descrição
		chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
	Analisar as extensões definidas pelo utilizador	Apenas as extensões especificadas pelo utilizador serão analisadas. Estas extensões têm de estar separadas por ";".
Abrir programas compactados		Verifica todos os ficheiros compactados.
Abrir arquivos		Analisa interior dos arquivos.
Abrir arquivos do e-mail		Analisa o interior dos arquivos de e-mail.
Analisar os sectores de arranque		Analisa o sector de arranque do sistema.
Analisar Memória		Analisa a memória em busca de vírus e outro malware.
Analisar registo		Analisa entradas de registo.
Analisar cookies		Analisa os ficheiros cookie.

- Especifique a acção a tomar sobre ficheiros infectados, suspeitos ou ocultos na categoria **Opções de acção**. Pode especificar uma acção diferente para cada categoria.
  - Seleccione a acção a ser tomada sobre o ficheiro infectado. Estão disponíveis as seguintes opções:

Acção	Descrição
Nenhum (objectos de relatório)	Nenhuma acção será levada a cabo sobre os ficheiros infectados. Estes ficheiros aparecerão no ficheiro de relatório.
Desinfectar ficheiros	Desinfecta os ficheiros infectados.
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.

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

Acção	Descrição
Nenhum (objectos de relatório)	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.

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
Nenhum (objectos de relatório)	Nenhuma acção será levada a cabo sobre os ficheiros ocultos. Estes ficheiros aparecerão no ficheiro de relatório.
Mover ficheiros para a quarentena	Move os ficheiros ocultos para a quarentena.
Tornar visível	Revela ficheiros ocultos de forma a que os possa ver.

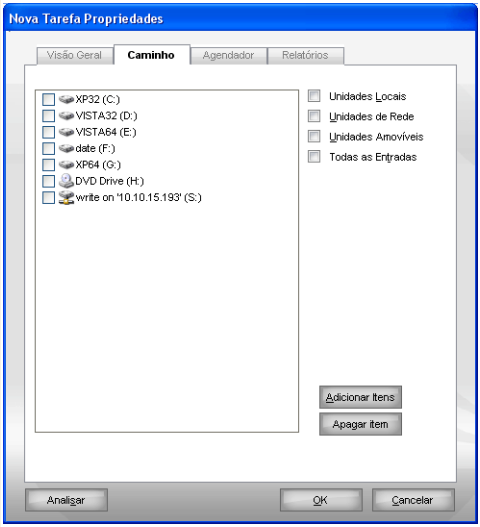
Nota
Se escolher ignorar os ficheiros detectados ou se a acção escolhida falhar, terá de escolher uma acção no assistente de análise.

- Para ser alertado quanto a enviar os ficheiros suspeitos para o Laboratório BitDefender após terminar o processo de análise, seleccione **Enviar ficheiros suspeitos para o Laboratório BitDefender** na categoria **Outras opções**.

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 tarefa de análise de um utilizador em especial, faça clique com o botão direito do rato sobre a mesma e seleccione **Alterar Alvo da Análise**. A seguinte análise irá aparecer:



Alvo da Análise

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 Item** - abre uma janela de exploração, onde pode seleccionar o(s) ficheiro(s) e pasta(s), que pretende analisar.

  Nota
  Pode usar o drag and drop para adicionar ficheiros/pastas à lista.

- **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.

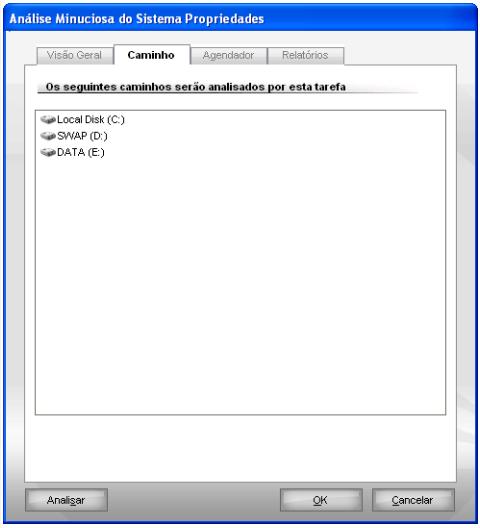
Nota
Se pretende analisar em busca de vírus todo o seu computador, seleccione a caixa de selecção correspondente a **Todas as entradas**.

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

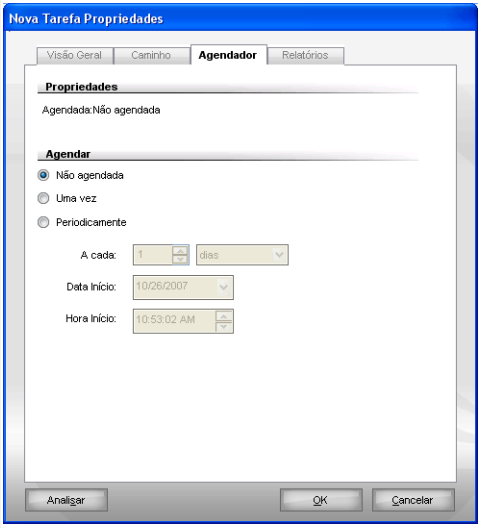
Análise Completa do Sistema e **Análise Minuciosa do Sistema** analisarão todas as drives locais, enquanto **Análise Rápida do Sistema** apenas analisará as pastas `Windows` e `Programas`.

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

Agendar Tarefas de Análise

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

Para ver o agendamento de uma determinada tarefa ou modificá-la, faça clique com o botão direito do rato sobre a tarefa seleccione **Agendar Tarefa**. A seguinte análise irá aparecer:



Agendar

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, a um determinado intervalo de tempo (horas, dias, semanas, meses, anos) começando numa 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**.

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

8.2.5. Analisar objectos

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

Nota

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

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 - faça duplo-clique com o botão direito do rato sobre um ficheiro ou pasta e seleccione BitDefender Antivirus 2008;
- 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.

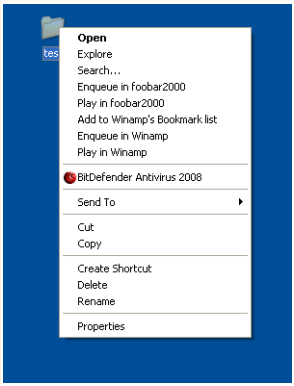
Para executar uma tarefa de análise, use um dos seguintes métodos:

- 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 Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 68).

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.



Análise contextual

Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar e seleccione **BitDefender Antivirus 2008**.

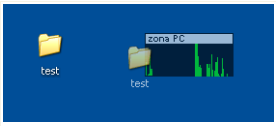
O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 68).

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 Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 68).

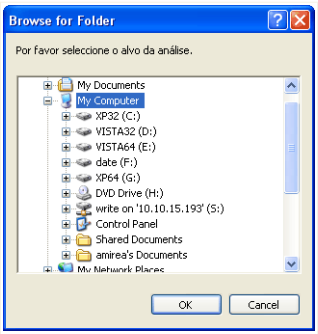
Análise Manual

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 por BitDefender, no menu Iniciar do Windows, siga o seguinte caminho **Iniciar** → **Programas** → **BitDefender 2008** → **Análise Manual BitDefender**.

A seguinte análise irá aparecer:



Análise Manual

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

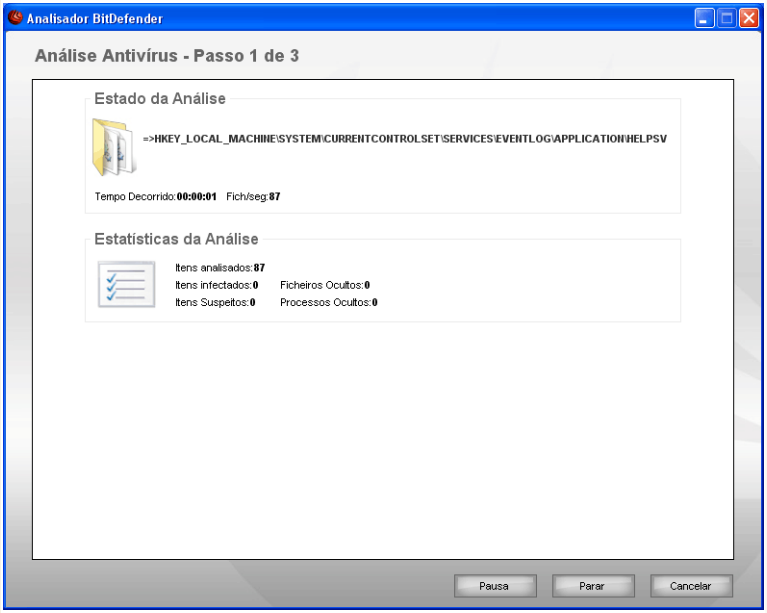
O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 68).

Analisador BitDefender

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

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

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

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

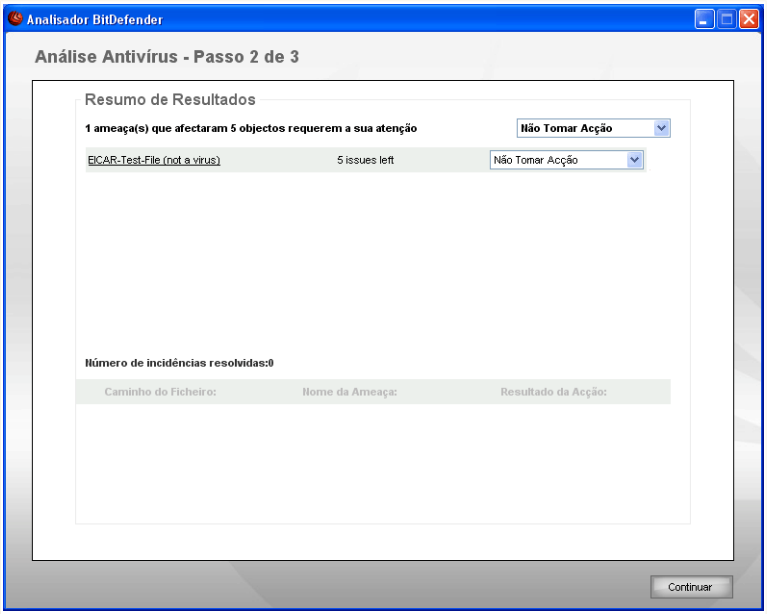
Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

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

Espere que o BitDefender termine a análise.

Passo 2/3 - Seleccionar as acções

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



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 tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.

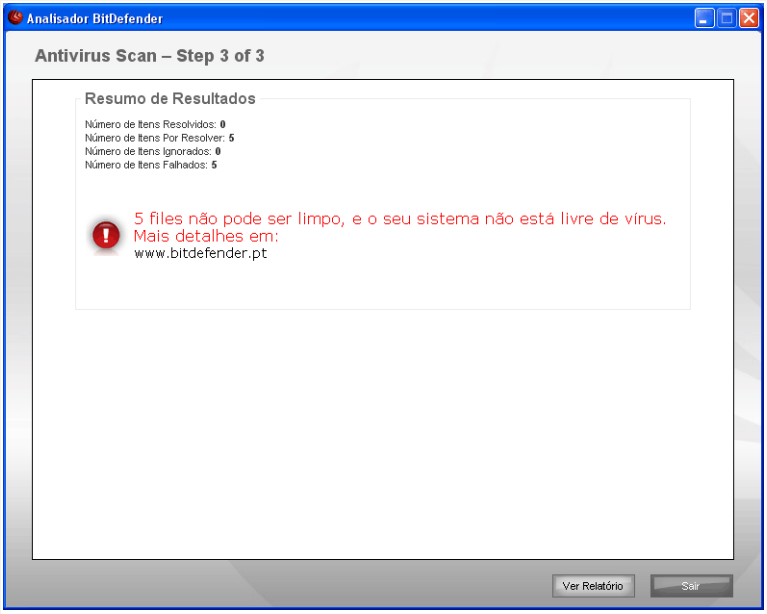
As seguintes opções podem aparecer no menu:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros detectados.
Desinfectar	Desinfecta os ficheiros infectados.
Apagar	Apaga os ficheiros detectados.
Desocultar	Torna visíveis objectos ocultos.

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

Passo 3/3 - Ver Resultados

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



Resumo

Pode ver o resumo dos resultados. O ficheiro do relatório é guardado automaticamente na secção de Logs a partir da janela **Propriedades** da respectiva tarefa.

Importante
Ser-lhe-á solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação.

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

BitDefender Não pode Resolver Algumas Incidências

Na maioria dos casos BitDefender desinfecta com sucesso os ficheiros infectados ou isola a infecção. No entanto, há incidências que não podem ser resolvidas.

Se existirem incidências não resolvidas, recomendamos que contacte o Suporte Técnico BitDefender em www.bitdefender.pt. O nosso suporte técnico ajuda-lo-á a resover as incidências que está a experimentar.

BitDefender Detectou Itens protegidos por Palavra-passe

A categoria de protegidos por palavra-passe inclui dois tipos de itens: arquivos e instaladores. Eles não representam uma verdadeira ameça à segurança do sistema a não ser que contenham ficheiros infectados e apenas quando são executados.

Para ter a certeza de que estes itens estão limpos:

- Se o item protegido por palavra-passe for um arquivo que protegeu com uma palavra-passe, extraia os ficheiros do mesmo e analise-os separadamente. A forma mais fácil de os analisar é clique botão-direito do rato sobre eles e seleccionar **BitDefender Antivirus 2008** a partir do menu.
- Se o item protegido por palavra-passe for um instalador, certifique-se que a protecção em tempo-real está activa antes de executar esse mesmo instalador. Se o instalador estiver infectado, o BitDefender detectará a situação e isolará a infecção.

Se não deseja que estes objectos sejam detectados novamente pelo BitDefender tem de os adiconar como excepções ao processo de análise. Para adicionar excepções à análise, clique em, **Definições** para abrir a consola das configurações e depois vá para **Antivírus > Excepções** . Para mais informação, consulteObjectos Excluídos da Análise

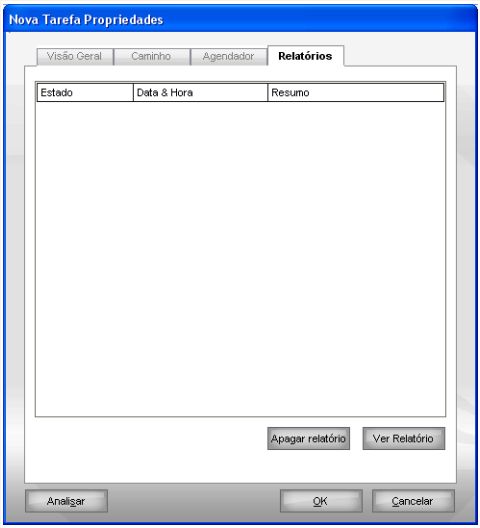
BitDefender Detectou Ficheiros Suspeitos

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 uma análise mais avançada no laboratório do BitDefender.

8.2.6. 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 **Ver os Relatórios da Análise**. A seguinte análise irá aparecer:



Relatórios da Análise

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

Cada 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:

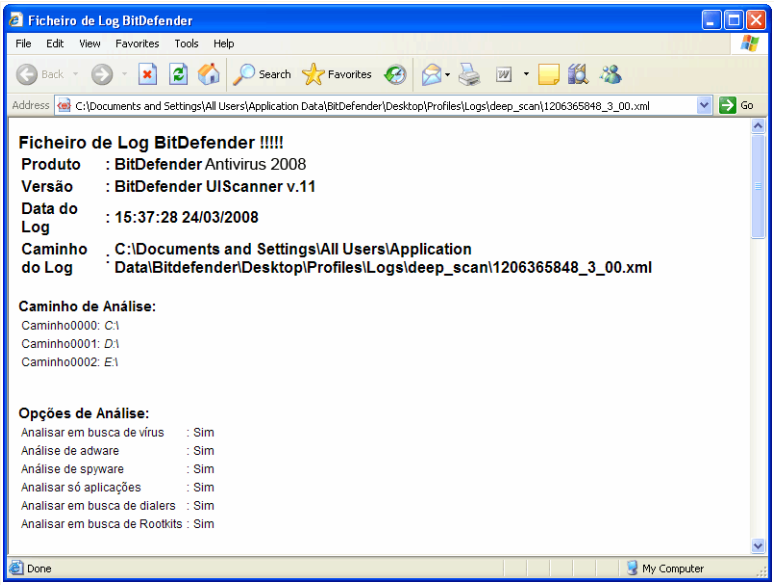
- **Apagar Relatório** - para apagar o relatório seleccionado.
- **Mostrar Relatório** - para ver o relatório seleccionado. O relatório da análise será aberto no seu explorador da internet.

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.

8.3. Objectos a Excluir 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.

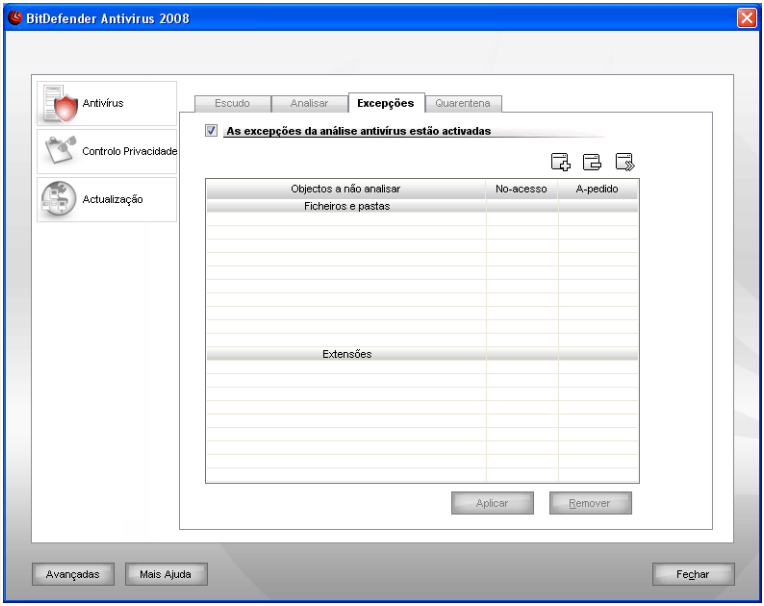
BitDefender permite-lhe excluir objectos da análise no-acesso e da análise a-pedido, ou de ambas. Esta definição tem o propósito de diminuir o tempo de análise e evitar interferência com o seu trabalho.

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 os objectos excluídos da análise, clique em **Antivírus>Excepções** na consola de configuração. A seguinte análise irá aparecer:



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.

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**.

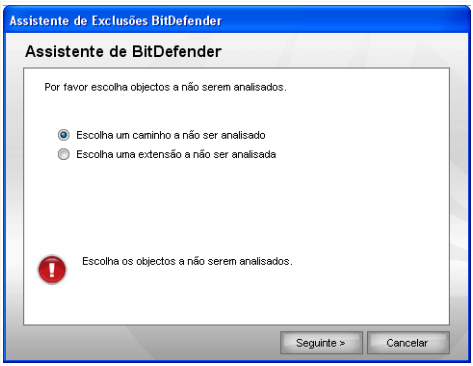
Nota
Pode também clicar no objecto usando o botão direito do rato e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

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

8.3.1. 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 1/3 - Seleccionar o Tipo de Objecto

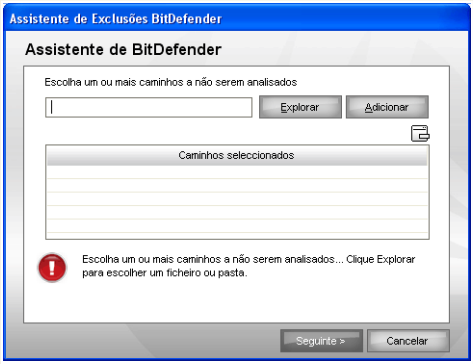


Tipo de Objecto

Seleccione a opção de excluir um caminho da análise.

Clique em **Seguinte**.

Passo 2/3 - 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**.

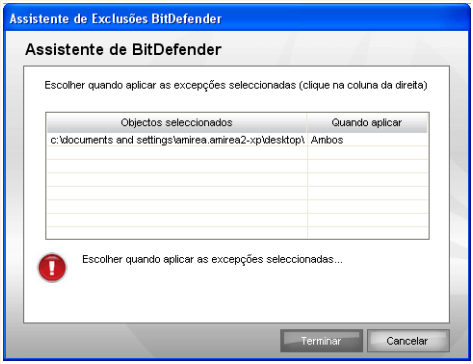
> ***Nota***
> Se o caminho inserido não existe, uma mensagem de erro surgirá. Clique em **OK** e verifique se o caminho é válido ou não.

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 em **Seguinte**.

Passo 3/3 - Seleccionar o Tipo de Análise



Tipo de Análise

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

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

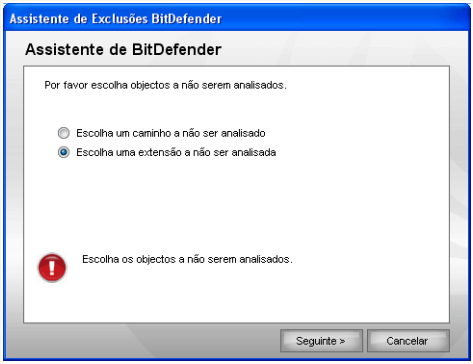
Clique em **Terminar**.

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

8.3.2. Excluir Extensões da Análise

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

Passo 1/3 - Seleccionar o Tipo de Objecto

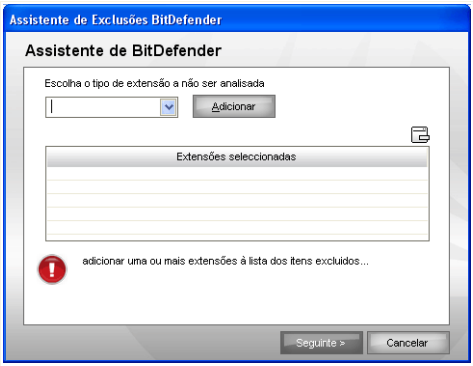


Tipo de Objecto

Seleccione a opção de excluir uma extensão da análise.

Clique em **Seguinte**.

Passo 2/3 – 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.

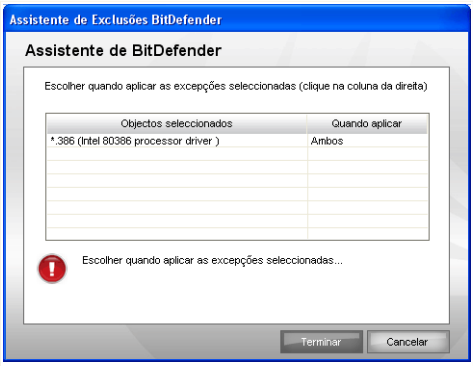
- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

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 em **Seguinte**.

Passo 3/3 - Seleccionar o Tipo de Análise



Tipo de Análise

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

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

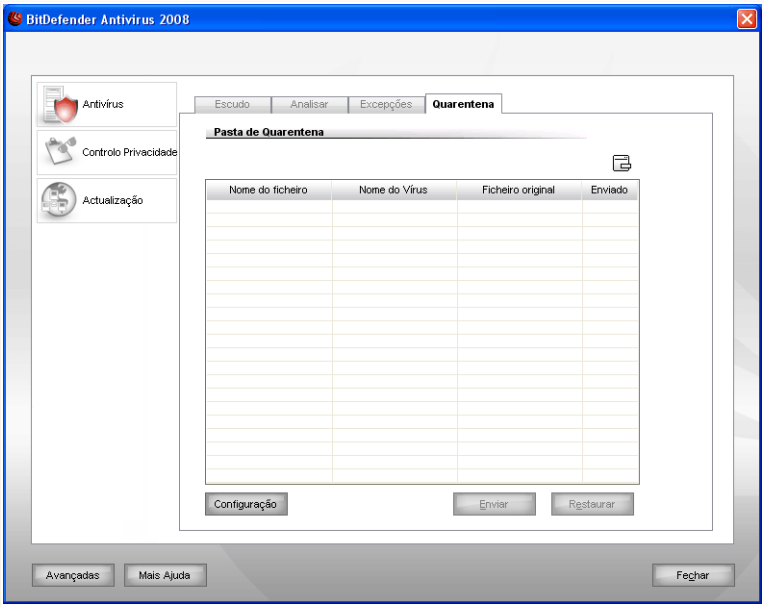
Clique em **Terminar**.

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

8.4. 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.

Para ver e gerir os ficheiros em quarentena e configurar as definições da quarentena, clique em **Antivírus>Quarentena** na consola de configuração.



Quarentena

8.4.1. Gerir Ficheiros em Quarentena

Como pode ver, a secção da **Quarentena** contém uma lista de todos os ficheiros isolados até então. Todo o ficheiro tem incluído o seu nome, tamanho, data de isolamento e de submissão.

Nota
Quando o vírus se encontra na quarentena não pode provocar nenhum mal, porque não podem ser lidos nem executados.

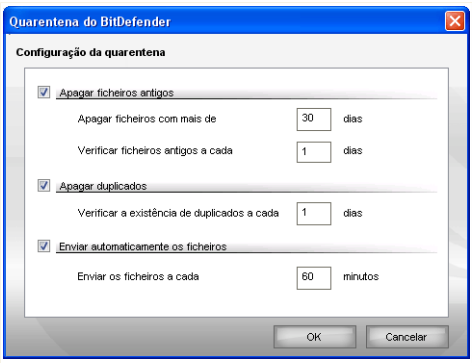
Para apagar um ficheiro seleccionado da lista de quarentena clique no botão **Remover** . Se deseja restaurar o ficheiro seleccionado para a sua localização original clique em **Restaurar**.

Pode enviar qualquer ficheiro seleccionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**.

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.

8.4.2. Configuração da Quarentena

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



Configuração da quarentena

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 10 dias de existência.

Apagar 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.

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

9. Controlo 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.

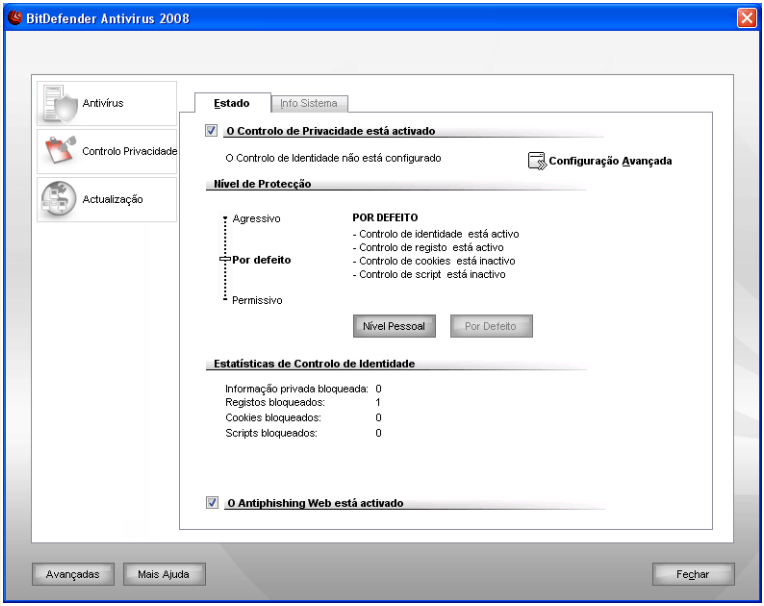
BitDefender também analisa os sites Internet que visita e alerta-o caso seja detectada alguma ameça de phishing.

A secção de **Controlo de Privacidade** deste manual do utilizador contém os seguintes tópicos:

- Estado do Controlo de Privacidade
- Configuração Avançada - Controlo de Identidade
- Configuração Avançada - Controlo de Registo
- Configuração Avançada - Controlo de Cookies
- Configuração Avançada - Controlo de Script
- Informação do Sistema
- Barra de Tarefas Antiphishing

9.1. Estado do Controlo de Privacidade

Para configurar o Controlo de Privacidade e ver informação quanto à sua actividade, clique em **Controlo de Privacidade>Estado** na consola de configuração. A seguinte análise irá aparecer:



Estado do Controlo de Privacidade

9.1.1. Controlo Privacidade

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 5 tipos de controlo de protecção importantes:

- Controlo de Identidade - protege os seus dados confidenciais ao filtrar o tráfego HTTP e SMTP de acordo com as regras que criou na secção de Identidade.

Nota
Ao fundo da secção poderá ver as **Estatísticas do Controlo 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 um cookie.
- O Controlo de script irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

Para definir as configurações para estes controlos clique em Configuração Avançada.

Configurar Nível de Protecção

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

Existem 3 níveis de protecção:

Nível de Protecção	Descrição
Permissivo	Apenas o **Controlo de Registo** está activo.
Por Defeito	O **Controlo de Registo** e o **Controlo de Identidade** estão activos.
Agressivo	O **Controlo de Registo**, o **Controlo de Identidade** e o **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.

9.1.2. Protecção Antiphishing

O phishing é uma actividade criminal na Internet que utiliza técnicas maliciosas de forma a enganar as pessoas e levá-las a dar informação considerada privada.

A maior parte das vezes, as tentativas de phishing resumem-se a enviar massivos e-mails que se apresentam como tendo sido enviados por uma empresa legítima e idónea. Estas mensagens enganosas são enviadas com o intuíto de que pelo menos

alguns dos destinatários estejam dentro do perfil que o autor do phishing procura e possam ser persuadidos a divulgar informação considerada privada.

Uma mensagem de phishing normalmente apresenta uma situação que tem a ver com a sua conta online. Tenta convencê-lo a clicar no link que vem na mensagem de forma a que aceda a um suposto site web legítimo (que na verdade trata-se de um site forjado) onde a sua informação privada é solicitada. Poderá, por exemplo, ser solicitada a confirmar a informação da sua conta, tal como a palavra-passe e o utilizador da mesma, e a fornecer o seu número de conta bancária ou o seu número de segurança social. Por vezes, para ser mais convincente, a mensagem indica que a sua conta já foi ou está em vias de ser cancelada se não aceder ao link que vem na mensagem.

O phishing também faz uso do spyware, tais como os Trojan keyloggers, para roubarem a informação bancária directamente do seu computador.

Os principais alvos do phishing são os clientes de pagamento de serviços on-line, tais como o eBay e o PayPal, como também os clientes de bancos que ofereçam serviços online. Recentemente, utilizadores de websites com rede social foram também alvo de phishing com o intuíto de obterem dados de informação pessoal para serem usados para roubo de identidade.

Para estar protegido contra as mais recentes tentativas de phishing quando está a navegar na Internet, mantenha o **Antiphishing** activado. Desta forma, BitDefender irá analisar cada web site antes que lhe aceda e irá alertá-lo da existência de alguma ameaça de phishing. Uma Lista Branca de sites web que não serão analisados pelo BitDefender pode ser configurada.

Ide forma a gerir facilmente a protecção antiphishing e a Lista Branca, use a barra de tarefas do Antiphishing BitDefender que se encontra no integrada no Internet Explorer. Para mais informação, por favor consulte “*Barra de Ferramentas do Antiphishing*” (p. 104).

9.2. Configuração Avançada - Controlo de Identidade

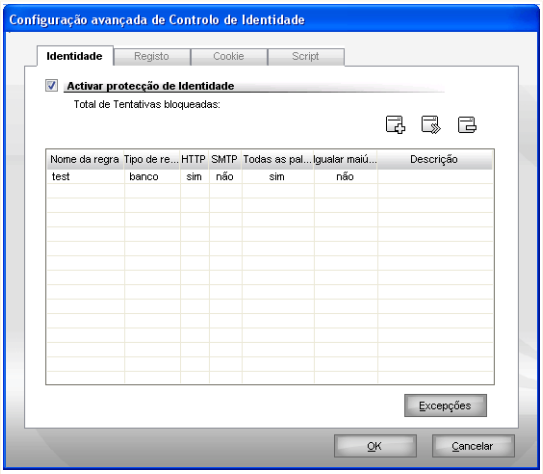
Manter informação confidencial segura é um assunto importante que nos preocupa a todos. O roubo de dados tem crescido com o desenvolvimento das comunicações Internet e actualmente fazem-se uso de novos métodos para enganar as pessoas e retirar-lhes informação privada.

Controlo de Identidade ajuda-o a manter a sua informação confidencial em segurança. Analisa o tráfego HTTP ou SMTP, ou ambos, em busca de certos caracteres que definiu. Se for encontrada uma correspondência, a respectiva página web ou e-mail são bloqueados.

Suporte multi-utilizador é fornecido de forma a que nenhum utilizador do sistema possa ver as regras que você configurou.

As regras de privacidade podem ser configuradas na secção **Identidade**. Para aceder a esta secção abra a janela **Configuração Avançada de Controlo Privacidade** e clique na barra **Identidade**.

Nota
Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



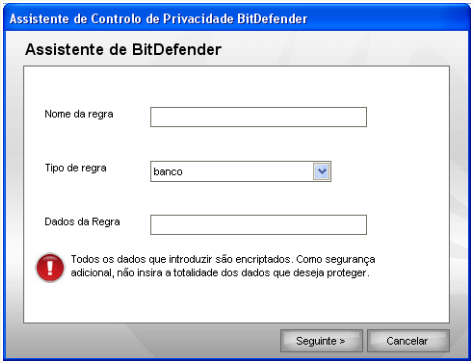
Controlo de Identidade

9.2.1. Criar Regras de Identidade

As regras podem ser introduzidas manualmente (clique no botão **Adicionar** e escolha os parâmetros da regra). O assistente de configuração irá aparecer.

O assistente de configuração é um procedimento composto por 3 passos.

Passo 1/3 - Definir Tipo de Regra e Dados



Definir Tipo de Regra e Dados

Insira o nome da regra no campo de edição.

Deve definir os seguintes parâmetros:

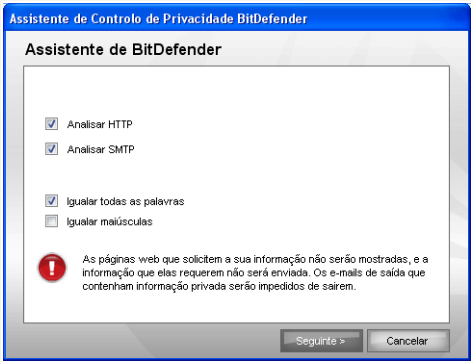
- **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
- **Dados de Regra** - insira os dados da regra.

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

Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

Clique em **Seguinte**.

Passo 2/3 - Seleccionar Tráfego



Seleccionar Tráfego

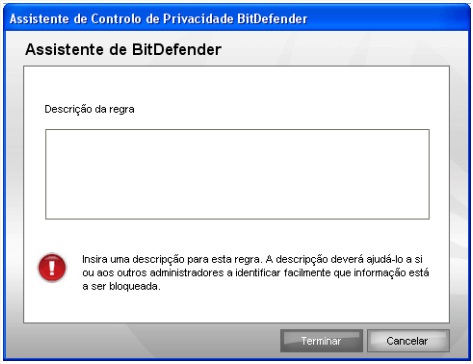
Seleccione o tráfego que quer que o BitDefender analise. Estão disponíveis as seguintes opções:

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

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

Clique em **Seguinte**.

Passo 3/3 - Descrever Regra



Descrever Regra

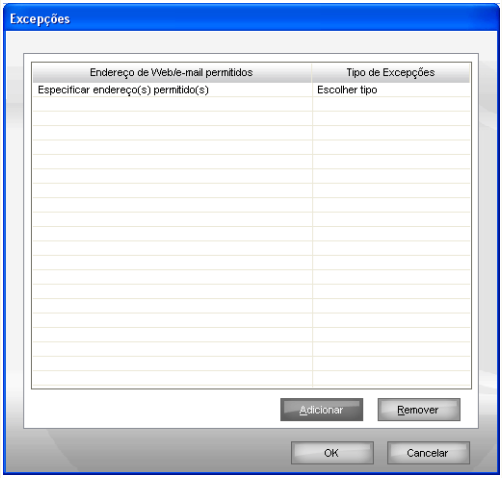
Insira uma breve descrição da regra no campo de edição.

Clique em **Terminar**.

9.2.2. 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**.



Excepções

Para adicionar uma excepção, siga os seguintes passos:

1. Clique **Adicionar** para adicionar uma nova entrada na lista.
2. Duplo-clique em **Especificar endereço permitido** e inserir o endereço web ou endereço de e-mail que deseja adicionar como excepção.
3. Duplo-clique em**Escolher Tipo** e escolha do menu a opção correspondente ao tipo de endereço que inseriu anteriormente.
   - Se especificou um endereço web, seleccione **HTTP**.
   - Se especificou um endereço de e-mail, seleccione**SMTP**.

Para remover uma excepção da lista, seleccione-a e clique **Remover**.

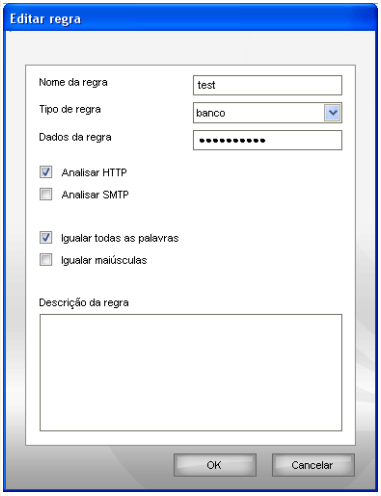
Clique em **OK** para guardar as alterações.

9.2.3. Gerir Regras

Pode ver as regras listadas na tabela.

Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para desactivar temporariamente uma regra sem a apagar, limpe a caixa de selecção correspondente.

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.

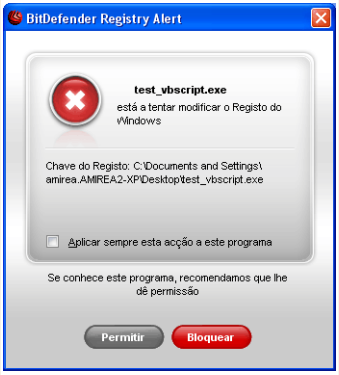
Clique em **OK** para guardar as alterações e fechar a janela.

9.3. Configuração Avançada - Controlo de registo

Uma parte muito importante do sistema operativo do Windows é chamado de **Registo**. Aqui é o local onde o guarda as suas definições, programas instalados, informação acerca do utilizador e por aí fora.

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

Pode negar esta modificação ao clicar em **Não** ou pode permitir ao clicar em **Sim**.

Se deseja que o BitDefender memorize a sua resposta tem de seleccionar a caixa de selecção: **Aplicar sempre esta acção a este programa**. Desta forma, uma regra será criada e a mesma acção será aplicada sempre que este programa tente modificar uma entrada no registo de forma a ser executado no iniciar do Windows.

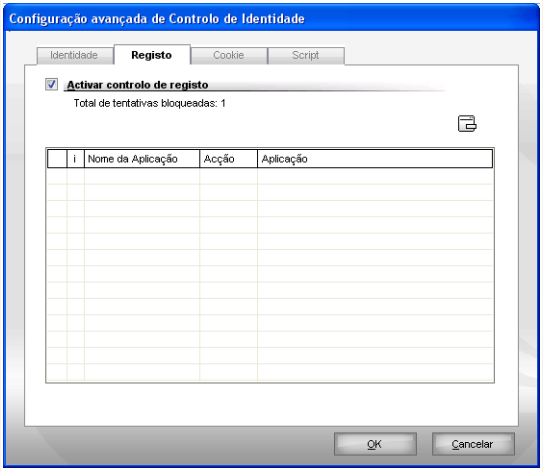
Nota

O BitDefender irá, normalmente, alertá-lo quando instalar novos programas que necessitem de se executar durante o iniciar do seu computador. Na maioria dos casos, estes programas são legítimos e de confiança.

Cada regra que foi memorizada pode ser acedida na secção **Registo** para futura afinação. Para aceder a esta secção abrir a janela**Configuração Avançada de Controlo de Privacidade**e clique na barra**Registo**.

Nota

Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



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**. Para temporariamente desactivar uma regra sem a apagar, deseleccione a respectiva caixa de selecção.

Para alterar a acção de uma regra,, faça duplo-clique do campo da acção e seleccione a opção correspondente do menu.

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

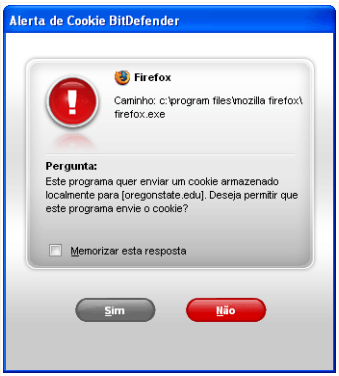
9.4. Configuração Avançada - Controlo de Cookies

As Cookies são uma ocurrência muito comum na Internet. Elas são ficheiros pequenos armazenados no seu computador. Os sites da Web criam estas cookies para manter um rasto de informação específica sobre 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 os voltar a introduzir sempre que os visitar.

Mas as cookies também podem ser usadas para comprometer a sua privacidade, ao seguir o rasto do seu padrão de 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.

Seleccione **Memorizar esta pergunta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Já não será notificado quando se ligar ao mesmo site.

Isto irá ajudá-lo a escolher quais os sites da web em que pode confiar ou não.

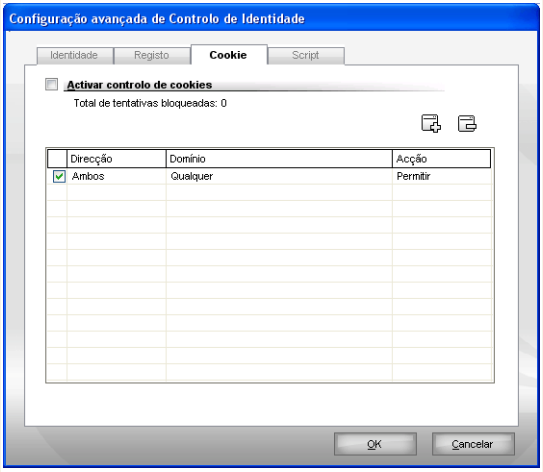
Nota

Devido ao grande número de cookies usadas hoje na Internet, o **Controlo de Cookie** pode ser um pouco aborrecido de início. 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 de regras, a navegação tornar-se-á tão fácil como antes.

Toda a regra que foi memorizada pode ser acedida na secção **Cookies** para uma maior afinação. Para aceder a esta secção, abra a janela **AConfiguração Avançada do Controlo de Privacidade** e clique na barra**Cookie**.

Nota

Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



Controlo de Cookies

Pode ver as regras criadas até agora listadas na tabela.

Importante
A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

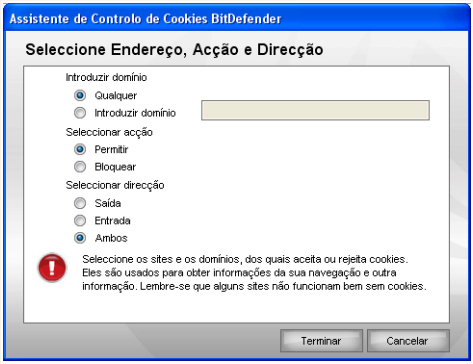
Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

9.4.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Endereço, Acção e Direcção



Seleccionar Endereço, Acção e Direcção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, ao 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 para o site a que está ligado.
Entrada	A regra será aplicada apenas às cookies que são recebidas do site a que está ligado.
Ambos	A regra aplica-se em ambos os sentidos.

Clique em **Terminar**.

Nota
Pode aceitar cookies sem nunca as devolver, ao estabelecer a acção para **Negar** e a direcção para **Saída**.

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

9.5. Configuração Avançada - Controlo de Script

Scripts 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 nocivos. 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 está ligado. 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 um script ou outro conteúdo activo:

Alerta de Script

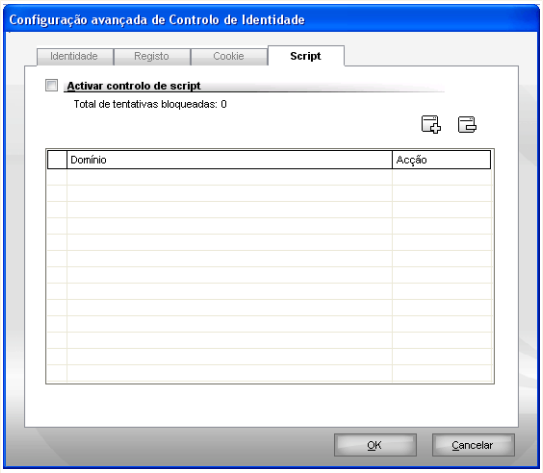
Pode ver o nome do recurso.

Seleccione **memorizar esta pergunta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Já não será notificado quando o mesmo site tentar enviar-lhe conteúdo activo.

Toda a regra que foi memorizada pode ser acedida na secção **Script** para futura afinação. Para aceder a esta secção, abra a janela**Configuração Avançada do Controlo de Privacidade** e clique na barra**Script**.

Nota

Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



Controlo de script

Pode ver as regras criadas até agora listadas na tabela.

Importante

A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

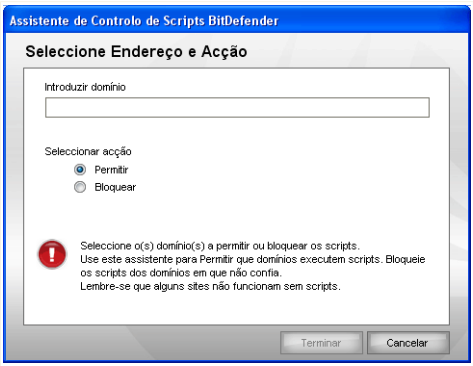
Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

9.5.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Endereço e Acção



Seleccionar Endereço e Acção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, ao 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**.

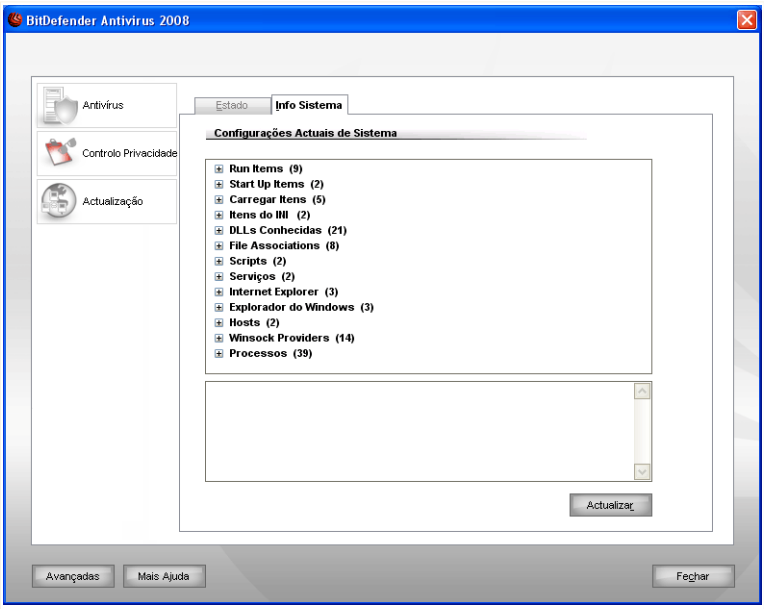
Clique em **OK** para guardar as alterações e fechar a janela.

9.6. Info 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, clique em **Controlo de Privacidade>Info Sistema** na consola de configuração. A seguinte análise irá aparecer:



Info 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:

- **Remover** - apaga o item seleccionado. Tem de clicar em **Sim** para confirmar a sua escolha.

Nota
Se não deseja ser mais notificado novamente para confirmar a sua escolha durante a actual sessão, seleccione **Não me questionem mais durante esta sessão**.

- **Ir para** - abre uma janela onde o item seleccionado é colocado (o **Registo** por exemplo).
- **Actualizar** - reabre a secção de **Info Sistema**.

Nota
Dependendo do item seleccionado, um ou ambos os botões **Remover** ou **Ir Para** poderão não aparecer.

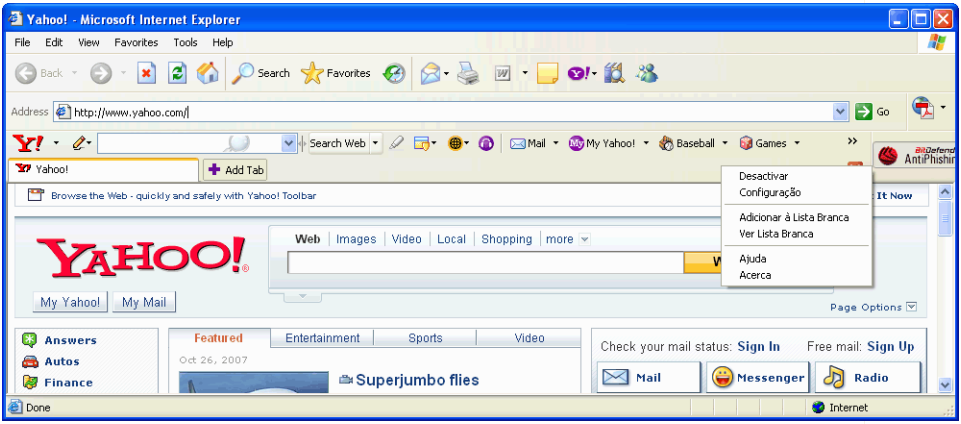
9.7. Barra de Ferramentas do Antiphishing

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.

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.

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

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



Barra de Ferramentas do Antiphishing

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

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

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

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

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

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

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

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

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

Pode adicionar sites à Lista Branca nos quais confia absolutamente, de forma a que eles não sejam mais analisados pelos motores antiphishing. Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

- **Ajuda**- abre o ficheiro de ajuda.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

10. 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 for detectada, dependendo das opções definidas na secção Definições da Actualização Automática, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

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 existem nas seguintes formas:

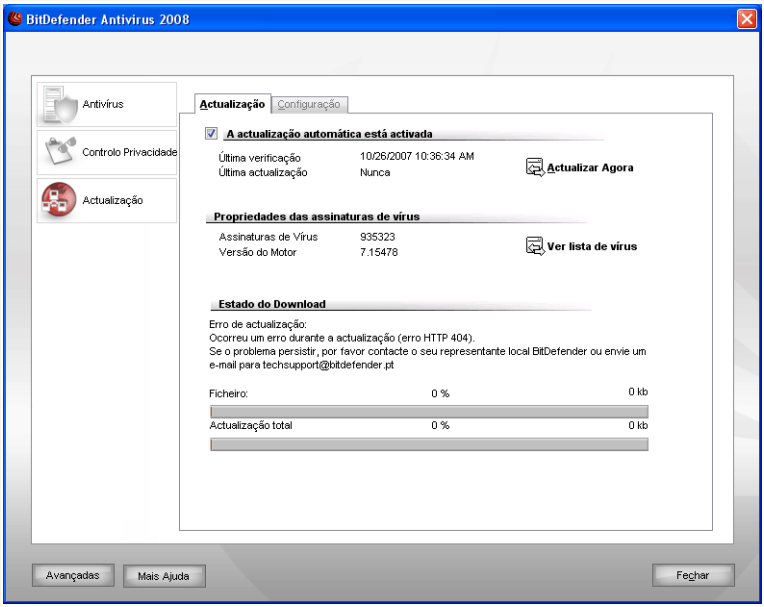
- **Actualizações do motor antivírus** - à medida que surgem novas ameaças, os ficheiros que contêm as assinaturas de vírus têm de ser actualizados para assegurar uma protecção permanentemente actualizada contra elas. Esta actualização também é conhecida como **Actualização das Definições de Vírus**.
- **Actualizações para o motor de Antispyware** - novas assinaturas de spyware serão adicionadas à base de dados. Esta actualização é também conhecida como **Actualização Antispyware**.
- **Upgrades do produto** - quando é lançada uma nova versão do produto, são introduzidas novas configurações e técnicas de análise, com o objectivo de melhorar o desempenho do produto. Esta actualização também é conhecida como **Mudança de Versão**.

A secção de **Actualização** deste guia do utilizador contém os seguintes tópicos:

- Actualização Automática
- Configurações da Actualização

10.1. Actualização Automática

Para ver informação relacionada com actualizações e executar actualizações automáticas, clique em **Actualização>Actualização** na consola de configuração. A seguinte análise irá aparecer:



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.

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.

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.

10.1.1. Solicitar uma Actualização

A actualização automática pode ser feita a qualquer altura que deseje clicando no botão **Actualizar Agora**. Esta actualização é também conhecida como **Actualização a pedido do utilizador**.

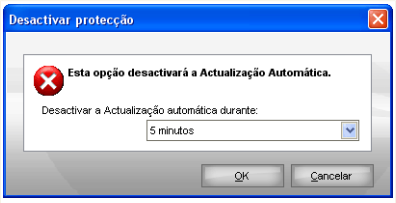
O módulo de **Actualização** estabelece ligação ao servidor de actualizações do BitDefender e verificará se há actualizações disponíveis. Se detectar uma actualização, dependendo das opções definidas na secção Opções da Actualização Manual, ser-lhe-á solicitada a confirmação para a actualização ou a 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.

10.1.2. Desactivar Actualização Automática

Se deseja desactivar a actualização automática, uma janela de aviso aparecerá.



Desactivar Actualização Automática

Tem de confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a actualização automática fique desactivada. Pode desactivar a actualização

automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

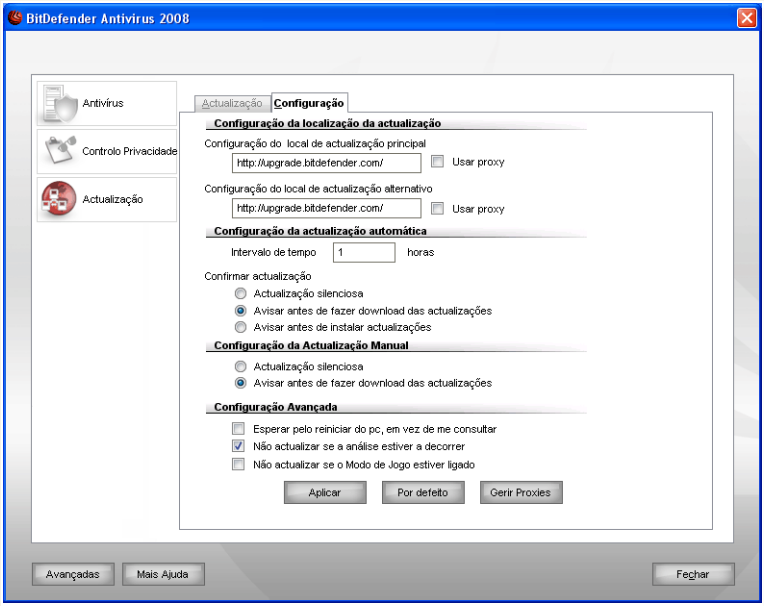
Atenção

Esta é uma incidência de segurança critica. recomendamos que desactive a actualização automática pelo menor tempo possível. Se o BitDefender não for actualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.

10.2. Definições de 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>Configuração** na consola de configuração. A seguinte análise irá aparecer:



Definições de actualização

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

10.2.1. 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.

Nota
Para mais informação, por favor consulte "*Gerir Proxies*" (p. 113)

10.2.2. 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 **Interval Tempo**. Por defeito, o intervalo de tempo da actualização é de 1 hora.

Para definir como é que o processo de actualização automática tem de ser feito, seleccione uma das seguintes opções:

- **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.

Nota
Será avisado antes das actualizações serem descarregadas mesmo que saia do Centro de Segurança.

- **Avisar antes de instalar actualizações** - cada vez que uma actualização for descarregada, será consultado antes da sua instalação ser feita.

Nota
Será avisado antes das actualizações serem instaladas mesmo que saia do Centro de Segurança.

10.2.3. 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.

Nota
Será avisado antes das actualizações serem descarregadas mesmo que saia do Centro de Segurança.

10.2.4. 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 de 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 cancelado.

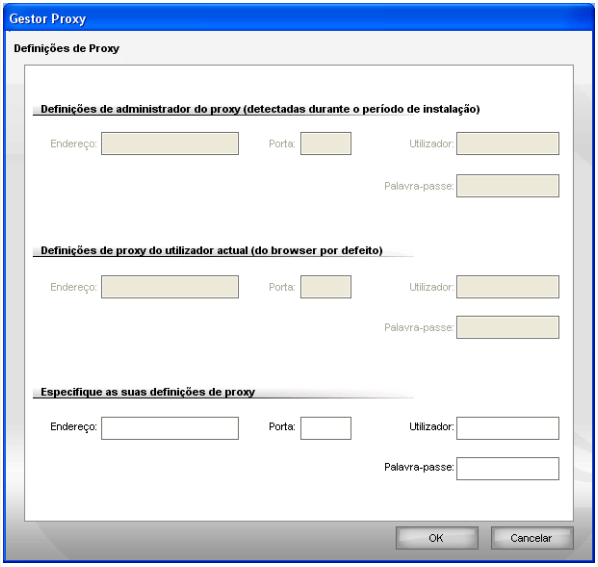
- **Não actualizar se o modo de jogo estiver ligado** - O BitDefender não actualizará se o Modo de Jogo estiver ligado. Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.

10.2.5. 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 do proxy, clique em **Gerir proxies**. A janela **Gsetor Proxy** irá aparecer.



Gestor Proxy

Existem três categorias de definições de proxy:

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

Nota

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

- **O seu próprio conjunto de definições de proxy** - definições de proxy que pode configurar se estiver logged in como administrador.

  As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o BitDefender usa para se ligar ao servidor proxy.
  - **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 **Por Defeito** para retornar às definições por defeito.

CD de Emergência BitDefender

11. Geral

BitDefender Antivirus 2008 vem num CD de arranque (CD de Emergência BitDefender), o qual pode ser utilizado para analisar e desinfectar todo o sistema antes do sistema operativo arrancar.

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 do BitDefender pode ser descarregado deste link: http://download.bitdefender.com/rescue_cd/

11.1. 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.

11.2. 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.

12. 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.

12.1. 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.

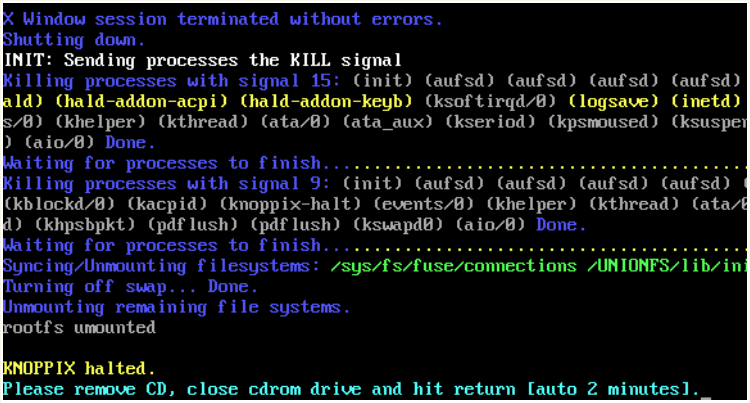
O Ambiente de Trabalho

12.2. 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

12.3. 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 deseja analisar uma determinada directoria apenas, faça o seguinte:

Explore as suas pastas, clique botão-direito 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/
```

12.4. Como posso actualizar o BitDefender através de um proxy?

Se existe um servidor proxy entre o vosso computador e a internet, algumas configurações têm de ser feitas de forma a poder actualizar o seu BitDefender.

Para actualizar o BitDefender através de um proxy, siga os seguintes passos:

1. Clique botão direito do 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**.

12.5. 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:

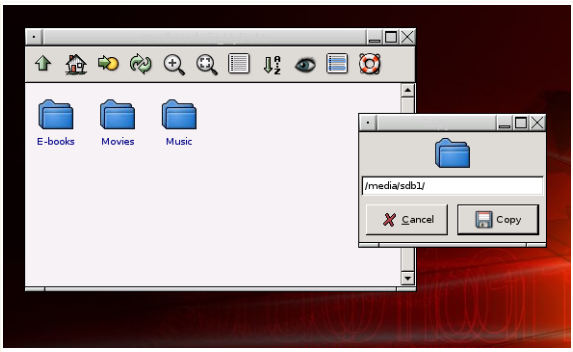
1. Coloque o CD de Emergência BitDefender na drive de CDs, e o stick de memória na entrada USB e depois reinicie o computador.
2. Espere que o CD de Emergência BitDefender termine de arrancar o PC. A seguinte janela irá aparecer.

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.

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**.

Obter Ajuda

13. Suporte

Como um fornecedor importante, a BitDefender esforça-se por fornecer aos seus clientes um nível de suporte técnico sem igual de uma forma rápida e precisa. O Centro de Suporte (o qual poderá contactar nos endereços que lhe fornecemos abaixo) é continuamente mantido a par das mais recentes ameaças, e é aqui onde todas as suas questões são respondidas de uma forma rápida.

Com o BitDefender, tem sido sempre a nossa prioridade poupar aos nossos clientes tempo e dinheiro ao fornecer-lhes os produtos mais avançados aos preços mais económicos. Mais ainda, pensamos que um negócio de sucesso é baseado numa boa comunicação e num compromisso de excelência no suporte ao cliente.

Convidamo-lo desde já a colocar as suas questões em techsupport@bitdefender.pt a qualquer altura. Para uma resposta rápida, por favor inclua no seu e-mail o máximo de detalhes que consiga acerca do seu BitDefender, acerca do seu sistema e uma descrição do problema tão completa e fiel quanto possível.

13.1. 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.

13.2. Pedir Ajuda

13.2.1. Vá até ao Self-Service Web

Tem uma dúvida? Os nossos peritos em segurança estão disponíveis para o ajudar 24/7 via e-mail ou chat sem custos adicionais.

Por favor siga os seguintes links:

English

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

German

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

French

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

13.2.2. Abrir um ticket de suporte

Se deseja abrir um ticket de suporte e receber ajuda via e-mail, siga os seguintes links:

English: http://www.bitdefender.com/site/Main/contact/1/
German: http://www.bitdefender.de/site/Main/contact/1/
French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

13.3. Informação de Contacto

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.

13.3.1. Endereços Web

Departmento Comercial: comercial@bitdefender.pt
Suporte Técnico: support@bitdefender.com
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

13.3.2. Escritórios

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.

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
Suporte Técnico:

- support@bitdefender.com

- Telefone:
  - 1-888-868-1873 (Registered Users Only; accessible in United States only)
  - 1-954-776-6262 (Registered Users Only)

Serviço ao Cliente:

- E-mail: customerservice@bitdefender.com
- Telefone:
  - 1-888-868-1873 (Registered Users Only; accessible in United States only)
  - 1-954-776-6262 (Registered Users Only)

Alemanha

BitDefender GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Alemanha
Tel: +49 7542 9444 60
Fax: +49 7542 9444 99
Email: info@bitdefender.com
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Suporte Técnico: support@bitdefender.com

UK e Irlanda

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: info@bitdefender.com
Sales: sales@bitdefender.com
Web: http://www.bitdefender.co.uk
Suporte Técnico: support@bitdefender.com

Espanha

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006

Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender.pt
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

Romania

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Suporte Técnico: support@bitdefender.com
Sales: sales@bitdefender.com
Phone: +40 21 4085600
Fax: +40 21 2330763
Site internacional do produto: http://www.bitdefender.com

Glossário

ActiveX

O ActiveX é um modelo para fazer programas de forma a que outros programas e o sistema operativo os possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e comportam-se como programas de computador, em vez de páginas estáticas. 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 por uma falta completa 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 das 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.

Backdoor

Um buraco na segurança de um sistema deliberadamente criado pelos desenhadores ou responsáveis da manutenção. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, que trazem contas privilegiadas, criadas para serem usadas pelos técnicos de serviço ou pelo vendedor dos programas de manutenção.

Sector de arranque

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí fora). Para discos de inicialização, o sector de saída também contém um programa que carrega o sistema operativo.

Vírus de boot

Um vírus que infecta o sector boot de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infectada por um vírus de boot, irá causar a activação do vírus em memória. Sempre que iniciar o seu sistema daquele ponto, terá o vírus activo em 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

Dentro 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 procurar atingi-lo com publicidade naquilo que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado é 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 " (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 exacto.

drive de disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma drive de disco rígido lê e escreve nos discos rígidos.

Uma drive de disquetes acede às disquetes.

As drives dos discos tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Download (Descarga)

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 redes locais ou 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, tal como ficar sem memória.

Falso positivo

Ocorre quando o analisador 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 análise que não se baseia em assinaturas específicas de vírus. A vantagem da análise heurística, 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 que é responsável dos endereços de IP, rotas, e a fragmentação e reassemblagem dos pacotes de IP.

Java applet

Um programa em Java desenhado para funcionar apenas numa página web. Para usar uma applet numa página web, 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 browser descarrega a applet de um servidor e corre-a apenas na máquina do utilizador (o cliente). As applets diferem das aplicações, pois são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets correrem no cliente, elas não podem escrever nem ler dados na máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas ler e escrever dados provenientes do mesmo domínio do 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 cassetes ou discos. Todo o computador vem com uma certa quantidade de memória física, normalmente referida como memória principal ou RAM.

Não-heurístico

Este método de análise depende da assinaturas de vírus especificas. A vantagem de uma análise não-heurística, é que ela 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 serem substituidos. Neste caso, os dez espaços iriam requerer 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 dois quaisquer pontos, tal como os canais de comunicação entre dois computadores.

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 pessoal, tal como palavras-passe 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 padrão de patente binária consistente, tais vírus são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais têm vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs, e teclados. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto final 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 relatório

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender mantém um ficheiro de relatório que lista o caminho analisado, 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.

Script

Outro termo para macro ou batch file, um script 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 palavras-passe 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 no Startup

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.

Área de notificação

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 largamente usados na Internet e que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operativos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para conectar redes e rotas de tráfego.

Trojan

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 insidiosos 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 módulo de actualização que lhe permite verificar actualizações manualmente, ou actualizar o produto automaticamente.

Vírus

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se 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. Um tipo de vírus ainda mais perigoso é aquele que é capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

assinatura de vírus

O padrão binário de um vírus, usado pelo programa antivírus para detectar e eliminar o vírus.

Worm

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.